

Security

ON DEMAND BUSINESS™

© 2008 IBM Corporation

Highlights

- Support for mixed-case passwords
 - ◆ New PSWDC parameter

- Security auditing improvements
 - ◆ Consistency for SMF logging requests
 - ◆ New AUTHLOG parameter that affects CHNG|AUTH call processing
 - Controls SMF logging and auditing
 - Supports suppression of the ICH408I message

- Enhanced security for IMS conversations

- **SMU support is removed**

IMS V10 provides several enhancements in the security area:

- Support for mixed-case passwords through a new parameter, PSWDC.
- Greater consistency in how IMS requests SMF logging.
- A new AUTHLOG parameter that enhances auditing requests during DL/I CHNG|AUTH call requests even when DFSC TSE0 (Security Reverification Exit) exists.
- Enhanced security for IMS conversations when the terminal has been disconnected with an active conversation in progress.

Most importantly, IMS V10 removes SMU security and all the components associated with SMU. Migration from SMU to SAF/RACF (or equivalent product) is easiest if accomplished before the IMS V10 migration, otherwise the migration from SMU to SAF will need to coincide with the migration to IMS V10.



Support for Mixed-case Passwords

- New startup parameter
 - ◆ PSWDC = M | U
 - M requests mixed-case support
 - U converts to upper-case and is compatible with previous releases

- Mixed-case support in IMS relies on mixed-case enablement in the security environment
 - RACF - z/OS v1.7 or later
 - SETROPTS PASSWORD(MIXEDCASE)
 - Requests the RACF use of mixed-case
 - SETROPTS PASSWORD(RULE...)
 - Sets password content-keyword rules (MIXEDCONSONANT, MIXEDVOWEL, MIXEDNUM) to allow mixed case characters

Support for mixed-case passwords is requested through a new startup parameter PSWDC. Setting the value to M (mixed-case) assumes that RACF has also been set up for mixed-case support.

For reference purposes, the applicable RACF commands include:

- SETROPTS PASSWORD(MIXEDCASE|NOMIXEDCASE). MIXEDCASE indicates that all applications on this system and those that share the RACF database support mixed-case passwords. The syntax rules must also be modified to allow mixed-case characters. When this option is activated, the RACF ALTUSER, ADDUSER, PASSWORD and RACLINK commands will no longer translate passwords to uppercase, nor will applications that request mixed-case password support such as IMS systems that specify PSWDC=M. This option is inactive by default.

- SETROPTS PASSWORD(RULE...) defines up to 8 syntax rules for new passwords and will be used to verify that the new password meets the criteria. The rules specifying mixed-case characters should only be set when the MIXEDCASE option is in effect. When the password rules are changed, there will be no immediate impact on the users. The only time the change will have an effect is when the users change their passwords. The rules are only used to verify that a new password meets the criteria. Any existing passwords are just verified against what is entered and what is in the database. The users will not be asked to change their password just because the syntax rules have changed. If multiple rules are defined, a password that passes at least one rule is accepted.

- SETROPTS LIST can be used to display the current setting

Support for Mixed-case Passwords ...

- IMS support affects:
 - ◆ /SIGN ON and /OPNDST
 - ◆ Reverification of a new password
 - ◆ Password in parentheses after transaction or command (excluding MFS OPT=3)
 - ◆ MFS password field in message input descriptor (MID)
 - ◆ MFS password field in device input format (DIF)
 - ◆ Password in parentheses after an IMS command parameter

- Consideration when mixed-case is in effect.
 - ◆ Users that used to enter passwords in lowercase when values were always converted to upper case will now need to enter their passwords in uppercase.

Since IMS provides several areas for a password to be entered, the new mixed-case support affects all these areas.

Be careful when enabling this capability. Users that were used to entering their passwords in any mode – lower, upper, mixed – may have their signon rejected if a specific case is expected.



Security Auditing Improvements

- Enhanced performance of SMF logging requests during authorization processing
 - ◆ Single authorization call
 - FASTAUTH call uses LOG=ASIS specification
 - SMF Logging occurs as part of the same RACF call
 - Assumes RACF (or security product) has requested auditing
 - Provides consistency across IMS authorization requests
 - Some authorization requests in previous releases required two RACF calls
 - FASTAUTH call for the initial authorization
 - Optional second call using an AUTH call (normal authorization checking) to request the SMF logging

In previous releases, IMS authorization requests were inconsistent with respect to the auditing capability, i.e., SMF logging and writing the ICH408I message to the system console. Some SAF requests used the normal authorization request call (AUTH) which could determine whether the security product required auditing and requested the function as part of the call. Other requests used the fast authorization call (FASTAUTH) and, when auditing was needed, performed a second AUTH call; and yet other requests issued the FASTAUTH with the additional specification of LOG=ASIS to perform auditing, when required, as part of the fast authorization.

IMS V10 provides a consistent method of requesting auditing. IMS authorization requests have been changed, where needed, to use the FASTAUTH call with LOG=ASIS specification to honor SMF logging requests as part of the same SAF call thereby eliminating the optional second AUTH call that was previously required just to request SMF logging.

The RACF implementation of auditing and the way the installation requests this capability from RACF have not changed. RACF continues to perform auditing if the authorization check results in success (RC=0) or failure (RC=8), and determines that auditing is necessary based on the following conditions:

- the user's UAUDIT setting
- the AUDIT, GLOBALAUDIT, and WARNING options in effect for the resource
- the SETROPTS SECLABELAUDIT is in effect
- the AUDIT options in the resource SECLABEL profile
- the pre-processing or post-processing installation exit's indication of whether or not to do auditing.

Security Auditing Improvements ...

- Additional enhancement during application AUTH call processing
 - ◆ New DFSDCxxx parameter that controls auditing calls even when the IMS system includes DFSTSE0 (Security Reverification Exit)
 - ◆ AUTHLOG = ALL | NONE | NOMSG
 - ALL – SMF log record written and ICH408I message to console (default)
 - NONE – No SMF log record and ICH408I message
 - NOMSG – Only SMF log record written

A new DFSDCxxx startup parameter provides a system level specification on how IMS is to handle auditing for application programs that issue the AUTH calls.

- AUTHLOG=ALL (default) requests that SMF logging occur and RACF error message ICH408I be issued when appropriate
- AUTHLOG=NOMSG allows SMF logging to occur when appropriate but suppresses the RACF error message ICH408I
- AUTHLOG=NONE requests suppress of both SMF logging and RACF error message ICH408I

Security Auditing Improvements ...

- Additional enhancement during application CHNG or AUTH call processing ...
 - ◆ Prior releases
 - IMS would not perform auditing if DFSCCTSE0 existed in the system
 - If auditing was required, DFSCCTSE0 had to perform the function
 - ◆ IMS V10 provides new flags for DFSCCTSE0 (Security Reverification Exit Routine) to facilitate auditing
 - CTSEAUDR in flag CTSEFLG1
 - Tells the exit that the auditing function is needed
 - CTSEDAUD in flag CTSEFLG2
 - Allows the exit to tell IMS to perform auditing

Another issue in prior releases was that IMS would not perform auditing if the IMS user exit DFSCCTSE0 existed in the system. The documentation indicated that the user exit had to perform the auditing function.

In IMS V10, IMS provides new flags that allow the exit routine to request that IMS issue an authorization call in a form that will allow auditing to take place. To take advantage of this capability, the DFSCCTSE0 exit routine will need to check a new flag (CTSEAUDR in CTSEFLG1) which indicates that the auditing function is needed, and when needed, set another new flag (CTSEDAUD in CTSEFLG2) to tell IMS to issue the authorization call and request auditing. The exit will only be able to set CTSEDAUD if CTSEAUDR is on.

Security Auditing Improvements ...

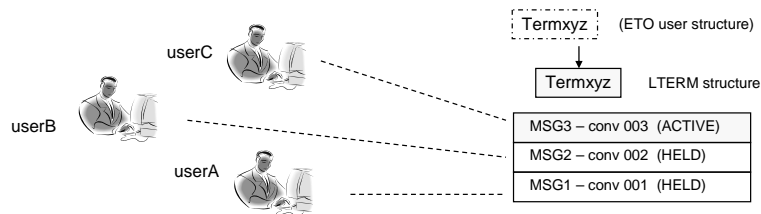
- Additional enhancement during application CHNG or AUTH call processing ...
 - ◆ IMS V10 auditing dependencies for CHNG, AUTH
 - The installation security product has requesting auditing
 - The existence of DFSCCTSE0
 - Whether or not auditing flags are set – CTSEAUDR and CTSEDAUD
 - The specification in the AUTHLOG parameter
 - ◆ Consideration
 - DFSCCTSE0 from prior releases will continue to work in IMS V10
 - No modification required
 - Leveraging the new capability requires modification

Security auditing in IMS V10 is based on:

- The installation's specifications that requests auditing of resources, and
- The presence/absence of the IMS user exit DFSCCTSE0 - if it exists, then the setting of the CTSEDAUD flag, and
- The specification of the AUTHLOG parameter requesting that a form of auditing be done

Enhanced Security for IMS Conversations

- Ensures that on reconnecting to an active IMS conversation
 - ◆ After a system crash, session crash or normal termination
 - ◆ Only the userid authorized to an active conversation is allowed to access that conversation
 - ◆ Applicable to static terminals and ETO terminals where user structure is not unique to userid (e.g., LUname=USERname=LTERMname)
 - Previous releases - access to an active conversation is allowed for all userids associated with the active or any held conversations



IMS V10 enhances security for IMS conversational processing in the situation where a user attempts to signon from a terminal that is associated with an active conversation.

In prior releases, as long as a user signing on from the terminal was authorized to one of the conversations (the active one or any of the ones on hold), that user could gain access to the active conversation even if they were not authorized to the active conversation. This situation affected all static terminals as well as ETO terminals where the control block structure of the USER was not unique to a signing on userid. For ETO, the environment in question was one where all userids logging on from the terminal accessed the same control blocks, e.g., LUname=USERname=LTERMname.

Enhanced Security for IMS Conversations ...

- With IMS 10,
 - ◆ Signon accepted only if:
 - User signing on is authorized to the active conversation, or
 - No active conversation exist, i.e., all conversations are held
 - ◆ Error results in DFS2469

 - ◆ Static terminals
 - If user signing on is not authorized to active conversation
 - Enter /HOLD, /SIGN ON, /RELEASE of desired conversation

 - ◆ ETO terminals
 - Only user authorized to active conversation can sign on
 - /HOLD is not allowed prior to a sign on
 - More restrictive

The IMS V10 change ensures that a signon will be successful only if:

- (a) the userid attempting the signon is authorized to use the active conversation, or
- (b) no active conversations exist, i.e., all the conversations are held.

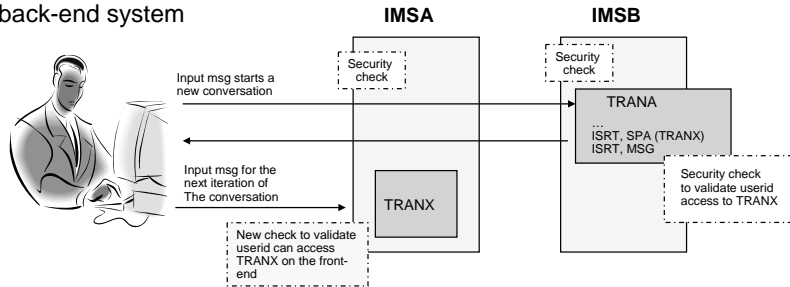
The impact to static and ETO terminals when an active conversation exists includes the following:

- Static: A user that is not authorized to the active conversation will fail signon. The user can issue /HOLD on the conversation and then reissue the /SIGN ON command. /RELEASE of the conversation to which the user is authorized can be entered to resume the appropriate interaction.

- ETO: Users that attempt a signon in environments that have generic naming conventions (e.g., LUNAME=USERNAME=LTERMNAME) must be authorized to the active conversation if one exists, otherwise the signon will fail. /HOLD is not allowed prior to a /SIGN ON.

Enhanced Security for IMS Conversations

- When an appl pgm inserts a deferred conversational program switch
 - ◆ IMS validates that the user has authorization to access the new transaction for the subsequent iteration of the conversation when the next input is received
 - Enhances the security environment for MSC and Shared Queues
 - ◆ Addresses the issue when the application issuing the deferred switch runs on a back-end system



- Also delivered in IMS V8 (PK07022) and IMS V9 (PK31739)

Terminology: - A *deferred conversational program switch* is one that responds to the terminal but causes the next input from the terminal to go to another conversational program. An *immediate program switch* passes the conversation directly to another conversational program. This capability addresses the deferred model.

When an application program inserts a deferred conversation program switch, IMS security mechanisms provide a method to validate authorization to the new transaction name when the SPA is inserted. The authorization check is done wherever the program runs using the security authorizations of that IMS system. IMS V10 addresses the concern that the program issuing the deferred conversation program switch could run on a back-end MSC or Shared Queues system where the authorizations might differ from the system where the switched-to transaction might actually run.

IMS V10 ensures that the user is authorized to access the switched-to transaction by adding an authorization check on the subsequent input from the end user. This check is made to validate that the user is authorized to access the switched-to transaction. If the terminal is disconnected during the conversation, and the conversation remains active, then the authorization check is made when the next signon is attempted.

SMU Support Removed

- IMS 10 removes SMU and SMU components
 - ◆ IMS-provided security
 - ◆ The Security Maintenance Utility
 - ◆ Application Group Name Exit Routine (DFSISIS0)
 - ◆ IMS.MATRIXx data sets

- Primary consideration
 - ◆ If migration from SMU to SAF/RACF has not already been done, migration to IMS 10 will also need to include migration from SMU to SAF/RACF

IMS V10 no longer supports the Security Maintenance Utility (SMU) capability. As a result, SMU components have been removed including the SMU Utility, the AGN Exit Routine (DFSISIS0) and the MATRIX data sets. Note that the IMS.MATRIXx data sets have been deleted and removed from all IMS procedures and logic.

A primary consideration in this area includes migration. IMS systems that use SMU must migrate to the SAF interface at the time that the upgrade to IMS V10 occurs.

SMU Support Removed - Impact

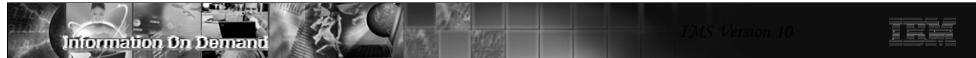
- System definition macros - SMU specifications ignored
 - **COMM** OPTIONS= (<NOPSWD|PASSWD|FORPSW><,NOTERMNL|
TERMINAL |FORCTERM>)
 - **IMSGEN** PSWDSEC=,TERMSEC=
 - **SECURITY** PASSWD=,TERMSEC=,TRANCMD=,
TYPE=(<NOAGN|RACFAGN|AGNEXIT>)

- Utilities
 - ◆ SMU Utility no longer supported
 - ◆ Online Change Utility ignores MATRIX dataset DD cards

The impact of removing SMU affects the IMS environment in several ways.

- All SMU specifications in any of the system definition macros are ignored. These specifications were previously found in the COMM, IMSGEN and SECURITY macros.

- The Security Maintenance Utility no longer is available in IMS V10. Additionally, the Online Change Utility will no longer support the IMS.MATRIX data set. If the MATRIX dataset DD cards exist in the online change utility JCL, the utility will ignore those specific DD cards.



SMU Support Removed - Impact

- Initialization, start-up parameters and procedures
 - ◆ Specifications that are ignored: AGN, AOI1=S, ISIS=<0|1|2>
 - ◆ Specifications that are no longer documented but are compatible with functionality in previous releases (requests for SAF and bypassing of SMU)
 - TRN=<E|X>, RCF=<B|R>, SGN=<D|E|W|X>
 - ◆ Specifications that have changed meanings
 - MSCSEC – values allow SAF/RACF or no security
 - SMU defaults no longer applicable

The changes to the startup parameters fall into several categories:

- (a) Parameter values requesting the use of SMU continue to be accepted in IMS V10 but are ignored. These include AGN (specification of an AGN name), AOI1=S (request to use SMU security for AOI Type 1 command authorization) and ISIS=<0|1|2>. The ISIS parameter is still supported for specification of combinations of SAF and user exit authorization. Only the three values of 0, 1, or 2 which were previously associated with SMU are now ignored.
- (b) Specifications that are no longer documented but are compatible with functionality in previous releases of IMS. Certain parameter values in previous releases allowed the use of SAF/RACF along with negating the loading of the signon security tables from the MATRIX data set. The specifications included: TRN=<E|X>, RCF=<B|R>, and SGN=<D|E|W|. Although these values are no longer documented in the IMS V10 System Definition Guide because they request negation of loading tables from the MATRIX data set which is no longer supported, the values will be accepted for compatibility purposes and function in the same manner as the supported counterparts. For example, TRN=E is equivalent to the supported value of TRN=F (TRN=E → TRN=F). This is because TRN=E, in previous releases, requested option F plus the negation of loading the SMU signon tables. Likewise, TRN=X → TRN=Y, RCF=B → RCF=A, RCF=R → RCF=S, SGN=D → SGN=F, SGN=E → SGN=G, SGN=W → SGN=Y and SGN=X → SGN=Z.
- (c) Specifications that have changed their meaning because the SMU capability no longer applies include some of the values that can be specified. The MSCSEC parameter previously included values that allowed SMU security to be used for non-directed routing requests. In IMS V10 the parameter values specify the use of SAF/RACF or no security.



SMU Support Removed – Impact ...

- Commands that are no longer valid
 - /CHANGE PASSWORD and /DELETE PASSWORD|TERMINAL
 - Rejected with: DFS181 INVALID OR MISSING KEYWORD

- Commands that support SAF/RACF security and no longer support SMU security
 - ◆ /SET, /LOCK, /UNLOCK
 - SAF/RACF enhancements in IMS V9
 - Userid access to transactions (TIMS/GIMS), PSBs (IIMS/JIMS), LTERMs (LIMS/MIMS), and databases (PIMS/QIMS)
 - Based on specification of LOCKSEC=Y|N
 - Password access to resources through RACF REVERIFY capability

Certain commands such as /CHANGE PASSWORD and /DELETE PASSWORD|TERMINAL were strictly associated with SMU security. These commands are no longer supported in IMS V10 and, if entered, will result in error message DFS181.

SAF/RACF support for the resources associated in the /SET, /LOCK and /UNLOCK commands was introduced in IMS V9 along with the LOCKSEC parameter and additional resource classes for PSBS (IIMS/JIMS) and LTERMs (LIMS/MIMS). IMS V10 removes the SMU check and supports the SAF/RACF security check which includes two checks: both a validation that the userid of the signed on user is authorized to invoke the /SET, /LOCK, or /UNLOCK command; and a second check that userid is authorized against the resource being accessed – Transactions, LTERMs, Programs, Databases.

Password security is different when using SAF/RACF versus the previous capability with SMU. SAF/RACF uses the signed on user's password in a reverify capability whereas SMU used a global password as defined in the SMU tables. Note that the use of a password after the parameter defining the resource will continue to be supported for all keywords except PTERM and NODE. This restriction has not changed. The SAF/RACF check is accomplished using the RACF REVERIFY support. The REVERIFY support assumes that the RACF profile for the IMS resource is defined with the parameter "APPLDATA('REVERIFY')", then IMS (assuming RVFY=Y is specified as an IMS startup parameter) checks that the password is the same as the user's signon password. If the resource is defined to RACF but is not authorized for use, the command is rejected with message DFS3689W USE OF <TRANSACTION|LTERM|DB|PROG> resourcename BY <LOCK|UNLOCK> REJECTED.

SMU Support Removed – Impact ...

- Restart commands - /NRE and /ERE
 - ◆ SMU keywords are ignored
 - TERMINAL, NOTERMINAL, PASSWORD, NOPASSWORD, TRANCMDs, NOTRANCMDs

- Online Change commands
 - ◆ /Modify
 - PASSWORD, TERMINAL and TRANCMDs keywords are ignored

 - ◆ INIT OLC
 - PASSWORD, TERMINAL and TRANCMDs keywords
 - Ignored for IMS V10 systems
 - Passed on to other IMS V8 or V9 systems if multiple releases exist in the sysplex environment

All SMU keywords are ignored when any of the restart commands are issued.

For Online Change requests, the PASSWORD, TERMINAL and TRANCMDs keywords do not apply to the IMS V10 system for either a /MODIFY or INIT OLC command. For INIT OLC, the keywords are still processed, and the appropriate flags in the MWA are set, so that in a sysplexed environment that consists of a mixture of V8, V9 and V10 systems, the keywords can be passed on to the IMS systems at the V8 or V9 level.

SMU Support Removed – Impact ...

- Documentation – areas that no longer apply and have been removed
 - ◆ Messages
 - DFS062, DFS066, DFS067, DFS095, DFS109, DFS123, DFS125, DFS126, DFS162, DFS171, DFS287, DFS288, DFS1913, DFS1919, DSF2181, DFS2468, DFS2556, DFS3436, DFS3437, DFS3440, DFS3458
 - ◆ Abend codes
 - ABENDU0171, ABENDU0901, ABENDU0902, ABENDU0903, ABENDU1050
 - ◆ MNOTEs
 - AGT001, AGT002, AGT003, AGT004, AGT005

The removal of the SMU support has also affected the documentation for certain messages and abend codes as well as specific application program status and return/reason codes. The documentation in the appropriate manuals has been changed to remove references to SMU-based security.

SMU Support Removed – Impact ...

- Documentation changes
 - ◆ Messages
 - DFS158, DFS1990I, DFS1991I, DFS2854A, DFS3430I, DFS3480I, DFS3654, DFS3690
 - ◆ Abend codes
 - ABENDU0107, ABENDU0437, ABENDU0718
 - ◆ MNOTEs
 - G972
 - ◆ Application program - status codes and return/reason Codes
 - A4, 0108/0308

IMS documentation has also changed to remove references to SMU security.

SMU to SAF/RACF Migration

- Migration to SAF (RACF or equivalent) can begin in IMS V8 or IMS V9
 - ◆ V9 includes RACF enhancements for SMU functions which previously had no alternatives
 - Enhancements include areas of AGN, AOI, TCO, MSC link receive, signon verification, and /LOCK and /UNLOCK
 - V9 is a transition release where SMU is still available
 - ◆ Migration from SMU to SAF and from IMS V8 to IMVS V10 is a valid option
 - Begin SMU to SAF migration in IMS V8
 - Migration using V9 enhancements will have to occur during the V10 migration
- Migration references
 - ◆ Chapter 6, IMS V9 Implementation Guide redbook (SG24-6398)
 - ◆ Chapter 4, IMS V9 Administration Guide: System (SC18-7807)
 - ◆ Chapter 3 and 4, IMS V9 Release Planning Guide (GC17-7831)

Both IMS V8 and V9 provide migration paths to the use of SAF/RACF security. IMS V9 provides migration capabilities that are not available with IMS V8.