Defense Health Agency

TECHNICAL MANUAL

NUMBER 6430.02, Volume 2
April 7, 2022

DAD MEDLOG

SUBJECT: Defense Medical Logistics Standard Support (DMLSS)Volume 2: Systems Administration

References: See Enclosure 1.

1. PURPOSE. This Defense Health Agency-Technical Manual (DHA-TM), based on the authority of References (a) and (b), and in accordance with the guidance of References (c) through (o), establishes the DHA's instructions for using the Defense Medical Logistics Standard Support (DMLSS) application. This DHA-TM provides Medical Logistics (MEDLOG) and other DMLSS users with the technical guidance procedures necessary to use the application effectively and efficiently to carry out the mission of MEDLOG support. The technical guidance contained in this DHA-TM volumes 1 through 10 are intended for use of the automated information system in support of MEDLOG business including contingency materiel management in the DHA.

2. APPLICABILITY. This DHA-TM applies to the DHA, Activities under the authority, direction, and control of DHA, and all personnel assigned, who have need to reference the enclosed technical guidance information for use of DMLSS automated information system.

3. POLICY IMPLEMENTATION. It is DHA's instruction, pursuant to References (e) through (o), that:

a. DHA will exercise management responsibilities of Military Health System (MHS) MEDLOG functions in the MHS including implementing procedures, administering budgets and performing financial oversight at an enterprise level in order to ensure consistency, optimize performance, and meet strategic priorities across MHS MEDLOG activities consistent with guidance from the Assistant Secretary of Defense for Health Affairs(ASD(HA)).

b. DHA will develop consistent standards for materiel management (MM) necessary for programmatic oversight of the Defense Health Program.

c. DHA established DMLSS as the authoritative information system that serves as the feeder system to financially accountable systems for DROs, and accountable property officers as outlined in Reference (d).

d. DROs must use the DMLSS system, as prescribed in Reference (d), for all MEDLOG business functions in the following modules, including, but not limited to: Customer Area Inventory Management (CAIM), Inventory Management (IM), Equipment Management (EM), Equipment Maintenance (MA), Assemblage Management (AM), Systems Services (SS), and Facility Management (FM). These DMLSS modules provide a processing environment where personnel can accomplish following automated processing for: inventorying, ordering, receiving, and issuing of materiel associated with operations, research and support prescribed by the DHA mission.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. PROPONENT AND WAIVERS. The proponent of this publication is the Deputy Assistant Director (DAD), MEDLOG. When Activities are unable to comply with this publication the activity may request a waiver that must include a justification, to include an analysis of the risk associated with not granting the waiver. The requesting activity director or senior leader will submit the waiver request through their supervisory chain to the DAD MEDLOG to determine if the waiver may be granted by the Director, DHA or their designee.

7. RELEASABILITY. **Cleared for public release**. This DHA-TM is available on the Internet from the Health.mil site at: https://health.mil/Reference-Center/Policies and is also available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx.

8. EFFECTIVE DATE. This DHA-TM:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or canceled before this date in accordance with Reference (c).

9. FORMS. The following DD Forms are available on the internet at https://www.esd.whs.mil/Directives/forms/.

a. DD Form 1155, Order for Supplies or Service.

b. DD Form 2875, System Authorization Access Request.

/S/
RONALD J. PLACE
LTG, MC, USA
Director

Enclosures
1. References
2. Responsibilities
3. Procedures
4. Defense Medical Logistics Standard Support Military Medical Treatment Facility/Organization-Service and Logistics Department
5. User Privilege and Role Management

Glossary

TABLE OF CONTENTS

TABLES

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013, as amended
(c) DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018
(d) DHA-Procedural Instruction 6430.04, "Use of the Defense Medical Logistics Standard Support (DMLSS) as the Authoritative Information System (IS) of Record for the Medical Logistics (MEDLOG) Enterprise Activity (EA)
(e) United States Code, Title 10, Section 1073c, National Defense Authorization Act for Fiscal Years 2017, 2018, 2019, and 2020
(f) DHA-Procedural Instruction 6430.02 "Defense Medical Logistics (MEDLOG) Enterprise Activity (EA)," September 27, 2018
(g) DHA-Procedural Instruction 8100.01 "Information Security Compliance for Defense Health Agency Financially Auditable Information Systems" January 12, 2021
(h) DoD Directive 6000.12E, "Health Services Support," January 6, 2011, as amended
(i) DoD Instruction 6430.02, "Defense Medical Logistics Program," August 23, 2017
(j) DoD Manual 6025.18-R, "DoD Health Information Portability and Accountability Act (HIPAA) Privacy Rule in DoD Healthcare Programs," March 13, 2019
(k) DoD Instruction 8500.01, "Cybersecurity," March 12, 2014, as amended
(l) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(m) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015
(n) GAO-09-232G, "Federal Information System Controls Audit Manual (FISCAM)," Dacey, R.F., United States Government Accountability Office, Washington, DC, February 2, 2009
(o) Code of Federal Regulation, Title 21, Section 1300

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA will assign all DHA Headquarters Staff elements and DAD, MEDLOG to implement this DHA-TM in accordance with Reference (b), (e), and (f).

2. DAD, MEDLOG. The DAD, MEDLOG or designee must perform oversight of the delivery of all MEDLOG business functions in accordance with References (f) and (h).

3. DRO DIRECTORS. The DRO Directors must:

a. Ensure DROs implement this DHA-TM.

b. Ensure Compliance with this DHA-TM.

c. Ensure the Chief, MEDLOG maintains and accounts for all accountable medical and dental property and financial records on the stock record account in DMLSS.

d. Use the following DMLSS modules including, but not limited to: CAIM, IM, EM, MA, AM, SS, and FM.

e. Appoint a DMLSS System Administrator (SA) in writing; may delegate by-direction signature authority to Chief, MEDLOG as necessary.

f. Implement procedures, guidance, and instructions for this DMLSS-TM.

4. DRO CHIEF, MEDLOG. The DRO Chief MEDLOG must:

a. Maintain and account for all accountable medical and dental property and financial records on the stock record account in DMLSS.

b. If designated by Director in paragraph 5.c. of this enclosure, appoint DMLSS System Administrator (SA) in writing.

5. DRO, DMLSS SA. The DRO DMLSS SA must:

a. Establish, manage and maintain DMLSS user accounts, roles and privileges. The least privilege principle must be followed when creating or modifying user accounts.

b. Ensure system backups and maintenance tapes are installed at pre-defined periodic intervals and perform manual backup procedures as necessary and as specified in this DHA-TM.

c. Monitor the DMLSS Communications Management (DCM) functionality to identify and resolve transmission errors.

d. Follow database (DB) auditing procedures as defined in DMLSS SA guide.

e. Establish local procedures to ensure monitoring for cybersecurity threats and prevent unauthorized access to DMLSS.

f. Coordinate with DRO Director, Information Systems to house DMLSS hardware and install and update DMLSS system software as required.

f. Create and manage DMLSS tutorial databases.

g. Review DMLSS advisory notices and notify users as required.

6. DHA MEDLOG PERSONNEL. DHA MEDLOG personnel must follow the instruction (CSTs, Divisions, Training, etc.) as appropriate for each volume of this DHA-TM.

ENCLOSURE 3

PROCEDURES

1. SA. This Enclosure contains instructions for the site System Administrators (SA) managing the DMLSS system. Also, specific information is provided to ensure the secure operation of this information system by using system privileges and protective mechanisms.

a. Scope. Refer to Reference (n) for an overview of the basic system navigation features.

(1) DMLSS functionality for SAs exists primarily within the System Administration Tool located on the server's webpage and with the DMLSS application under the System Services (SS) module.

(2) In addition to the instructions in this DHA-TM, additional SA resources may be obtained online at the Military Service managed MEDLOG websites and DHA/Solution Delivery Division/Health Information Technology's Resource Center webpage.

b. Access Control

(1) The SA must review user access and roles at minimum twice annually, during the month of April and October and will be prompted for such action through the System Administration Tool. Review the Audit: Active Users (Apps/Roles) report available in the SA Tool. To the fullest extent possible, determine that a single person is not responsible for all functions. Organizations with limited resources to segregate duties should have compensating controls in accordance with Reference (l), such as supervisory review of transactions performed. Produce and sign annually a Memorandum for Record (MFR) documenting that all users have been reviewed and validated except as otherwise annotated on the Active User Report. The DMLSS SA must: attach the annotated Active User Report to the MFR, sign and date the MFR bi-annually during April and October reviews, and retain the signed MFRs for 2 years.

(2) DMLSS automatically locks Common Access Card (CAC) user accounts after 30 consecutive days of inactivity. User accounts with 60 continuous days of inactivity are automatically de-provisioned. SAs can use the Audit: Active Users, and Audit: Deleted Users reports in the System Administration Tool to easily identify the status of user accounts and verify deletion of obsolete accounts. This includes suspended and terminated employees and users with emergency/temporary access to the system.

(3) MEDLOG must ensure removal of network/DMLSS system access for departing users during out-processing, if notified. For example, military medical treatment facility (MTF)/dental treatment facility (DTF) out processing checklists must include both Information Systems (CAC-authenticated access to the DMLSS system requires Local Area Network access), and MEDLOG (Customer Service and/or Medical Equipment Branch, Division, or Office). Annotate the date a user's access to DMLSS was removed on the DD Form 2875, or other Systems Authorization Access Request (SAAR), and maintain form on site for 2 years.

c. System Backups

(1) Backups are the first line of defense against the loss of valuable information. Currently, the DMLSS system uses an external tape drive and magnetic data tape (Linear Tape-Open-4 (LTO-4) technology to back-up critical server and DB files. The server automatically initiates the DB file backup daily based on configuration of time at the site.

(2) Daily, Monthly, and end-of-fiscal-year (EOFY) Processing. The DMLSS system performs each of these end-of-period (EOP) cycles/tape backups automatically. Coordinate the exchange and storage of tapes with the Medical Information Systems. For procedures regarding Tape Storage, refer to paragraph 1.g.(2) of this Enclosure. Verify the automatic backup processed. If backup failed contact DHA Global Service Center (GSC) help desk at 1-800-600-9332 or dhagsc@mail.mil.

(a) All DMLSS sites should be set on a minimum 7-day backup schedule. Insert a new LTO-4 tape into the tape drive each Monday and allow it to automatically backup. The tape is set to automatically eject each Monday morning after the backup.

(b) Monthly EOP data is written to the same tape as the final daily of the month. Similarly, EOFY data is written to the same tape as the final daily/monthly of the Fiscal Year (FY). Additional tapes or storage requirements are not needed for either of these cycles.

(c) SAs should maintain a rotation of four EOP backup-tapes. SAs should also maintain two spare tapes on-hand (O/H) at all times.

(3) Audit Backup Tape. At a minimum, run on the first day of each month or more often depending on the size of the facility. DMLSS SA will regularly check Last audit log backup in the Main Menu (Services and Process Dates) of the System Administration Tool. A red box indicates it is time to back up the sites audit data. Site personnel must safeguard and store audit backups for 1 year, and up to 7 years, if possible. Failure to back up on a monthly basis may result in loss of data. For procedures regarding Tape Storage, refer to paragraph 1.g.(2), of this Enclosure.

(a) Logon to the DMLSS System Administration Tool/navigate to Manage Backup/and select Backup
Audit Data.

(b) Follow the instructions that are presented on the Backup Audit Data page regarding how to label the audit backup tape and/or which tape to mount.

(c) SAs need three audit backup tapes for three different 6-month periods of backups. Tape 1 should contain the first 6 months of audit data for the period January–June. Tape 2 should contain the following 6 months of data, July–December, and Tape 3 should contain the following 6 months of data, January–June, so there is always 1 year of audit data available.

(d) When performing a monthly audit backup, the instructions within the System Administration Tool provides guidance to use the current 6-month tape and append the additional month's data to the same tape.

(4) Verify automatic EOP and/or manual audit backups worked. If they failed, perform a manual backup.

(5) Data tapes that are used frequently wear out and lose their recording ability. SAs should track the life of these tapes and create a replacement schedule where all tapes are replaced according to manufacturer specification. For example, if the manufacturer states their tapes are tested to withstand a minimum of 100 full backups, and there is a 5-week rotation, calculate an appropriate replacement schedule. In this scenario, replacing them at 3 years would be more cost effective and still not extend them beyond their life expectancy.

d. System Maintenance. SAs should complete the following tasks in order to keep the server secure and the DB operating smoothly.

(1) Review the Status of Services and Process Dates. Daily, the SA should log on to the System Administration Tool and review the list of services and process dates that appear on the SA home window. This table provides a complete overview of the server's resources and whether or not system processing is up to date, see Figure 42, System Administration Tool, Manage DCM Service of this Enclosure. Each of the services or processes listed has a corresponding message and colored box to indicate its status. If any red boxes appear, investigate the problem.

(2) Clean the Tape Drive. Clean the tape drive weekly using a designated LTO-4 cleaning tape whenever the cleaning indicator lights or sooner if the light emitting diode read-out indicates cleaning the drive.

(a) To use a cleaning tape, the tape is inserted into the tape drive. The tape runs automatically for about 30 seconds, and then it self-ejects. If it does not self-eject, eject it manually.

(b) Use the cleaning tape once every 2 weeks. Use the check-off sheet included with each cleaning tape. Each time a cleaning is completed, check off one of the boxes. Once all the boxes are checked, discard the cleaning tape.

(3) For System Reboot information see paragraph 1.g.(8) of this Enclosure.

e. Monitor the DCM Module

(1) This module, viewable in SS, is an automated tool used for bi-directional communication with trading partners. It is also the conduit for receiving transmission of incoming status files, and it provides tools that allow SAs to monitor progress of these files and troubleshoot any errors.

(2) Identify transmission errors via the IM inbox or DCM Search/Monitor.

(a) SAs are notified via the IM inbox when there are failed outgoing transmissions. These include failed orders, financial files, Quality Assurance (QA), and transportation files.

(b) Inbound errors, for example, ASSOCERR or MISTPCD can only be caught by reviewing the DCM Search function.

(c) In addition to IM inbox messages, SAs may monitor the DCM directly using the DCM Search or Monitor options in SS. This module keeps a record of all transmissions to ensure all transaction files are successfully transmitted and received as a result of the previous day's business. The DCM Search window provides multiple search options. Enter specific and detailed search criteria to narrow search results or minimize search criteria to receive a broad range of search results. To identify formatting errors or failed transmissions, monitor the Status code for ERROR and the corresponding process code. The process code for that item indicates in which stage the error occurred.

(d) Specifically, DMLSS SA must verify the prime vendor (PV) order are successfully sent via Electronic Data Interchange (EDI) 850 and PV status received via EDI 855. DMLSS SAs should check the IM inbox or the DCM daily to verify financial files were successfully transmitted to the Service Financial System.

(3) Resolve DCM Problems

(a) Contact Medical Information Systems to determine if local network-related problems are causing the errors in transmission. Also, check to see if there is power to the server, connection to the Juniper Secure Services Gateway (GW), and Cisco switch is secure.

(b) For DMLSS system related problems, contact the DHA GSC help desk at 1-800-600-9332 or dhagsc@mail.mil.

(4) Data Retransmission. The SA or DCM monitor at the MTF/DTF need to resend failed files. First, verify with the Medical Information Systems that the base network is up, and all ports and firewalls are open. Upon verification, use the DCM Resubmit or failed Financial Resubmit options to retransmit the transaction files, see, paragraph l., in this Enclosure.

(5) Manual Orders. When the DCM is down completely for an extended period of time, the MEDLOG account should consult with DHA MEDLOG and refer to local installation and medical unit Continuity of Operations guidance.

f. System and DB Auditing Procedures

(1) The first step to an effective audit process is selecting both a DB Auditor Reviewer and System Audit Reviewer. Use the Create DMLSS User Account window to initially assign one of these roles or modify a current user's role by selecting the Manage DMLSS User Accounts and then select the Update Roles link.

(2) It is important to understand that SAs and audit reviewers each have vital roles in the audit process.

(a) With regard to the audit process, the DMLSS SA enforces the overall security policy, and detects any attempts to violate protection or privilege mechanisms. Also, they are responsible for restricting access to the audit subsystem to only authorized users.

(b) DMLSS system audit mechanisms exist at both the database (DB) and operating system (OS) level. Reviewers/auditors are individuals specifically authorized to review the audit trail regularly to monitor system usage, detect penetration of the system, and detect any misuse of resources.

(c) SAs and audit reviewers must ensure the following resources are used to routinely audit the system:

1. DMLSS Application Audits. Use the Auditing Tool in SS/UP-Management window to view the application audit records. This function provides Application Security Managers with the ability to check which users were in the system, when, how long, or problems associated with connecting. It can also be used to track what application(s) a user accessed, when it was accessed, and for how long. This file can also be viewed in the "System Logs" area of the System Administration Tool on the server. DMLSS SAs, DB reviewers, and/or supervisors should routinely review user activity logs for incompatible actions and investigate any abnormalities.

2. DMLSS DB Audits. Every major event that occurs within the system database (DB) is recorded and made available to the auditor on the DMLSS Audit Report which may be accessed on the DMLSS Start Page. As warranted, monitor the security of the DMLSS using this report to look for DB abuses and attacks. Examples of events to look for are failed logins, unusual hour logins, or detection of events such as attackers attempting to log on and/or alter the DB. Both DB and system tabs are displayed on this report, but they are only visible if the user is privileged with both the DB audit reviewer and system audit reviewer roles. Records are maintained for 1 year.

3. DMLSS OS Audits. System audits occur for every major system event that occurs on the DMLSS server. Examples of events are deletions, removals, and modifications of files. Back up critical Operating System (OS) audits using an audit backup tape on the first day of each month or more often as directed in the System Administration Tool.

4. Use these resources along with enforcement of the security policy, examining access patterns, and observing the actions of users to help detect any unauthorized attempts to access the system. Perform audit reviews in accordance with DoD and site requirements.

g. Additional Responsibilities

(1) Managing DMLSS Installations and Updates. Installing and updating DMLSS system software usually requires the assistance of the local IT administrator or possibly DHA Global Service Center (GSC).

(a) DMLSS Installation. Refer to the Client Installation Guide on the Joint Medical Logistics Functional Development Center (JMLFDC) Resource Center website, https://jml149.dmlss.detrick.army.mil/resourcecenter/index.html# when installing DMLSS or other commercial-off-the-shelf applications used on DMLSS personal computers/workstations.

(b) DMLSS Software Releases. DAD-IO will announce future system builds and provide installation packages and software release notes explaining changes to the system. Additionally, DMLSS software can be downloaded from the server's homepage when a manual installation of the client is required. The installation package can be found at the JMLFDC Resource Center website provided in DMLSS.

(2) Tape Storage. Verify EOP, and audit tapes are produced, and a tape backup system is in place. Backup tapes should be stored in a secure location away from the server, and safeguarded against fire, moisture, high electrical currents, and reuse. Label all used tapes with the type and date of backup, DMLSS build number, and the name of the person performing the backup. Additionally, a tape backup system may include an inventory record of backup tapes, consideration of when and how files are rotated off site (e.g., advancing natural disaster), retention periods, and security involved in transport.

(3) Peripheral Device Management

(a) Barcode Printer. On occasion, DMLSS SAs may need to install a new barcode printer. For assistance, contact the DHA GSC help desk at 1-800-600-9332 or dhagsc@mail.mil.

(b) DMLSS Hand-held Terminals. SAs should maintain awareness of their site's hand-held terminals and docking stations. DHA MEDLOG must maintain the hand-held terminal software and provide training on their use for expediting replenishment, receiving, and inventory. When used wirelessly, SAs should be familiar with setting up user profiles on the hand-held terminals and how to connect them to the wireless local area network. For assistance, contact the DHA GSC help desk at 1-800-600-9332 or dhagsc@mail.mil.

(4) Coordinate with Medical Information Systems to maintain DMLSS Hardware Inventory. Ensure DMLSS Hardware is appropriately accounted for on property records in accordance with DHA or Military Service policies.

(5) Manage Tutorial DBs. DMLSS SAs manage tutorial DBs as described in paragraph 2.j.(3) of this Enclosure. Tutorial DBs are sanitized copies of the specific site production DB and may be used for practicing or testing of procedures without affecting actual system DB conditions. For example, orders are not actually transmitted in the tutorial DB as the Internet Protocol (IP) addresses for site associated trading partners have been removed. Tutorial DBs should be leveraged to the maximum extent possible when conducting training, or when there is uncertainty in processing specific steps in DMLSS.

(6) FM Responsibilities. DMLSS SAs with a Facility Management (FM) Administrator role assigned in the System Administration Tool have additional responsibilities as described in paragraph 2.l. of this Enclosure.

(7) Review DANs. DAD-IO publishes DMLSS Advisory Notices (DAN) on the U.S. Air Force MEDLOG website as a way to notifying users of known problems. These notices typically state the problem, background information, a work-around solution if one exists, and an estimated get-well date.

(8) Reporting System Problems. For any questions or problems with DMLSS, use the following resources, in order, to find solutions:

(a) For network-related problems, contact the local network administration support group.

(b) For system-related problems, contact the DHA GSC Help Desk at 1-800-600-9332 or dhagsc@mail.mil.

1. The DHA GSC assists DMLSS SAs in resolving problems associated with the application software, hardware, and OS software-related problems to Dell.

2. The DHA GSC assigns a ticket number to each call reporting a problem. Please make a note of this ticket number for future reference.

(c) For problems with equipment purchased under the Dell contract, contact the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil.

(d) For problems with equipment not purchased under the Dell contract, use the appropriate contract vehicle in place for that specific piece of equipment.

2. SYSTEM ADMINISTRATION TOOL

a. DMLSS Website. The DMLSS server at each site has a portion allocated as a Web server area, referred to as the DMLSS website. This is the area where the System Administration Tool resides, as well as other important links.

(1) Access the DMLSS server webpage. In the browser address line, enter https:// and the server name or IP address of the DMLSS server. Initially, the Notice and Consent Logon Banner Screen appears (Figure 1).

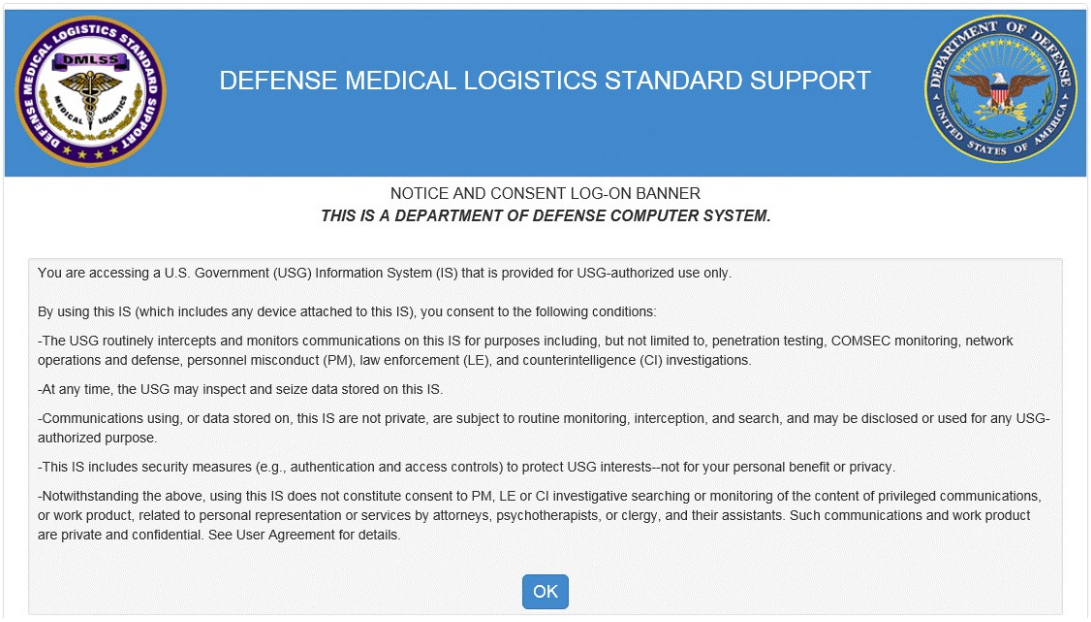


Figure 1. Defense Medical Logistics Standard Support Webserver–Notice and Consent Logon Screen

(2) DMLSS Web Server Start Page. The DMLSS web server Start Page is then displayed after consenting to the conditions listed on the first page, see Figure 2. SAs use the Web Server Start Page for a variety of reasons including accessing installation software, viewing documentation, logging onto to the DMLSS System Administration Tool, and associating a Smart Card/CAC. All users may access the information on this page without having to log onto the SA Tool.

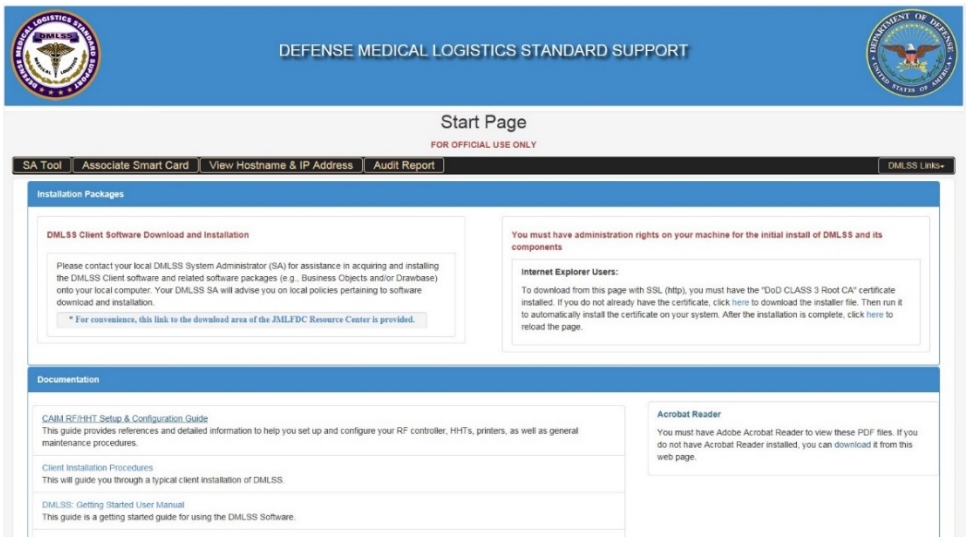


Figure 2. Defense Medical Logistics Standard Support Web Server Start Page

b. System Administration Tool Overview. The SA Tool provides the capability to manage the server, external devices, backup of DB, and user access.

(1) System Administration Tool Access. Select SA Tool tab at the top left of the DMLSS web service Start Page. The System Administration Login window is displayed in Figure 3. To log in, select Smart Card Login.

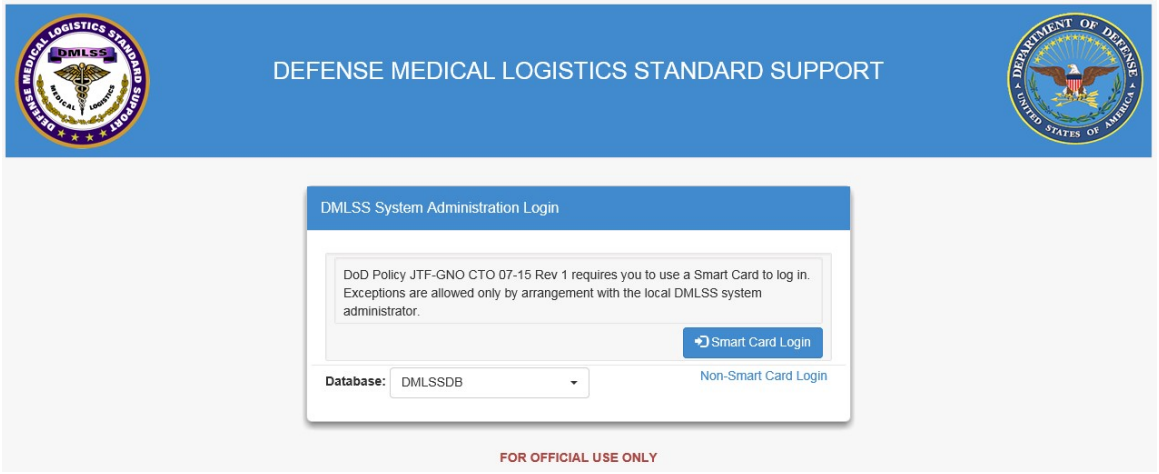


Figure 3. Defense Medical Logistics Standard Support System Administration Tool Login Window

(2) Upon logging in, the DMLSS System Administration Menu opens (Figure 4). The Navigation Pane includes a list of Task Areas, Quick Links, and DMLSS Links.

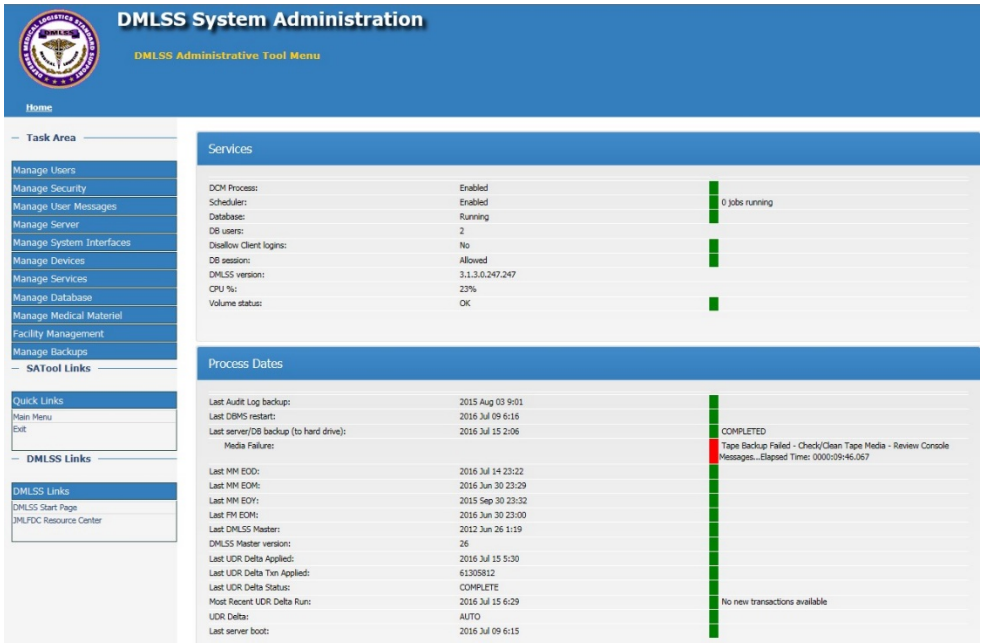


Figure 4. Defense Medical Logistics Standard Support System Administration Menu

(a) Services and Process Dates. The list of Services and Process Dates are both critical sections on the System Administration home window. As the name indicates, Services shows the services available on the server, while Process Dates displays the most recent dates that particular processes have run on the server. Monitoring both of these areas is a key responsibility of the SA.

1. If Services/Process Dates are enabled, working, or up to date, a green box is displayed. A yellow box indicates a warning. If resources are disabled, at a critical stage, or processes have not run, a red box appears. For example, the Volume status box reports available disk space. If one of the two drives fall below 20 percent, the Volume status box turns yellow. If the volume falls below 10 percent, the box turns red. In both instances, the message: *Contact the MHS helpdesk* appears.

2. Any non-green status needs to be addressed immediately. Also, in some cases, the precise value or entry is not significant, but variances from the routine should be investigated or reported to the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil.

3. Selecting the red box with a yellow star sends the user to another page within the DMLSS System Administration Tool where the problem might be resolved or where more information might be available.

4. Scheduler Status reflects the number of DMLSS-related jobs currently running in the scheduler DB. They are listed to the right of the Enabled/Green status. If the number of jobs is greater than zero, the text is selectable and displays the new View Running Scheduler Jobs page when selected.

5. Audit Backups. Periodically, a message under Process Dates indicates the backup threshold has been reached with a status of Backup of Audit Required, Last Status, followed by the date the last backup was run and a red indicator. If this occurs, go to the Manage Backups menu and select the Backup Audit Data menu item as described in paragraph 2.m.(2), "Backup Audit Data" of this Enclosure.

(b) Use the dropdown menus within the Task Area to manage System Administration activities. SAs have full access to all these menus with the exception of the FM menu. Only those with the FM Administrator role have access to the FM menu.

c. Manage Users. The first dropdown menu in the System Administration Tool Task Area is Manage Users (Figure 5). It is used to manage the accounts of DMLSS users by including some of the most common tasks performed by SAs. The following options are available from this menu:

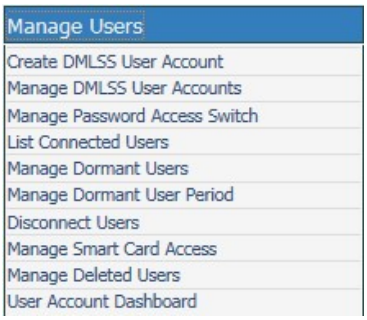


Figure 5. Manage Users Menu

(1) Create DMLSS User Account, Figure 6. Use this function to set up new user accounts. Each DMLSS user must have a unique account consisting of a username with approved access via CAC, or a username with password if approved by DHA MEDLOG.

(a) Create DMLSS User Account with Smart Card Access. First, the SA verifies that both the Distinguished Name (DN) and Employee Identification belong to the person the requesting account access. If the name or employee identification number does not match the new user or user signature on the DD Form 2875 or other System Authorized Access Request (SAAR), the SA must not approve the account.

1. Upon verification of the user, SAs may choose to create a new user account with access via the Smart Card/CAC by first establishing a username for the new user. Follow the rules for establishing a valid username that are listed on this tab.

2. The SA must enter the Department of Defense Identification (DoD ID) Number, the 10-digit number found on the back of a CAC, also known as the EDI personal identifier. If provided here, the user account created is automatically approved and operational when the account is associated with a corresponding CAC, and the SA does not need to approve the account as a separate step.

3. The SA selects the correct user type—User or Administrator, and then adds any of the three user roles that apply—DB Audit Reviewer, System Audit Reviewer, and/or Facilities Management Administrator.

4. After selecting the user type and user roles, the SA selects Create User. The system provides a message screen informing the SA whether the account was created or if any errors occurred. Select OK to continue.

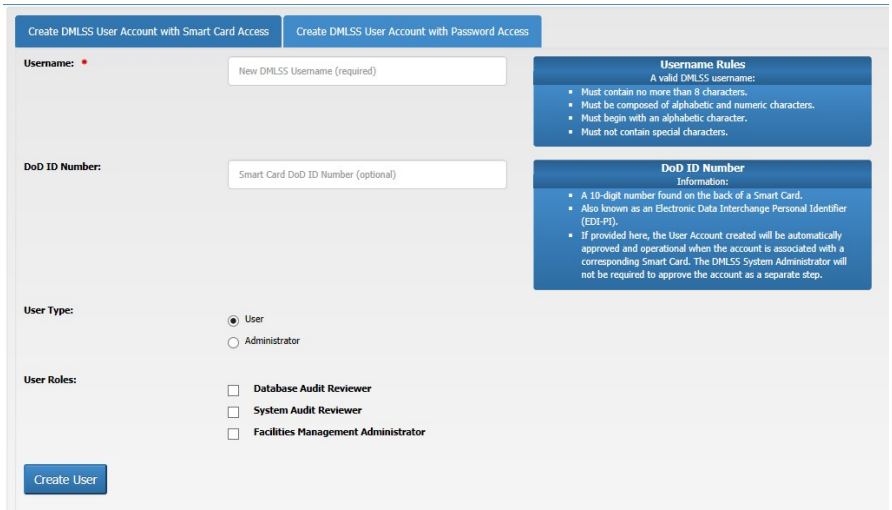


Figure 6. Create Defense Medical Logistics Standard Support User Account page

5. After the SA has created the user account, he/she notifies the user(s), so they may associate their CAC information. The new user accesses the DMLSS Start Page and selects the Associate Smart Card tab in the horizontal menu. The Associate DMLSS user with Smart Card screen appears (Figure 7), and the user enters their Username and selects Submit. After the results message Success, please close this window appears. Select the X in the upper-right corner to close the window.

6. If the DoD ID Number was not provided in the new user set-up, the SA must return to the Manage Users menu and select Manage Smart Card Access. From this screen, the SA performs a search for the new user. Using the Manage Smart Card Access screen, the SA selects the user(s) and then selects the Approve selected users link from the list of update actions. The Manage Smart Card Access screen then displays the user's status as Approved. The DMLSS SA can exit the System Administration Tool. Note: Only users with a status of Pending may be approved. If the status reads Enabled, not approved, the new user has not properly associated their Smart Card.

Figure 7. Associate Defense Medical Logistics Standard Support user with Smart Card Screen

(b) Create DMLSS User Account with Password Access located in the second tab as shown in Figure 6. Granting password access for a user first requires the password master switch be turned on for the site by DHA MEDLOG, see paragraph 2.c.(3), "Manage User Password Switch" of this Enclosure. If a new, non-Smart Card, user account is approved, perform the following steps:

1. Enter the username for the new user.

2. Enter the user's initial password, twice. The initial password must meet certain requirements that are listed on this tab.

3. Select the correct user type: User or Administrator, and then add any of the three user roles that apply, for example, DB Audit Reviewer, System Audit Reviewer, or Facilities Management Administrator.

4. Select Create user. A message appears indicating if the user was added. Note: New users must change their temporary password at the next login.

(2) Manage DMLSS User Accounts. This option allows the administrator to perform a variety of management functions, such as managing Smart Card Access, updating roles, setting temporary passwords, locking and unlocking users, promoting, demoting or deleting users, and reactivating or expiring user accounts.

(a) In order to display users, enter a value in the Search Criteria entry field, see Figure 8, select the type of user to display, such as All Users, Active Users, Locked Users, or Audit Reviewers, and select Search. In addition, the search criteria portion allows users to search by the following additional fields: User Type, LOG (logistics) User or SA, Status, Last Login Date, Roles, Account Type, Smart Card or Password Access, and Smart Card Status. The search results are provided together with columns of status that assist SAs with the management,

security, and integrity of DMLSS. A Print selection is also available to launch a Portable Document Format (PDF) version of the list which can be viewed and printed.

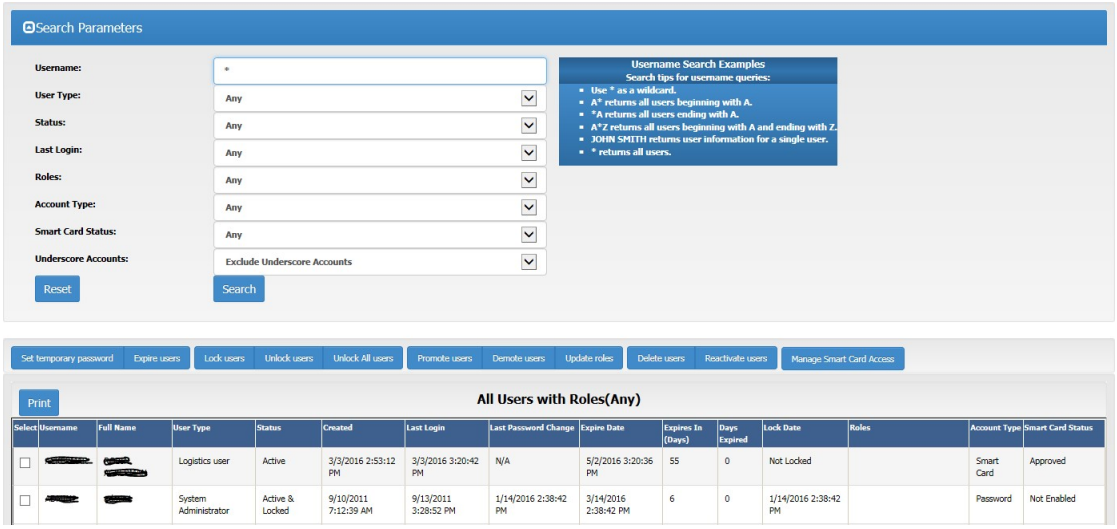


Figure 8. User Search Criteria Screen

(b) Once the list of users is displayed all of the user actions ('lock', 'unlock', etc.) can be initiated from that list.

1. Set temporary password. Use this function to set a temporary password for one or more selected usernames. This process forces a password change the next time the user logs into DMLSS.

2. Delete users. This option allows the SA to delete selected user accounts, for example, when a user is transferred to another assignment or location. The SA must remove all roles and applications in the application prior to deleting the user on the server or else the system ghosts those users on the application side. DB access permissions are revoked when a user account is deleted, and users cannot log onto the server. If necessary, users can be re-created. To delete a user account, select Manage DMLSS User Accounts and then display the user(s). Select the users and select Delete Users. Select Yes on the prompt. Are you sure you want to delete the following users? A confirmation message displays indicating the user was deleted. A user account can also be deleted through the Manage User Accounts in DMLSS window. SAs cannot delete their own account; another SA-level user must perform this action.

3. Lock users. This function allows the SA to lock selected users. The user receives the message, "Your account is locked." Locked users cannot log onto the DMLSS system. To regain access, they must have the SA unlock their username. SAs can perform a search to identify all Locked Users. As a result, username status and lock date fields appear on the search results screen.

4. Unlock users. Use this function to unlock selected users.

5. Promote users. This option allows an existing user to be promoted to SA status. If a user has been a LOG user but is moving to a position with SA responsibilities, use this function instead of creating a separate account.

6. Demote users. This function allows an SA to demote an existing SA to LOG user level status. If a user has been a DMLSS SA but is moving to a position with no SA responsibilities, use this function rather than creating a separate account. SAs may not demote themselves to a typical-user level; another SA-level user must perform the action.

7. Reactivate users. Use this option to reactivate selected inactive DMLSS users. An inactive user account is one in which the user's password is expired. Note: System users are required to log into the system at least once every 30 days and change their password every 60 days.

8. Expire users. Use this option to expire passwords of selected users. An inactive user account is one in which the user's password has expired. This list also reflects the number of days since expiration. An SA uses this list to determine which accounts require reactivation and which accounts should be deleted.

9. Update roles. Use this option to update auditor roles for the selected users. The available roles for DMLSS users are DB Audit Reviewer, System Audit Reviewer, and Facilities Management Administrator. Select the appropriate box on the Manage DMLSS User Accounts/Update roles screen and select the Update Roles.

(3) Manage Password Access Switch, viewable only by underscore accounts. This master switch allows underscore accounts to turn on/off a site's ability to create User ID/password accounts.

(a) Password Access Switch is Enabled. The DMLSS SA can create username/password accounts at their own discretion.

(b) Password Access Switch is Disabled. The DMLSS SA cannot create username/password accounts and cannot unlock or reset the password on existing username/password accounts.

(c) Password Access Switch is turned from Enabled to Disabled. All existing username/password accounts are locked immediately. Additionally, DMLSS requires the SA to enter a justification when the switch is changed from Disabled to Enabled.

(4) List Connected Users. To view the List Connected Users, select this option in the Manage User menu. SAs can view or print the Connected Users ID along with Program, Server, Start Time and Duration information.

(5) Manage Dormant Users. To view the Manage Dormant Users, select the Manage Dormant Users link in the Manage User menu. The results screen offers the opportunity to delete selected dormant users.

(6) Manage Dormant User Period. This option allows the SA to define the number of days a user account remains inactive before it is displayed on the Manage Dormant Users page. Type the new dormant days setting and select the Save Days Dormant Settings. The default is set at 180 days.

(7) Disconnect Users. Select the Disconnect all Users bar to disconnect all users that are currently using the DMLSS Client application.

(8) Manage Smart Card Access. This screen together with the Create DMLSS User Account with Smart Card Access option provides a full range of management options for controlling the Smart Card process. This window is used to approve/reject selected users, reset, enable/disable Smart Card usage, and edit the DoD ID number (Figure 9).

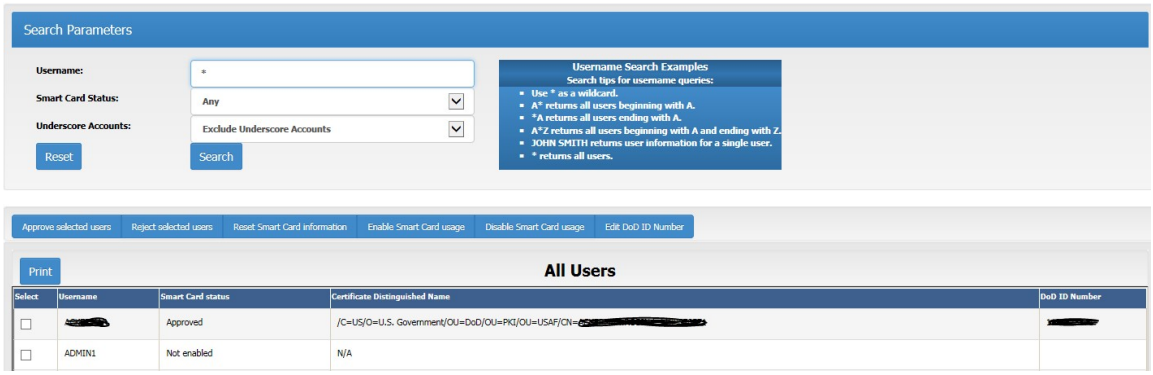


Figure 9. Manage Common Access Card Access Results Screen

(a) Smart Card-enabling an existing User. To Smart Card-enable an existing user, the SA first performs a search in the Search Parameters portion of the page (see paragraph 2.c.(1)(a), "Create DMLSS User Account with Smart Card Access" of this Enclosure). Using the results, the SA marks the checkbox of the selected user(s) and selects Enable Smart Card usage located above the search results. Two confirmation screens follow—select the Yes or No on the first screen, then OK on the next screen.

1. Once the DMLSS SA completes this step, the SA notifies the new user. The user will then open the browser with the CAC in the reader and access the DMLSS Start Page. The user then selects the Associate Smart Card tab in the horizontal menu. The Associate DMLSS user with Smart Card screen appears, Figure 7, and the user enters Username and selects Submit. After the results message, "Success: Please close this window appears," select the X in the upper-right corner to close the window.

2. After the user completes the Associate Smart Card procedures, the SA accesses the Manage Smart Card access task area, selects the user(s) and selects the Approve selected users link. The Smart Card status must be Pending to be approved. Two confirmation screens follow—select Yes or No on the first screen, then OK on the next screen. After this action, the Manage Smart Card Access screen displays with a status as Approved.

(b) Reject selected users. The DMLSS SA rejects Smart Card-username pairings if they are invalid. If the recorded CAC certificate's DN is not a match for the user, the SA will reject it. It might also be necessary to reject the request if the SA cannot validate the user as someone that should have access via Smart Card. Only users with status 'Pending' may be rejected. On the Users screen, select the user(s) and select the Reject selected users' option. Two confirmation screens follow—select Yes or No on the first screen, then OK on the next. After this action, the Manage Smart Card Access screen displays with a status of Rejected.

(c) Reset Smart Card information. The DMLSS SA uses this option to reset the certificate DN information associated with an account. On the All Users screen, select the user(s) and then select Reset Smart Card information. Two confirmation screens follow—select Yes or No on the first screen, then OK on the next. After this action, the Manage Smart Card Access screen displays with a status Enabled, not approved. From this point, re-enter the DoD ID Number, last tab on Manage CAC Access Results Screen, paragraph 2.c.(8) of this Enclosure, and then the user can complete the Associate Smart Card procedure.

(d) Disable Smart Card usage. Use this function to disable selected users. On the Users screen, select the user and then select Disable Smart Card usage option. Two confirmation screens follow—select Yes or No on the first screen, then OK on the next. After this action, the Manage Smart Card Access screen displays with a status of Not enabled.

(e) Edit DoD ID Number. The DoD ID Number may only be edited if the Smart Card status is Enabled, Not Approved. If the DoD ID Number associated with the User Account needs to be changed, select the username and select Reset Smart Card Information. This resets the account Smart Card status, Certificate DN, and DoD ID Number. Once the account is reset, then edit the DoD ID Number. The user owning this account may then return to the DMLSS Start Page and select Associate Smart Card to associate the account with a Smart Card.

(9) Manage Deleted Users. With the Manage Deleted Users capability, DMLSS SAs can now query and view details for deleted users and reactivate a deleted user. Previously, a DMLSS SA had to know the exact username of a deleted user in order to reactivate it.

(10) User Account Dashboard. The System Administration Tool User Account Dashboard (Figure 10), summarizes the status of all user accounts. It provides the SA the means to quickly identify users requiring corrective action as well as a host of other management status and metrics. For example:

(a) Account Status by type of account.

(b) Number of DMLSS User Accounts in each Smart Card Status.

(c) Number of User Accounts (DMLSS and SA) with the three System Administration Tool roles (FM Administrator, Audit Reviewer, and DB Audit Reviewer).

(d) Count of Existing and Deleted User Accounts.

(e) Number of DMLSS SA Accounts in each login date range: today, 1-7 days, 8-30 days, 31-60 days, > 60 days, or has not logged on.

(f) SAs can select any number within any table to perform a search that specifically identifies the users in a selected category.

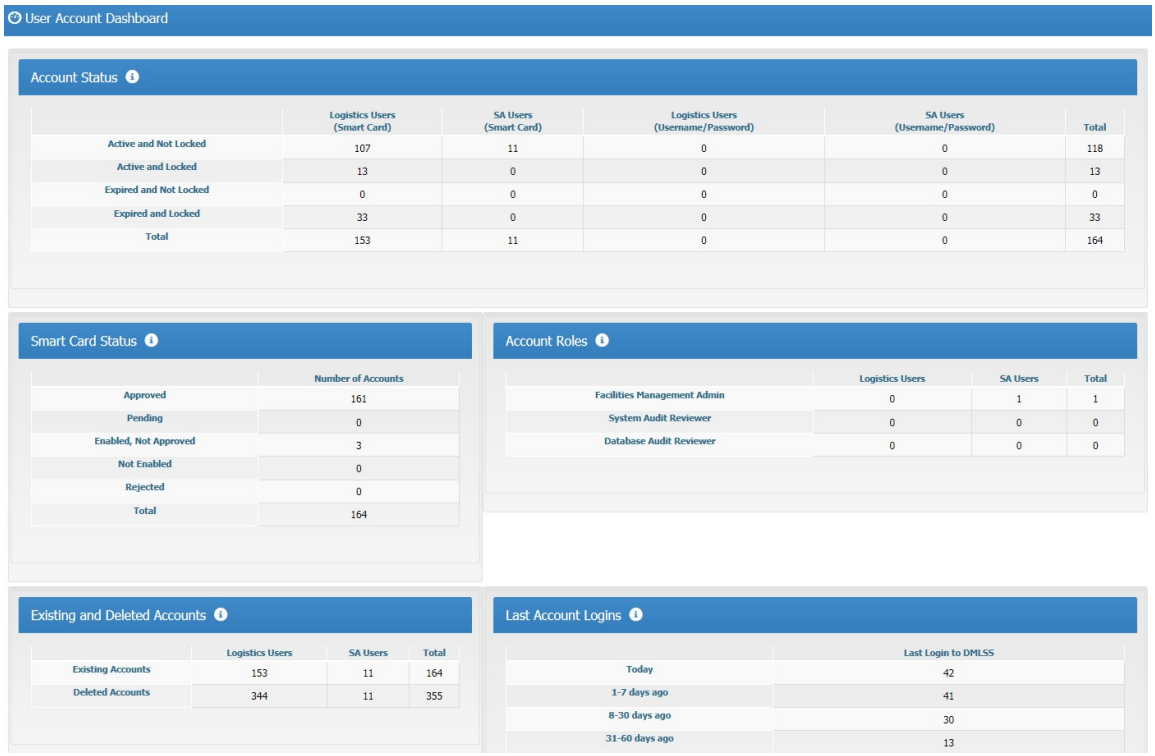


Figure 10. System Administration Tool User Account Dashboard

d. Manage Security. Using the Manage Security Menu (Figure 11), SAs view and manage the security settings for the DMLSS server, manage access to the server, and audit files. To access this window, select the Manage Security link under the list of Task Areas in the System Administration Tool.

Figure 11. Manage Security Menu

(1) View Windows Hotfixes. To view notes pertaining to DMLSS software HotFix, select Manage Security and then View Windows Hotfixes. A frame appears in the browser with a description of the current hotfixes and their identification. Select Print and a PDF file appears in the browser to view or print.

(2) Site Idle Timeout. Due to cyber security requirements, the timeout option is set to 15 minutes and is no longer editable.

(3) View Open Ports. To view a list of open ports on the DMLSS server, select Manage Security and then View Open Ports. A frame appears in the browser with open ports identifying their protocol, local address, foreign address, and state. Select Print and a PDF file appears in the browser, listing the open port information on the server.

(4) View Security Login Denials. To view a list of failed secure login attempts, select Manage Security and then View Security Login Denials. A note appears with the message, NOTE: This report may take several minutes to generate. To generate the report, select Generate Report. A frame appears in the browser with login denial information including user, date/time, source, category, event type, and message. Select Print and a PDF file appears in the browser to view or print.

(5) View Audit Reviewer Log. To view the Audit Reviewers Logs, select Manage Security and then View Audit Reviewers Log. Enter the start date and end date, format is YYYYMMMDD, for example, 2018JAN15, and select Refresh. If there are any logs for the period selected, a frame appears with the information from the logs. Select Print and a PDF file appears in the browser to view or print.

(6) List Audit Reviewers. Audit reviewers are individuals who have been authorized to view the Windows event logs. To access the list of audit reviewers, select Manage Security and

then List Audit Reviewers. A frame appears in the browser with the list of audit reviewers and associated information. Select Print and a PDF file appears in the browser to view or print.

(7) View Web Server Logs. To view the DMLSS web server logs, select Manage Security and then View Web Server Logs. A frame appears with a dropdown text box for selecting the appropriate log. Some of these logs may be very large and could take a minute or longer to display. Select Print and a PDF file appears in the browser with the logs.

(8) Manage Smart Card/Certificate Revocation List (CRL). To enable or disable the Smart Card or CRL functionality, use the Manage Smart Card/CRL link located in the Manage Security menu. If either option is currently enabled, Disable displays. Likewise, if currently disabled, the Enable selection displays. Note: Selecting Disable Smart Card causes the Smart Card/CRL to be disabled, as well. The CR state is changed to Disabled and the Enable/Disable CRL is disabled, as well. If one or both options are disabled, enter a reason in the Reason for the change field.

(9) Manage Status Refresh Rate. To change the refresh interval on the main page or disable it, select Manage Security and then Manage Status Refresh Rate. A valid range is a number of minutes from "2" to "30" or enter "0" to disable the feature.

(10) Manage Apache X.509 Access. Apache X.509 is a critical component of user authentication-related security requirements. This screen contains two tabs—File Transfer and Apache X.509 Access. To enable Apache X.509 access, select the Select checkbox for the DN and select Grant Access. To disable access, select the Select checkbox for the DN and select the Delete.

(a) Changes to this configuration are audited in order to provide visibility of changes meeting cyber security and auditing requirements. Therefore, when the X.509 configuration is modified, the user's activities are logged to the audit table.

(b) The JMLFDC deploys the DMLSS server in a compliant manner. Communication with trading partners should be supported in the deployed configuration. By adjusting these settings, the administrator and the administrator's accrediting agency accept the introduction of one or more Category I findings.

(11) Manage Keep-Alive Timeout. This feature allows the administrator to change an Apache setting for more efficient wireless handheld usage. To enable, select Enable Keep-Alive Timeout. To disable, select Disable Keep-Alive Timeout. Warning: The JMLFDC deploys the DMLSS server in a compliant manner. By adjusting this setting, the administrator and the administrator's accrediting agency accept the introduction of one or more findings.

(12) Manage Point of Care System Interface Access. When used, the Point of Care-Inventory Management System interface significantly improves efficiencies and virtually eliminates errors introduced by manual entry of data in both the DMLSS and the Point of Care-Inventory Management System such as a pharmacy line of business application. Customers no

longer are required to perform dual data entry for cataloging, checking status, receiving goods or reconciling data.

(13) Manage Hypertext Transfer Protocol (HTTP) Endpoints. At this time, the Point of Care System is the only HTTP Endpoint that can be configured for the DMLSS Server. In future releases, additional endpoints may be added. This screen allows the DMLSS SA to manage all HTTP Endpoints which are basically Web Services that other systems would use to interact with the system.

e. Manage User Messages. Using the Manage Users Messages Menu (Figure 12), SAs can send messages to the DMLSS users, review or delete previously transmitted messages, and specify IP addresses that should not receive messages. To access this window, select the User Messages link under the list of Task Areas.

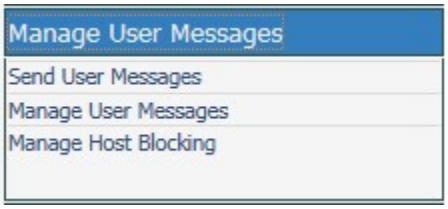


Figure 12. Manage Users Messages Menu

(1) Send User Messages. This function is used to send a message to all DMLSS users, even if they are not currently logged on to the system. This is particularly useful if, for example, maintenance needs to be performed on the server. The message reaches the users who are currently logged on, allowing them to log off before losing any data. The message also reaches the users who are not currently logged on, warning them not to log on until the maintenance is complete. To access this option, select the Send User Messages link located in the Manage User Messages menu. In the Create/Send a Message to Users window (Figure 13), enter the message to be sent. Do not press Enter to add line returns between parts of the message. Text entered after a line return does not appear in the message. Enter an expiration date and time for the message. Select Create Message, and OK in response to the confirmation message. The message appears from when any user attempts to logon until the specified date and time.

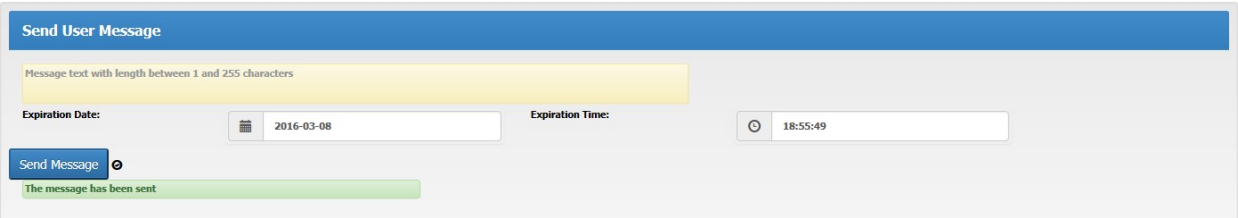


Figure 13. Send User Message

(2) Manage User Messages. Use this option to view or delete user messages.

(a) View Unexpired Messages. In the Manage User Messages window (Figure 14) select Expired Type: Unexpired. Using the results of the search, SAs can view or print the list.

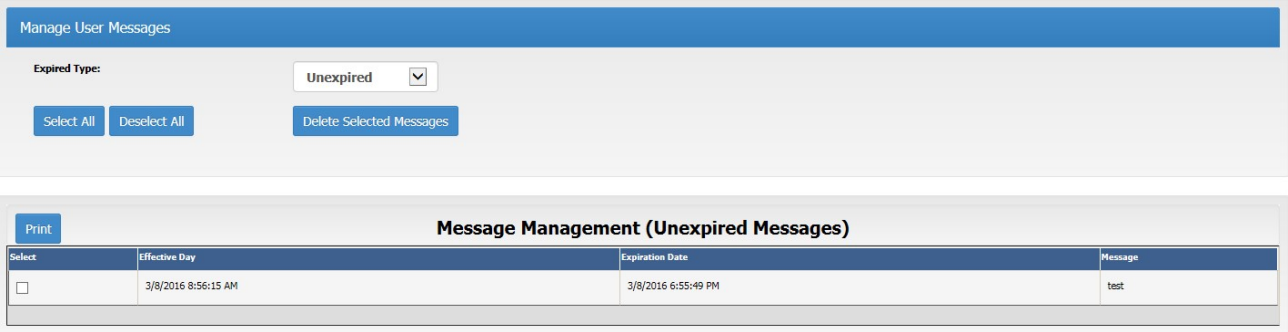


Figure 14. Manage Users Messages, Deleting Messages

(b) Delete User Messages. To delete a message, use the dropdown list to narrow the scope of the search between Unexpired or Expired messages. Then use the results of that search to select the desired message(s) to delete. Select the Delete Selected Messages bar. A system message indicates if the messages were deleted.

(3) Manage Host Blocking. SAs use this option to identify particular IP addresses that should not receive messages or unblock previously blocked users, so they can view messages again. To access this feature, select Manage Host Blocking from the Manage User Messages task menu. Use the Blocked Type dropdown window to narrow the scope of the search and use the results of the search to identify the particular IP address to block or unblock. Depending on the action desired, select either the Block Selected Host or UnBlock Selected Host bar. A system message indicates whether the action was successful.

f. Manage Server. SAs can manage multiple server functions using the Manage Server Menu in the System Administration Tool (see Figure 15).

(1) View DMLSS Server Processes. This screen produces a list of current processes running on the DMLSS server with their corresponding file sizes. The report grid can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. SAs can view or print the list in PDF.

(2) View Configuration Status. This screen displays the DMLSS server hostname, IP address, media access control address and available DBs. SAs can view or print the data in PDF.

Figure 15. Manage Server Menu

(3) View File System Status. This screen displays a brief summary of the DMLSS Server file system status by drive with corresponding status and any error messages. Check the disk space every few days to verify no more than 90 percent of the space is being used. The report grid can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. The size, free space, and percent free column cells are shaded green, yellow, or red based on percentage of free space available for the file. SAs can view or print the data in PDF. If space usage exceeds 90 percent contact the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil for further instructions.

(4) View OS Services and Devices. This screen displays a list of operating SS and devices running on the server. Use the dropdown list at the bottom of the page to select between Services, Devices, or Services and Devices. The report grid shows display name, service name, service type, and status. The results can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. SAs can view or print the data in PDF.

(5) View Server Event Log. This screen shows a list of the current event log entries on the DMLSS server. Using the Select Log dropdown list at the top of the page, the SA can select the desired log: application, Internet Explorer, Operations Manager, Security, or Systems.

(a) The SA can also designate level security and/or time/date criteria prior to the search.

(b) The report grid can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. SAs can view or print the data in a PDF.

(6) View DMLSS DB Log. SAs use this page to view entries in the system's DB log. Using the Select category dropdown list at the top of the page, SAs select the desired log with a start date and end date. The report grid can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. SAs can view or print the data in a PDF.

(7) View Running Scheduler Jobs. SAs use this page to view jobs currently being run by the scheduler. The report grid can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. SAs can view or print the data in a PDF.

(8) DMLSS Server Hardware. SAs use this page to view the DMLSS server hardware report and manage hardware resources.

(a) Server Reboot and Shutdown. Selections for Shutdown DB Server, Reboot DB Server, and Cancel Shutdown or Reboot reside under the DB Server Hardware heading. Note: The server should only be shut down when directed to do so by DAD-IO/Health Information Technology.

(b) Compact Disk (CD) Drive. Open CD Drive and Close CD Drive are located under the DB Server Drives heading.

(c) Select the Print DB Server Settings bar to produce a PDF version of the DMLSS DB Server Hardware Report.

(9) Manage Common Log Levels. This page is used to manage the DMLSS Common Log Levels. On this screen the SA can change the level at which the system writes logs using the Combo box drop-down. Normally the default values are OK. If a problem exists where more details are needed, then the minimum log levels can be set to a lower level, meaning the logs provide more detail. Example: If the minimum log level is set at Debug, the system logs all levels (Debug, Information, Warning, Error, and Critical). If the user sets the minimum log level at Critical, then the logs are only written for critical items. If the level is set at Do Not Log, no items are written to the logs.

(10) View Data Patches. This link allows the administrator to view the data patches that have been applied to their server. With this capability, a DMLSS SA can make a more informed determination as to whether or not a problem they may be experiencing is related to a data patch deployment. This page displays data patches for the last 36 months.

g. Manage System Interfaces. This menu manages a new interface with the Electronic Healthcare Record (EHR) system and supports synchronization and the ordering of products using the DMLSS system as the host system. This interface must be a two-way channel. Manage EHR Interface Access places EDI formatted orders to the DMLSS and communicates status of orders with the EHR system (see Figure 16).

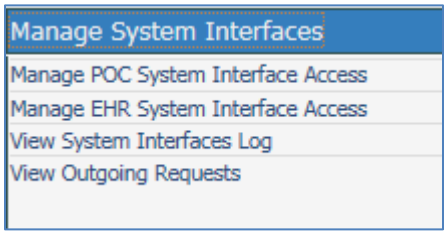


Figure 16. Manage System Interfaces Menu

(1) Manage Point of Contact (POC) System Interface Access.

(2) Manage EHR System Interface Access.

(3) View System Interfaces Log.

(4) View Outgoing Requests.

h. Manage Devices. Using the Manage Devices menu (Figure 17), SAs can create and manage system barcode printers, Radio Frequency (RF) configuration, and view RF logs. To access this window, select the Manage Devices link under the list of Task Areas.

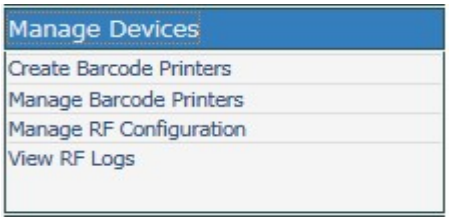


Figure 17. Manage Devices Menu

(1) Create Barcode Printers. To create or add a barcode printer, select Create Barcode Printers in the Manage Device task menu. Enter the printer name, for example, "bc pharm" and IP address for the printer. Select the label type, narrow or wide, and connection type, network or mobile. Select Create Barcode Printer and a message displays indicating if the printer was added. Create/add the local printer on the desired DMLSS client workstations.

(2) Manage Barcode Printers. From this page, the SA has four options: change barcode printer label type, test printer connectivity, delete selected printers, or change barcode connection type.

(a) Changing the Label Type for a Barcode Printer. To change the label type for a barcode printer (from narrow labels to wide labels, or vice versa), select the printer to be updated and select change barcode printer type. Inside the update window, choose the new label type and select Change barcode printer label type. A message appears if the printer was updated successfully.

(b) Test Barcode Printer Connectivity. Select the checkbox of the printer to be tested and select Test printer connectivity. A message appears stating that the barcode printer was either tested successfully or an error has occurred. Select OK to return to main screen.

(c) Removing a Barcode Printer. To remove a barcode printer, select the checkbox of the printer to be updated and then select Delete selected printers. The system displays a message indicating whether the printer was removed successfully.

(d) Change Barcode Printer Connection Type. Select the appropriate connection type, mobile or network. A mobile connection is usually a handheld barcode printer that operates via Universal Serial Bus or Bluetooth.

(3) Manage RF Configuration. To edit the RF Link configuration (which is usually not necessary), select Manage RF Link Configuration in the Manage Devices window and enter a new value for any parameter listed. Select Update configuration to save the changes. RF Link must be stopped before the configuration can be edited and saved. Use extreme caution when editing the RF Link configuration, because if it is edited incorrectly, it could cause the RF connection to malfunction. Note: The Web Server service located in Manage Services has to be restarted in order to have the changes take effect. This is used to support real-time location systems.

(4) View RF Logs. To view the RF Link log, select View RF Logs, select the log to view, and select Refresh. The log entries display in the window. Select Print to display the entries in a PDF.

i. Manage Services. The Manage Services window in the System Administration tool is used to manage the communication information for the DCM (Figure 18), which is found in the DMLSS Application. Privileged users can monitor DCM transactions in the SS application, and re-submit them, if necessary. To access this window, select Manage Services under the list of Task Areas.

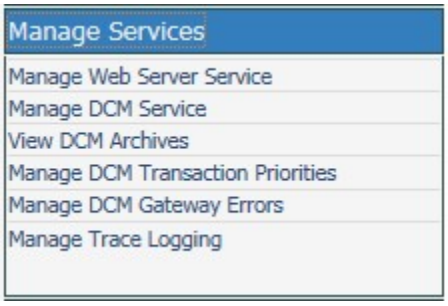


Figure 18. Manage Services Menu

(1) Manage Web Server Service. This link is used to manage the Apache and extender session protocol services on the web server. Upon selecting this link, the Manage Event Services window appears with the status of the web server status and a selection to restart the system's Web Server service.

(2) Manage DCM Service. Administrators use this window to set the number of retries that the DCM makes when attempting to send a transmission. Settings are available for both HTTP Secure and file transfer protocol retries. Also, an enable/disable for the DCM service is located on this page to engage or suspend service. The DCM settings can be displayed in a PDF by selecting Print DCM Settings.

(3) View DCM Archives. Using this link, administrators access the report grid to select desired serial(s). Results from the report grid can be resorted by selecting the desired column name and choosing the up arrow for ascending or the down arrow for descending. Select Show archive details bar and entries for that serial number are displayed below the report. Administrators can view or print the data in a PDF by selecting Print.

(4) Manage DCM GW Errors. This function supports compliance with federal Financial Management Improvement Act by ensuring data integrity of transactions from other systems into the DCM. DCM users authorized to view and dismiss inbound DCM and GW errors require the Communications Management Update role/privilege. The Manage DCM GW Errors window displays the record of any INBOUND file(s) that fail at the GW for any reason. When a file is displayed, the DMLSS SA must investigate and validate the error. The SA should take appropriate actions to correct the problem. Transactions errors must be maintained and tracked until corrected, posted, or deleted by an authorized user to enable performance measurement.

(5) Manage Trace Logging. This is a tool used by JMLFDC staff to capture keystrokes by users for troubleshooting purposes. The SA is not able to enable or disable this capability.

j. Manage DB Menu. Using the Manage DB Menu (Figure 19), SAs can manage the DMLSS DB and view DB usage statistics. To access this window, select Manage Database under the list of Task Areas.

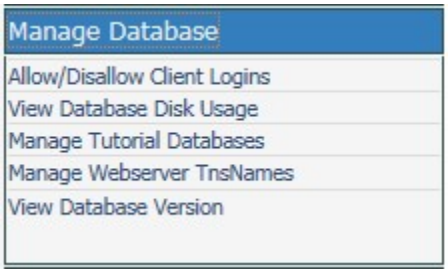


Figure 19. Manage Database Menu

(1) Allow/Disallow Client Logins. The first option in the Manage DB menu is used by the SA to either allow or disallow client logins. If access is currently allowed, Disallow selection displays. Likewise, if access is currently disallowed, the Allowed selection displays. The system prompts if the login was allowed or disallowed.

(2) Viewing DB Disk Usage. Use this window to view the DB disk usage and status. Results from the report grid can be resorted by selecting the desired column name and choosing

the up arrow for ascending or the down arrow for descending. Select Print and a PDF file appears in the browser with a summary of the DB disk usage.

(3) Manage Tutorial DBs. Tutorial DBs are copies of the account's production DB that may be used for practicing or testing of procedures without affecting actual operational data and balances. Orders are not placed in a tutorial DB as the IP addresses of the base associated trading partners have been removed. After a tutorial DB is created, the DB is available to every user for all system applications. Users have the option of logging into the tutorial DB when they first launch the application.

(a) Select the tutorial DB to manage and then select one of the following:

1. Create Tutorial DB—creates the selected DB.

2. Refresh Tutorial DB—deletes the selected DB and recreates it.

3. Drop Tutorial DB—deletes the selected DB.

4. Refresh DB Statuses—refreshes the DB status displayed above.

5. Start Tutorial DB—starts the selected DB.

6. Stop Tutorial DB—stops the selected DB.

7. Test Tutorial DB—attempts to connect to the selected DB and reports the result of the attempt.

8. View Tutorial DB History—displays a page that shows the history of the tutorial DB when it was created and deleted.

(b) Tutorial DBs are not retained when the DMLSS system is upgraded at the site. After each new version/DMLSS build, the tutorial DB must be recreated.

(c) After selecting Manage Tutorial DBs in the Manage DB menu, a frame appears with the available tutorial DBs and their status (Figure 20). Select the appropriate tutorial DB and then choose one of the actions located at the bottom of the frame. The Demo Account Prefix is the prefix that starts all user accounts in the tutorial DB. The Demo Account Number should reflect the number of user accounts to create in the tutorial DB.

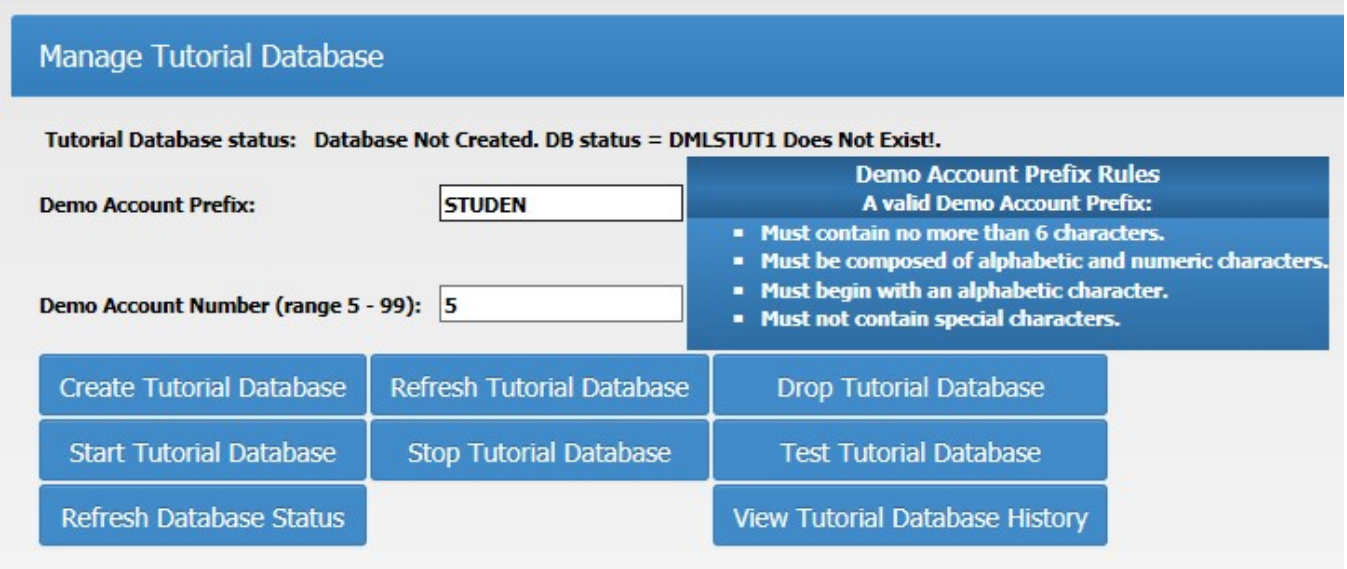


Figure 20. Manage Tutorial Database

(d) This screen is used to configure and manage the Tutorial DB. Once configured, users are then able to access the Tutorial DB. When logging on, users have the option to select the Tutorial checkbox or Production DB. Upon login, Tutorial DB is displayed in the title bar of every window. Also, the Tutorial DB name and highlighted Tutorial DB notice are displayed in the bottom bar (lower right). In order to reconnect to a production DB, users need to exit the system, uncheck the Tutorial checkbox, and log in to DMLSS again.

(4) Manage Webserver TnsNames. TnsNames is the name of an Oracle file that defines DB addresses. SID is the name of the DB. To manage the TnsNames or a file, go to this link in the Manage DB file. A frame appears in the browser with the contents of the tnsnames.ora file in a scrollable text window. The frame also contains a list of editable entries from the file. A menu across the top of the frame enables the user to remove one or more entries, add a new entry, or test one or more entries.

(5) View DB Version. This window shows the current version and patch level of the DMLSS DB.

k. Manage Medical Materiel Menu. From the Manage Medical Materiel Menu (Figure 21), the user can manage the settings for the DMLSS EOP process, import PV orders or export PV requisition status, and manage the settings of for the Universal Data Repository (UDR) process. To access this window, select Manage Medical Materiel under the list of Task Areas.

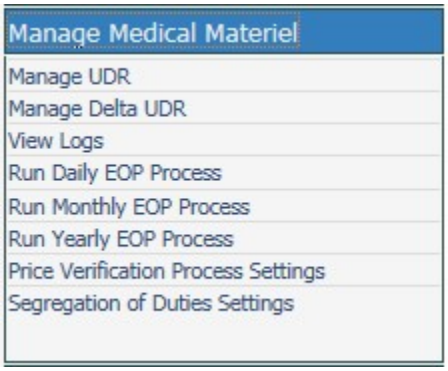


Figure 21. Manage Medical Materiel Window

(1) Manage UDR. The UDR Medical Catalog is a DMLSS sponsored catalog product that consolidates medical and pharmaceutical information from a variety of federal government sources as well as commercial/industry sources. The first option in the Manage Medical Materiel menu is the Manage UDR window, Figure 22. It allows the SA to view load status, perform a pre-process validation, and start a manual UDR load.

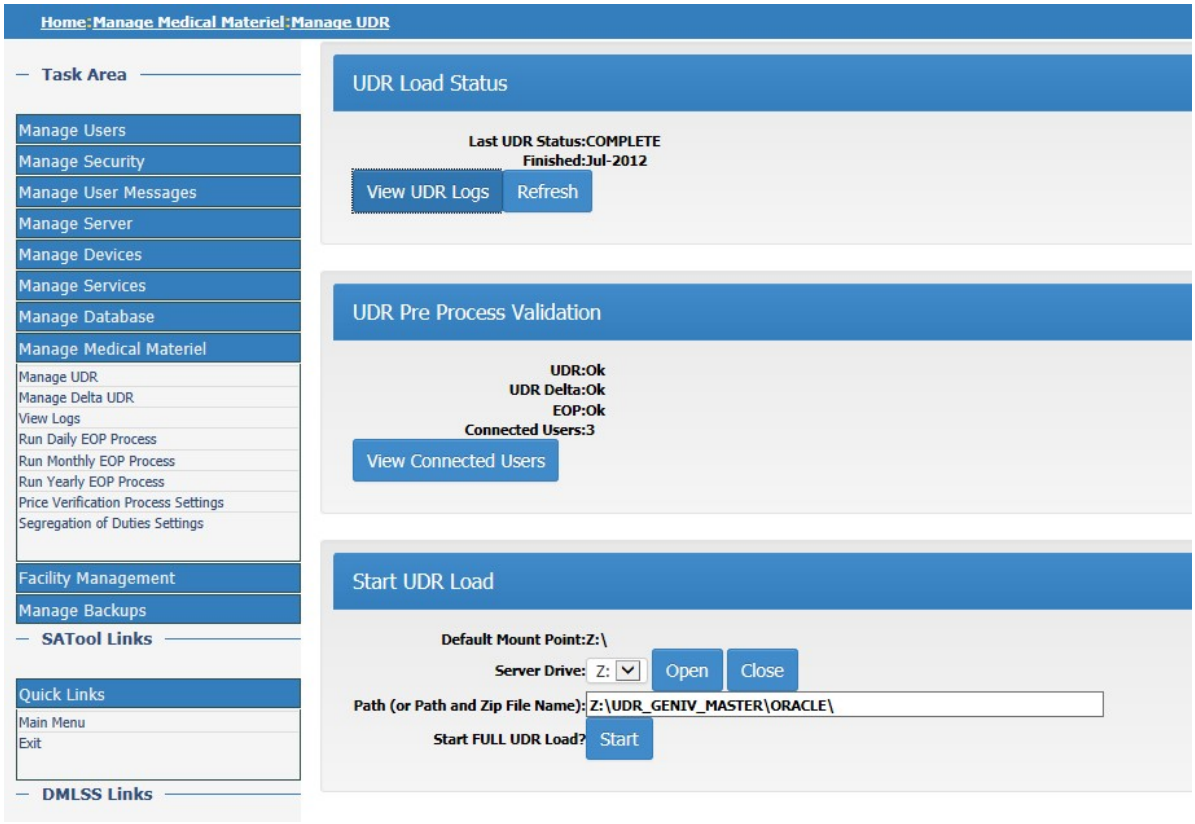


Figure 22. Manage Universal Data Repository Window

(a) UDR Load Status. Select View UDR Logs in the Manage UDR screen to view the logs for the UDR processes.

(b) UDR Pre-Process Validation. Although users are not kicked out of the system during this process, SA may select View Connected Users to view the connected users. This screen also contains an available message to send to users by selecting Send Logout Message located directly below the message. Refresh and Back selections are also available at the bottom of the page.

(c) Start UDR Load. In general, the UDR Delta Process automatically updates catalog records. However, in the event that the UDR Delta Process cannot be used, contact the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil to request that either a DMLSS Extract CD-Read Only Memory be sent by overnight mail, or that the latest UDR table extract be laid on the DMLSS server. If the table extract file is applied, instructions for processing are furnished by the DHA GSC.

(2) Manage Delta UDR (Figure 23). The UDR Delta Process is a web-based process that uploads catalog updates to the DMLSS production servers. In this screen, status is provided to see when the last UDR Delta Run processed with additional options to View UDR delta logs, set the automatic indicator, enable/disable the delta process, view detailed properties, and Start Full UDR Load.

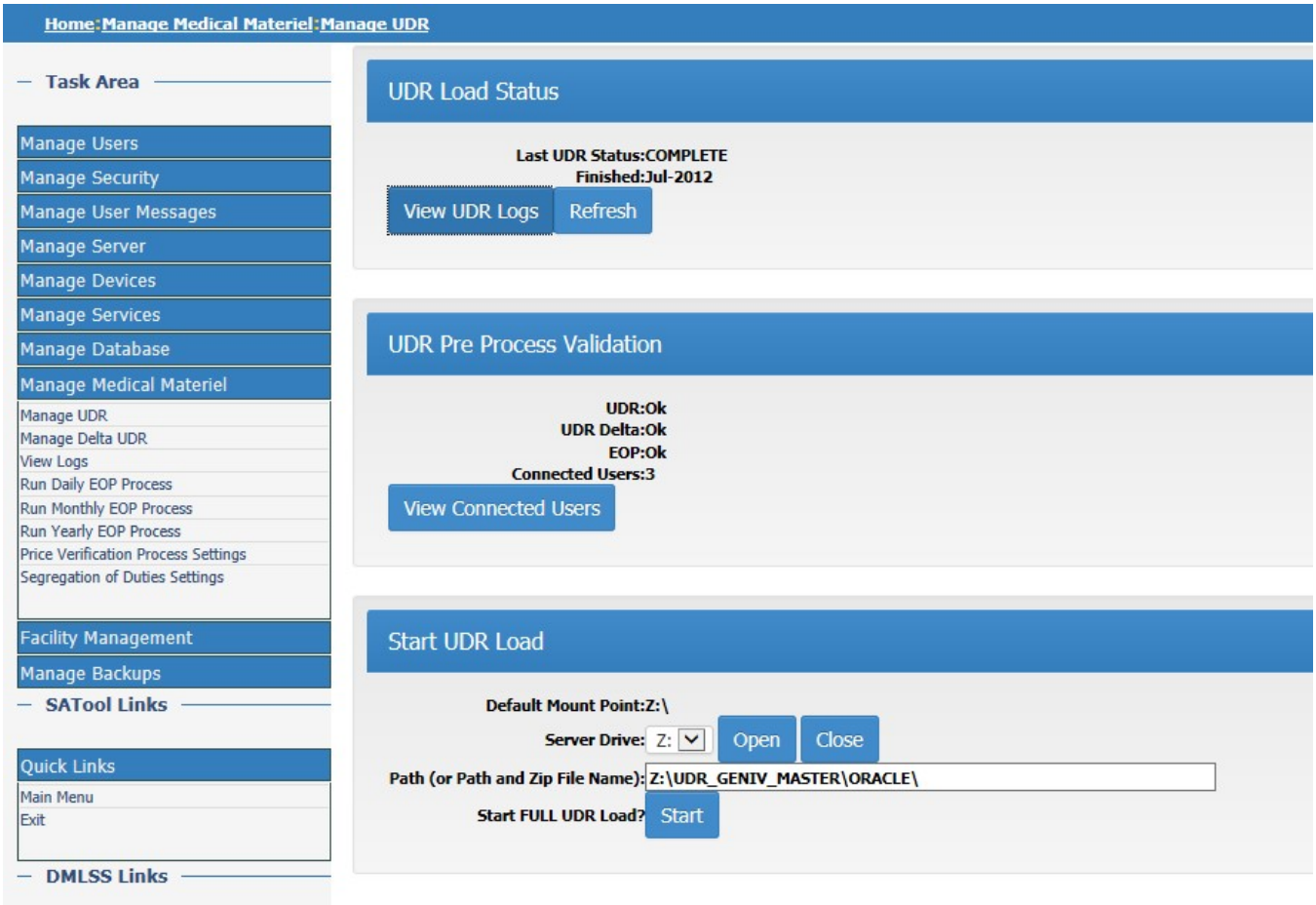


Figure 23. Manage Universal Data Repository Window

(a) In general, the UDR Delta Process should always be set to "Automatic" and "Enabled". After making these settings, the UDR Delta posts daily as updates are received from Defense Logistics Agency (DLA).

(b) New parameters allow the user to view the number of times the Delta process attempts to check for updates per run and to change the value, Connection Attempts. Also, the user can view/change the number of minutes that the process waits for a response from the underlying Web Service it calls before timing out, Connection Timeout.

(c) If the process is set to run manually, run it from the Manage Delta UDR window by selecting Start under the Start UDR Load heading. A system message indicates if the process started.

(3) View Logs. Use this link to view or print logs for the EOP process. This window shows a summary for each of the next scheduled EOP processes. It also provides status for the daily, monthly, and yearly runs with View History and View Detail Log. SAs can view or print the detail log data in a PDF. FM has its own EOP processes that run independently of the Medical Materiel processes.

(4) DMLSS EOP Processes. EOP processing automatically provides the necessary reports, activates the required processes, backs up the required records, and purges the information no longer needed in the system.

(a) Normally, these processes run automatically based on a schedule created in SS. In rare cases, SAs may need to start these processes manually from the Daily, Monthly, and Yearly Process windows; however, SAs may only process a manual EOP cycle when first directed to do so by the DHA GSC.

(b) When these processes are running, users are locked out of the system applications. Prior to the start time, user messages are automatically sent to DMLSS users warning that the end-of-day (EOD) process is set to begin in 10 minutes. After those 10 minutes, the process begins, and users are locked out of the DMLSS application suite until the process is complete. The Reset Lock allows the SA to override the lockout process, so that users can still use the system, even though the EOP processes have been started. Contact the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil, and then select Reset Lock to reset the EOP lock.

(c) FM has its own EOP processes that run independently of the general DMLSS EOP processes.

(5) Run Daily EOP Process. EOD processing transmits unsent executed orders, posts incoming status to due-in records, performs follow-up processes, produces the receipt file and transmits to legacy systems, purges aged data, generates management reports, and performs a DB backup. If necessary, use the Run Daily EOP Process window (Figure 24) to initiate a manual EOD Run; however, SAs should only process a manual EOD when first directed to do so by the DHA GSC.

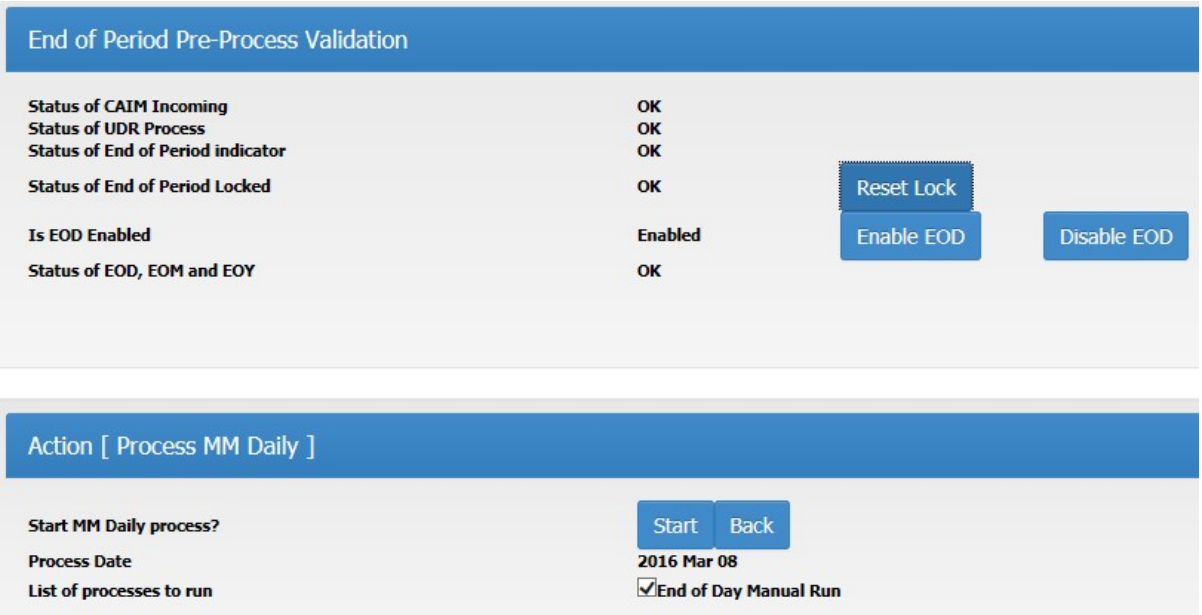


Figure 24. Run Daily End-of-Period Process Window

(6) Run Monthly EOP Process. The end-of-month (EOM) processing includes automatic leveling, purging of aged data, generation of management reports, and a backup of the DB. Normally, this process runs automatically based on a schedule set up in SS. In rare cases there may be a need to start the process manually from the Run Monthly EOP Process window; however, SAs may only process a manual EOM when first directed to do so by the DHA GSC.

(7) Run Yearly EOP Process. The end-of-year (EOY) processing resets financial records, starts new FY financial records, runs a DB backup, generates a report detailing the position of the log fund and all project (PROJ) centers and expense (EXP) centers, cancels any orders that have not been submitted for processing, cancels any Customer Due Out transactions that do not have any associated due-in, and zeroes out targets for Operations and Maintenance funded organizations. If the EOY process fails, contact the DHA GSC at (800) 600-9332 or dhagsc@mail.mil immediately. Under no circumstance should a user manually start the EOY cycle, unless directed to do so by the DHA GSC.

(8) Price Verification Process Settings. Do not change the setting of the Price Verification process unless instructed to do so by DAD-IO or the DHA GSC.

(9) Segregation of Duties Settings. This page allows the administrator to change the Federal Information Systems Controls Audit Manual Segregation of Duties rule for the processing of receipts. The Segregation of Duties function in DMLSS SS remains enabled unless written waiver to this policy is approved by DHA/MEDLOG.

l. FM Menu. The FM menu (Figure 25) allows users to perform FM-specific management functions such as running manual EOP processes, managing the FM tutorial DB, and managing

access to the master area and the transfer area. To access the FM menu, users must be a DMLSS SA or have the FM Administrator role assigned to their username within the System Administration Tool. To access this window, select FM under the list of Task Areas.

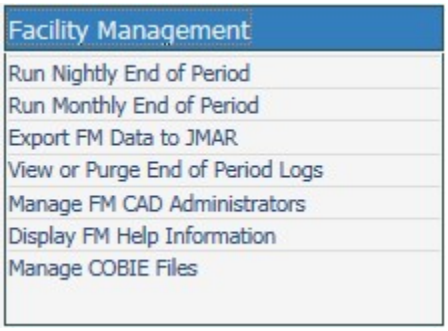


Figure 25. Facility Management Menu Window

(1) Run Nightly EOP. FM EOP processing runs independently of the Medical Materiel EOP processing. FM EOD processing is also called the Nightly process. It normally runs automatically at 00:01 AM every day, 365 days per year. If the FM Nightly fails due to a power outage, server problem, etc., it can be run manually using this menu option. Select Start under the Action Process FM Nightly heading in the Run Nightly EOP window.

(2) Run Monthly EOP. FM EOM processing is also called the monthly process. The EOM process performs two specific tasks. It creates the PM Scheduled Work Pending reminder message and the Regulatory Compliance (RC) Scheduled Work Pending reminder. The FM EOM process normally runs automatically at 00:01 AM. If the FM Monthly fails due to a power outage, server problem, etc., it can be run manually using this menu option. Use this link to start the process manually by selecting Start under the Action Process FM Monthly heading in the Run Monthly EOP window.

(3) Export FM Data to Joint Medical Asset Repository (JMAR). The Export FM Data to JMAR process performs the single task of sending updated data on Facility Inventory, Real Property Installed Equipment (RPIE) Inventory, Room Inventory, PROJs, and Requirements to JMAR. The Export FM Data to JMAR process normally runs automatically as part of the Medical Materiel Monthly EOP process, which runs at the date/time established for each month in the EOP module of SS. However, if the monthly process fails due to a power outage, server problem, and so forth, the SA may run the Export FM Data to JMAR process manually using this menu option. To export FM data to JMAR, select Export FM Data to JMAR and then Start under the Action Process JMAR Export heading.

(4) View or Purge EOP Logs. SAs use this option to view the process logs, identify any errors that may have occurred, and purge process logs. In this window, the FM EOP status is displayed with three options for each process: view automatic process logs, view manual process logs, and purge logs. Select the desired function and a PDF file displays in the browser with the process logs, allowing user to view or print the logs.

(5) Manage FM Computer-Aided Design (CAD) Administrators. This option is used to assign users to the FM CAD Administrator group. Users who belong to this group and have the FM CAD Administrator role (within the SS UP Assign module), assigned to their username are able to perform specific tasks related to the management of the electronic CAD drawings in the DMLSS-FM system.

(6) Display FM Help Information. Use this link to display FM help information. A PDF file download window appears to view or print.

(7) Manage Construction Operations Building Information Exchange (COBIE) Files. There are four main COBIE related processes in DMLSS. The upload and download processes are performed in the System Administration Tool. The Import and Export COBIE Data are performed in the FM application. A user must be properly privileged to perform COBIE exchange processes. In the System Administration Tool, a user must have the Facilities Management Administrator role. Within the DMLSS application, the user must have the FM COBIE Administrator role.

(a) COBIE Upload Process. Select the file to upload. Ensure the file is a valid COBIE file with .xml extension. Uploaded files are automatically purged after 7 days. Proceed with the IMPORT COBIE Data process in the FM application within 7 days of the upload action to avoid the need to re-upload in the System Administration Tool.

(b) COBIE Download Process. In the COBIE DOWNLOAD section at the bottom of the screen, locate the file to download and select Retrieve. The Retrieve selection only appears if there are COBIE export files to download.

m. Manage Backups Menu. The DMLSS server and DB files are automatically backed up daily at 02:00. In the Manage Backups window, the SAs can see the status of the last backup, view DB backup logs, and run the backup manually when the automatic backup failed. To access this window select Manage Backups under the list of Task Areas (Figure 26).

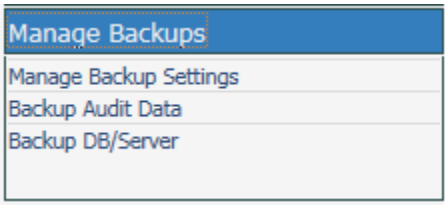


Figure 26. Manage Backups Menu Window

(1) Manage Backup Settings. The DMLSS server is configured to automatically back up file systems on a nightly basis. As part of this process, the DB Scheduler archives and empties the Windows Event Logs nightly so there is no administration required at the site. Event logs are automatically archived and cleared nightly.

(a) Use the Manage Backup Settings link to enable or disable the backup function or select the number of backups that can be included per LTO-4 tape.

(b) DHA/MEDLOG has determined that all sites should be set to a minimum 7-day backup schedule as noted in paragraph 1.c.(2)(a) of this Enclosure. SAs insert a tape once a week in the tape drive to ensure the backup information is available if required. The tape is set to automatically eject each Monday morning after the 0200 backup. When the tape fails to eject, this is usually due to the backup failing.

(2) Backup Audit Data. The Security Technical Implementation Guide requires that Oracle DB Audit records, Oracle Archive Logs, OS Event Logs, and Web Server Logs be backed up and kept for a period of 1 year. DMLSS provides sites with the capability of periodically backing up this audit data to tape.

(a) This audit data is stored on the file system under D:\STIG_AUDITS. When this directory reaches 25 gigabytes of data stored, a flag is set in the DB. The next time an SA uses the System Administration Tool, the home page displays a red indicator box beside the text reading Last Audit Log backup. This red box indicates that it is time to back up the site's audit data. It is important to note that there is currently a 5-day grace period that the SA has in order to complete this Audit backup. On the sixth day, the audit data is purged from the file system in order to conserve space and the next cycle starts. In accordance with paragraph 1.c.(3) of this Enclosure, SAs should run an audit backup on the first day of each month regardless of the indicator status.

(b) SAs initiate the backup by properly labeling a tape designated for the audit backup, inserting the tape into the server, and selecting Backup Audit Log on the Audit Backup page. It takes approximately 2.5 hours to backup 25 gigabytes. The <Refresh Status> selection keeps the SA informed of the elapsed time.

(c) One tape (1.6 terabyte capacity) can hold 6 months of audit backups.

(3) Backup DB/Server

(a) Verify whether or not the automatic backup worked by viewing the backup details displayed at the top of the Backup DB/Server screen (see Figure 27). If it failed, use the Backup DB/Server window to perform a manual backup. If an attempt to do a manual backup fails, contact DHA GSC-help desk at 1-800-600-9332 or dhagsc@mail.mil.

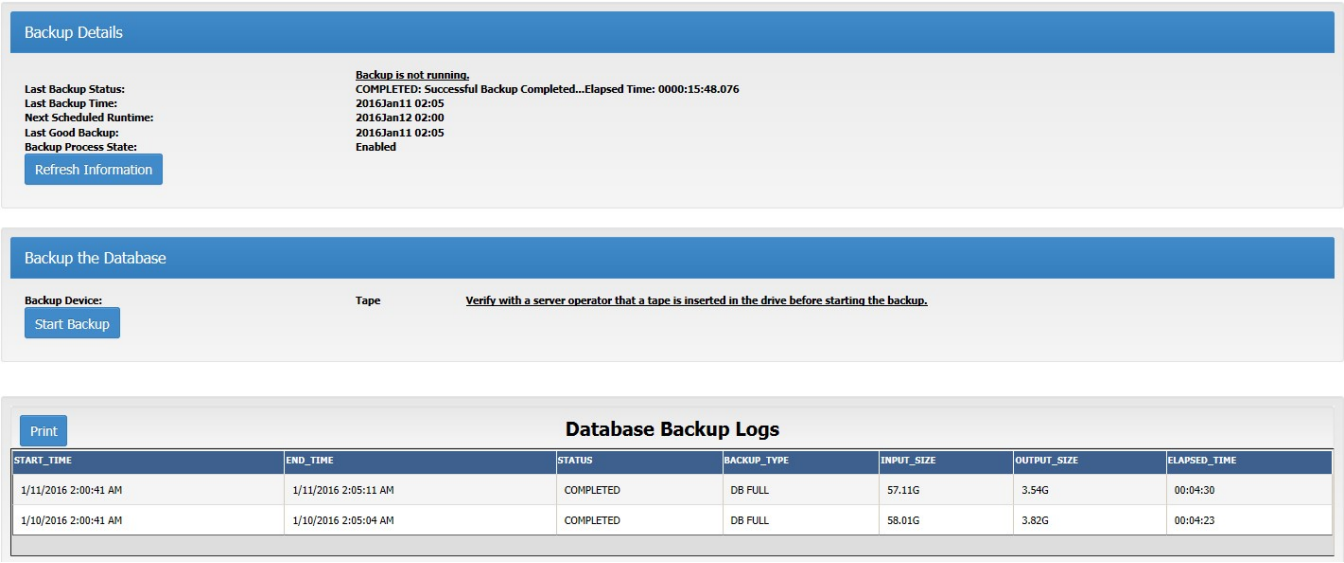


Figure 27. Backup Database/Server Window

(b) Initiate the backup by properly labeling a tape designated for the DB/server backup, inserting the tape into the server, and then selecting Start Backup.

(c) The bottom frame in the Backup DB/Server window is used to view or print a detailed log of the most recent backup of the server and DB files. It includes backup details and log information for the last two DB backup attempts.

(d) Administrators that need to recover a file system should contact the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil. The System Administration Tool does not provide this capability.

n. Data Tapes

(1) The Dell PowerEdge R720 server/LTO Ultrium 3/4 tape drive uses the LTO Ultrium 3/4 Data Cartridge backup tape and LTO Ultrium cleaning tapes. LTO tapes are inserted into the tape drive and stay there for 1 week storing five to seven consecutive EOD backups onto the 1.6 terabyte LTO-4 backup tape prior to ejecting. See also paragraph 1.c.(5) of this Enclosure.

(2) The write protect switch should be set to the left (unprotected) to allow data recording on the cartridge. Tape backups fail if the tape is set to write-protect. Make sure labels are stuck to the cartridge in the label areas, and do not stick more than one label onto each label area. Extra labels can cause the cartridges to jam in the tape drive.

(3) See paragraph 1.g.(2) of this Enclosure for information on the storage of backup tapes.

o. Cleaning Tape Drives. See paragraph 1.g.(2) of this Enclosure for instructions on cleaning tape drives.

3. SS. The SS module encompasses many of the controls required for users to navigate throughout DMLSS.

a. Overview. On the server side, SS automatically supports several types of background processing for all DMLSS applications. On the computer application side, SS does the following:

(1) Supports security for the other applications, UPs. The DMLSS SA provides the appropriate level of access to the system when MEDLOG personnel and supply or equipment custodians require access to DMLSS. Specific privileges are assigned to users based on the information obtained from the DMLSS System User Appointment Letter. The SA or Application Security Manager should be familiar with the management of UPs before attempting to assign UPs. See Figure 38.

(2) Controls the data accessed in the Table Maintenance Utility (TMU) application, archive management, and MTF/Org (organization) setup and management.

(3) Allows SAs to monitor and interact with some processes generally managed on the server, such as EOP processing and the DCM.

(4) Some thought and care should be given prior to assigning privileges for the SS module. Most of the functions play a direct role in how DMLSS organizational structure, funds, document control, EOP processing, and interfaces are managed. It is highly recommended that only experienced logisticians with knowledge and training be afforded privileges to these functions.

b. Organizational Structure. Materiel and fund managers should be very familiar with the organizational structure in DMLSS. The three main components to this structure, MTF/DTF (ORGs), Department (DEPT), and service/customer (SVC/CUST), are based on a set of hierarchal rules and parent-child relationships. Use the Tree View, Search, ORG, DEPT, and SVC/CUST groupings to understand, review, or make changes to the MTF/DTF's organizational structure.

c. DMLSS Auditable Changes. Business rules require several processes of the MTF/Unit module to be audited by the system. Changes made in these audited areas are captured along with the date, User ID, and other information viewable from the Transaction History window. Document numbers are also viewable when the transaction is saved.

(1) Transaction codes are intended for user-initiated additions or changes that affect the following data elements: Appropriation Fund type code, default EXP centers, ORG IDs, ORG types, materiel ownership codes, and level algorithm changes.

(2) For example, ECC, or establish cost center, and RCCC, or responsibility center/cost center, transaction codes are generated when establishing and revising records within the LOG

DEPT and service detail records, plus MTF/Unit, also known as ORG, DEPT, and SVC/CUST detail records.

d. Tree View. The Tree View Record Selection window displays a hierarchy view of all MTF/Units ORGs and sub-organizations that DMLSS manages. Use Tree View to browse a site's organizational structure, open an organizational record, print the Tree View display, or move a from one DEPT or MTF/Unit to another. Tree View icons represent the associated customer level within the MTF. Figure 28 reflects the Tree View icons and proper hierarchal structure using MTF/Unit, DEPT, and SVC/CUST. Creating new ORG, DEPT, and SVC/CUST records are explained in paragraph 3.f. of this enclosure. Within the Tree View:

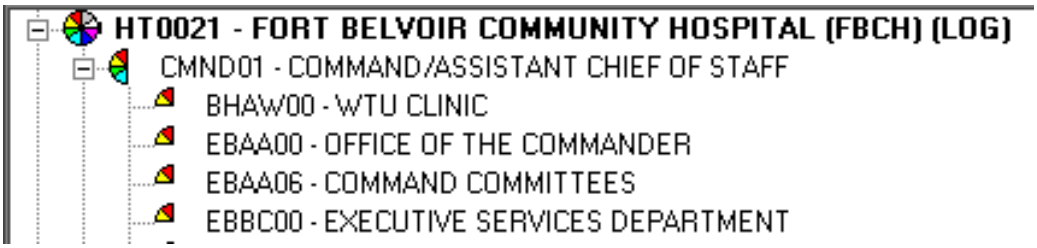


Figure 28. Tree View and Hierarchal Structure of Organization, Department, and Service/Customer

(1) MTF/Units ORGs are identified by a full pie.

(2) DEPTs are identified with a half pie.

(3) SVC/CUSTs are identified with a quarter pie.

e. Search. The SS Search function provides a method to search for MTF/Unit ORG or sub-organization records to review, update, and/or print lists of organizational records. The Organizational Search window appears by selecting the Search icon located on the horizontal toolbar or by selecting Search from the Navigate menu. Search criteria available for use include: ID (SVC/CUST, ORG, or DEPT ID), Name, Type, Medical Expense and Performance Reporting System Code, Office Symbol, and Cost Center. All records are displayed if search fields are left empty/blank, and the search icon located on the vertical toolbar is selected. Select a specific organizational record by double-clicking or highlighting the record, and select Details located on the vertical toolbar to view and/or modify details of that record.

f. ORG. Use this option to create an MTF/Unit ORG. Multiple records can be created and maintained in a single DMLSS DB; however, only one can be assigned as the LOG or Service Department of Defense Activity Address Code (DoDAAC). The LOG DEPT is also associated to all other LOG services, i.e., Medical Maintenance Activity (MA). Note: See Figures 45-47, for a complete description of these details. The information and associations that are edited or created here affect many things throughout the system. As a user of MTF/Org, the following qualifications exist. To ensure the integrity of the organizational structure, it is recommended that only Accountable MEDLOG Officers, MEDLOG senior enlisted or civilian in charge, be authorized to create new and modify existing MTF/Unit records.

(1) Prior to creating an MTF/Unit ORG detail record. Review the online help function to identify required information and validate all data prior to creating the detail record.

(2) Creating New MTF/Unit ORG Records. To create a new MTF/Unit ORG record, select MTF/Unit from the Navigate dropdown menu. The Basic tab of the MTF/Unit Detail – (New) window appears. Note: Existing MTF/Unit records can also be accessed from this window by using Find located on the vertical toolbar.

(a) Basic Tab. All required fields must be completed. At the bottom of the Basic tab, associate new MTF/Unit details to the correct Primary Support Activities. Refer to Figures 45-47. Upon saving data in the Basic tab, the remaining tabs become available.

(b) DEPT Tab. In the DEPT tab, use the < and > icons to associate and/or disassociate DEPTs to/from the MTF/Unit. Select Details located between the windows to view an existing DEPT's record. Select New to create a new DEPT. If both the associated and non-associated boxes are empty, then no DEPTs were linked to the MTF/Unit when the new DEPT record was created.

(c) SVC/CUST Tab. In this tab, use the < and > icons to associate and/or disassociate SVC/CUST to/from the MTF/Unit. Select Details located between the windows to view an existing SVC/CUST's record. Select New to create a new SVC/CUST. If both the associated and non-associated boxes are empty, then no SVC/CUST records were linked to the MTF/Unit and/or DEPT when the new SVC/CUST record was created.

(d) FM Installations Tab. In the FM Installations tab, use the < and > icons to associate and/or disassociate an FM installation to/from the MTF/Unit. An FM installation should always be associated to the LOG DEPT, but it is not necessary to be associated to MTF/Unit ORG record types.

(e) Assemblages Tab. The Assemblage tab provides a list of assemblages associated to the MTF/Unit. If no assemblages are associated to the MTF/Unit then this tab is not available.

(f) Existing MTF/Unit ORG Detail Records. Using the Search function, access existing MTF/Unit ORG detail records by selecting ORG–Med Facility/MTF in the Type field and then selecting Search. All ORG records are displayed in the Organizational Search selection window. This list includes the LOG DEPT record. To access only the LOG DEPT record using the Search function, select LOG–Logistics Dept in the Type field and select Search. Double-click a record or highlight one and select Detail to access the MTF/Unit ORG Detail window for the specified MTF/Unit ORG. Existing MTF/Unit ORG records can be modified and/or marked for deletion. To undelete an MTF/Unit record, unselect Mark for Deletion and the MTF/Unit ORG record becomes usable.

g. DEPT. Use this option to create a new DEPT. DEPTs are in the center of the organizational structure. Using the LOG DEPT, MTF/Unit record, as an example, a DEPT for each squadron within the MTF could be created (e.g., Aerospace Medical Squadron, Dental

Squadron, Medical Operations Squadron, and Medical Support Squadron which are associated to the LOG MTF/Unit).

(1) Creating New DEPTs. To create a new DEPT record, select DEPT from the SS Navigate dropdown menu. The DEPT Detail – New window appears. An existing MTF/Unit ORG record must be immediately associated to the new DEPT. Upon associating to an MTF/Unit ORG record, certain data fields in the DEPT record automatically populate and the remaining fields become available. After saving data in the Basic tab, the SVC/CUST and Funding tabs become available. Note: Existing DEPT records can also be accessed from this window by selecting Find located on the vertical toolbar.

(a) Basic Tab. The DEPT ID, Name, and Military Service fields are the only mandatory fields in the Basic tab; however, all fields should contain valid information, if possible. Theoretically, the DEPT ID should correlate to the DEPT Name. Once data is saved to the Basic tab, the SVC/CUST and Funding tabs become available.

(b) SVC/CUST Tab. Use the < and > functions to associate and/or disassociate existing SVC/CUST records to the DEPT. Select Detail to view detailed data for SVC/CUST records. Select New to create a new SVC/CUST record.

(c) Funding Tab. Use the < and > to associate and/or disassociate existing PROJ center records to the DEPT. Select Detail to view detailed data for a PROJ center record. Select New to create a new PROJ center record.

(2) Existing DEPTs. Using the Search function, select DEPT – DEPT in the Type field and select Search located on the vertical toolbar. All existing DEPT records are displayed in the Query/List Record Selection window. A check in the DEL, or deleted, column indicates that the DEPT record is marked for deletion and cannot be used. To access a DEPT record, double-click a record or highlight one and select Detail. In the DEPT Detail window, data fields can be modified, and the DEPT can be marked for deletion by checking the Mark for Deletion box. To undelete a DEPT, click in the same box to remove the check and the DEPT becomes available for use.

h. SVC/CUST. Use this option to create a new Service Customer. SVC/CUST are at the bottom of the organizational structure. These types of records should be associated to a DEPT. Additionally, all SVC/CUST accounts must be associated to an EXP center, and that EXP center must be associated to a PROJ center. Customer requests are not allowed if any of these links are broken.

(1) Creating New SVC/CUSTs. To create a new SVC/CUST record, select SVC/CUST from the Navigate dropdown menu. DMLSS immediately prompts the user to assign the associated MTF/Unit and DEPT. While the DEPT association is not mandatory, it is highly recommended that one be associated at this time to maintain a clear and concise organizational structure. Upon associating to an MTF/Unit ORG and DEPT, the SVC/CUST Detail (New) window appears (Figure 29). Upon entering and saving mandatory data in the Basic and

Materiel tabs, the Funding tab becomes available. If the SVC/CUST is associated to a customer owned assemblage, the Assemblage tab becomes available listing all associated assemblages.

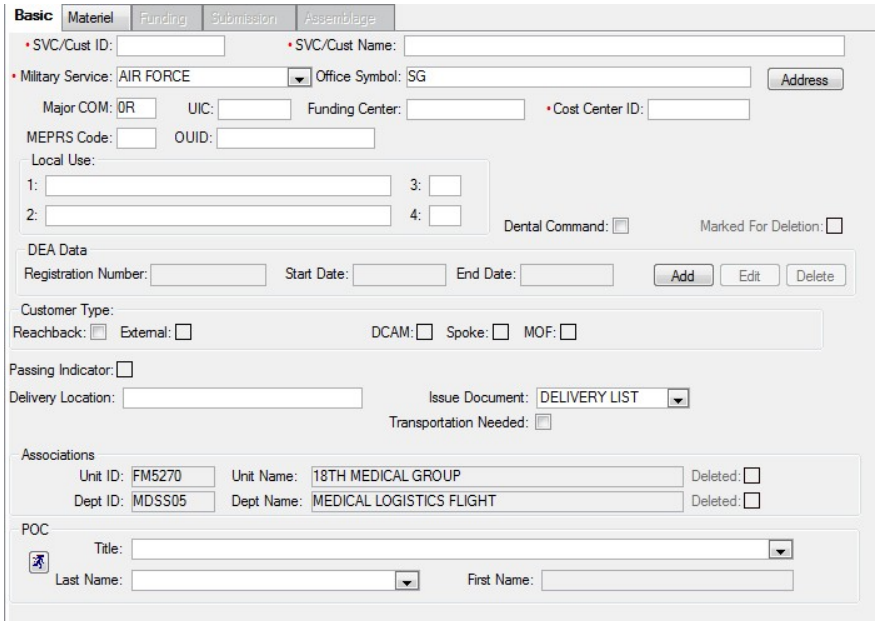


Figure 29. Service/Customer Detail–(New)–Basic Tab

(a) Basic Tab. The SVC/CUST ID, SVC/CUST Name, and Military Service fields are the only mandatory fields in the Basic tab; however, all fields should contain valid information, if possible. Associate the custodian's POC record in the POC field. Custodians should be assigned POC type codes DMLSS User and Custodian.

(b) Materiel Tab, Figure 30. The Default Location field is the only mandatory field in the Materiel tab; however, all fields should be completed if possible. Assign a default location prior to saving changes and making the remaining tabs available.

1. Computation Method. The computation option should always be set to Days of Stock.

2. Days/Inv. Freq. Fields. The days and inventory defaults are set to 7 and 3 days respectively. These numbers indicate how many days of stock the customer is maintaining and how many times within that period the customer conducts an inventory and produces an order. For example, if the defaults are maintained, the customer produces three orders within each 7-day period.

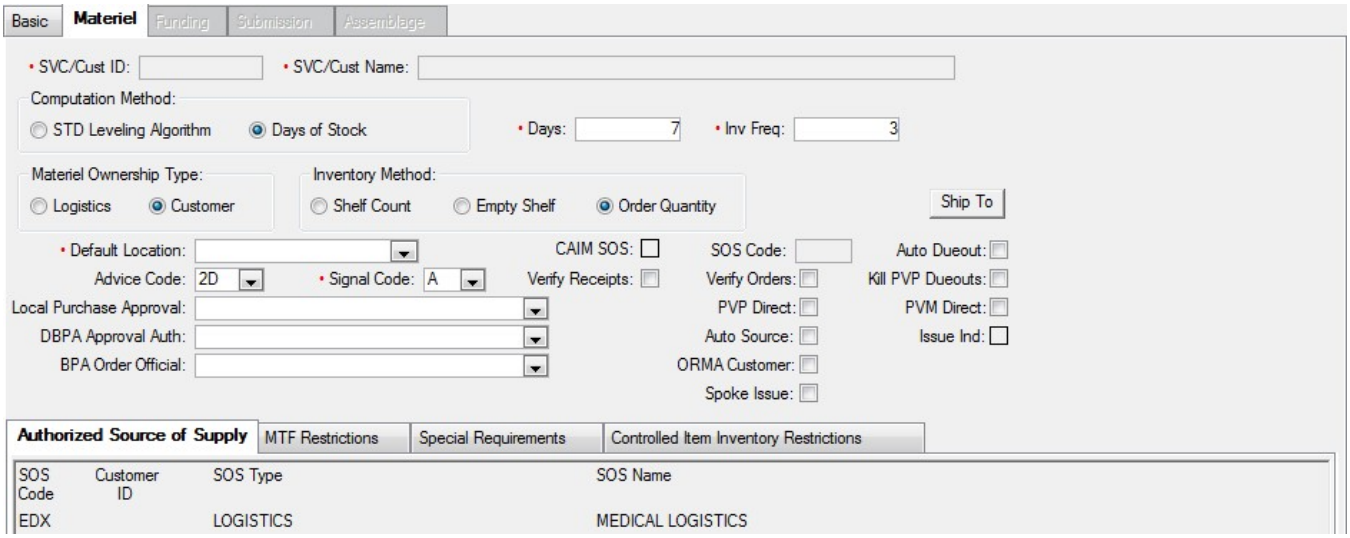


Figure 30. Service/Customer Detail–(New)–Materiel Tab

3. Inventory Method. In most instances, Order Quantity is assigned for all customers. Inventory Method Shelf Count can be assigned when stricter inventory control is needed.

4. Default Location. The Default Location is a mandatory entry that should identify the customer's main supply storage area. This should coincide with the Delivery Location located in the Basic tab (identifies where MEDLOG delivers supply requests).

5. Ship to Address. The shipping data is only relevant to CAIM Source of Supply (SOS) accounts that are authorized to place orders to an SOS.

6. CAIM SOS. This indicator identifies whether or not the customer is authorized to sell materiel to other internal customers and can therefore bypass LOG by placing supply orders directly to an SOS. The Accountable MEDLOG Officer is responsible for determining whether or not an activity is authorized to order direct. If the activity is coded as a CAIM SOS, the system prompts the user for an SOS Code, Estimated Lead Days, and CAIM SOS Name. Upon saving, the SOS Code box in the Materiel tab is populated.

7. Advice Code. This code only affects CAIM activities. The system default Advice Code is 2D which stands for Furnish Exact Quantity. A list of authorized advice codes is visible in TMU by selecting IM and then Advice Code table.

8. Signal Code. This code only affects CAIM activities. The system default Signal Code is A, which stands for Ship to Requisitioner; Bill to Requisitioner. A list of authorized signal codes is visible in TMU by selecting IM and then Signal Code/Military Standard Requisitioning and Procedures (MILSTRIP) table.

9. Auto Due-out. This checkbox is available only if the CAIM SOS checkbox is selected. Selecting this checkbox causes due-out quantities to be increased to match the due-in

quantities if the U/S is not equal to the unit of purchase. It only applies to catalog records assigned Core or Static level type and the location records are marked for Resale.

10. Verify Receipts. If selected, this checkbox ensures that the user receiving supplies verifies the receipt against what is actually received. When this checkbox is not selected, DMLSS automatically updates balance records with the quantities shown on the internal source's receipt. When LOG processes receipts, and generates the delivery list, DMLSS automatically processes receipts for CAIM customers, changes the status of those receipts from active to inactive, and updates the customer's estimated O/H balance. CAIM SOSs check this box, and, as a result, CAIM receipts are manually processed.

11. Verify Orders. When this checkbox is selected, individual orders must be manually verified within the CAIM Build/Process/Submit module before they are submitted to LOG. This option is not recommended because it impedes a customer's normal ordering procedures. Note: Verify Orders is mandatory for CAIM SOS activities.

12. Kill Prime Vendor Pharmacy (PVP) Due-outs. This function is used only in conjunction with the PVP Direct option. When this box is checked, any time a due-in from PVP is reduced or canceled, a like amount of customer due-outs is reduced or canceled.

13. PVP Direct. Select this checkbox if the customer is authorized to order directly from the PVP. When this option is used, the customer's orders are rolled into separate call numbers and are not commingled with other customer requirements. Coordinate with the DHA MEDLOG PV representative prior to selecting this option.

14. Med/Surge PV Direct. Select this checkbox if the customer is authorized to order directly from the Med/Surg PV. When this option is used, the customer's orders are rolled into separate call numbers and are not commingled with other customer requirements, coordinate with the DHA MEDLOG PV representative prior to selecting this option.

15. Auto Source. The Auto Source code is used when the customer is coded as a Reachback Customer (located in the Basic tab). If this checkbox is selected, and an item does not have a catalog record for the Reachback PV, the item is automatically sourced to LOG's default supplier.

16. Operating Room Management Application Customer. This function is no longer in use.

17. Spoke Issue. Select to mark a service customer as a Spoke Customer.

18. Authorized SOS. The SOS codes in which the customer is authorized to purchase materiel without going through LOG. The Accountable MEDLOG Officer is the responsible approval authority.

19. MTF Restrictions. Use the MTF Restrictions tab to restrict the customer from requesting certain types of materiel. If the customer is restricted against ordering an item,

the customer cannot create a CAIM catalog record for the item. For example, to restrict the customer from creating catalog records and requesting controlled substances, add the MTF restrictions for Code Q and R. These restrictions directly relate the assigned Controlled Item Inventory Code (CIIC) within each catalog record. Use the edit icon to associate and disassociate restrictions.

20. Special Requirements. Use the Special Requirements tab to further identify customer restrictions. These restrictions directly relate the assigned CIIC within each catalog record. Use the edit icon to associate and disassociate restrictions.

21. Controlled Item Inventory Restrictions. Use this tab to further identify customer restrictions. For example, if the customer is not authorized to request controlled pharmaceuticals, add codes Q and R to this tab. These restrictions directly relate the assigned CIIC within each catalog record. Use the Edit icon to associate and disassociate these restrictions.

(c) Funding Tab (Figures 31-33). Use the < and > to associate and/or disassociate existing EXP center records to the SVC/CUST. Select Detail to view detailed data for an EXP center record. Refer to Military Service policies regarding creation and management of a new EXP center record and Funding Tab.

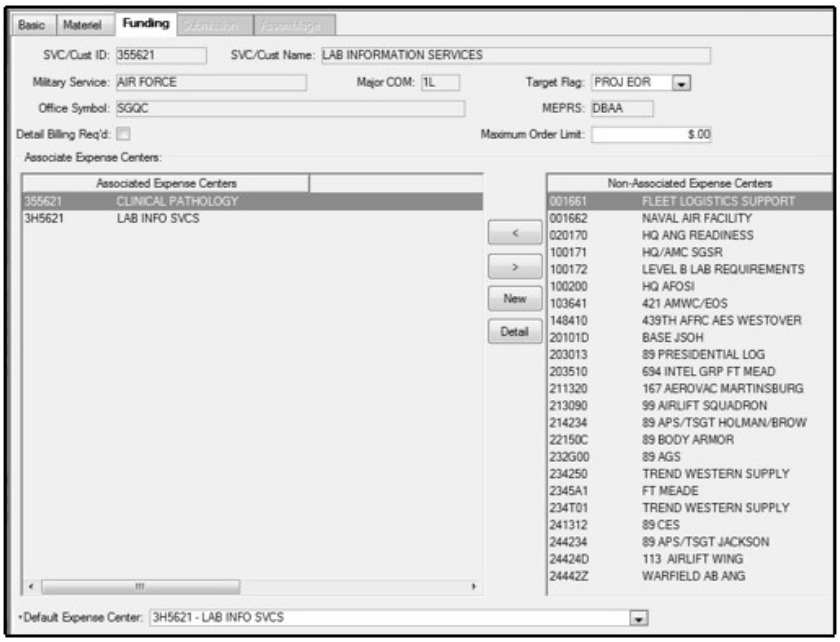


Figure 31. Service/Customer Detail–(New)–Funding Tab (Air Force)

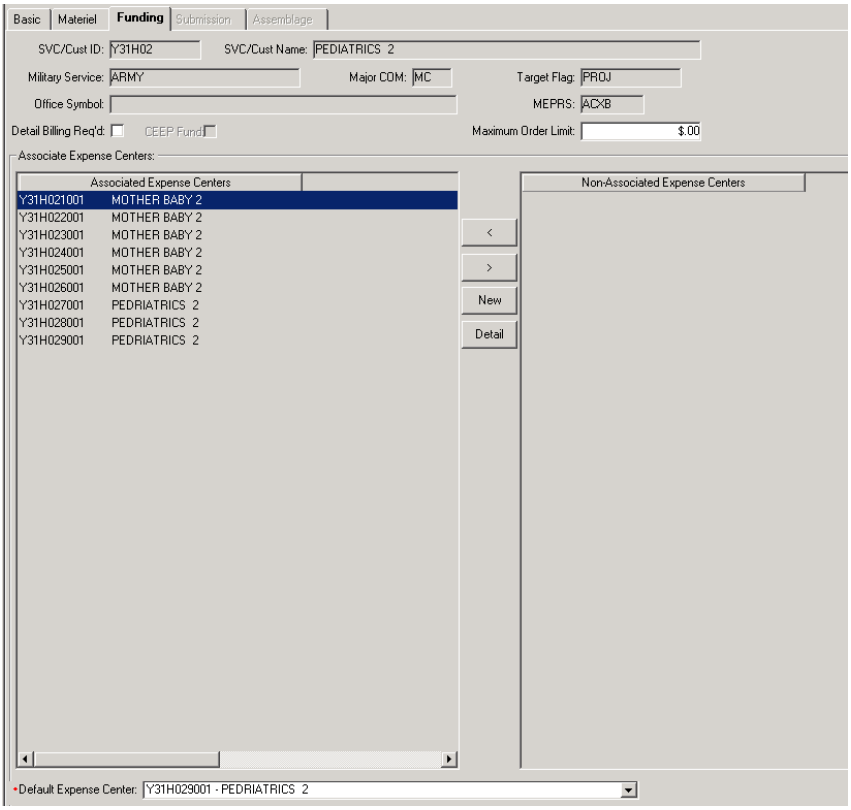


Figure 32. Service/Customer Detail–(New)–Funding Tab (Army)

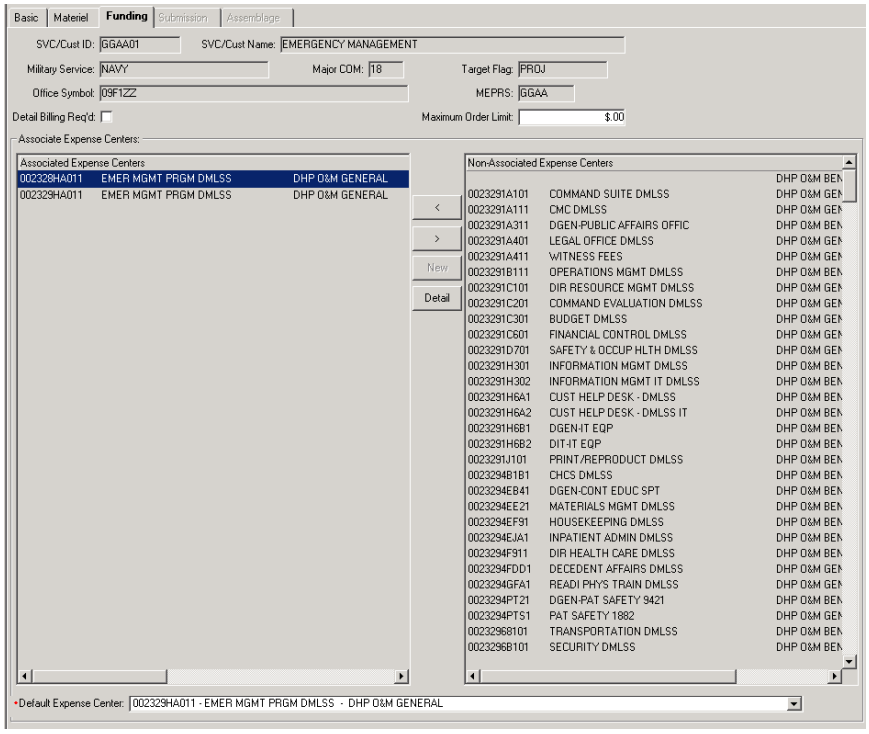


Figure 33. Service/Customer Detail–(New)–Funding Tab (Navy)

1. Target Flag. The target flag instructs DMLSS to enforce a target amount at the PROJ center, EXP center, or Elements of Resource (EOR) level. The setting prevents orders at this level and all subordinate levels from exceeding the established financial target amounts.

a. PROJ EOR. DMLSS validates funds availability at the PROJ center and EOR level.

b. PROJ. The target amounts set for each PROJ center cannot be exceeded by the PROJ center's dependent service customers. DMLSS validates funds availability at the PROJ center level regardless of which EOR the funds are available.

c. EXP EOR. DMLSS validates funds availability at the EXP center and EOR level.

d. EXP. The target amounts set for each EXP center cannot be exceeded by the EXP center's dependent customers. The system validates funds availability at the EXP center level regardless of which EOR the funds are available.

e. NONE. When the target flag is set to NONE, DMLSS does not validate funds availability when obligations occur. In other words, the associated EXP and PROJ centers are allowed to go negative.

2. Detail Billing Required. This function is no longer applicable.

3. Maximum Order Limit. Use this field to restrict the price limit for any one item ordered by the customer.

4. Default EXP Center. Because SVC/CUST accounts can be simultaneously associated to multiple EXP centers, an active default EXP center must be identified. The association identifies which EXP center or PROJ center that are used for transactions.

(d) Submission Tab. This tab is only available if the SVC/CUST account is coded as a Reachback for Air Force customers, Defense MEDLOG Customer Assistance Module, External, or Spoke customer. All of the aforementioned indicators reside in the Basic tab. Defense MEDLOG Customer Assistance Module and external customers are considered external to the local MTF/DTF and mission requirements dictate that orders be filled by special procedures in the IM application. A Spoke customer is one who has an operating DoDAAC on another DMLSS server and procures materiel from the Hub account. In order for the spoke customer to become active in DMLSS, the Hub indicator must be set within the Materiel Management Service detail. Refer to Military Service policies when setting up external customers in the Submission Tab.

(e) Assemblage Tab. The Assemblage tab is visible if the SVC/CUST account is associated to customer owned assemblages in the AM module. Modifications are not allowed in this window.

i. Funds

(1) Management of funds in DMLSS is critical to system operations and can dramatically impact the DRO and how MEDLOG operates, if not properly managed. The funds module provides MEDLOG and Resource Management Office the flexibility to manage most aspects of the DRO's funding. DMLSS funds management allows the ability to:

(a) View and manage funds through EXP centers, PROJ centers, and the LOG fund.

(b) Gather information on EORs and commodity classes.

(c) View and manage details such as commitments, obligations, and target amounts.

(d) View and manage single-and multi-year funds.

(2) Select Funds from the SS navigate dropdown menu or select the Funds icon located on the horizontal toolbar to access the Funds-Search window. Fund managers can search for records by Fund Center Number, Fund Center Name, or Fund Type (i.e., S-Log Fund, P-Project Center, E-Expense Center). To retrieve all fund records, leave all search criteria fields blank and select the Search icon located on the vertical toolbar.

(3) LOG Fund

(a) The LOG fund detail window displays all funding for the Default Logistics Fund. Other criteria associated with the LOG fund are:

1. The target cannot be exceeded with orders, price changes, and/or receipts.

2. Default Log Fund-Refer to Military Service policies until DHA policies have been published and are in effect.

3. The Log Fund target amount is cumulative for the FY.

4. The target is reset to zero during EOFY processing.

(b) LOG Fund Detail–LOG–Air Force Working Capital Fund window (Figure 34). This figure is provided as an example. The upper portion of the window displays information from the LOG fund as well as funds disbursements. The LOG Fund ID and Fund Code must be present.

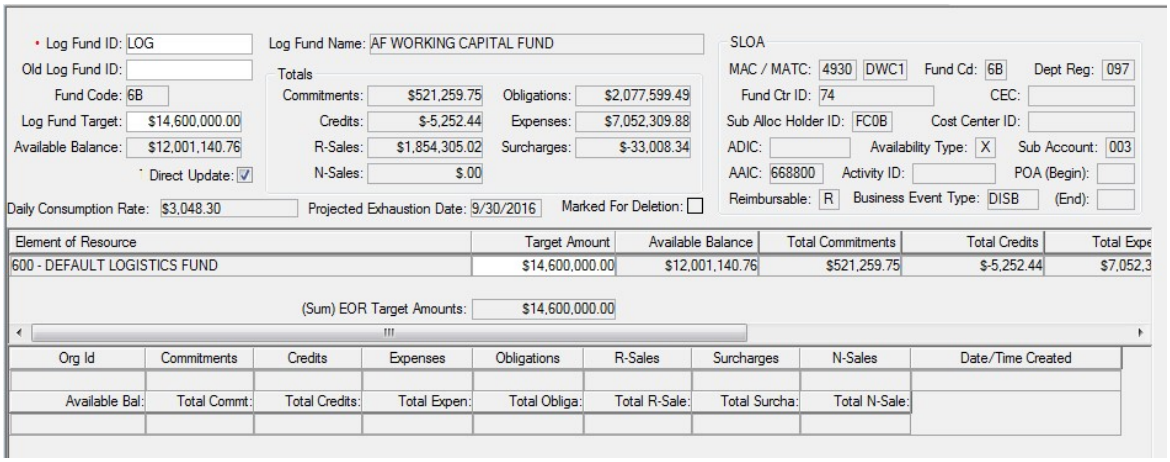


Figure 34. Logistics Fund Detail–Logistics–Air Force Working Capital Fund Window

(c) The LOG fund target restricts the amount of funds a LOG account is allowed to obligate during the FY and prevents negative balances based on the target and available balance. The target flag indicator for the LOG fund is located in the Appropriation tab of the Materiel Management Service Detail record. It is important to work closely with the DRO Resource Management Office to ensure that funding is set up and managed correctly.

(d) The Direct Update field controls how funds update in DMLSS. MEDLOG must check the Direct Update field for all accounts. If the box is checked, funds are updated at the time of transaction execution. If the box is unchecked, the LOG fund account is reconciled either manually by tallying funds lower window or during the next EOD process.

(e) The middle window displays the EOR and all current funding information. Changes to the amounts in these fields directly impact the funds availability for the DRO. When these fields are modified, the corresponding fields in the upper window are updated to reflect the new figures.

(f) For more information on the financial structure including the LOG fund, PROJ centers, and EXP centers, refer to Military Service policies until DHA policies have been published.

j. PROJ Center. PROJ center fund records provide visibility of fund management at the PROJ center level. They are associated to SVC/CUSTs indirectly through an EXP center. PROJ center transactions are internally audited by the system, DMLSS captures the type of change along with the date, User ID, and other information. This data is recorded in the Transaction History using transaction code ESP.

(1) Refer to Military Service policies until DHA policies have been published regarding information on accessing or loading fund targets in an existing PROJ center.

(2) Retired Indicator Checkbox. Use this checkbox to designate retired PROJ centers. This indicator identifies a PROJ center that is no longer intended for use but cannot be marked for deletion until due-outs and/or equipment data records have been removed.

(3) Marked for Deletion Checkbox. Check the Marked for Deletion box to mark a PROJ center fund record for deletion. Usually, the Resource Manager/ Resource Advisor will direct this action if/when the PROJ center is no longer required. A record that is marked for deletion still appears in the system but does not support any further financial activity. The PROJ center is removed during EOFY processing as long as there are no financial ties. If there are still financial obligations not cleared prior to EOFY, the PROJ center remains visible in DMLSS but continues rejecting additional financial activity.

(4) To view additional PROJ centers, select the Find icon to open the PROJ Center Search window. Enter a PROJ center to view or select Search to view a list of all PROJ centers. Select the PROJ center and select Details to view the PROJ center information.

k. EXP Center. EXP centers capture funding data from associated SVC/CUST records, which is rolled up to the associated PROJ center. EXP centers can have program targets the same as PROJ centers. These targets represent the EXP centers' budget. EXP center transactions are internally audited by the system; meaning, DMLSS captures the type of change along with the date, User ID, and other information. This data is recorded in the Transaction History using transaction code ESP.

(1) Accessing an Existing EXP Center. To access an existing EXP center, either select Funds from the SS Navigate menu or select the Funds icon located on the horizontal toolbar. The Funding-Search window appears. This window can be used to search all fund records. To retrieve an EXP center fund record, do one of the following:

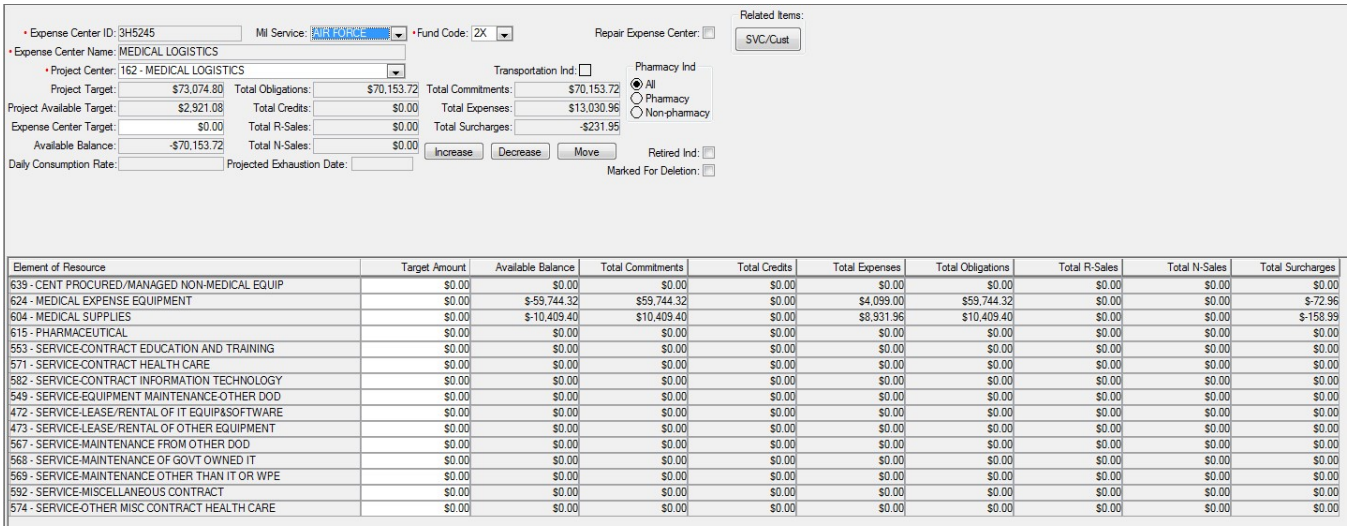
(a) Enter the EXP center into the Fund Center field and select Search.

(b) Enter the EXP center name into the Fund Center Name field and select Search.

(c) Select E-MM Expense Center in the Fund Type dropdown menu and select Search. This option retrieves all EXP center records.

(d) All fund records are retrieved by selecting Search when all three search criteria fields are empty.

(2) The EXP Center Detail window, Figure 35, is similar to the PROJ Center Detail window. The financial manager can view current totals for commitments, obligations, available balances, credits, sales, and surcharge figures for the selected EXP center. Select the SVC/CUST box located in the Related Items window to see a list of SVC/CUSTs associated to the selected EXP center.



Element of Resource	Target Amount	Available Balance	Total Commitments	Total Credits	Total Expenses	Total Obligations	Total R-Sales	Total N-Sales	Total Surcharges
639 - CENT PROCURED/MANAGED NON-MEDICAL EQUIP	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
624 - MEDICAL EXPENSE EQUIPMENT	$0.00	$-59,744.32	$59,744.32	$0.00	$4,099.00	$59,744.32	$0.00	$0.00	$-72.96
604 - MEDICAL SUPPLIES	$0.00	$-10,409.40	$10,409.40	$0.00	$8,931.96	$10,409.40	$0.00	$0.00	$-158.99
615 - PHARMACEUTICAL	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
553 - SERVICE-CONTRACT EDUCATION AND TRAINING	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
571 - SERVICE-CONTRACT HEALTH CARE	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
582 - SERVICE-CONTRACT INFORMATION TECHNOLOGY	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
549 - SERVICE-EQUIPMENT MAINTENANCE-OTHER DOD	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
472 - SERVICE-LEASE/RENTAL OF IT EQUIP&SOFTWARE	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
473 - SERVICE-LEASE/RENTAL OF OTHER EQUIPMENT	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
567 - SERVICE-MAINTENANCE FROM OTHER DOD	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
568 - SERVICE-MAINTENANCE OF GOVT OWNED IT	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
569 - SERVICE-MAINTENANCE OTHER THAN IT OR WPE	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
592 - SERVICE-MISCELLANEOUS CONTRACT	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
574 - SERVICE-OTHER MISC CONTRACT HEALTH CARE	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00

Figure 35. Material Management Expense Center Detail Window

(a) Updates to EXP center name, EXP center target amounts, and target amounts for individual EORs within the EXP center are accomplished in this window. While the Military Service and fund fields are editable, fund managers should not change these settings without proper authorization and documentation. The financial manager (assigned required privileges), can update fund targets or expenditures by selecting the field to be updated and changing the totals. The screen does not auto refresh after the update. Changes are only visible after logging out and returning to the window.

(b) If necessary, fund managers can change an EXP center from one PROJ center to another. When changing PROJ centers, all financial data is moved to the new PROJ center. A message box warning of the change precedes the action. Changing an EXP center to a different PROJ center should only be accomplished when approved by the resource manager (RM)/resource advisor (RA). Documentation should be received and maintained for all changes.

(c) Retired Indicator Checkbox. Use this checkbox to designate retired EXP centers. This indicator identifies a cost center that is no longer intended for use but cannot be marked for deletion until due-outs and/or equipment data records have been removed. When checked, the EXP Center is ineligible for selection in all ordering processes such as IM Customer Requests, Offline Non-submit orders, Non-routine issues, etc.

(d) Marked for Deletion Checkbox. Check the Marked for Deletion box to mark an EXP center fund record for deletion. Usually, the RM/RA directs this action if/when the EXP center is no longer required. A record that is marked for deletion still appears in the system but does not support any further financial activity. The EXP center is removed during EOFY processing as long as there are no further financial actions. If there are still financial obligations not cleared prior to EOFY, the EXP center remains visible in DMLSS but continues rejecting additional financial activity.

(3) To view additional EXP centers, select the Find icon to open the EXP Center Search window. Enter an EXP center to view or select Search to view a list of all EXP centers. Select the EXP center and select the Details" icon to view the EXP center's information.

l. AM Funds. Use the AM Funds module to maintain funds associated to contingency-type assemblages. AM funds are appropriated in writing by Service MEDLOG Agency for the purpose of purchasing new materiel or replacing existing materiel for contingency-type assemblages. Refer to Military Service policies until DHA policies have been published.

m. Other Procurement (OP) Funds. OP funds are classified as funds used to purchase capital equipment, meaning, equipment with an acquisition cost greater than $249,999.99. Establish an OP fund record as a prerequisite to processing capital equipment requisitions in DMLSS. Because OP funds can span a period of three FYs, DMLSS allows fund managers to establish and update OP fund targets for three FYs (current year plus 2 previous years). OP funds are rarely distributed to the bases, but a pseudo-fund record must be loaded in DMLSS to allow processing of orders. DMLSS maintains OP fund records for 8 years; 3 active and 5 inactive. OP funds are recorded but not executed; they are notational in nature.

(1) Establishing a New OP Fund Record. In the OP Fund-Search window, select the New Fund icon located on the vertical toolbar to establish a new OP fund record. In the OP Funds Detail-New window, enter all required information as follows:

(a) FY–Funds can be loaded for current plus two previous FYs. Enter the applicable FY in accordance with the funding authorization letter.

(b) MTF/Unit–Load the applicable organization.

(c) Fund Code–Provided by Service MEDLOG agency.

(d) BLIC, or budget line item code–If required, provided by Service MEDLOG agency.

(e) Proj Code–If required, provided by Service MEDLOG agency.

(f) Appropriation, or APPN, 1–If required, provided by Service MEDLOG agency.

(g) Appropriation, or APPN, 2–If required, provided by Service MEDLOG agency.

(h) Target–Enter target amount indicated on the funding authorization letter.

(i) Reference–Enter reference number from the funding authorization letter.

(j) EOR Target Amount – Enter same value that was entered into the Target field. Funds must be added to the EOR target amount in order to process equipment requests.

(2) Accessing/Modifying an Existing OP Fund Record. Select OP Funds from the Navigate menu or the OP Funds icon located on the vertical toolbar to access the OP Funds-Search window. Search for OP funds by FY and fund code or leave these fields blank and select Search to view all OP Funds balances by FY. The search results window displays the FY, fund code, commitments, obligations, and available balance for each fund record. Either double-click on the desired fund record or highlight it and select the Detail icon located on the vertical toolbar to access Fund Records Details. The OP Funds-Detail window contains two tabs: Funds Ledger and Funds Status tabs.

(a) Funds Ledger Tab. The Funds Ledger tab allows the fund manager to edit an existing OP fund record (and create a new one). The OP Funds-Detail window includes the same information as the OP Fund-New window, but also includes a Funding Reference that is comparable to an electronic checkbook keeping track of all monetary transactions associated to the fund record. Fund target increases, and decreases are also accomplished here.

1. Select the Increase or Decrease icon to add or remove target amounts to or from the OP fund record. Enter the adjustment amount referenced on the funding authorization letter in the Amount field, the applicable reference, and select Save. Upon saving, the OP fund target field and the funding reference history is updated with the transaction information for audit purposes. Update the EOR Target Amount by entering the new total OP fund target amount. When completed, verify the dollar value in the (Sum) EOR Target Amounts field is equal to the OP fund Target field.

2. When the fund updates occur, an ADP transaction is written to the Transaction History file. The ADP transaction captures the target adjustment (whether positive or negative figure) and assigns a Fund Type of OP Fund. The document is made up of the DoDAAC, Julian date, and serial number beginning with F and 001, 002, 003, etc. The serial number resets after each EOP processing cycle.

(b) Funds Status Tab. The Funds Status tab displays OP fund records details along with equipment request data linked to the OP fund record. This tab is updated with all changes that occur to an OP purchase.

n. POC

(1) A POC is a person within the organization. Keeping valid and current POC information on all users is an important part of DMLSS SA. The POC window allows authorized users to search, view, edit, add, and delete POC information as necessary. The POC is usually responsible for managing the area that the organizational record describes, such as an SVC/CUST account, a DEPT, or an MTF/Unit. POC information is entered into the POC Detail Update–New–Window, Figure 36, and is available for association to the organizational records.

(2) Select POC from the Navigate dropdown menus to access the POC Detail window. The last name, first name, title, phone number, and e-mail address are the only mandatory data fields for new records; however, all data fields should be completed if possible. If the POC address is not already loaded in DMLSS address table, select "Jump To" and load the address

and associate it to his/her record. DMLSS establishes an electronic interface between DMLSS and Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) that generates a Receipt Acceptance (EDI 861 file) to iRAPT, in addition to sending the Receipt (EDI 527) to DLA Troop Support. The Receipt Acceptance contains POC information to include the receiver's name, phone number, e-mail address, and User ID. Users must enter accurate first/last names, phone numbers without parenthesis, spaces, or dashes, and a valid .mil e-mail address.

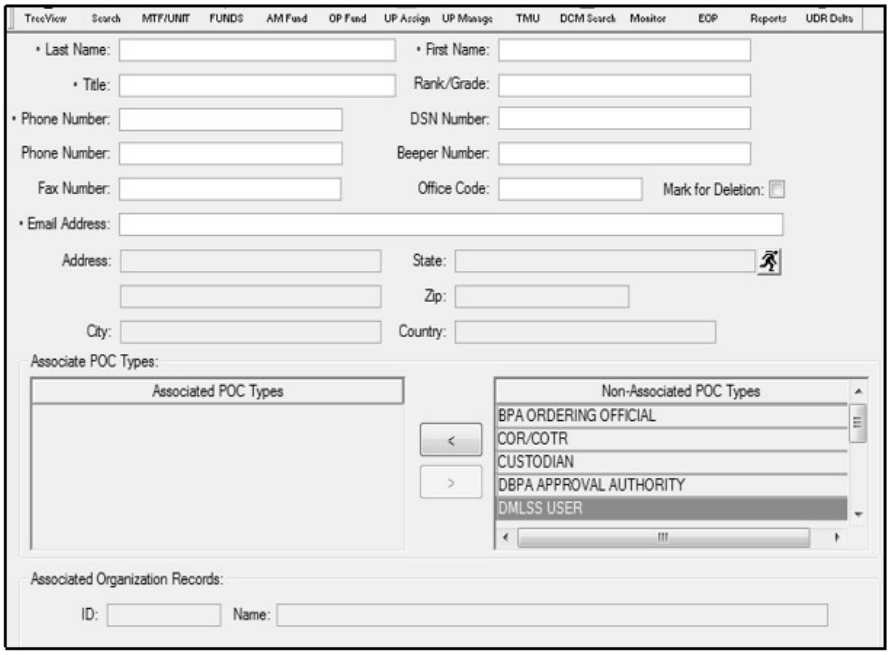


Figure 36. Point of Contact Detail Update–(New) Window

(3) Use the < and > to associate and/or disassociate the types of services the POC is assigned to perform. Most custodians and customers should be assigned Custodian and DMLSS User POC types. Users may be assigned multiple POC types. Some of the common types are:

(a) EM Service: Associate this POC type to the assigned accountable equipment property officer.

(b) FM–Assign to the facility manager.

(c) Maintenance Staff–Associate to all maintenance personnel.

(d) Custodian–Associate this type to all assigned equipment and supply custodians.

(e) DMLSS User–Associate this POC type to routine DMLSS users.

o. UP Assignment

(1) A user's access to DMLSS is determined by the applications and roles privileges assigned to their User ID. The roles assigned to users grant and/or restrict access to certain modules and functions within the system and ultimately protect the DB from unauthorized access. In the UP Assign window, an authorized user can assign one or more applications and/or roles to another user. Only those with Security Manager roles are authorized to access UP Assign and grant privileges to other users. Normally, this is assigned to the designated SA. The SA should have a basic knowledge about what each role performs before assigning a role to a user. See Figure 38 for a complete table of standard roles, descriptions, and general application rules.

(2) Select User Privilege (UP)-Assignment from the Navigate menu or select the UP Assign on the horizontal toolbar to open the UP—Assignment window (Figure 37). The window is divided into the following sections:

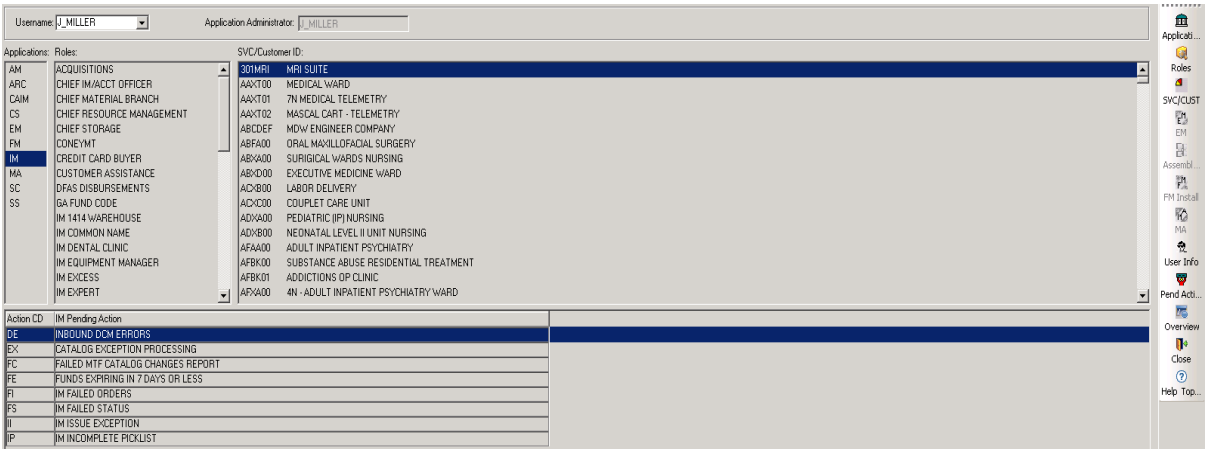


Figure 37. User Privilege–Assignment Window

(a) Username. Select a name from a list of users stored in the DMLSS server. This is the User ID of the person being assigned privileges.

(b) Application Administrator. This is the login name of the person who was assigned with Application Security Manager rights for the selected module. This field cannot be changed.

(c) Applications. These are the applications assigned to the selected user.

(d) Roles. Roles are assigned for each application and identify which tables and functions a user has access to within the application. A centrally managed set of generic roles are available for use; however, locally managed roles can be developed to meet more specific business practices.

(e) Assemblages/SVC/CUST/MA. The selected application determines what information is shown in this field. Assign SVC/CUST IDs in applicable applications. For AM, assigned assemblages are displayed and in MA the primary MA is shown. Note: This area is blank for new users unless they are an SA.

(3) To assign applications to a user, select a username and select Applications on the vertical toolbar. Associate applications to the user by selecting the application(s) and selecting the < icon between the window boxes. To select all applications, select the <<" icon. If an application needs to be disassociated, highlight the application in the associated box and select the >. Save the changes.

(4) Next, assign roles to a user by selecting an application and selecting the Roles. Roles are selected by application. Associate role(s) to users by selecting the role(s) and selecting the < between the window boxes. Select the << to assign all available roles. To disassociate a role(s), highlight the role in the associated box and select the >. Use the >> to disassociate all roles. Save the changes.

(5) Associate SVC/CUST, Assemblage(s), EM, FM, and MA activities. In addition to adding and user's roles, users must also be privileged to access certain SVC/CUSTs and Assemblage(s). If a user is granted roles in EM, FM, and/or MA, the user is required to be assigned to the corresponding activity.

(a) SVC/CUST can only be assigned via the CAIM, Customer Support, or IM modules. To do so, select the SVC/CUST icon on the vertical toolbar. Associate SVC/CUST to the user by selecting the SVC/CUST and selecting the < between the window boxes. To assign all SVC/CUSTs select the <<. Use the > and >> to disassociate SVC/CUST as needed. Save all changes. Custodians/customers may have access to their own customer ID(s), while MEDLOG personnel may have access to all customer IDs if determined in local business practices.

(b) Assemblages can only be assigned within the AM application. To assign assemblages to a new user, select Assemblage located on the vertical toolbar. Select the assemblages being assigned to the user and select the < between the window boxes. To select all assemblages, select the <<. Use the > or >> to disassociate assemblage(s) when necessary. Changes must be saved prior to being applied. Only MEDLOG personnel should be granted access to LOG owned assemblages. Some custodians require access to customer-owned assemblages assigned to their SVC/CUST. Some users may be authorized viewing privileges if determined in local business practices.

(c) To associate an EM activity to a user, highlight EM in the Application window. Select the EM icon located on the vertical toolbar. Use the < to associate the appropriate EM activity and save changes.

(d) To associate a FM activity to a user, highlight FM in the Application window. Select the FM icon located on the vertical toolbar. Use the < to associate the appropriate FM activity and save changes.

(e) To assign a MA to a user, highlight MA in the Application window. Select MA located on the vertical toolbar. Use the < to associate the appropriate MA and save changes.

(6) Associated Pending Actions. In addition to assigning roles, particular AM, CAIM, or IM pending action messages can be associated in the Pending Action window. This way, for example, the user who is responsible for receipts can automatically get any receipts to related pending action messages in their inbox, while a user who has nothing to do with receipts, never sees these pending actions. To manage pending actions, select the Pend Action selection on the vertical toolbar. Associate pending actions to users by selecting the desired pending action and selecting the <, or the << to assign all available pending actions. To disassociate pending actions, highlight the role in the associated box and select the >. Use the >> to disassociate all pending actions. Save all changes.

(7) Changes to roles and privileges are updated upon selecting Close to exit the UP Assign module. If users are logged on when the changes are made, they must exit DMLSS and log back into the application to gain access to new changes.

(8) Overview. Within UP Assign, the Overview located on the vertical toolbar provides a way to preview or print a list of users granted privileges to specific applications, roles within specific applications, associated SVC/CUST, assemblages, or Maintenance Activities. This list is helpful when determining and updating UPs.

(9) User Information. By selecting the User Information icon located on the vertical toolbar, the SA can view the user information associated to the User ID identified in the Username box.

(a) All fields of the user information box require input. Users should ensure they complete all fields with accurate information. The address fields are not mandatory but are provided for customers that may be geographically separated from the MTF. The address information is helpful when delivering supplies and equipment or when mailing items.

(b) Both the User and Address Information fields should reflect the most current information. The SA should periodically review DMLSS users to validate their need to access the system and to verify their user information is accurate.

p. UPs–Management

(1) Roles within each DMLSS application can be created or deleted, and existing roles may be modified by changing the attributes of the resources of that role. The User Privilege–Management function is used to view, add, modify, and/or delete roles by application. Only SAs and application security managers can gain access to the User Privilege–Management window.

(2) To access the UP–Management window (Figure 38), select User Privilege–Management from the Navigate menu or select the UP Manage located on the horizontal toolbar. The window has three sections:

(a) Applications. These are the different applications associated with DMLSS. Each application has assigned roles, which in turn have resources assigned to them.

(b) Roles. Roles are parts of an application that structure what a user may do within a specific application.

(c) Resource. The smallest piece of an application. Each resource defines how the user can perform a specific task within a role. A resource includes four elements in its makeup: read, update, create, and delete. Resources elements contain the following attributes/privileges:

1. Read. Read is the lowest level of the resource granted to users that only allows the ability to read the information associated to a specific resource.

2. Update. Update allows users to update, change, or modify information for selected records associated to the specific resource.

3. Create. Create allows users to create new record information associated with a specific resource.

4. Delete. Delete is the highest level of resource privileges allowing users to delete selected records or information associated with a specific resource.

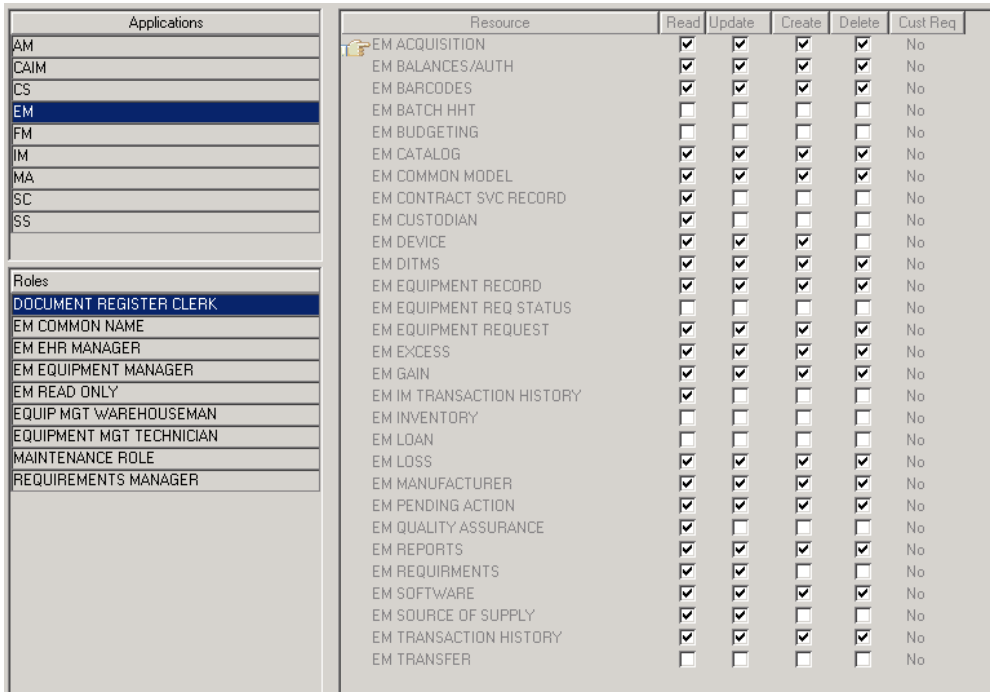


Figure 38. User Privilege–Management Window

(3) Modifying Roles. Modifications can be made to existing resource data if the data is visible and not subdued. DMLSS or centrally managed roles (roles that appear grayed out)

cannot be modified or deleted. Select an application and role to view the associated resource data. Resource privileges can be given or taken away to the read, update, create, or delete fields as necessary. The following rules apply when resources are assigned to a role:

(a) Delete is the highest-level privilege and read is the lowest. The order of precedence is delete, create, update, and then read. When a privilege is selected for a resource, all the lower privileges are automatically selected. For example, if update for a resource is selected, read is automatically selected.

(b) The last column in the table, Customer Required (Cust Req), is assigned Yes or No indicating whether or not SVC/CUSTs must be assigned in order to use that role.

(4) Adding Roles. In some cases, the resources assigned to a role may not accommodate local business practices. Therefore, an option is available to add roles and resources to different applications.

(a) Add a role by selecting the Add Role located on the vertical toolbar within the User Privilege–Management window. The Add Role window opens. Enter the new role name and select the resource elements and privileges to be associated to the role.

(b) Remember that privileges are a high-low assigning process. If delete privileges are to be given to a user, the system also assigns create, update, and read privileges to the resource. If update is selected, the system assigns read privileges to the resource.

(c) Select Save to move the new role to the Roles box in the User Privilege–Management window.

(5) Deleting Roles. Roles that are no longer required can be deleted by selecting the role and selecting Delete Role located on the vertical toolbar. Centrally managed roles cannot be deleted. In addition, locally developed roles must be disassociated from all users before being deleted.

(6) Auditing. The Auditing function provides the ability to check which users were in the system, when they were in, how long they were in, and/or problems associated with connecting. It can also be used to track which applications a user accessed, when they were accessed, and for how long they were accessed. Select Auditing located on the vertical toolbar to access the Application Auditing window. Administrators can search by username, application, activity, or host name. When the search completes, the username, date/time, application, activity, description, and host name are displayed in the Application Auditing window.

q. TMU

(1) TMU provides a centralized listing of all the values and codes used throughout DMLSS applications. Use TMU to view, add, or delete data elements that appear in the different applications. To view tables in TMU, users must have the appropriate TMU resource(s) assigned to their User ID. These privileges are assigned using the UP Assign function.

(2) At each DRO, one or more individuals should be assigned to manage these tables. Before being assigned this task, the individual should have some basic knowledge of MEDLOG data elements and codes including DLA and military specific codes, such as advice codes and device codes.

(3) There are three types of tables viewable in this window:

(a) DMLSS Wide (Centralized). These tables are not editable since the information must remain common across all DROs.

(b) DMLSS and Site Managed. Some of the data in these tables vary depending on the site. The table contains common information (centralized) for all DROs; however, users can edit, add, and delete local (decentralized) information based on their common business practices and terminology.

(c) Site Data. These decentralized tables contain data unique to the local DRO, and they are completely editable.

(4) To view or modify a TMU table, first select an application from the Application dropdown menu and then select a table from the list. The table type is displayed for each table; DMLSS Wide, Site Data, or DMLSS & Site Managed. Table information that cannot be modified is displayed with a gray background. Upon saving changes, the new data is included in the table and is visible in the application fields.

(5) When updating tables within TMU, the following guidelines are applicable:

(a) The Currency Code table/SS application. Changes made on the currency code table in TMU are audited by the system.

(b) The Document Number Configuration table. The following guidelines apply to the CAIM Document Number Configuration table in the TMU application:

1. All data entered, with the exception of fund numbers, must consist of four numeric digits. If the number entered has less than four digits, the system automatically adds zeros to make a four-digit number. For example, "4" is changed to "0004" and "25" is changed to "0025".

2. The pattern of an End number must match the pattern of the Start number. If one is totally numeric, the other must be also. If the Start number or End number in a fund range is alphanumeric (one letter and three numbers), the other must be as well.

3. The End number must always be larger than the Start number.

4. When the user enters a new Start number/End number range, the system checks to see whether the new value range overlaps with an existing range. If so, a message to correct the new range is displayed.

5. When a number range has not yet been used by the system, the Last Number Used and Date fields do not contain any data. These fields are protected by the system and cannot be changed by the user.

6. When the Start/End number range is changed for a grouping that contains data in the Last number and Date fields, the system determines if the Last number and the Date should be updated. If the current Last number does not fall within the new Start/End range, the Last number is set equal to the new Start number and the Date is incremented by 1 day. If the new range does encompass the current Last number, the system makes no changes to the Last number or Date field.

(c) The Registration Table in the TMU module is a list of all the computers at the MTF/DTF that have logged into DMLSS. Messages sent by the site SA from the System Administration Tool are then received on all computers listed in the table. Although this table is a Site Data type, entries may not be edited or added, rather only deleted which then prevents that computer from receiving messages. Only DMLSS can make entries. If an entry is removed and a user logs onto DMLSS from that computer, it is again added to this table. The system automatically deletes any computer that has not accessed DMLSS in 30 days.

(d) The RPIE Maintenance Procedure table located in the TMU/FM application allows users to select a maintenance procedure from the dropdown field in order to view, add, or print the steps to that procedure.

(e) The RPIE Nomenclature table found in the TMU/FM table allows users to add a new nomenclature by selecting Insert on the vertical toolbar.

r. DCM. The DCM is an automated tool within DMLSS used to transmit data to external agencies. Information flowing from the system includes requisition files, financial data, and PV Usage information. The DCM is also the conduit for receiving transmission of incoming status files, and it provides tools that allow SAs to monitor progress of these files and to troubleshoot any errors. For more information on the DCM, refer to paragraph 3. in this Enclosure.

s. EOP Process Management. Use the EOP Process Management window to view and update the EOP process schedule, Figure 39. To access, select EOP Process Management from the Navigate dropdown menu or select EOP located on the horizontal toolbar. Note: Use this information along with the EOP processing instructions found in paragraph 2. of this Enclosure to further manage the EOD, EOM, and EOFY or EOY processing cycles in DMLSS.

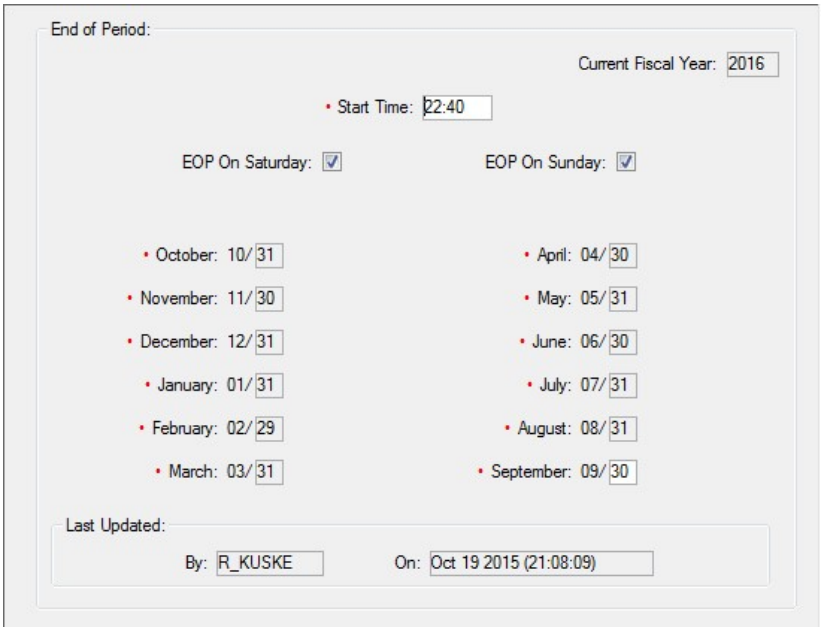


Figure 39. End-of-Period Process Management Window

(1) EOP Cycles

(a) EOD. The EOD automatically processes Monday through Friday at the designated Start Time and on Saturdays and Sundays when the EOP on Saturday and/or Sunday indicators are selected.

(b) EOM. The EOM process automatically begins once the last EOD process for that month completes successfully.

(c) EOY. The EOY process corresponds to the EOFY and runs automatically on 30 September or otherwise designated date after the EOD and EOM processes are complete.

(2) EOP Settings. The current fiscal year (CFY), process start time, EOM process date, and last update fields are displayed. Users assigned the MM Security Manager role are authorized to update data fields with a white background.

(a) CFY. Not editable.

(b) Start Time. Identifies the start time applied to all EOP cycles.

1. SAs have an option to change the start time so EOP processes begin at a more convenient time. Do not change the EOP Start Time once that time has been reached or during the EOP process. The system becomes corrupt and then requires intervention from the DHA GSC to continue normal processing.

2. Refrain from changing the time within a 30-minute window of the original start time in order to avoid potential system complications. For example, if the EOP is scheduled to start at 16:05 hrs, do not attempt to alter the start time at 15:40 hrs. Attempting to adjust the start time may result in a conflict between scheduled Command Run On (CRON) cycles. In addition, avoid setting start times that start precisely at the top of the hour, 19:00, 20:00, 21:00, etc., or on any 15-minute increment after the top of the hour, 20:15, 21:30, 22:45. DMLSS has embedded CRON cycles designed to automatically process incoming status, point of use files, etc., and encroaching on these CRON cycles leads to a potential threat of failure to launch the EOP. Adjust the start times accordingly (Example: 21:06, 22:09, etc.).

(c) EOP on Saturday/Sunday. If checked, DMLSS automatically processes an EOD on Saturday and/or Sunday at the assigned start time. As a general rule, EOPs are not processed on Saturdays and Sundays. In addition, coordinate with DLA Troop Support as PV orders and receipts could be transmitted to the DLA Business Systems Modernization system over the weekend.

(d) EOM Process Dates. The EOM process dates should always equal the last day of each calendar month to include Saturdays and Sundays. Once an EOM has processed, that field is not editable until the next FY.

(e) Last Updated. These fields identify the User ID of the user who last updated the EOP data and reflects the date and time the update was accomplished.

t. Record Management. The Record Management function is strictly used by FM personnel for setting FM records to inactive in the DB. In order to use this function, users must be assigned the SS Expert role or a customized role, usually titled one of the following: FM Related, FM TMU Inactive, or FM Inactive.

(1) Assigning inactive status to a record allows it to be separated from the active records. Thus, it is important to keep the system updated and when it becomes necessary, records should be set to inactive so that the information is maintained for historical purposes.

(2) To access the Record Management window, select Record Management from the Navigate menu or the Record Mgt on the toolbar. Select Set Inactive or Set Active from the Action window. Select the items to be activated/inactivated from the Achievable Objects section in the window. On the right side of the window, select the actual object(s) to be set active/inactive and select Process Rqst on the vertical toolbar. A message is displayed to confirm that the action was processed. If the message indicates there were problems, ensure that the process met the guidelines stated in the previous paragraphs.

(3) Data meets specific guidelines before being set to inactive. DMLSS displays a message stating what to do before the inactive command can be processed. The following object types and rules apply to the inactivating and activating of FM objects:

(a) Facility. DMLSS checks for active work requests, PROJs, and FM requirements that have a relationship with the specified facility. If a relationship exists with any of these, the

system displays a warning prompt identifying the type and number of relationships that exist. Any active rooms and RPIE that a facility may have are automatically be set to inactive along with the facility.

(b) Installation. All associated facilities should already be set inactive.

(c) Maintenance Procedure. The linked Preventive Maintenance schedule, if any, must have a valid end date; there must not be any scheduled work in the Work Projected table. When set inactive, all related schedules are deleted.

(d) Organization. Organizations cannot be referenced in/on any active installations, facilities, POCs, specialty shops, RPIE, Preventative Maintenance schedules, work requests, PROJs, Regulatory Compliance (RC) requirements, or FM requirements.

(e) Points of Contact. POCs cannot be referenced in/on any active installations, facilities, specialty shops, RPIE, work requests, PROJs, or RM requirements.

(f) PROJ. All associated work requests are also to be set to inactive.

(g) RC Procedure. Only those RC procedures, which are not being utilized, are allowed to be set inactive.

(h) RC/The Joint Commission on Accreditation of Healthcare Organizations. The RC requirement must have a valid end date and there must not be any scheduled work in the Work Projected table.

(i) RPIE cannot be a parent to any child RPIE or have active work requests or PROJs. If it is a parent RPIE, first set the child to inactive.

(j) Requirement. A requirement must have the status of closed or canceled in order to be set inactive.

(k) Room. All associated work requests, RPIE, and PROJs must already be set inactive and the room must not be linked to a drawing.

(l) Work Request. A work request must have the status of closed or canceled in order to be set inactive. It cannot be associated with an active PROJ. Work requests that are associated to open PROJs do not appear in the list. Associated closed PROJs are not set inactive with the work requests.

(4) When a record is set to inactive, it no longer appears in query results or other lists within the FM application. Exceptions: Users can search inactive records in the Work Request module, and inactive objects may be viewed using a Business Objects query as long as they are not excluded. Inactive records may also be set back to active, so they can be accessed through the FM application and updated, if needed.

u. Change EXP Center. Within DMLSS, a customer's catalog records including item locations are associated to the EXP center similarly to the way the catalog records are associated to the SVC/CUST. Use the Change EXP Center function to process a mass update to EXP center record associations, rather than processing one at a time. The process is similar to associating/disassociating EXP centers under the SVC/CUST window.

v. Assign Customer to SOS. This window is used to associate a SOS with multiple SVC/CUST accounts en masse. Associating a SOS to a customer authorizes that customer to bypass LOG and place orders directly to the SOS.

w. Assign Customers to User IDs. Use this option to associate or disassociate an SVC/CUST to users en masse. This function is helpful when a new SVC/CUST is established, and the SA needs to simultaneously assign that new customer to multiple users.

x. Assign Role to User IDs. This mass update feature allows administrators to simultaneously associate or disassociate a single role to or from multiple users. This function may be beneficial when new system roles are added to DMLSS as a result of a software upgrade.

y. Assign Assemblages to User IDs. Use this option to associate or disassociate War Reserve Materiel assemblages to users en masse. This option is useful when newly assigned assemblages have been gained into DMLSS and multiple users require privileges to those assemblages.

z. Standard Reports. The SS application contains several canned reports available for managing operating funds and AM funds as well as monitoring and managing system user accounts.

4. DCM. The DCM in SS is an automatic tool used to transmit a myriad of data including orders and financial files. It also has tools that allow the user to monitor progress and troubleshoot any errors as needed. The DCM Monitor window can be used to see only the most recent status for each transaction; then, if there is some error or delay in the process, DCM Search can be used to view the item's progress. An item can also be resubmitted through processing stages that were not completed.

a. DLA Transaction Services. DMLSS primary connection method is via the DLA Transaction Services value-added network. DLA Transaction Services is responsible for the receiving, editing, validating, and routing of logistic transactions; performing as the DoD electronic commerce processing point; and maintaining a history of all transactions routed through their system. It has the ability to receive and transmit LOG data across various networks, supporting numerous protocols and formats. The DLA Transaction Services customer base is extremely diverse, and supports not only the DoD but also civilian activities, with links to commercial activities as well. All interfaces are protected through their firewall. DLA Transaction Services has two processing sites located in Tracy, California, and Dayton, Ohio. They forward transactions to the DLA Troop Support for PV payments, to Defense Finance and Accounting System (DFAS) for non-PV payments, and to other agencies which include the

General Services Administration (GSA), Theatre Enterprise Wide Logistics Systems, and other DMLSS systems.

b. DCM EDI Transactions. Files are transferred to and from the DCM module using EDI transactions. This communication method establishes formatting standards, so data can be exchanged between the sender and receiver.

(1) Table 1 is a short list of the top EDI transaction sets that pass through the DCM.

Table 1. Common Electronic Data Interchange Transaction Sets

EDI File	Description	DCM Retention Period
511R	This file is used to pass requisitions to DLA and GSA-type vendors.511R replaces MILSTRIP document identifier code A0A and A01 transaction sets.	60 days
527R	This file is used to acknowledge receipt of materiel from Prime Vendor (PV), DLA, Electronic Catalog, and GSA. 527R replaces MILSTRIP document identifier code DRA, or Defense Receipt Acknowledgement, transaction sets.	31 days
850	This file set is used to pass DMLSS requisitions to PVs. The 850 contains both header and trailer information. DLA Troop Support looks at the Dunn & Bradstreet Serial Number information within the header record portion of the file in order to place the requisition file into the correct prime vendor's mailbox.	90 days
855	This file is a purchase order acknowledgement file provided by the PV. The vendor uses this image to pass item pricing, status code, quantity adjustment information. 855 status images post to the Status Edit Report and active due-in detail record. Posting automatically triggers the DLA Troop Support price adjudication process between DMLSS and DLA Troop Support.	90 days
856	This file is a Ship Notice/Manifest that is used primarily in DMLSS/PV ordering partnerships. The PV sends this image to DMLSS via iRAPT after the call number has been picked and packed for delivery within the PV's distribution center. Shipment status updates the LOG due-in detail record with ID status. The 856 also carries an invoice number. This invoice number resides within iRAPT and is used to finalize payment actions after the receipt is processed within DMLSS.	Varies
860	The EDI 860 is a purchase order change request that is buyer initiated. MTFs can send the PV an EDI 860 file requesting cancellation for items that have been placed on backorder (IB status).	90 days
861	The EDI 861 is a receipt file. This file has a dual role in DMLSS. During the EOD cycle, this file is generated and forwarded to DLA Troop Support. DLA Troop Support then reformats the image and forwards it to Standard Material Accounting System at DFAS for processing. The 861 contains receipt information. The 861 is also generated for PV receipts and is forwarded to iRAPT. iRAPT gathers invoicing data from the file in order to complete vendor payment actions.	Varies
865	This file is a purchase order change acknowledgement/request that is seller initiated. PVs must acknowledge requests for cancellation (EDI 860 file) with an EDI 865 file. The vendor can concur with the MTF's request and furnish QD cancellation status or deny the request and provide RC status.	90 days

(2) Example of an EDI Sequence. Certain LOG processes require a sequence of EDIs. For example, the PV ordering process involves the following EDIs:

(a) The DMLSS order file (EDI 850) transmits to the PV.

(b) The PV provides an acknowledgement file (EDI 855) containing requisition status.

(c) The EDI 855 file/status hits DMLSS. Status posts to the due-in detail(s) record.

(d) DMLSS invokes price verification action based upon status price furnished by the vendor.

(e) The PV pulls stock from Distribution Center and generates an EDI 856 file.

(f) The EDI 856 file flows through iRAPT and hits the DMLSS server.

(g) The EDI 856 file contains invoice data which updates due-in record.

(h) A DMLSS user processes the LOG receipt. Log receipt generates both an EDI 861 file to DFAS and iRAPT, as well as an EDI 527R file. The EDI 861 to iRAPT contains POC information and invoice data. The EDI 527R file is forwarded to DLA Troop Support as a receipt acknowledgement.

(i) The EDI 861 arrives at iRAPT and triggers internal reconciliation. Invoice reconciliation is then complete.

c. DCM Transaction Retention. For File retention of some DCM EDI Transaction records, see Table 1. Point of Use server files are retained for 7 days. Financial files and their status/process records are all currently retained in the system until archived. These files and the transfer status of viewed via the DCM Monitor or DCM Search.

d. Access to the DCM Search. The elevated privileges required to configure and update the DCM should be granted on a limited basis. The DCM must be configured before any transactions can occur. Use the DCM Configuration window to establish and/or edit electronic interfaces. These parameters are already set in DMLSS. If modification to any DCM information is required, a ticket should be submitted to the DHA GSC help desk at 1-800-600-9332 or dhagsc@mail.mil.

e. Access to DCM Pending Actions. Managing the success of DCM inbound/outbound files requires access to applicable IM pending actions as well as roles necessary to view and correct errors in the DCM Search.

(1) DCM Pending Actions. SAs are notified by the IM inbox when there are failed outgoing or incoming transmissions provided they have the correct pending actions assigned to them in SS, UP Assign/IM application.

(2) File transmission type pending actions include:

(a) IM Failed Orders. This pending action indicates DMLSS tried and failed five times to submit orders to an SOS.

(b) IM Failed Status. This message appears when DMLSS attempted to transmit order status to an external customer but failed.

(c) DFAS Failure. This message occurs when Step 1, DFAS, of the EOD cycle failed to complete successfully.

(d) QA File Transfer Protocol Import Failed. This message appears when DMLSS failed to import the QA file.

(e) IM QA Import Failed. This message occurs when DMLSS attempts to import the QA file and there are invalid record counts within the body of the message.

(f) Failed Financial Transactions. This message indicates the financial transactions that could not be processed.

(g) Unable to Send Transportation Request to Cargo Movement Operations System (CMOS). This message occurs after an unsuccessful attempt to transmit a Transportation Request (EDI 940R) to CMOS.

(h) Unable to Send Transportation File. This message occurs after an unsuccessful attempt to transmit a Transportation File (EDI 856/861) to CMOS.

(i) Inbound DCM and GW Errors. Inbound DCM files that contain errors do not process; however, DMLSS still maintains and tracks these erroneous transactions until they are corrected, posted, or deleted. These include all inbound records with an error code, as well as any good transactions for the same call number, until the error has been dismissed. Once the error has been dismissed, all related records are purged. Authorized DMLSS DCM users are responsible for reviewing rejected incoming files and dismissing errors.

1. Inbound DCM Errors. DCM users can view and dismiss inbound files that failed validation in the DCM for any reason. Use the related IM pending action to jump straight from the IM Inbox to reach the View/Dismiss Inbound DCM Errors window or select DCM Errors on the vertical toolbar in DCM Search.

2. Inbound GW Errors. Likewise, SAs have visibility of any inbound file that fails at the GW/point of entry for any reason, and these errors also must be reviewed and dismissed by an authorized user. DCM users can use the related pending action to jump straight from the IM Inbox to the View/Dismiss Inbound DCM Errors window or select GW Errors on the vertical toolbar in DCM Search. Inbound GW Errors can also be resolved from the System Administration tool, Manage Services/Manage DCM GW Errors.

f. Daily Review. Use IM pending actions, the DCM Monitor, and DCM Search to ensure all transaction files were successfully transmitted and received as a result of the previous day's business.

(1) Specifically, SAs should check daily to verify requisition files were sent, financial files were transmitted, incoming status files were received from the SOS, JMAR files transmitted without error, and there are no DCM or GW errors.

(2) It is good practice to verify the PV order was successfully sent, EDI 850 file, and PV status received, EDI 855 file.

g. DCM Monitor. The DCM Monitor provides the DMLSS SA a quick status view of the most current inbound and outbound transactions. To access, select DCM Monitor from the SS/Navigate dropdown menu or select Monitor located on the horizontal toolbar. The SA determines what files appear in the DCM Monitor by specifying how many days of transactions appear and how often updates are desired. The DCM Monitor lists only those files meeting the set criteria. To view the entire life cycle of a transaction, use the DCM Search window.

h. DCM Search Window. In the DCM Search window, specific transactions can be searched, and a transaction's entire life cycle viewed by status code and process code. A DCM transaction file can be viewed directly or when necessary, one or more items can be resubmitted. The DCM Search window is designed to help view all transaction status for each item.

(1) Access the DCM Search window, Figure 40, by selecting DCM Search from the horizontal toolbar or selecting this option via the Navigate menu. The DCM search window provides multiple search options to view specific search criteria or a broad range of status.

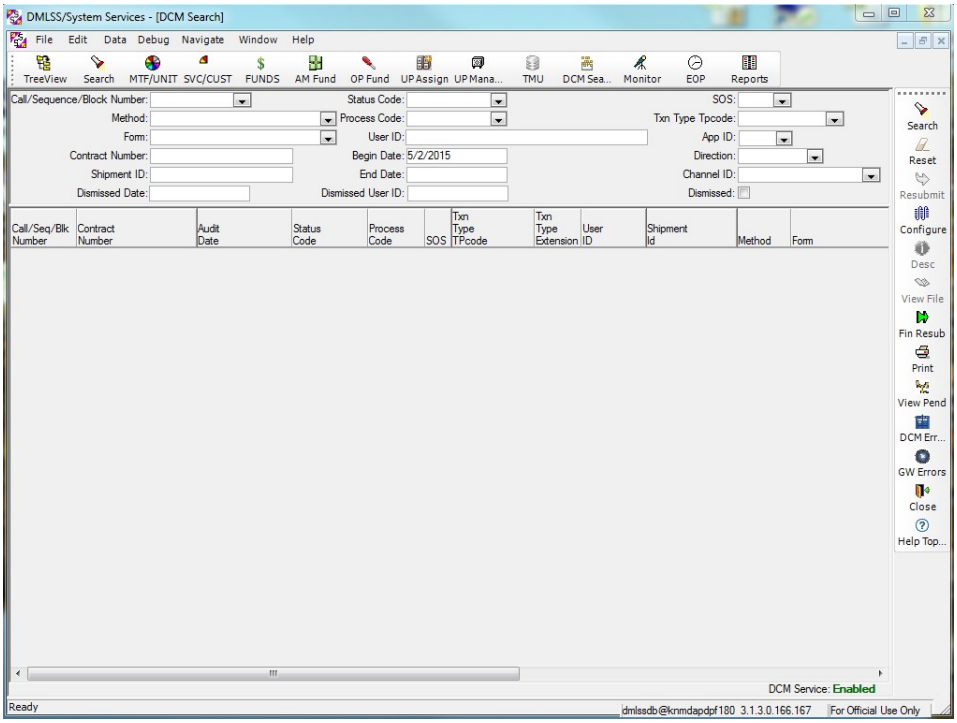


Figure 40. Defense Medical Logistics Standard Support Communications Management Search Results Window

(2) Call Number. This column contains a list of all call numbers and financial sequence numbers. Refer to Table 1.

(3) Contract Number. Used to search for transaction files associated to a specific contract number. For example:

(a) FINANCIAL-xxx refers to any of the finance files that DMLSS creates.

(b) Field Operating Agency (FOA)-REPORT refers to any of the 13 Air Force D0 reports transmitted to Air Force Medical Readiness Agency/SGMO during an EOP session.

(c) TO-JMAR represents DMLSS reports pushed to JMAR that affect the inventory.

i. DCM Status and Process Codes. In addition to the EDI file number, call, and contract number, the supervisor or the DMLSS SA must understand the DCM status and process codes.

(1) Use Table 2 to interpret these DCM status codes.

Table 2. Defense Medical Logistics Standard Support Communications Management Status Codes

DCM Status Code	Description
IN-PROCESS	Transaction is still within some stage of processing. As the transaction moves through processing, this status is reported again, but with a different process code.
TRANSMITTED	Transaction to an external source has been transmitted. This status code is reported only once for a transaction.
COMPLETE	The total life cycle of the request is complete. This status code is reported only once for a transaction.
ERROR	An error occurred in some stage of processing. The process code for that item indicates in which stage the error occurred.

(2) Process Codes/Determining Transmission Status. When searching transaction file history in DCM Search, look for three separate lines indicating the entire life cycle of the file was successful (applies to most file types). Using outbound transmissions as an example, look for (1) Process code ARCORGFL; description ARCHIVED ORIGINAL FILE; (2) Process code FMTGOOD; description FILE WAS SUCCESSFULLY FORMATTED; and (3) Process code TMTGOOD; description TRANSMISSION SUCCESSFUL. This sequence indicates the file was successfully archived, formatted, and then transmitted.

j. Identifying DCM errors. To identify formatting errors or failed transmissions, monitor the Status Code for ERROR (see Figure 40) and the corresponding process code. The process code for that item indicates in which stage the error occurred. In either case, the SA should troubleshoot problems with the local area network, interface connectivity, or an incorrect IP address, login, or password. All electronic communications activities are required to periodically update passwords, so the activity may need to be contacted and current passwords verified. The SA should track/monitor password update schedules to prevent transmission failures. Perform these additional steps when identifying DCM errors:

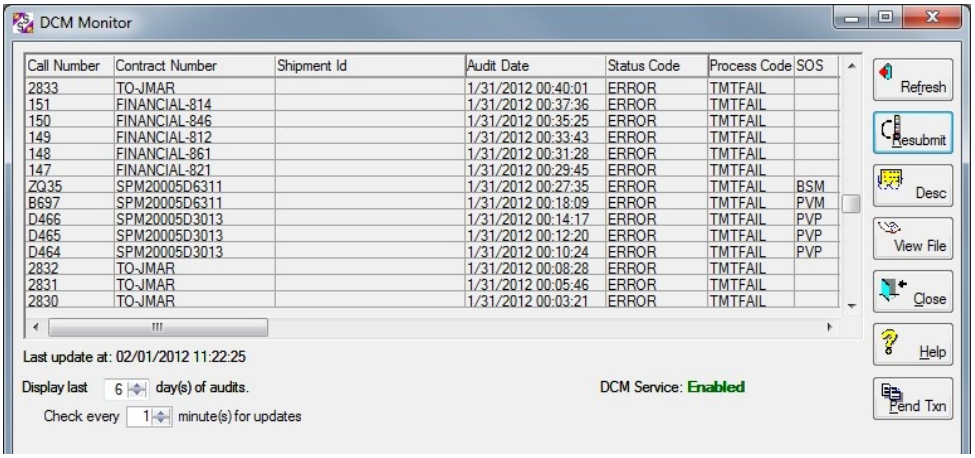


Figure 41. Defense Medical Logistics Standard Support Communications Management Monitor with Error Status Codes

(1) Review the Pending Action notifications within the IM inbox for failed transmissions.

(2) Check the System Administration Tool/Manage Services/Manage DCM Service to determine whether or not the DCM Service is disabled (see Figure 42).

(3) Scan DCM Search to determine the duration of the problem.

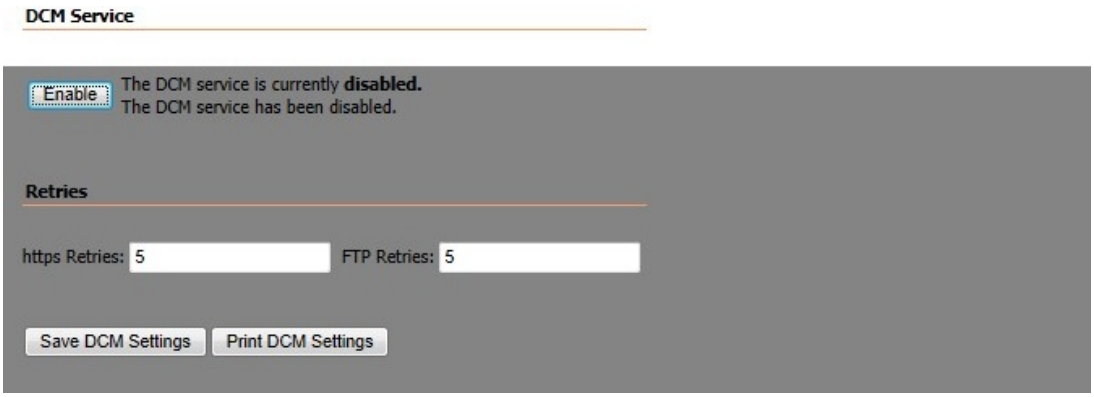


Figure 42. Systems Administration Tool, Manage Defense Medical Logistics Standard Support Communications Management Service

k. Resolving Communication Problems. If the DCM is down for an extended period of time, it is important to notify the following support activities:

(1) Assistance

(a) Medical Information Systems Communications. First, seek the assistance of Medical Information Systems. Determine if local network-related problems are causing the

errors in transmission. Also, check to see if there is power to the server and/or the server's connections to the Juniper Secure Services GW and Cisco switch are secure. Systems may contact Base Communications to assist in the effort to determine the cause of the loss of external connectivity, such as changes to routing or the firewall can interfere with connectivity.

(b) For additional assistance, contact the DHA GSC at 1-800-600-9332 or dhagsc@mail.mil.

(2) Notification. Depending on the duration of the outage, it may be necessary to inform both internal and external customers, PV representatives, and the Prime Vendor Program Manager (DHA MEDLOG).

l. Resubmit

(1) Upon notification of a failed transmissions due to connectivity issues, and as soon as DCM service is restored, the supervisor or SA should attempt to resubmit the file, see paragraph 4.o., of this Enclosure below titled, "Resubmit vs. Financial Resubmit of the Finance File" for financially related file resubmission instructions.

(2) Verify the source of the error. Select the transmission file and validate the reason the transmission erred. Review the process code action by selecting the Desc from the vertical toolbar. This code is a short description of the process code. The file can also be viewed by selecting View File on the toolbar. This opens the browser and opens the transmission data that is stored on the DMLSS server. Check the data to ensure there isn't any garbled text and that the data conforms to the standard file set-up. Close the browser to return to the search window.

(3) Resubmitting Failed Files. If the original file looks fine, and the transmission failed due to the local area network being down, or another reason not related to the IP address, login, or password, retransmit the file using Resubmit. To resubmit files, search on ERROR in the DCM Status Code to identify appropriate files.

m. Exceptions to Resubmitting Failed Files

(1) Failed Orders. Utilize the CAIM, AM, and IM Failed Orders Pending Actions (Figure 43) for retransmitting failed orders.

(2) The Financial Resubmit (Fin Resub) is used in some cases to resubmit failed financial files. Refer to paragraphs 4.n. and 4.o. of this Enclosure for additional guidance.

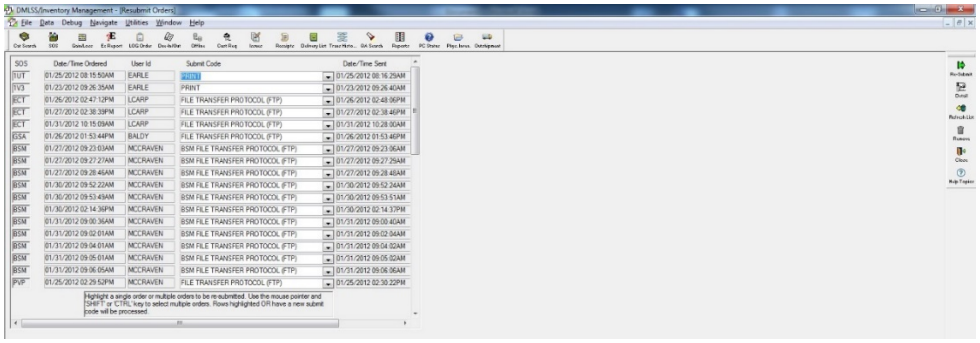


Figure 43. Failed Orders Pending Action

n. Transmitting Financial Files via the DCM. During EOP processing, the financial process is activated, and all transaction files are read. The finance transaction files are created and sent to DFAS from the DMLSS DCM module. In addition, the DCM keeps a record of all transmissions. Each interface is assigned an identification number to aid in processing these interfaces in the proper order. For example, sequence number 001 produced from the first EOD in January would be processed before sequence 002 produced from the second EOD in January. Note: Financial transaction files are retained in the system until archived. Refer to Table 1 above.

(1) DMLSS creates several finance files throughout the day. Refer to Military Service specific policy regarding the transmission of these files.

(2) The IM Inbox posts pending actions when the financial files do not transfer successfully. This can be due to a corrupt file, a failure of the proper EOD step to process, or another error. Being proactive minimizes the risk of potential funding disparities between DMLSS and supporting financial systems.

(3) Use the DCM Search function to manage the interface of DMLSS with financial systems. Specifically, use this window to check the status of files and submit/resubmit failed transmissions. To accomplish this, enter a User ID of DFAS and the previous day's date in the Begin Date Field and select Search. Review the status and process codes to verify all transaction files transmitted successfully. Status code TRANSMITTED with a process code TMTGOOD indicates the transmission was successful. To identify formatting errors or failed transmissions, monitor the Status code for ERROR and the corresponding process code TMTFAIL.

o. Resubmit vs. Financial Resubmit of the Finance File. If the transaction files did not successfully transmit, verify with the systems office that the network is up, and ports and firewalls are open. Upon verification, use the Submit or Resubmit options to retransmit the transaction files.

(1) Resubmit. If a financial file (contract number is —FINANCIAL-xxx), transfer fails due to network connectivity problems or another reason not related to the IP address, login, or password use the Resubmit option on the vertical toolbar to retransmit the existing file. DMLSS

immediately spawns a submission action through DCM and an attempt to transmit the data is accomplished within minutes.

(2) Financial Resubmit (Fin Resub). If the financial file transmission failure is due to an incorrect IP address, login, and password, use the Fin Resub function on the vertical toolbar of DCM Search, Figure 40, to rebuild the transaction file and retransmit to the supporting financial system, Figure 44. The Financial Resubmit is used in this case because the IP address, login, and password are embedded into the financial file; therefore, if any of this data changes, the file must be rebuilt. DMLSS attempts to re-transmit the failed financial files during the next scheduled EOD cycle.

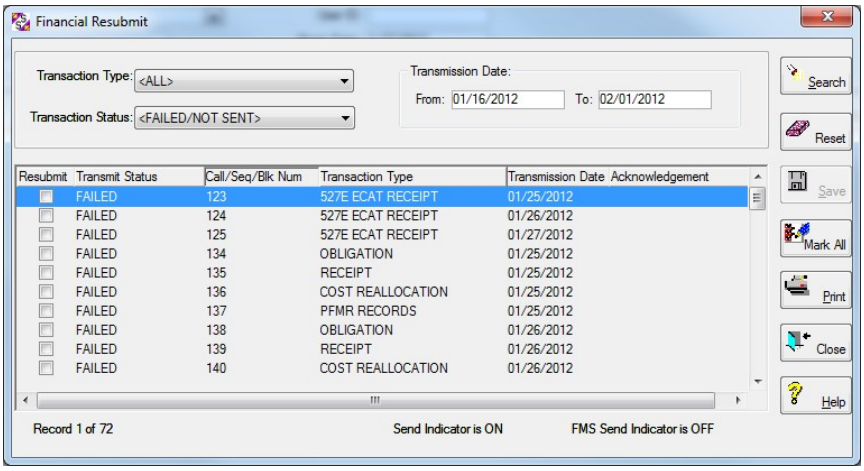


Figure 44. Defense Medical Logistics Standard Support Communications Management Financial Resubmit Window

p. Extended Downtime. If the site experiences an extended downtime, it may be necessary to transmit orders manually. Decide how many days are acceptable before invoking manual supply operations.

(1) If network connections are down for less than 24 hours, wait and utilize the IM FAILED ORDERS pending action to resubmit.

(2) If disruption lasts for greater than 24 hours then refer to DHA procedures regarding manual supply operations or Military Service policy as applicable.

(a) Perform Offline-Non-submit action on items required. Only use call numbers provided by DHA MEDLOG or Military Service MEDLOG Agency. Segregate items onto individual call numbers by delivery method, and special handling code, (for example, DRS (handling code for drop shipment) versus USE (handling code for usage item), refrigerated versus non-refrigerated.

(b) When DMLSS connectivity is restored, build the orders using the IM Offline Submit module, with the Non-Submit indicator checked.

1. Take particular care in entering each requisition in the precise sequence that it was furnished to the PVs.

2. Additionally, insert each item in the precise Contract Line Item Number sequence that it was provided to the PVs.

(c) Cancel all due-ins on the electronic order/call(s) which failed to transmit. To avoid duplication, PV calls should not be faxed to the vendor if the EDI 850 file is currently sitting as TMTFAIL.

(d) Maintain an active manual call register for PV sources.

ENCLOSURE 4

DEFENSE MEDICAL LOGISTICS STANDARD SUPPORT MILITARY MEDICAL TREATMENT FACILITY /UNIT ORGANIZATION–SERVICE AND LOGISTICS DEPARTMENT

1. SERVICE DETAIL RECORDS. Use Tree View or Search to view or edit information specific to the MM, EM, MA, and FM Service Detail records. To ensure the integrity of the organizational structure, privileges (create, update, and delete), should be tightly controlled. However, read only access is encouraged for all LOG users to facilitate better understanding of the organizational structure modules.

a. Primary Support Activities. Service detail records, MM, EM, MA, and FM, provide the necessary background data that equates to the primary support activities that must be selected when a new organization is created in the ORG Detail (New) window (Figures 45-47).

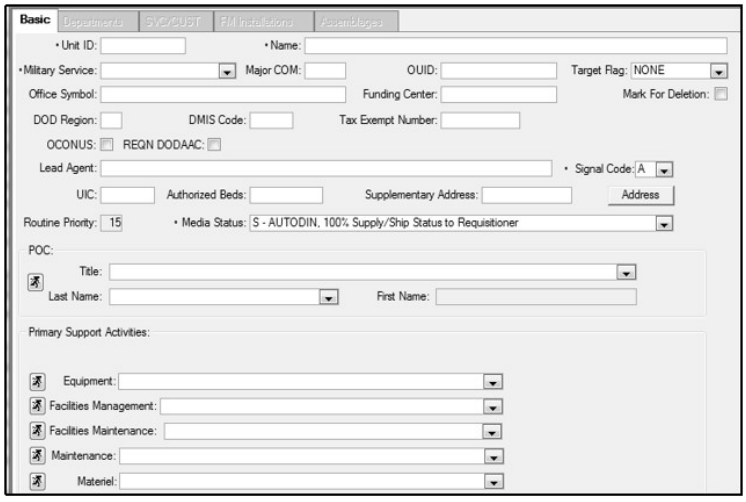


Figure 45. Military Medical Treatment Facility/Unit Detail (New)–Basic Tab Window (Air Force)

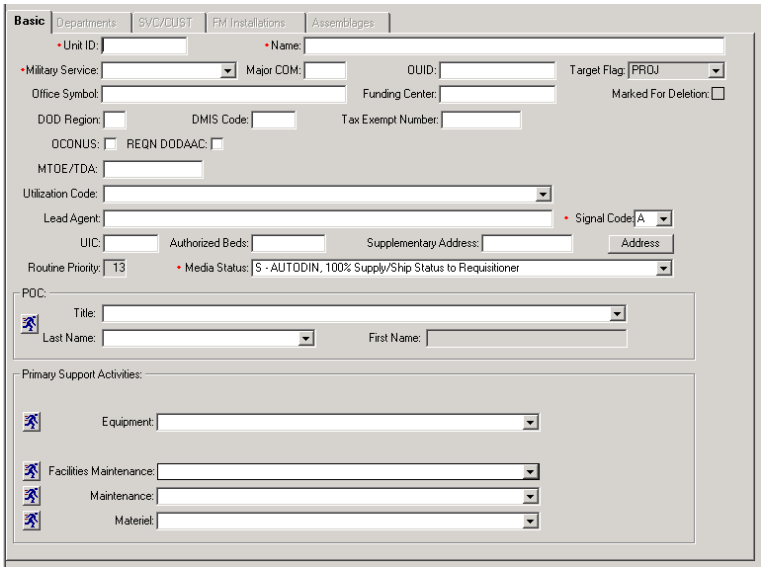


Figure 46. Medical Treatment Facility/Unit Detail (New)–Basic Tab Window (Army)

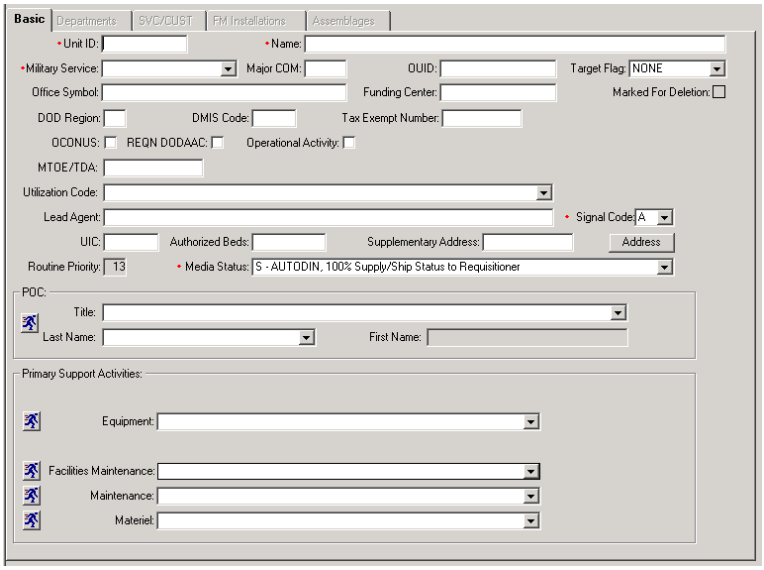


Figure 47. Medical Treatment Facility/Unit Detail (New)–Basic Tab Window (Navy)

b. MM Service Detail. Only one MM Service is authorized per DMLSS application. It was established on the DMLSS system during implementation at the site and may not be deleted. The MM Service identifies the Materiel Management Service and is always associated to the LOG MTF/Unit. This window is audited by the system. Settings on this record, especially the Appropriation Data tab (described below), critically impact the way the LOG DEPT and LOG Fund manage orders and allocate funds.

(1) In the MM Service Detail window, Materiel service information can be opened and edited. To access the MM Service detail record using the search function, select MM – Materiel

Management in the type field and select Search icon. Once retrieved, either double-click the MM Service record or highlight the record and select Detail. A link to the MM Service is also available in the Basic tab of the LOG detail record. The MM Service detail record is segmented into the Basic, Appropriation Data, and Computation tabs. Each tab contains some mandatory data fields, but not all fields require data input.

(2) MM Service Basic Tab, Figures 48-50. These data fields are present in the basic tab and should be utilized as described:

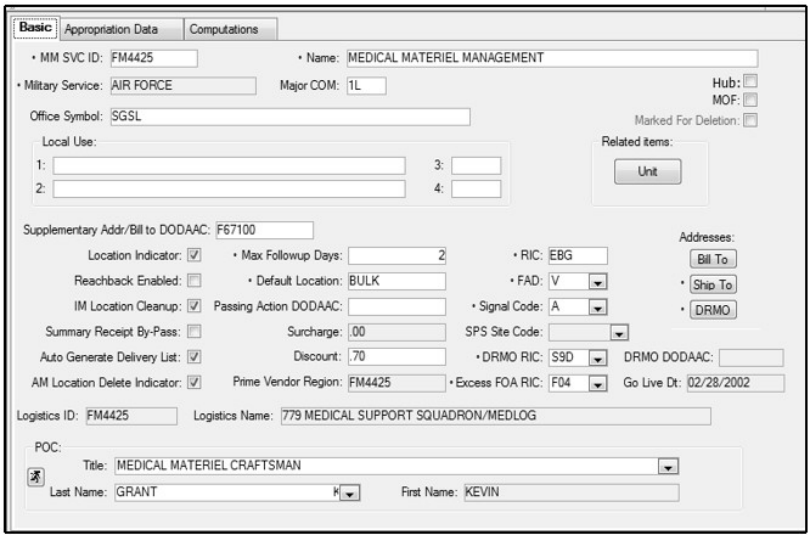


Figure 48. Materiel Management Service Detail–Basic Tab Window (Air Force)

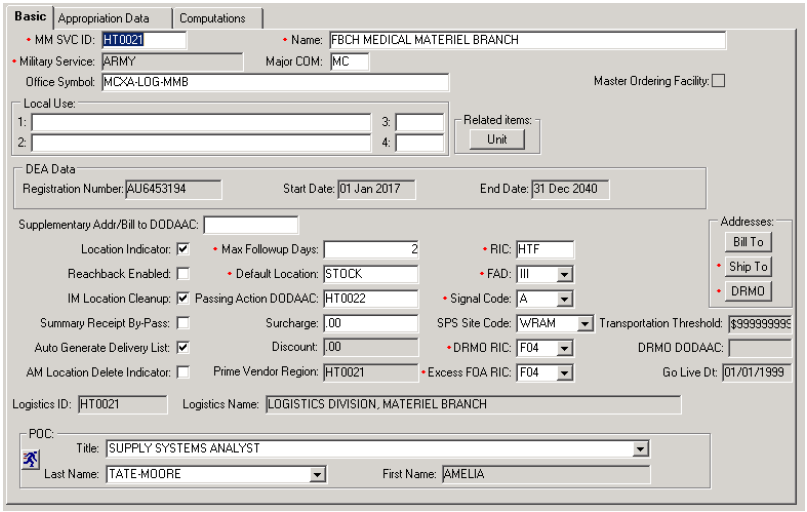


Figure 49. Materiel Management Service Detail–Basic Tab Window (Army)

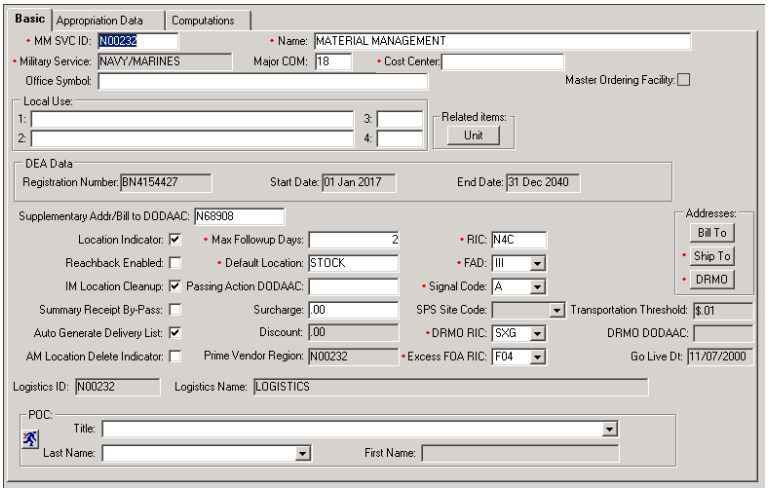


Figure 50. Materiel Management Service Detail–Basic Tab Window (Navy)

(a) MM SVC ID. This is a mandatory field, and it should always equal the LOG DEPT DoDAAC. Do not change this field without proper authorization and documentation.

(b) Name. Mandatory field should always equal "Medical Materiel Management."

(c) Military Service. Defaults to the appropriate Military Service.

(d) Major COM. Although identified as an optional field; materiel managers should load their corresponding Major Command (MAJCOM or MACOM) code.

(e) Cost Center. A Cost Center represents the work center incurring costs/charges (if required by Military Service).

(f) Hub. Hub and spoke is a capability allowing one stock fund account to place orders for another stock fund account. When selected, this box indicates the MM Service is Spoke enabled.

(g) Master Ordering Facility. This functionality allows selected accounts the ability to order from multiple PVs/Sources of Supply on behalf of a Routine Ordering Facility.

(h) Office Symbol. Optional field used to document the MM Service office symbol.

(i) Marked for Deletion. This box displays when the record has been marked for deletion.

(j) Local Use. The local use fields allow the entering of data which can later be accessed using Business Objects software.

(k) Related items. This selection opens the Related MTF/Units List window where the list of MTF/units associated with the service can be viewed or printed.

(l) Drug Enforcement Administration (DEA) Data Section

1. Registration Number. In accordance with section 1300 of Reference (n).

2. Start Date. The DEA certificate issuance date.

3. End Date. The DEA certificate expiration date.

(m) Supplementary Address/Bill to DoDAAC. Load the support DFAS DoDAAC into this field. When loaded, this DoDAAC prints to all DD Form 1155, Order for Supplies or Services, in the block 15 code field. This data is needed for entry into iRAPT (Wide Area Work Flow.

(n) Location Indicator. This checkbox identifies whether or not the MM Service Default location is used.

(o) Reachback Enabled. This indicator identifies whether or not the LOG account provides Reachback services. It should only be checked if officially tasked by DHA/MEDLOG or Military Service Logistics Agency.

(p) IM Location Cleanup. Should always be checked. Indicates location codes scheduled for deletion during the next EOD process when balances are zero.

(q) Summary Receipt By-Pass. Not used.

(r) Auto Generate Delivery List. Should always be checked. When selected DMLSS automatically generates a delivery list as part of processing a receipt or confirming a picklist.

(s) AM Location Delete Indicator. Should always be checked. When selected, this indicates that AM locations are deleted when the O/H quantity drops to zero. This action does not affect allowances.

(t) Max Follow-Up Days. Identifies the maximum number of days before follow-up transactions are sent to a supplier.

(u) Default Location. Identifies the default storage location within the MM Service, (e.g., the Warehouse).

(v) Passing Action DoDAAC. Serves as the requesting DoDAAC for customer requests when requested materiel is not O/H for host DoDAAC. For Army use only.

(w) Surcharge. Air Force and DLA Working Capital Fund sites only. Identifies the CFY surcharge rate. The surcharge rate could change annually and is provided to all sites via DHA/MEDLOG prior to each EOFY. This field does not apply to a Defense Health Program funded site.

(x) Discount. The discount field is essentially a negative surcharge rate, allowing the billed price to be less than the advertised unit of purchase price. This applies to Air Force only.

(y) PV Region. Defaults to local DoDAAC.

(z) Routing Identifier Code (RIC). RICs are assigned for processing inter/intra service/agency transactions. This is a mandatory field that identifies the RIC assigned to the MM Service. Do not change the RIC without proper authorization and documentation.

(aa) Force Activity Designator (FAD). This is a mandatory field that identifies the FAD being used by the MM Service. The FAD is associated to the Urgency of Need Designator; which, determine what priority codes are available to apply to requisitions. The FAD/Urgency of Need Designator table is available in the TMU.

(ab) Signal Code. All requisitions contain a signal code to designate the intended consignee, ship to, and the activity to receive and effect payment of bills. Always assign meaning ship to and bill to requisitioner. Signal codes are listed in the TMU.

(ac) Standard Procurement System Site Code. Not editable. Aligns to a Regional Health Command Contracting Office. Unique only to the Army.

(ad) Transportation Threshold. Field is no longer relevant.

(ae) Defense Reutilization and Marketing Office (DRMO) RIC. DRMO is a legacy office symbol/code for the office which is now DLA-Disposition Services. DRMO is still used in several DMLSS fields. Mandatory field identifies the local DRMO RIC. This RIC and the corresponding DLA-Disposition Services address are printed to all documents generated by DLA-Disposition Services turn-in actions.

(af) Excess FOA RIC. Excess FOA RIC is utilized by the Military Service for excess materiel. Should always be F04.

(ag) Addresses

1. Bill to Address (Bill to). Identifies the supporting DFAS address. This information is printed to requisition documents such as the DD Form 1155.

2. Ship To address. If at a Hub Location, enter the Ship To information for the Spoke Customer.

3. DRMO Address identifies the local DLA Disposition Services shipping address. This address is used in conjunction with the DRMO RIC and is printed to all documents generated by DLA-Disposition Services turn-in actions.

(ah) Go Live Date. Identifies the date of initial DMLSS implementation.

(ai) POC. Identifies the primary Point of Contact (POC) for the MM Service. Usually, the assigned POC is the Accountable MEDLOG Officer. When used in conjunction with POC type assignments, the POC name prints in the approving official block on requisition documents such as the DD Form 1155.

(aj) Distribution and Transportation Module. For Distribution and Transportation Module to be successful, the supplied data has to be accurate. It is imperative to verify that the DLA-Disposition Services RIC, DLA-Disposition Services DoDAAC, and DLA Disposition Service Address are the locally assigned DLA Disposition Services facility supporting the local area or base, not Headquarters, Battle Creek Michigan, RIC S9D.

(3) MM Service Appropriation Data Tab. In the MM Service Detail window–Appropriation Tab (Figures 51-53), the user can enter more specific information for a customer area, including appropriation segments. Most data fields in this tab are linked to the LOG detail record and are not editable. The few fields that are editable are explained below.

(a) Appropriation Fund Type is defined by Military Service guidance.

(b) Logistics and Customer Appropriation is defined by Military Service guidance.

(c) Premium Transportation/Appropriation Segment 1. Identifies the local premium transportation fund site. This changes each FY and should be obtained from the resource advisor.

(d) LOG Fund Target Flag. Do not use unless otherwise directed by DHA/MEDLOG.

(e) Use the Jump To icon to view/edit the LOG Fund record.

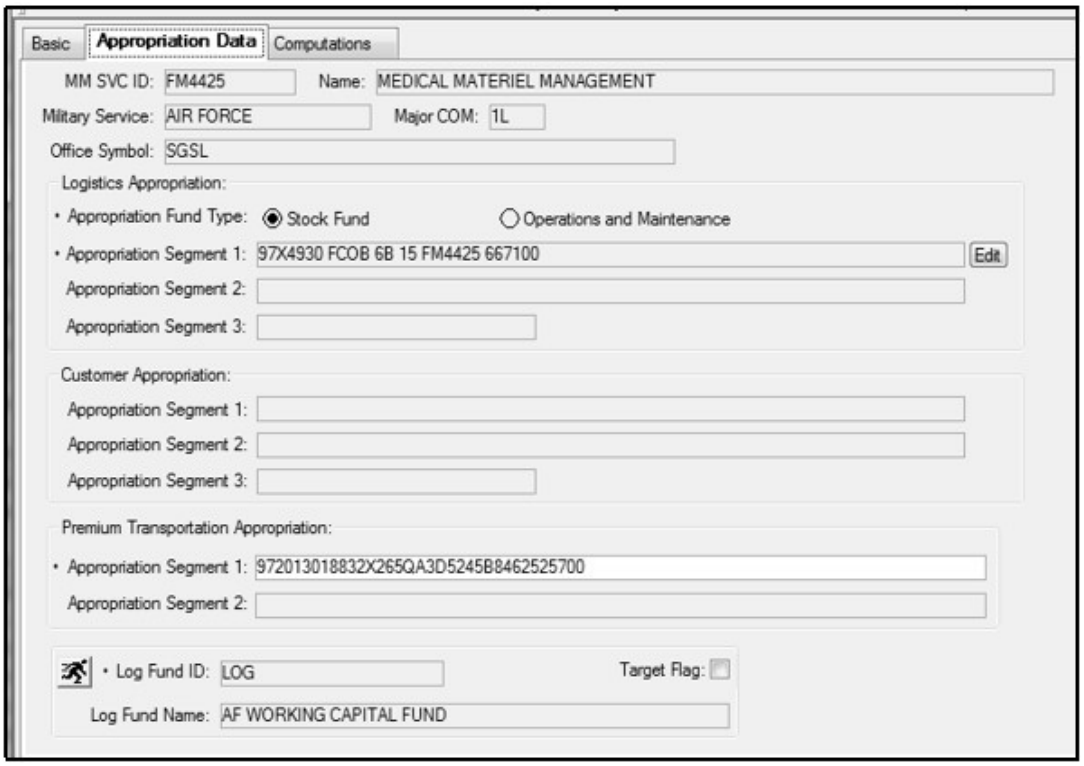


Figure 51. Materiel Management Service Detail–Appropriation Tab Window (Air Force)

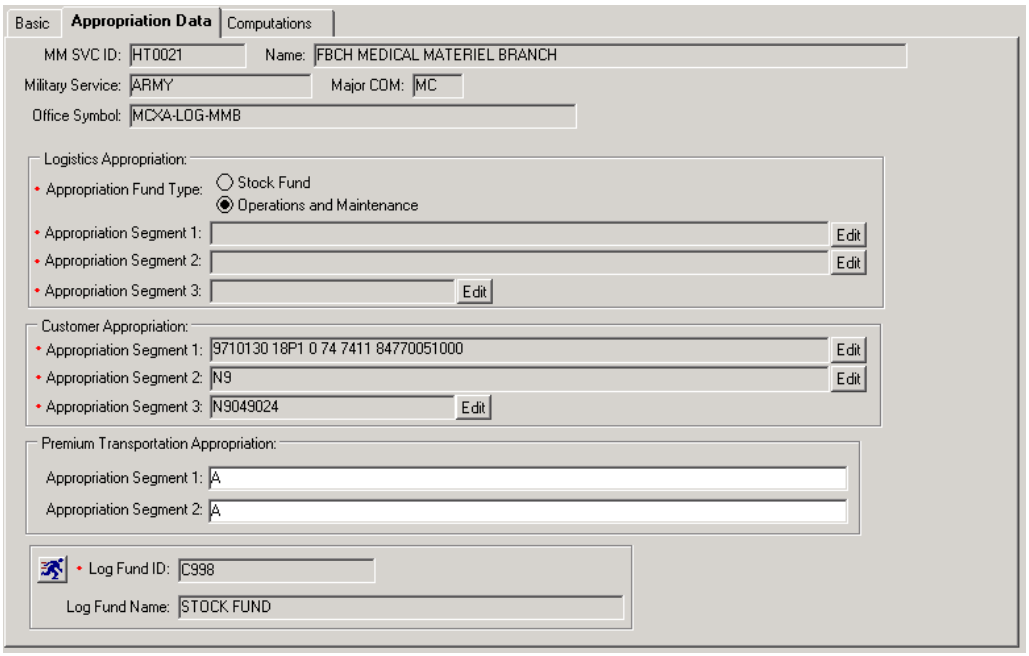


Figure 52. Materiel Management Service Detail–Appropriation Tab Window (Army)

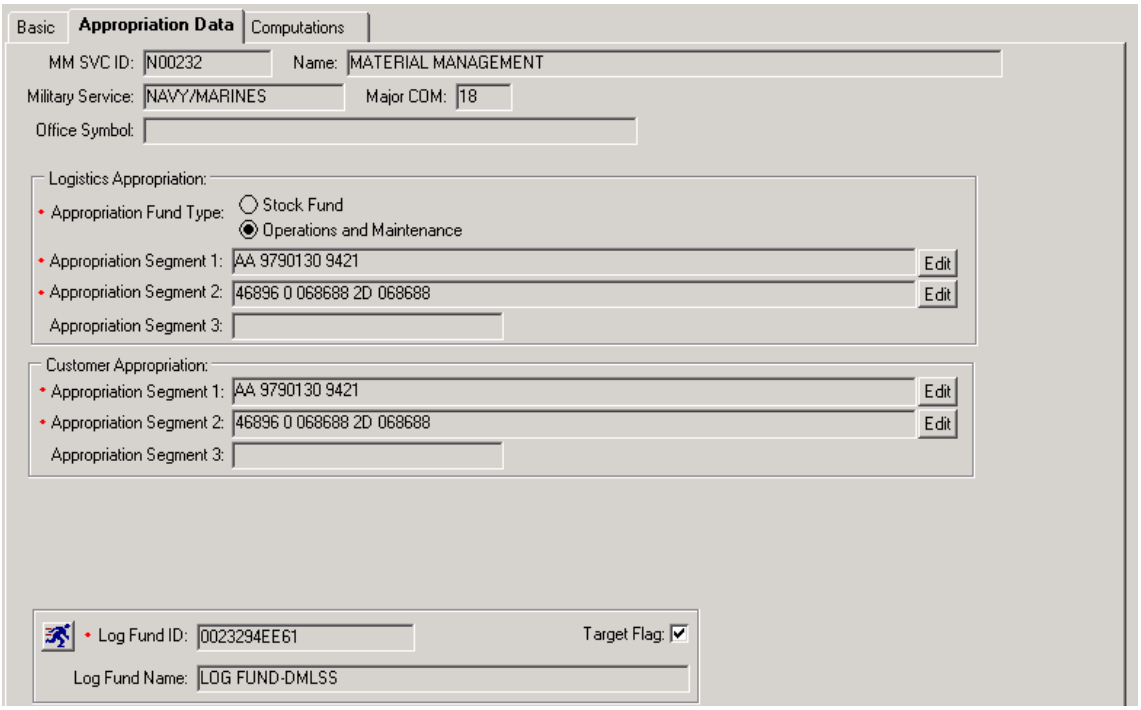


Figure 53. Materiel Management Service Detail–Appropriation Tab Window (Navy)

(4) MM Service Computations Tab. In the MM Service Detail window–Computations tab (Figures 54-56), excess computation factors can be monitored. The Major Receipt Price Change field is the only field that requires data entry. Although other fields are optional, they should not be changed.

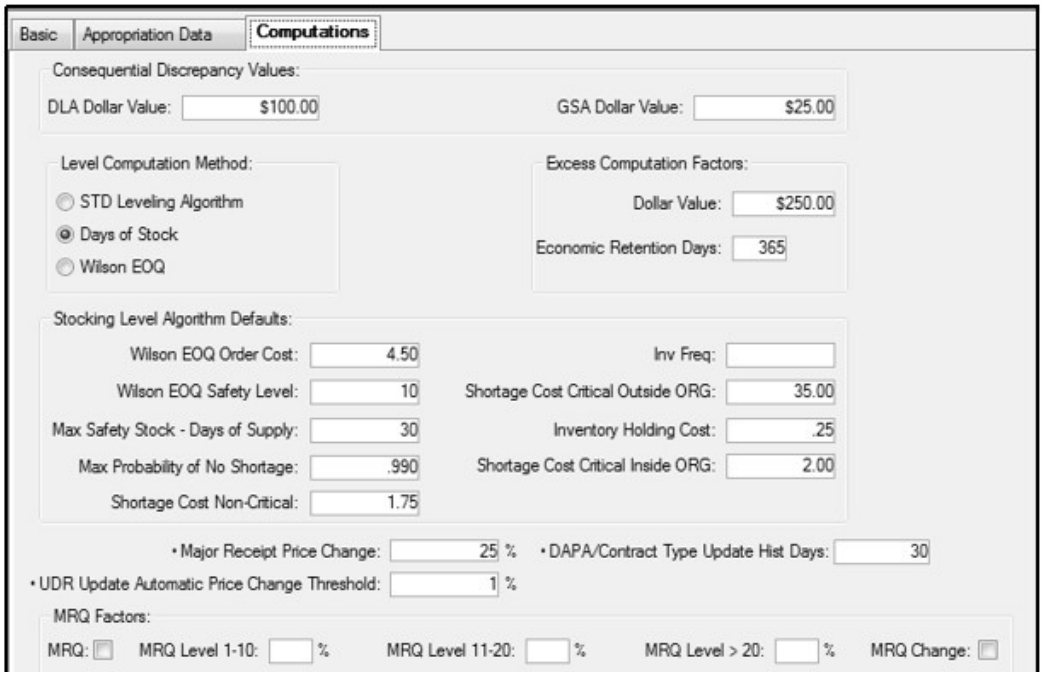


Figure 54. Materiel Management Service Detail–Computations Tab Window (Air Force)

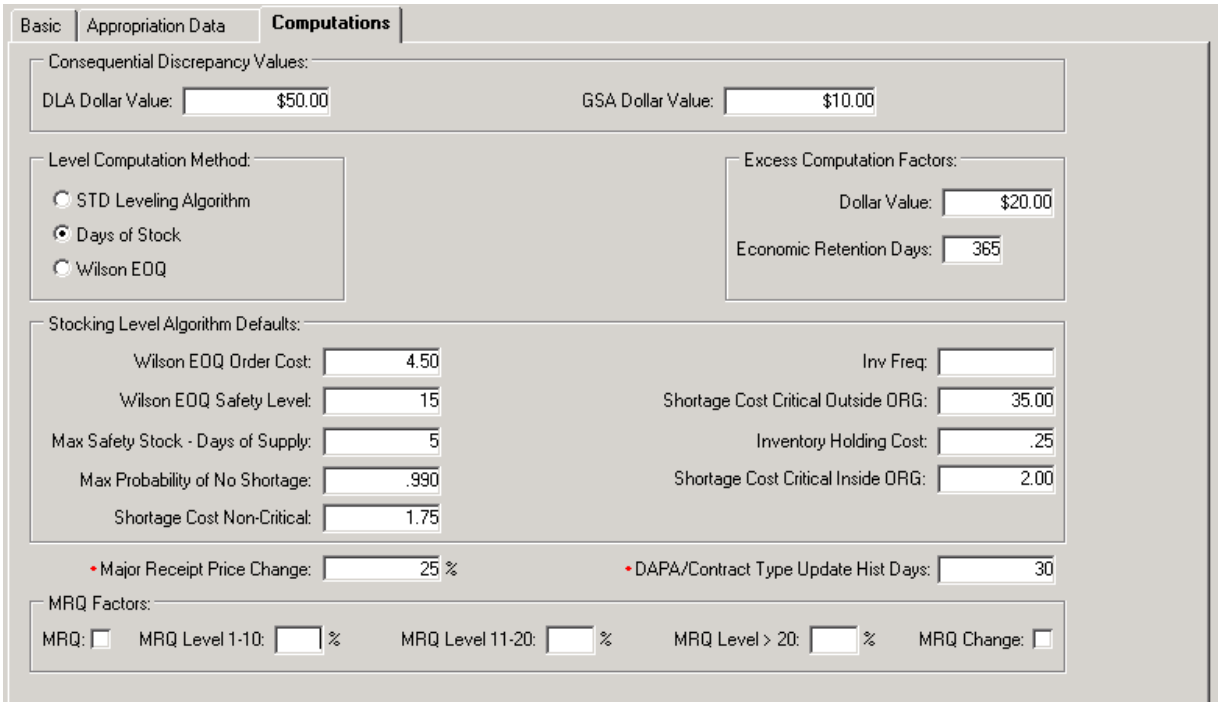


Figure 55. Materiel Management Service Detail–Computations Tab Window (Army)

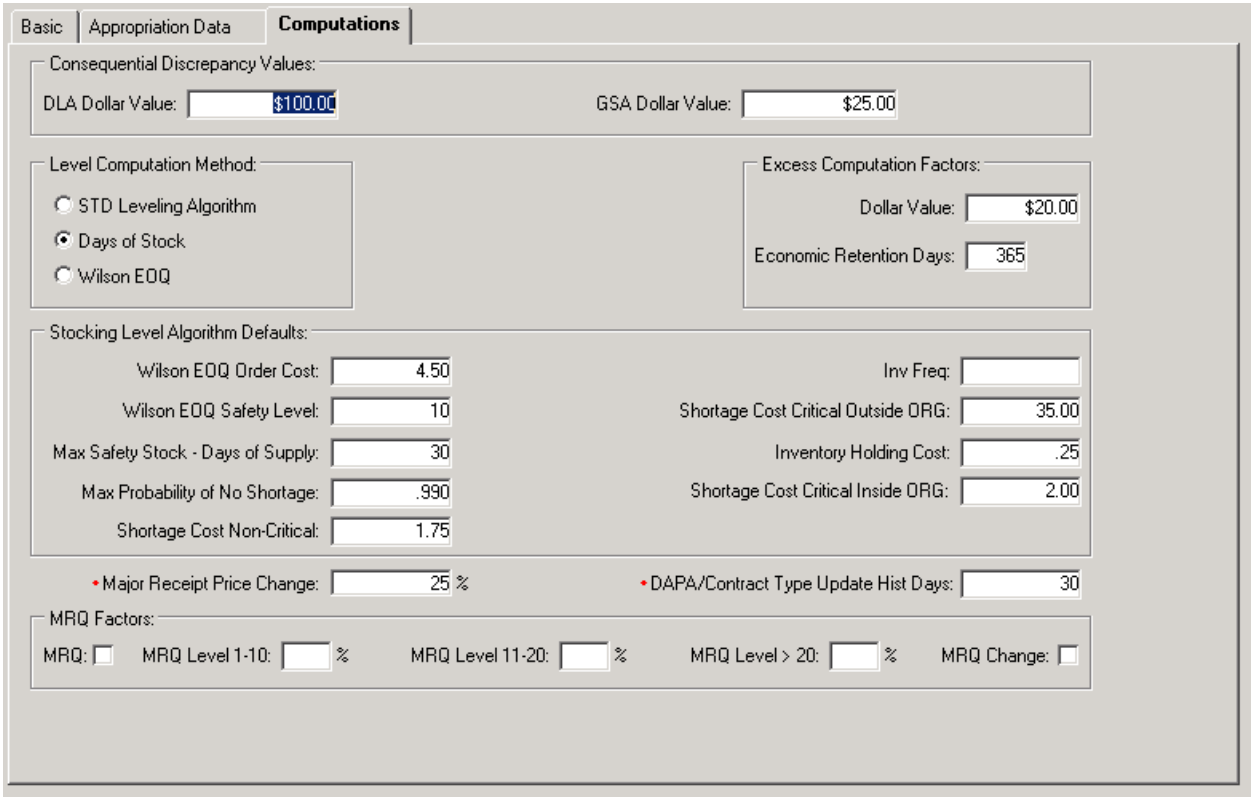


Figure 56. Materiel Management Service Detail–Computations Tab Window (Navy)

(a) Major Receipt Price Change. System defaults to 25 percent. Use this field to specify what percentage represents a significant difference between an order price and receipt price for an item. When an IM user processes a receipt and the receipt price is significantly different, (e.g., 25 percent change than the order price, a message is written to the IM Receipt Major Price Change pending action for review).

(b) Level Computation Method. Recommended to be Days of Stock.

(c) Do not change the following fields unless otherwise directed:

1. Consequential Discrepancy Values.

2. GSA Dollar Value.

3. Excess Computation Factors.

4. Stocking Level Algorithm Defaults.

5. Maximum Reorder Quantity Factors. Control factor used for inventory levels at values, do not want customers to exceed this percentage. Not recommended for Air Force use.

c. EM Service Detail. Only one Equipment Management (EM) Service is authorized per DMLSS application. It was established on the DMLSS system during implementation at the site and may not be deleted. The EM Service identifies the Medical Equipment Branch, Division, or Office and is always associated to the LOG MTF/Unit. This window is audited by the system.

(1) To access the EM Service Detail record (Figures 57-59), using the search function, select EM–Equipment Mgt in the Type field and select Search. Once retrieved, either double-click the EM Service record or highlight the record and select Detail. A link to the EM Service is also available in the Basic tab of the LOG detail record.

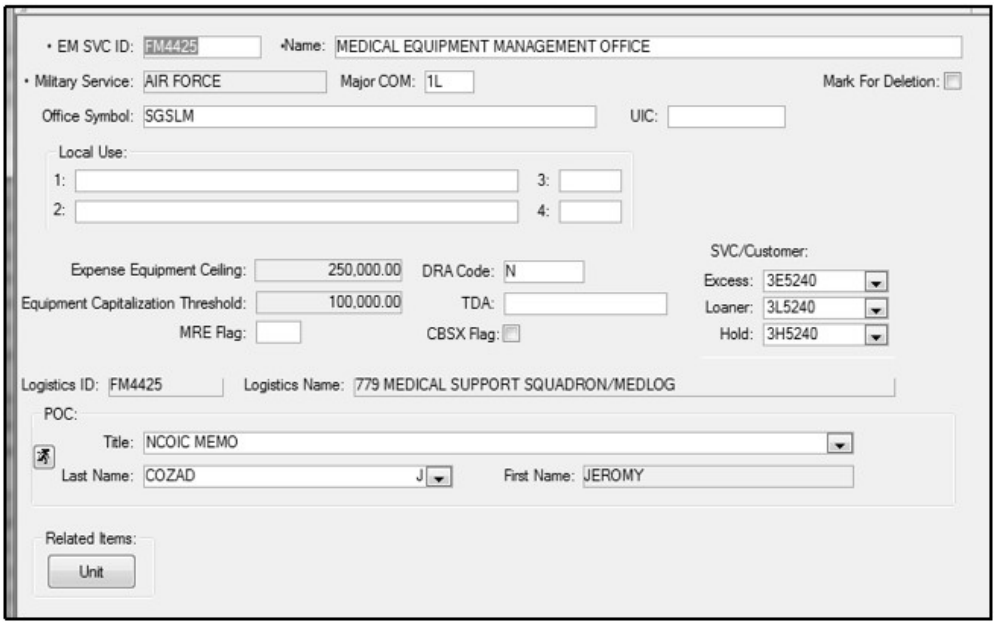


Figure 57. Equipment Management Service Detail Window (Air Force)

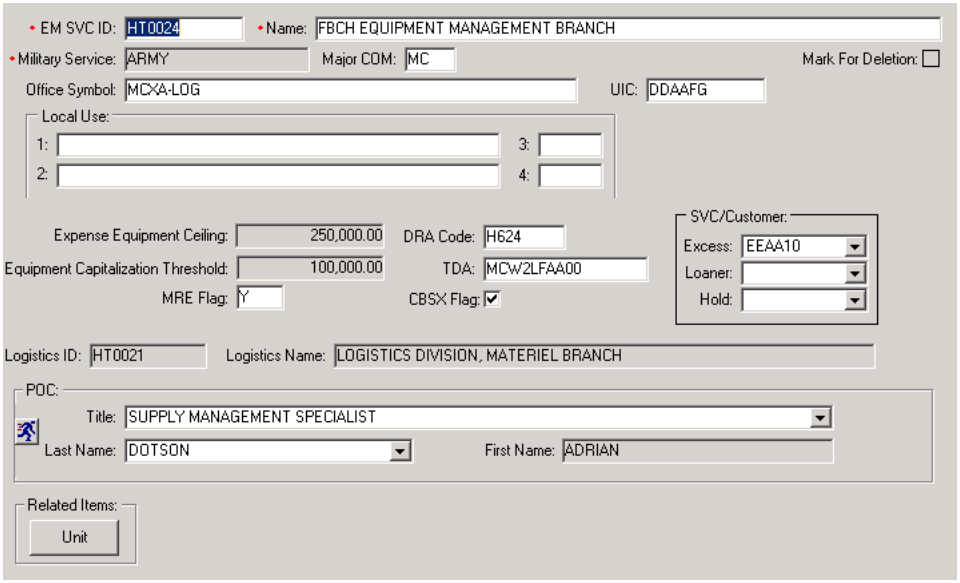


Figure 58. Equipment Management Service Detail Window (Army)

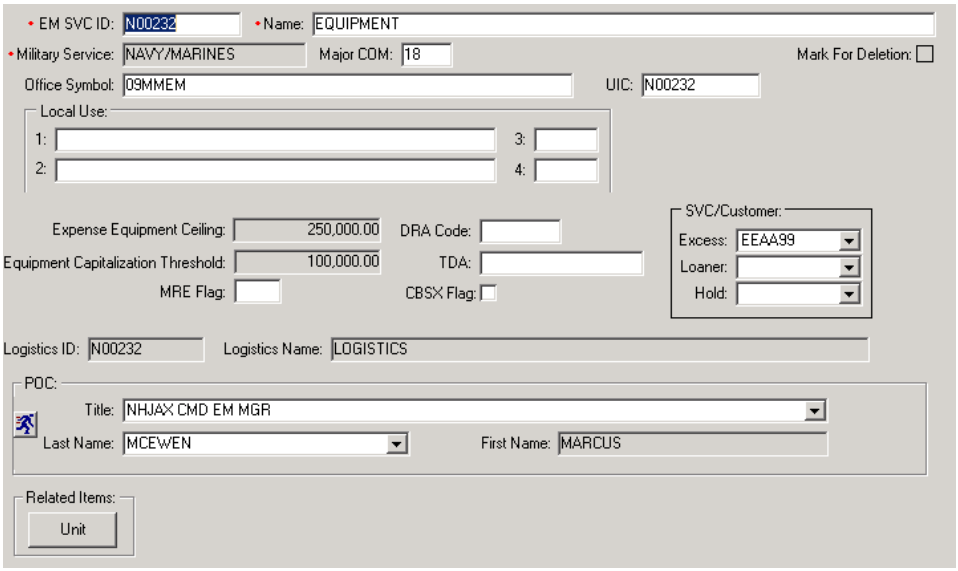


Figure 59. Equipment Management Service Detail Window (Navy)

(2) The EM Service Detail record contains several data fields; most of which should never be changed unless directed by higher authority. A few of these fields are explained below.

(a) EM SVC ID. Should always equal the LOG DoDAAC. Do not change unless directed to do so by a higher authority.

(b) Name. MTF name or Medical Equipment Branch Division or Office.

(c) Major COM. Optional field; however, materiel managers should load their corresponding MAJCOM/MACOM code.

(d) Office Symbol. Optional field used to document the EM Service office symbol.

(e) UIC. Unit Identifier Code.

(f) Mark for Deletion. Do not mark the EM Service for deletion unless it is being replaced with a new EM Service record. This action is directed by a higher authority.

(g) SVC/CUST Associations. This area sets the associations for SVC/CUST excess equipment, loaner and hold accounts.

1. Excess. The Excess Equipment field in this window can be used to specify the Service customer identification that serves as the Excess account. Then, in EM, excess records can be processed by transferring items to this Excess customer. The EM Service must be associated to an SVC/CUST record identified as the medical equipment Excess account before equipment items can be transferred and reported as excess.

2. Loaner. The EM Service must be associated to an SVC/CUST record identified as the Medical Equipment Branch, Division, or Office Loan account before equipment items can be coded as on-loan, used only by Air Force.

3. Hold. The EM Service must be associated to the SVC/CUST record identified as the one of the following: Medical Equipment Branch, Division, or Office Hold account prior to transferring equipment items to 'hold' status. This function is used by Air Force only.

(h) POC. Associate the POC record for the Medical Equipment Branch Division or Office. Within the POC detail record, this user should be associated to the POC type of EM Service.

(i) Related Items-Unit. This selection opens the Related MTF/Units List window where the list of MTF/units associated with the service can be viewed or printed.

d. MA Service Detail. An Equipment Maintenance Activity (MA) provides maintenance services for equipment owned by organizations and customers and can be both a provider and a user of services in the DMLSS system. As a service provider, it uses the following functionalities: equipment, work orders, manufacturer, and procedures. It also requires the use of the CAIM module to maintain an inventory of repair parts. In this role, it becomes a CAIM user and a customer of the MM service.

(1) The default MA service was established in DMLSS during implementation at the site and may not be deleted. MAs may exist in the host facility, as well as supported organizations, so they may or may not belong to the Logistics Activity. In addition, there may be one or more maintenance activities in each organization.

(2) The MA Service(s) identifies the Medical Equipment Branch, Division, or Office responsible for the supporting MTF/Unit ORG(s) such as LOG. Note: Within UP Assignment (UP Assign), users can be assigned to only one MA at a time; meaning, maintenance personnel can only access maintenance records for the MA associated to their User ID.

(3) Accessing an Existing MA Service record. To access the MA Service Detail record using the search function, select MA in the Type field and select Search. Once retrieved, either select the MA Service record or highlight the record and select Detail. A link to the MA Service is also available in the Basic tab of the LOG detail record. The MA Detail Record contains three tabs: Basic, Materiel, and Funding. These windows are audited by the system.

(a) Basic Tab, Figures 60-62. Most of the information in this tab does not require updating, but a few are explained below.

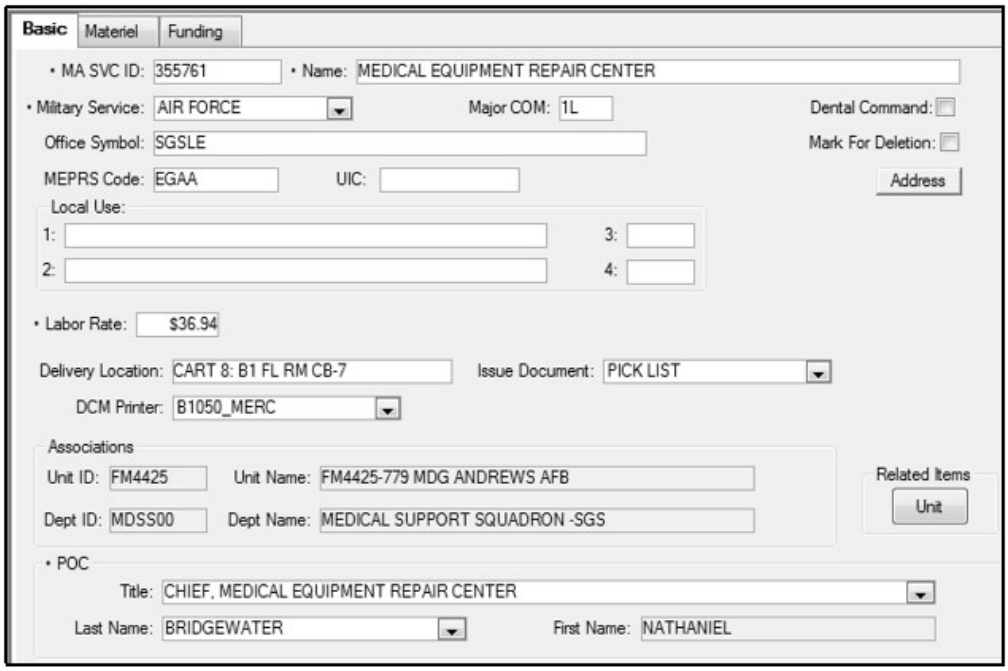


Figure 60. Equipment Maintenance Activity Service/Customer Detail Window–Basic Tab (Air Force)

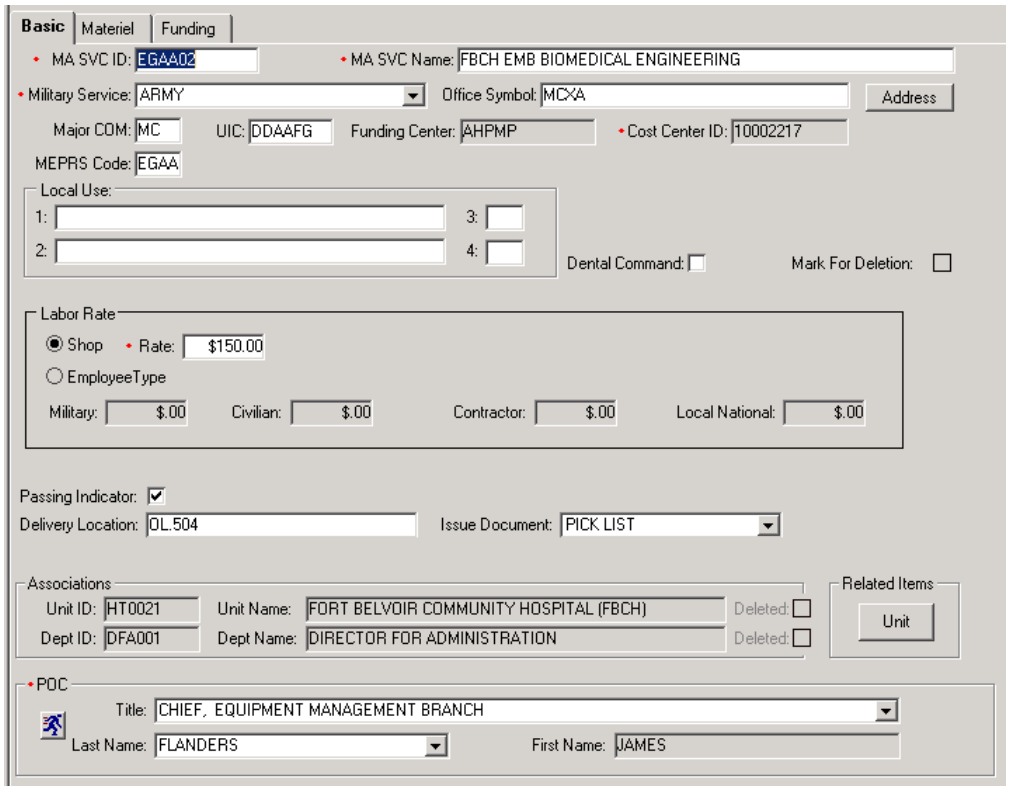


Figure 61. Equipment Maintenance Activity Service/Customer Detail Window–Basic Tab (Army)

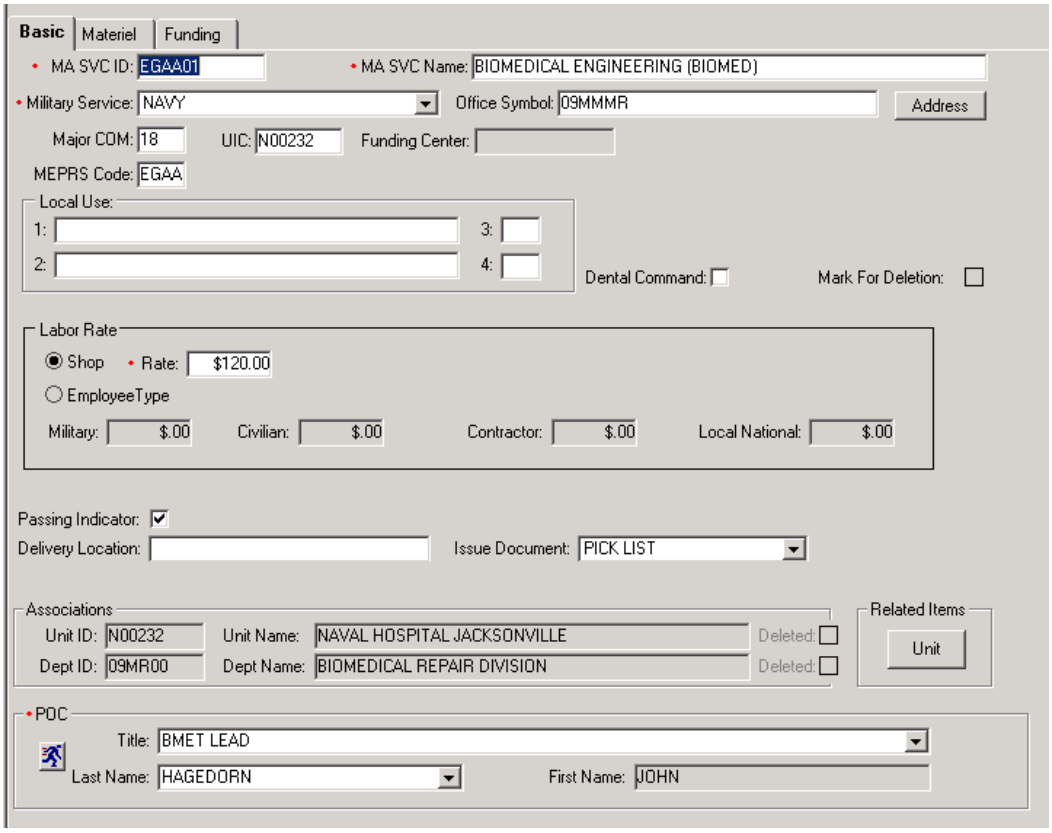


Figure 62. Equipment Maintenance Activity Service/Customer Detail Window–Basic Tab (Navy)

1. MA SVC ID. Identifies the MA's SVC/CUST account number. This field should not be modified unless directed to do so by DHA.

2. Name. The name should be as specified by the Military Service or DHA.

3. Military Service. Defaults to the Military Service. This field should not be modified unless directed to do so by DHA.

4. Major COM. Although this is an optional field; materiel managers should load their corresponding MAJCOM or MACOM code.

5. Office Symbol. Optional field used to document the MA Service office symbol.

6. Cost Center ID–A Cost Center represents the work center incurring costs/charges (if required by Military Service).

7. Medical Expense and Performance Reporting System Code. Optional field. This code is assigned by the local resource advisor and is used to track expenses associated to the MA.

8. Mark for Deletion. Do not mark the MA Service for deletion unless it is being replaced with a new MA Service record. This field should not be modified unless directed to do so by DHA.

9. Labor Rate–Mandatory field. The labor rate is determined by DHA/MEDLOG or Military Service and is used to calculate labor costs associated to maintaining equipment. The labor rate is recalculated annually and published prior to the beginning of each new FY.

10. Delivery Location. Identifies the MA delivery location for equipment items.

11. Issue Document. Should always be Pick List.

12. DCM Printer. Identifies the primary DCM printer for forms and issue documents.

13. POC. Associate the POC record for the Medical Maintenance Management Officer. Within the POC detail record, this user should be associated to the POC type listed for Maintenance Staff.

(b) Materiel Tab. The MA SVC/CUST Detail window–Materiel tab is used to manage critical ordering information. The default data in the Materiel tab should be accepted with the exception of the default location. In the default location field, identify the MA building and/or room location. If the Verify Receipts indicator is checked, maintenance personnel must manually verify and process customer receipts in CAIM, not recommended for Air Force.

(c) Funding Tab. The MA contains a Funding tab because it doubles as an SVC/CUST record for the maintenance account. This tab allows the SA to create or change the EXP center target and set the maximum order limit, as well manage EXP center associations. The MA must be associated to an EXP and PROJ center before maintenance personnel can order supplies and repair parts. Use the data fields as described below.

1. Target Flag. Should always be Proj EOR.

2. Detailed Billing Required. While not the preferred, it is used with authorized CAIM SOS accounts.

3. Maximum Order Limit. While not the preferred, it is used with authorized CAIM SOS accounts.

4. Associate EXP Centers. Refer to DHA-TM volume regarding financial procedures in draft. Sites should follow Service specific guidance until DHA procedures are published.

5. Default EXP Center. Refer to DHA-TM volume describing DMLSS use for financial procedures currently in draft. Sites should follow Service specific guidance until DHA procedures are published

(4) Creating a New MA Service

(a) The New MA function is located in the LOG MTF/Unit ORG detail record. Using Search function, select ORG – Med Facility/MTF in the Type field, and select Search. Once results are retrieved, either select the LOG record or highlight the record, and select Detail. Next, select New MA located on the vertical toolbar. The MA detail record contains three tabs: Basic, Materiel, and Funding.

(b) A window appears requiring the new MA to be associated to a DEPT. Once associated, complete the Basic, Materiel, and Funding tabs as explained above.

(c) DMLSS users can only be assigned to one MA at a time. Therefore, maintenance personnel can only access maintenance records for the MA associated to their User ID. Maintenance managers are only able to see maintenance reports for the MA assigned to their User ID, and they do not have a complete view of work throughout all MA activities. These limitations should be considered prior to using multiple MA.

e. FM Service Detail. In the FM Service Detail window, FM service information can be opened and edited. The FM service was established in DMLSS during implementation at the site and may not be deleted; however, multiple FM can be loaded within a single application. The FM Service(s) identifies the FM Office(s) responsible for supporting the ORG(s) such as LOG.

(1) New FM service records are created in the FM module and are accomplished by the facility manager or Accountable MEDLOG Officer. Select MTF Information from the FM Navigate dropdown menu and select New located on the vertical toolbar in the MTF Information window. Complete the mandatory data fields, annotated with an asterisk (*), and as many optional data fields as possible. Select Save before exiting. This window is audited by the system.

(2) Unlike MA service accounts, DMLSS users may be associated to multiple FM activities at the same time. Therefore, FM personnel can access records for all FM service accounts associated to their User ID.

f. LOG DEPT. Only one LOG DEPT is permitted for each DMLSS application. The sole LOG DEPT was established during implementation at the site and may not be deleted. The data contained in the LOG DEPT Detail (Figure 63-65), is critical for ordering and contains informative data such as the LOG ID, name, and office symbol; materiel and services currency types; conversion factors; LOGs associated FOA; the LOG POC and associated LOG service accounts. While most of the LOG DEPT data fields are editable, they should not be changed without proper approval by the Accountable MEDLOG Officer. Do not mark the LOG DEPT for deletion unless being replaced by a new LOG DEPT.

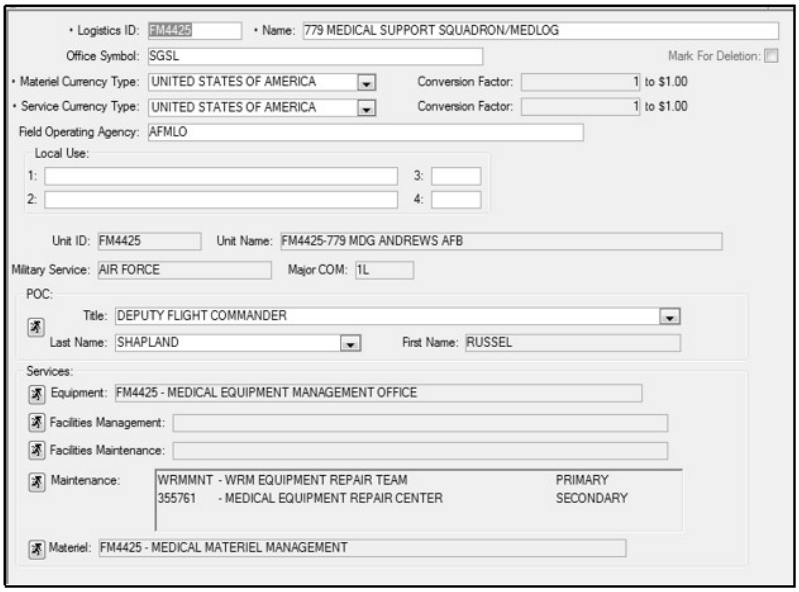


Figure 63. Logistics Department Detail Window (Air Force)

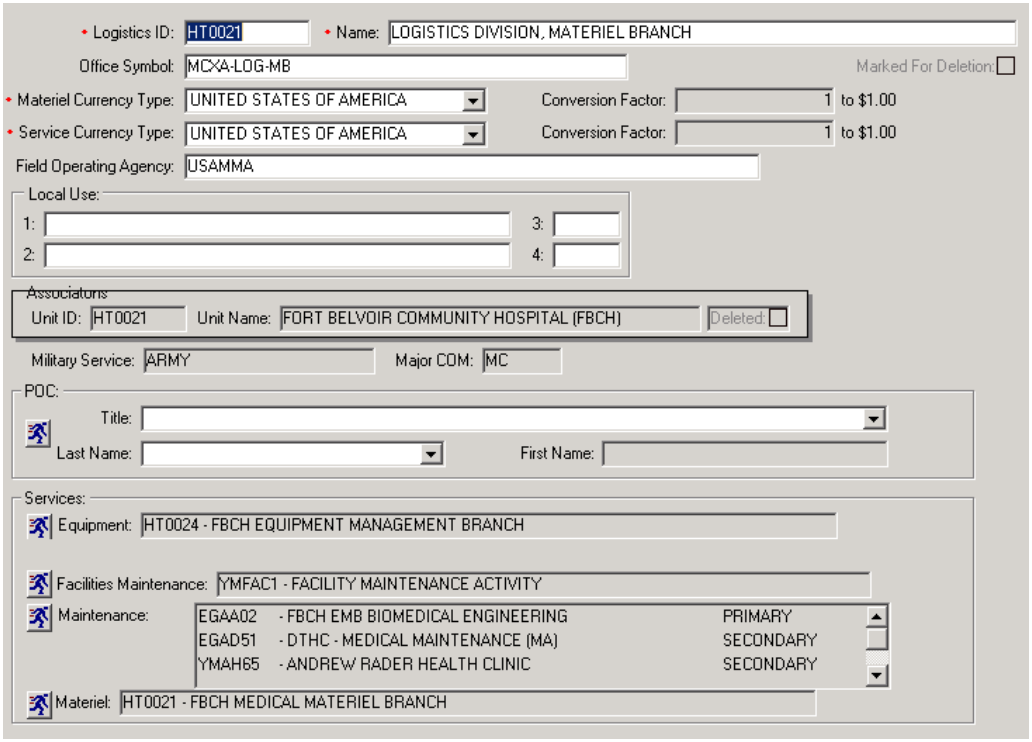


Figure 64. Logistics Department Detail Window (Army)

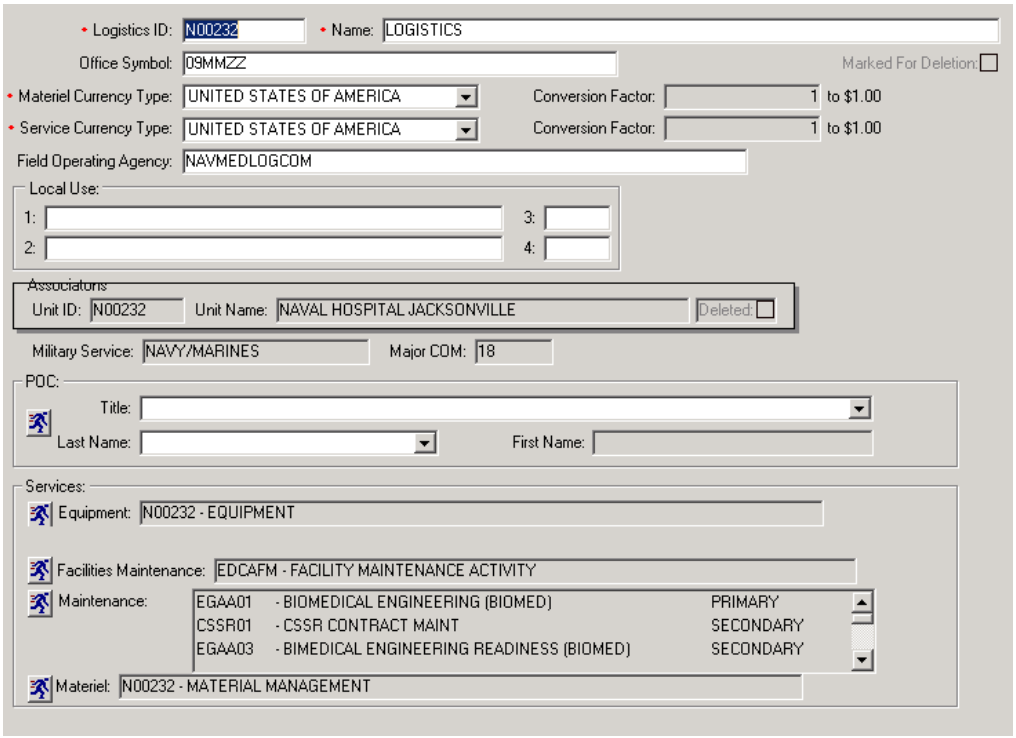


Figure 65. Logistics Department Detail Window (Navy)

ENCLOSURE 5

USER PRIVILEGE AND ROLE MANAGEMENT

1. OVERVIEW. Roles/privileges are assigned to every User ID on the DMLSS system to protect the DB from unauthorized access. It is the responsibility of the DMLSS SA to ensure that appropriate management controls are in place for assigning/routinely monitoring the access levels of all users.

2. CONCEPT OF LEAST PRIVILEGE. Effective access control occurs when an organization employs the concept of least privilege. The least privilege concept allows only authorized access for users who are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. To employ this concept, DMLSS SAs should:

a. Verify all users have the minimum level of access (least privilege) needed to complete their assigned duties.

b. Provide a higher-level review when additional access is requested. Note: The DMLSS SA does not always know when staff changes roles in the facility. When notified by a supervisor, the SA can adjust access levels. The SA must coordinate with other LOG sections when changes are requested to a user's privileges.

3. USER ROLES WITH ELEVATED PRIVILEGE. Limit access to the following roles with elevated privileges in DMLSS to those users with a legitimate need:

a. DMLSS SAs. This category also includes the FM SA and DB/System Audit Reviewers.

b. SS Security Manager. It is very important to note the elevated privilege of the SS security manager. This user can give virtually any rights in the system to themselves or others. Only the SS security manager has the unique ability to assign the security manager attribute for other applications; every other security manager is limited to their associated application. For example, the FM security manager can assign the FM security manager role to another user, whereas the SS security manager can assign security manager for Archive Management, EM, MA, IM, AM, SS, FM, Customer Support, MM, and Service Contracts to any user, including their own. Therefore, it is strongly recommended that there be only one security manager for each application per site.

c. Application Security Manager. The security manager role for each application is designed so that only a limited number of users can assign applications, functions within those applications, and privilege levels (read, update, create, and delete), to other users. These assignments determine what actions the user can perform on data in DMLSS. Therefore, it is strongly recommended that there be only one security manager for each application per site.

(1) Users may be assigned the security manager role for more than one application.

(2) A user does not need application access (have one or more application-user roles) to be a security manager for that application.

(3) A Security Manager role can only be granted or removed by a user with that same role.

(4) A Security Manager role cannot be removed from a user's own User ID.

d. Application Expert Roles. Only a limited number of users should be given an expert role due to the nearly unlimited access and capability it provides within the application.

e. SS. Most of the SS functions directly affect the system organizational structure, funds, document control, EOPs, and interfaces. It is highly recommended that only experienced logisticians with knowledge and training be afforded privileges to these functions. Likewise, only a limited number of users should be given access to the UP functionality (UP Assign and UP Manage) to assign powerful capabilities in areas such as Organization (Org) and Funding.

f. LOG Fund Manager Role. This role is assigned in SS and is used to load/adjust the LOG (Stock) Fund Target for MM. Coordination with the Military Service or DHA/MEDLOG and supporting documentation are both required to make adjustments to this target.

4. DMLSS UP Functionality. In the UP functionalities (UP Assign and UP Manage), an authorized user, i.e., a user with the security manager role, can assign one or more roles with various privileges to a User ID, modify a role, or create a new role. Roles are assigned to every User ID on the DMLSS system to protect the DB from changes that the user is not authorized to make.

a. Security Managers may access the UP Assignment (UP Assign) and UP–Management (UP Manage) functions from either the SS navigation menu or horizontal toolbar.

b. UP Assign. In this window an authorized user can assign one or more applications and/or roles to another user. In addition, SVC/Customer IDs, AM Organization Assemblages (ORG/Assm), the EM Organization (ORG/ID), the MA Service (MA SVC ID), the FM Installation Name, and Pending Actions for AM/CAIM/IM are all assigned from this screen.

c. UP Manage. Roles within each DMLSS application can be created, such as new customized role and/or privileges, deleted, and existing roles may be modified by changing the attributes of the resources of that role in the User Privilege–Management function.

d. The auditing function is available on the vertical toolbar of the UP Manage screen. This feature provides the ability to check which users accessed the system, when, how long, and/or problems associated with connecting. It also tracks what application(s) a user accessed, when these were accessed, and for how long.

5. ROLE/PRIVILEGE ASSIGNMENT RULES. The SA should have a basic knowledge about what each role performs before assigning that role to a user. Additionally, the SA should be aware of the following rules:

a. General Rules

(1) Each DMLSS module has standard roles that cannot be edited.

(2) Privilege Rule. Delete is the highest-level privilege; Read is the lowest. When a privilege is selected for a resource, all the lower privileges are automatically selected. For example, if a user is to be given Delete privileges, the system also assigns Create, Update, and Read privileges to the resource.

(3) If a user is logged in when the SA modifies their privileges, the user must exit DMLSS and log in again, before the change(s) take effect.

b. Specific Module Rules

(1) AM Module Roles. Certain roles in AM can only be assigned to users with one or more assemblages. If one of these roles is attempted to be assigned to a User ID that has no assemblages, the system notifies the user that the operation cannot be performed.

(2) CAIM Module Rules. DMLSS uses the SVC/CUST assignments to automatically populate certain data areas in CAIM and Customer Support. For CAIM, certain roles can be assigned only to a User ID that has one or more MM SVC/CUSTs. If one of these roles is attempted to be assigned to a User ID that has no MM SVC/CUSTs, the system notifies the user that the operation cannot be performed. Likewise, with the Customer Support application highlighted, assigning an SVC/CUST to a User ID equates to assigning membership to that SVC/CUST group.

(a) The user cannot remove the last CAIM SVC/CUST from a User ID that has a role requiring at least one MM SVC/CUST. If the user tries to remove the last SVC/CUST, the System displays a message with the reason the action cannot be accepted. If the user tries to remove all CAIM SVC/CUSTs at one time, the System removes all of those selected except the last one and informs the user that the last one has not been removed.

(b) Certain resources can only be set with either all privileges: read, update, create, and delete, or none. If the user selects one, all are automatically selected; if the user deselects one, all are automatically deselected.

(c) MA Module Roles. For MA, certain roles can be assigned only to a User ID that has one or more maintenance activities. If the user attempts to assign one of these roles to a User ID that has no maintenance activities, the system notifies the user that the operation cannot be performed.

(d) Service Contracts Module Roles. In the SVC/CUST Management window, the SA can assign or remove an SVC/CUST from a user's privileges.

(e) SS Module Roles

1. If the update privilege for MTF LOG is selected, the update privilege for MTF Funding is automatically added to the same role. The user cannot deselect the update privilege on the MTF LOG resource if update is selected for MTF Funding.

2. If the read privilege for DCM Configuration is selected, the read privilege for Communications Management is automatically added to the same role. The user cannot deselect the read privilege on the Communications Management resource if read is selected for DCM Configuration.

6. UP GUIDANCE FOR CUSTOMERS. The following general guidance is recommended when determining UPs for property/supply custodians and other roles. UPs should be invoked to limit DMLSS access to the least amount necessary to perform assigned duties. Refer to Military Service policies until DHA policies have been published and are in effect.

7. PENDING ACTION GUIDANCE FOR CUSTOMERS. In addition to UPs and roles, customers should only have access to the pending actions that are specific to their role. Refer to Military Service policies until DHA policies have been published and are in effect.

8. PV REPRESENTATIVES. Prime Vendor (PV) Representatives must only be allowed read only access in DMLSS. Note: Currently there is not a read only role for strategic sourcing; however, SAs can create a custom role via the UP Manage module in SS. This allows the customer or PV Representatives to view what is in Strategic Sourcing without accepting recommended changes.

9. REPORTS. In addition to the Auditing function and utilizing Business Objects reports, the SS Reports module offers several standard reports for reviewing DMLSS users and their assigned roles, resources, and privileges. The following reports provide a level of systems security provided they are reviewed periodically.

a. User Summary Report. This report is a broad list of all users and User IDs along with their assigned applications, roles, and Resource and privileges. The list can be quite long if printed, but it shows all users with their assigned privileges.

b. User Summary Report by Application. This report is similar to the User Summary Report except the user selects a specific application. The report then displays all users for the selected application. The report is useful when the user is searching for users with specific application privileges.

c. UP Summary Report. This report is similar to the User Summary Report except that the user selects a specific application and resource element. This is currently the most detailed search report available. The report is useful when the user is searching for users with specific resource privileges.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AM	Assemblage Management
CAC	common access card
CAD	computer-aided design
CAIM	Customer Area Inventory Management
CD	compact disk
CFY	current fiscal year
CIIC	Controlled Item Inventory Code
CMOS	Cargo Movement Operations System
COBIE	Construction Operations Building Information Exchange
CRL	Certificate Revocation List
CRON	command run on
CUST	customer
DAN	DMLSS Advisory Notice
DB	database
DCM	DMLSS Communications Management
DEA	Drug Enforcement Administration
DEPT	Department
DFAS	Defense Finance and Accounting System
DHA-TM	Defense Health Agency-Technical Manual
DHAR	Defense Health Agency Region
DLA	Defense Logistics Agency
DMLSS	Defense Medical Logistics Standard Support
DN	distinguished name
DoDAAC	Department of Defense Activity Address Code
DoD ID	Department of Defense Identification
DRMO	Defense Reutilization and Marketing Office
DRO	Direct Reporting Market
DTF	dental treatment facility
EDI	electronic data interchange
EHR	Electronic Healthcare Record
EOD	end-of-day
EOFY	end-of-fiscal year
EOM	end-of-month
EOP	end-of-period
EOY	end-of-year
EOR	elements of resource
EM	equipment management
EXP	expense

FAD	Force Activity Designator
FM	facility management
FOA	Field Operating Agency
FY	fiscal year
GSA	General Services Administration
GSC	Global Service Center
GW	gateway
HTTP	hypertext transfer protocol
IP	internet protocol
iRAPT	invoicing, receipt, acceptance, and property transfer
JMAR	Joint Medical Asset Repository
JMLFDC	Joint Medical Logistics Functional Development Center
LOG	logistics
LTO	linear tape-open
MA	Equipment Maintenance
MEDLOG	Medical Logistics
MFR	memorandum for record
MHS	Military Health System
MILSTRIP	Military Standard Requisitioning and Issue Procedures
MM	materiel management
MTF	military medical treatment facility
O/H	on-hand
OP	other procurement
ORG	organization
OS	operating system
PDF	portable document format
POC	point of contact
PROJ	project
PVP	prime vendor pharmacy
QA	quality assurance
RC	regulatory compliance
RF	radio frequency
RIC	routing identifier code
RPIE	Real Property Installed Equipment

SA	System Administrator
SOS	source of supply
SS	systems services
SSO	Small Market and Stand-Alone MTF Organization
SVC	service
TMU	table maintenance utility
UDR	Universal Data Repository
UND	Urgency of Need Designator
UP	user privilege

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this DHA-TM.

business continuity plan. Focuses on the DRO's ability to continue or quickly recover its mission-essential functions following any disruption short of a major catastrophe or national security emergency. Business continuity plan may be incorporated into a specific plan or, when appropriate, in documents such as standard operating procedures, and generally are distributed widely so that all relevant personnel are familiar with the required procedures and associated responsibilities.

console access. Access to all commands and files on a Linux or other Unix-like OS.

DAN. Messages indicating known issues, and estimated date for correction, to DMLSS users between system updates.

direct reporting organization. An activity that is outside the bounds of the standard DHA headquarters management hierarchy that provides broad general support to the DHA and its customers not available elsewhere, and that reports to either the Director, DHA or to an Assistant Director.

least privilege. Permits DMLSS access with the least amount of privileges that affords the user to accomplish assigned tasks in accordance with organization missions and business needs.

Medical Information Systems. The information technology support function or DEPT within the Medical Unit.

MTF. Any fixed facility of the DoD that is outside of a deployed environment and used primarily for health care; and any other location used for purposes of providing healthcare services as designated by the Secretary of Defense.

protected health information. Information regarding protected health information of an individual as defined in Reference (j).

security awareness plan. A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and should outline the duties of those who are responsible for overseeing security (the security management function), as well as those who own, use, or rely on the entity's computer resources.

security management. Administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees, and monitoring and evaluating policy and control effectiveness.