Personnel Accountability System
Full Application **(PAS-FA)**
Version 2.1

User's Guide

Table of Contents

1.0 PAS-FA

The Personnel Accountability System Full Application (PAS-FA) automates both shipboard and shore-based personnel accountability using the Common Access Card (CAC), TWIC, DBIDS, and GSA PIV II Smartcards; barcodes; and/or fingerprints for individual validation.

1.1 What is a Smartcard or Integrated Circuit Chip (ICC)?

CACs, TWICs, and PIV II Smartcards are the standard identification cards issued to uniformed service members of the Department of Defense (DoD), DoD employees, certain contractors, transportation workers, and other federal government employees (see Figure 1-1). Collectively referred to as ICC cards, each card is the size of a standard credit card, and contains an Integrated Circuit Chip (ICC) embedded in its plastic. The ICC consists of a microprocessor that securely stores, processes, and updates data. This allows the ICC card to manage valuable information, process transactions, authenticate identity, and provide access to networks or databases.

Figure 1-1 Sample ICC Card

1.2 What is PAS-FA?

The Personnel Accountability System Full Application, or PAS-FA, is a software application that automatically records the status of personnel as they check in and out of a facility or ship. Personnel are checked in or out by reading the Integrated Circuit Chip (ICC) on their Smartcard, scanning the 3x9 barcode located on the ICC Card or barcode ID Card, or capturing individual fingerprints. The fingerprint option expedites processing where security posture allows. An option to use the smartcard with fingerprint is permitted, but requires PIN entry. PAS-FA also displays digital photos of cardholders stored in the PAS database to enhance cardholder identity verification to the operator.

Operators and administrators can assign personnel processing out on Liberty to 'Buddy Groups', satisfying requirements of liberty policies while deployed overseas, and assign 'Liberty Risk' categories to individuals with limited or restricted privileges. PAS-FA includes a messaging capability, which alerts the operator the next time the intended recipient processes in or out. Operators and administrators can also view and print reports from PAS-FA.

PAS-FA supports the use of fingerprints, ICC cards, and barcodes as well as manual lookups of personnel to check-in or check-out a person from the system. Using those same methods, the application is capable of creating a new or selecting an existing roster event, and signing attendees into and out of that event.

2.0 Getting Started

2.1 System Requirements

In order to use PAS-FA, the hardware/software must meet the following minimum standards:

- Windows XP, Service Pack 3
- Pentium class processor, 1 GHz or higher
- Minimum 512 MB of RAM, 1 GB preferred
- 570 MB of available hard disk space
- 1024x768 or higher display resolution with 256 colors
- PC/SC Smart Card Reader
- USB or PS/2 barcode scanner with terminating keyboard wedge
- Cogent CSD200 USB Fingerprint Scanner (optional)

Note: If prompted for hardware drivers, locate the Device Driver folder on install media.

2.2 Installing PAS-FA Server

Important: Administrator privileges are required for installation. A smartcard reader and required drivers must be installed per manufacturer's instructions prior to installation.

2.2.1 New Installations

These procedures will occur during a new installation:

- Install Microsoft Windows Installer 3.1
- Install Microsoft .NET Framework 3.5 SP1
- Install Microsoft Windows Installer 4.5
- Install Microsoft PowerShell v1
- Install Microsoft SQL Server 2008 Express
- Create PAS Database
- Install Microsoft SQL database Encryption software
- Configure Microsoft SQL secure port conductivity
- Open TCP Port 15507 in Microsoft Firewall
- Install PAS Backup utility
- Automatically restart the computer when installation is complete

Note: Any required software that is already present on the computer will not be reinstalled.
Note: If using 3rd party firewall software, open TCP Port 15507 for remote database access.

2.2.1.1 PAS Database Installation

1) Insert the CD/DVD into the CD/DVD drive.
2) From the Windows 'Start' button, open 'Windows Explorer', or double click 'MY COMPUTER' on the desktop.
3) Select the drive designated for the CD/DVD.
4) Select the 'Install.exe' icon to launch the PAS-FA install menu shown in Figure 2-1.
5) Click 'INSTALL PAS 2.1 DATABASE'.

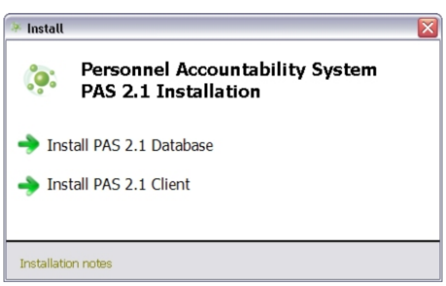

Figure 2-1 PAS Install Menu

6) Successive 'PAS DB Install Setup' screens will appear (see Figure 2-2) with license agreements for:
   - Microsoft Windows Installer 3.1
   - Microsoft .NET Framework 3.5 SP1
   - Microsoft Windows Installer 4.5
   - Microsoft SQL Server 2008

Figure 2-2 PAS DB install setup

7) Click 'ACCEPT' on each license agreement to proceed.

Note: If your computer already has any of this software installed, the license agreement for that software will not appear.

8) The installation proceeds automatically (except in the case of Windows Installer as noted below). Various progress screens appear throughout the installation as shown in Figures 2-3 through 2-5.

Note: After installation of either Windows Installer 3.1 or 4.5, a message displays alerting you that the computer must be rebooted before setup can proceed. The message prompts for an immediate reboot or manual reboot later. Click 'YES' to reboot immediately. After reboot you will need to login. The PAS installation process automatically resumes.

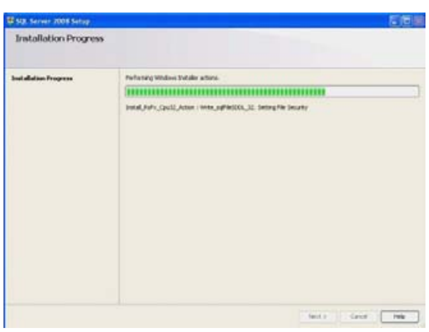

Figure 2-3 SQL Server 2008 Setup screen

Figure 2-4 Installing PAS Database screen

Figure 2-5 Encrypting PAS Database screen

9) When the installation is complete, an alert appears prompting an immediate reboot as shown in Figure 2-6. Click 'OK'.

Figure 2-6 Reboot of computer required

10) Proceed to Section 2.2.1.2, *PAS Client Installation*.

2.2.1.2 PAS Client Installation

1) Click 'INSTALL PAS 2.1 CLIENT' on the PAS-FA install menu shown in Figure 2-7.

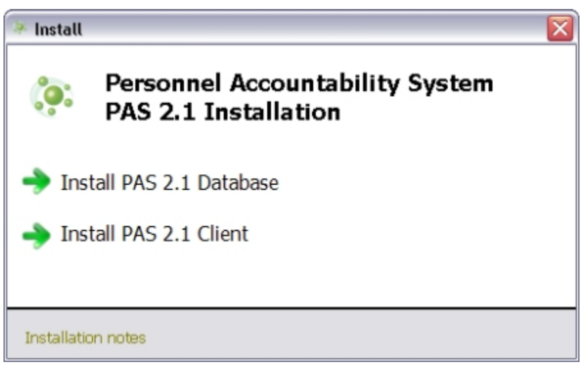

Figure 2-7 PAS Install menu

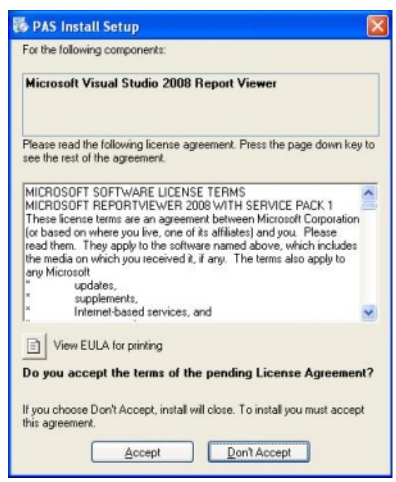

Figure 2-8 PAS Install Setup

2) A 'PAS Install Setup' window displays the license agreement for MS Visual Studios as shown in Figure 2-8. Click 'ACCEPT' to proceed. If your computer already has MS Visual Studios installed on it, this window will not appear.
3) A message appears reading 'Please wait while the setup Wizard installs PAS'. This may take several minutes.
4) When complete, a 'Completed the PAS Setup Wizard' window appears as shown in Figure 2-9. Click 'FINISH'.

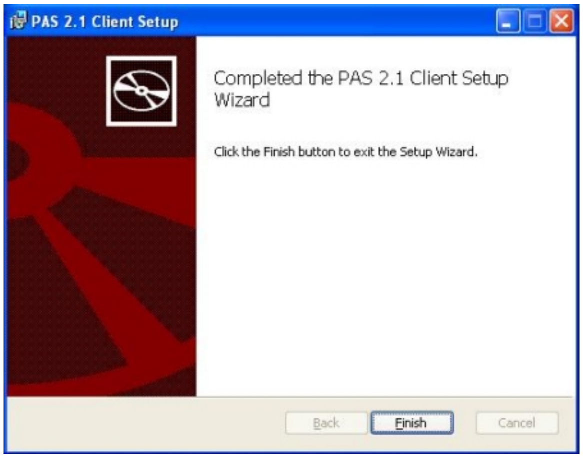

Figure 2-9 PAS 2.1 Client Setup

5) The PAS client is installed into C:\Program Files\CACPMO\PAS2 and a shortcut is placed on the desktop.
6) Activate the Fingerprint Match License
   a) Open the PAS application.
   b) Select 'Activate Fingerprint Match License' from the 'Help' menu. A screen will display 'Activation Succeeded'. Click 'OK'.

PAS Installation is complete.

2.2.2 Upgrades

Important: Any system upgrade has the potential to corrupt existing data. Before beginning an upgrade, backup existing data as described in Section 2.2.2.1, *Backup PASCAC v1.03*.

These procedures will occur during a system upgrade:

- Install Microsoft Windows Installer 3.1
- Install Microsoft .NET Framework 3.5 SP1
- Install Microsoft Windows Installer 4.5
- Install Microsoft PowerShell v1
- Upgrade Microsoft SQL Server 2008 Express
- Create PAS Database
- Upgrade Microsoft SQL database Encryption software
- Configure Microsoft SQL secure port conductivity
- Open TCP Port 15507 in Microsoft Firewall
- Install PAS Backup utility
- Automatically restart the computer when installation is complete

Note: Any required software that is already present on the computer will not be reinstalled.
Note: If using 3rd party firewall software, open TCP Port 15507 for remote database access.

2.2.2.1 Backup PASCAC v1.03

1) Insert the CD provided into the CD drive of the computer running v1.03 (if the 'Install' window appears, close the window).
2) From the CD, click on 'Backup_PASCAC_103.cmd'.
3) A screen will appear with a 'Preparing to back up PASCAC…' alert.

a. Press any key to continue.

4) After backup, the screen will display a message to confirm the backup process as displayed.
   a. Press any key to Exit.
5) A folder containing the backup named ‘USC_DB_BACKUP’ is automatically created on the computer’s ‘C’ Drive.

2.2.2.2 PAS 2.1 Database Installation

1) Insert the CD provided into the CD drive of the computer running v1.03.
2) The Install menu shown in Figure 2-10 should automatically display. If the menu does not display:
   a. From the Windows ‘Start’ button, open Windows Explorer, or double click ‘MY COMPUTER’ on the desktop.
   b. Select the drive containing the CD.
   c. From the CD, click the ‘Install.exe’ icon to launch the PAS-FA install menu.

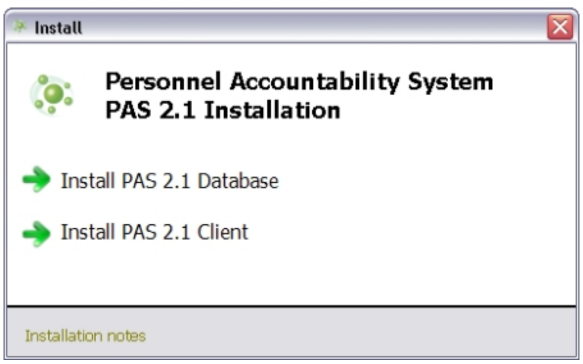

Figure 2-10 PAS Install Menu

3) Successive ‘PAS DB Install Setup’ screens will appear (see Figure 2-11) with license agreements for:
   - Microsoft Windows Installer 3.1
   - Microsoft .NET Framework 3.5 SP1
   - Microsoft Windows Installer 4.5
   - Microsoft SQL Server 2008

Figure 2-11 PAS DB install setup

4) Click ‘ACCEPT’ on each license agreement to proceed.

Note: If your computer already has any of this software installed, the license agreement for that software will not appear.

5) The installation proceeds automatically (except in the case of Windows Installer as noted below). Various progress screens appear throughout the installation as shown in Figures 2-12 through 2-14.

Note: After installation of either Windows Installer 3.1 or 4.5, a message displays alerting you that the computer must be rebooted before setup can proceed. The message prompts for an immediate reboot or manual reboot later. Click 'YES' to reboot immediately. After reboot you will need to login. The PAS installation process automatically resumes.

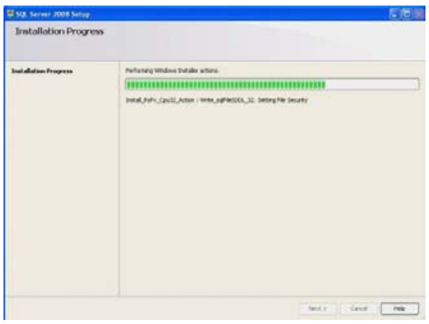

Figure 2-12 SQL Server 2008 Setup screen

Figure 2-13 Installing PAS Database screen

Figure 2-14 Encrypting PAS Database screen

6) When the installation is complete, an alert appears prompting an immediate reboot as shown in Figure 2-15. Click 'OK'.

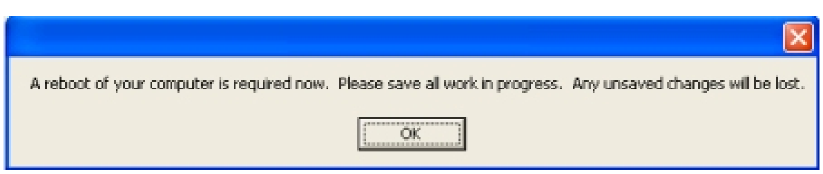

Figure 2-15 Reboot of computer required

7) Proceed to Section 2.2.2.3, *PAS 2.1 Client Installation*.

2.2.2.3 PAS 2.1 Client Installation

1) Click ‘INSTALL PAS 2.1 CLIENT’ on the PAS-FA install menu shown in Figure 2-16.

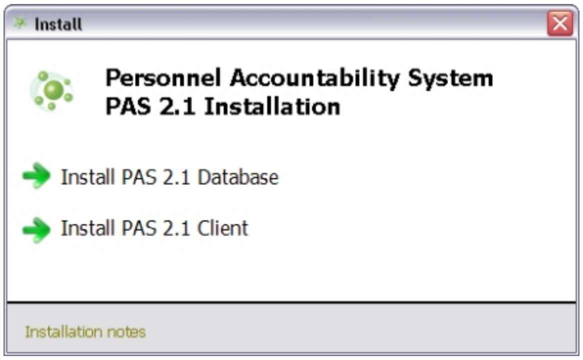

Figure 2-16 PAS Install menu

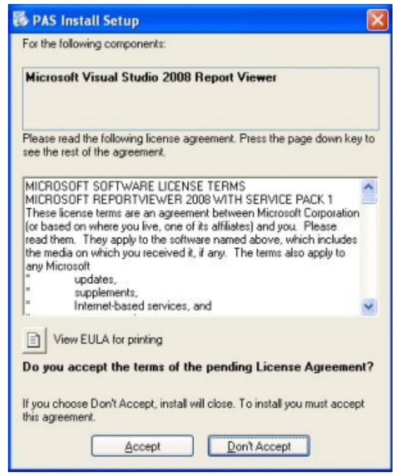

Figure 2-17 PAS Install Setup

2) A ‘PAS Install Setup’ window displays the license agreement for MS Visual Studios as shown in Figure 2-17. Click ‘ACCEPT’ to proceed. If your computer already has MS Visual Studios installed on it, this window will not appear.
3) A message appears reading ‘Please wait while the setup Wizard installs PAS’. This may take several minutes.
4) When complete, a ‘Completed the PAS Setup Wizard’ window appears as shown in Figure 2-18. Click ‘FINISH’.

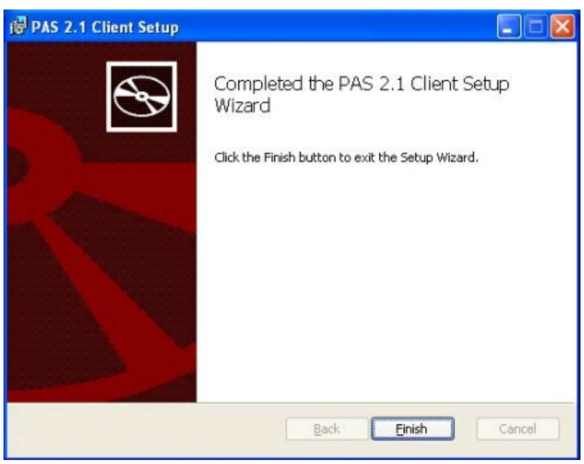

Figure 2-18 PAS 2.1 Client Setup

5) The PAS client is installed into C:\Program Files\CACPMO\PAS2 and a shortcut is placed on the desktop.
6) Activate the Fingerprint Match License
    a. Open the PAS application.
    b. Select ‘Activate Fingerprint Match License’ from the ‘Help’ menu. A screen will display ‘Activation Succeeded’. Click ‘OK’.

The PAS v2.1 upgrade is complete.

2.3 PAS-FA Client Activation

Important: Administrator privileges are required. A smartcard reader and associated drivers must be installed per manufacturer's instructions prior to activation. It is strongly recommended that two or more administrators have privileges in PAS-FA in the event an administrator is unavailable or an administrator's ICC card fails, is lost, or is stolen.

When the PAS-FA application is first started, the operator has several options:

1) Create a New Local Database. The operator creates a new database on the local machine. Administrative rights will be assigned to the first operator starting and logging into the system. As with all login attempts, the user must have a functioning ICC card and must know their PIN.
2) Connect to an Existing Local Database. The operator points to an existing database on the local machine where the application has been installed and administrative rights established.
3) Connect to an Existing Remote Database. The operator points to an existing database on a remote machine where the application has been installed and administrative rights established (for example, another instance of PAS-FA on a network).

2.3.1 Initial Local Login - Create a New Local Database

1) From the desktop, double-click the PAS-FA icon. A message appears on the main screen with a notification that the PAS installation has never been run before, and asks if you would like to connect to an existing database, or connect to a new database.
2) Click 'CONNECT TO A NEW DATABASE' only if you are not connecting to an existing database, and desire to setup a new administrator.
3) A second message displays asking you to set the initial Administrator. Click 'YES' to proceed with login, or 'NO' to cancel initial login.
4) When prompted, insert your ICC card.
5) Enter your ICC card PIN in the 'Enter PIN' window shown in Figure 2-19.
6) Click 'OK.'

Figure 2-19 Enter PIN window

Important: Three consecutive incorrect PIN entries will cause the CAC to lock. It can only be reset by a DEERS/RAPIDS issuance or CAC PIN Reset workstation.

7) PAS-FA assigns the user an administrator role. When prompted, remove your ICC card from the card reader.
8) An 'Add Administrator' dialog box appears so that another user can be added as an administrator.

Important: If the current number of administrators is ever less than two (2), the 'Add Administrator' dialog box will appear each time the administrator logs in until at least two administrator roles are designated.

9) Click 'OK' to add a second administrator, or 'CANCEL' to login the first administrator.
    a. If 'OK' is clicked in the 'Add Administrator' dialog box, the second administrator must insert their ICC card and enter their PIN when prompted.
10) PAS-FA creates a database when the administrator is logged in.

2.3.2 Initial Local Login - Connect to an Existing Local Database

1) From the desktop, double click the PAS-FA icon.
2) From the desktop, double-click the PAS-FA icon. A message appears on the main screen with a notification that the PAS installation has never been run before, and asks if you would like to connect to an existing database, or connect to a new database.
3) Click 'CONNECT TO AN EXISTING DATABASE'

Important: An operator must be an administrator on the target database as well as the database being created to have access and make changes.

4) A 'Select Server' screen appears displaying a list of network servers as shown in Figure 2-20. Highlight 'Default' and click 'OK'.

Figure 2-20 Select Server

5) When prompted, insert your ICC card.

Note: This person must be defined as a user in the existing database.

6) When prompted, enter your ICC card PIN.

Important: Three consecutive incorrect PIN entries will cause the CAC to lock. It can only be reset by a DEERS/RAPIDS issuance or CAC PIN Reset workstation.

7) Click 'OK'.
8) PAS-FA connects to a database when the administrator is logged in.

2.3.3 Initial Remote Login - Connect to an Existing Remote Database

1) From the desktop, double click the PAS-FA icon.
2) A PAS/CAC screen appears reading 'Current server is invalid. Do you wish to connect to another database?'. Click 'YES'.
3) A 'Select Server' screen appears as shown in Figure 2-20.
4) In the screen's 'Server' field, type the IP address of the remote PAS server followed by ',15507' in the following configuration: xxx.xxx.xxx.xxx,15507.

Figure 2-20 Select Server

5) Click 'OK'.
6) Click 'Login' to continue.

2.3.4 Upgrade Load Pictures Option

During initial login during an upgrade, PAS-FA loads existing pictures stored on the file system from PAS/CAC into the Master Database using SSNs as filenames to match to person records.

1) A message box displays stating the number of pictures copied to the Master Database.
2) The message box also displays the path of the previously existing pictures stored on the file system and advises that they should be deleted or removed.

2.4 Backup and Restore Database

2.4.1 Backup v2.1

1) From the Windows ‘Start’ button, select ‘All Programs’ > ‘PAS Backup’
2) A ‘PAS Database Backup and Restore’ screen appears as shown in Figure 2-21. If not already selected, select the ‘Backup’ tab from the top of the screen.

Figure 2-21 PAS Backup Utility

3) The ‘Please select the location for the PAS Database Backup’ box will automatically default to a folder named ‘PAS_DB_BACKUP’ located on the computer’s ‘C’ Drive.
4) Click ‘BACKUP NOW’.
5) A ‘Backup Complete!’ message will display at the bottom of the screen upon backup completion. Click ‘EXIT’.
   a. A window displays asking ‘Are you sure you would like to exit?’. Click ‘YES’
   b. A backup file is created in the PAS_DB_BACKUP directory with a date naming convention.

2.4.2 Restore v2.1

1) From the Windows ‘Start’ button of the new laptop provided, select ‘All Programs’ > ‘PAS Backup’
2) A ‘PAS Database Backup and Restore’ screen appears as shown in Figure 2-22. Select the ‘Restore’ tab from the top of the screen.

Figure 2-22 PAS Restore Utility

3) Use the ‘Browse’ button to find the restore file (.bak). The file should be located in the ‘PAS_DB_BACKUP’ folder on the computer’s ‘C’ Drive.
4) Highlight the appropriate backup file and click ‘OPEN’. The file’s name will appear in the ‘Please select the PAS DB file you would like to restore’ box.
5) Note: The file name will contain a date and time stamp corresponding to the backup procedure performed in 2.5.1, *Backup v2.1*.
6) Click ‘RESTORE NOW’.
7) An alert appears stating ‘You are about to restore the PAS database on this machine. Proceed?’. Click ‘YES’.
8) A ‘Restore Completed’ message appears. Click ‘EXIT’.
    a. A window displays asking ‘Are you sure you would like to exit?’. Click ‘YES’.

Backup and Restore are complete.

2.5 Removing PAS-FA and Master Database

2.5.1 Remove PAS-FA Application

1) From the ‘Start Menu’, click ‘SETTINGS’ and ‘CONTROL PANEL’ to open a ‘Control Panel’ window (see Figure 2-23).

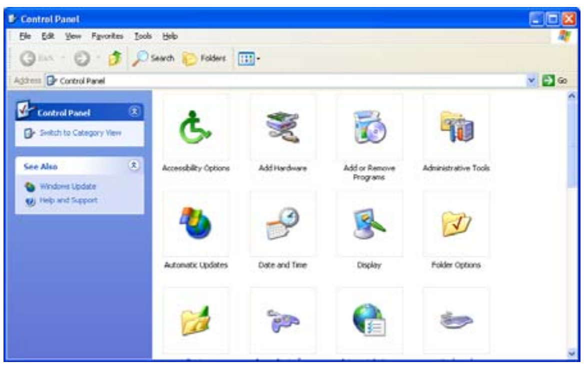

Figure 2-23 Control Panel

2) Double-click ‘Add or Remove Programs’ to display an ‘Add or Remove Programs’ window with installed programs listed alphabetically.
3) ‘PAS 2.1 Client’, ‘PAS’, and/or ‘PASCAC v1.03’ may appear on the list of installed programs. Highlight ‘PAS’ by clicking once as shown in Figure 2-24 and click ‘REMOVE’.
    a. Repeat for ‘PASCAC v1.03’ if listed.

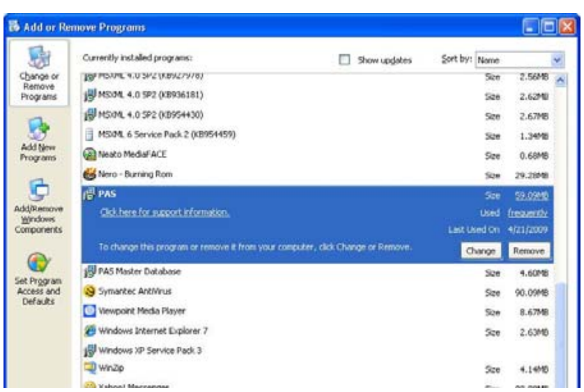

Figure 2-24 Add or Remove Programs screen

4) An ‘Add or Remove’ dialog box displays asking if you are sure you want to remove PAS. Click ‘YES.’
5) A Windows Installer displays a message to wait while Windows configures PAS. When it closes, PAS will be removed from your computer.
6) Repeat steps three through six above to remove PASCAC v1.03, if installed
7) From the Desktop, double click ‘My Computer’ and ‘Local Disk (C:)’. Go to ‘C:\Program Files’ and delete the ‘CACPMO’ folder.

2.5.2 Remove PAS-FA Master Database

1) From the ‘Start Menu’, click ‘Settings’ and ‘Control Panel’ to open a ‘Control Panel’ window
2) Double-click ‘Add or Remove Programs’ to display an ‘Add or Remove Programs’ window with installed programs listed alphabetically.
3) Scroll down to ‘PAS Master Database’ and click it once to highlight as shown in Figure 2-25.
4) Click ‘REMOVE’.

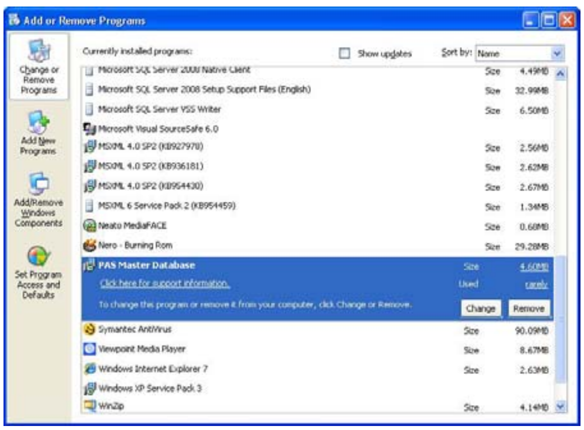

Figure 2-25 Remove PAS Master Database

5) An ‘Add or Remove’ dialog box displays asking if you are sure you want to remove PAS Master Database. Click ‘YES’.
6) A Windows Installer displays a message to wait while Windows configures PAS Master Database. When it closes, PAS Master Database will be removed from your computer.

2.5.3 Remove Microsoft SQL Server 2008

1) From the ‘Start Menu’, click ‘SETTINGS’ and ‘CONTROL PANEL’ to open a ‘Control Panel’ window
2) Double-click ‘Add or Remove Programs’ to display an ‘Add or Remove Programs’ window with installed programs listed alphabetically
3) Scroll down to ‘Microsoft SQL Server 2008 and highlight by clicking it once
4) Click the ‘CHANGE/REMOVE’ button. An ‘SQL Server 2008’ window displays with options to Add, Repair, or Remove SQL Server 2008 as shown in Figure 2-26.

Figure 2-26 SQL Server 2008 options

5) Click the 'REMOVE' link
6) A SQL Server 2008 message displays stating that you should wait while SQL Server processes the current operation
7) A 'Setup Support Rules' window opens displaying Setup Support Rules as shown in Figure 2-27. Click 'OK'.

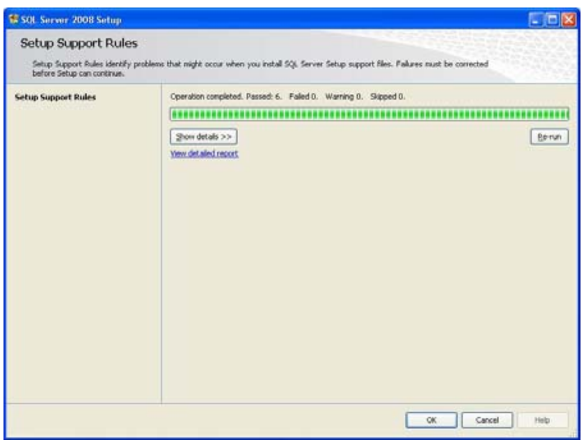

Figure 2-27 Setup Support Rules

8) A SQL Server 2008 message displays saying that you should wait while SQL Server processes the current operation.
9) A 'Select Instance' window displays as shown in Figure 2-28. Use the combo box to select the PASCAC instance of SQL Server, and click 'NEXT'.

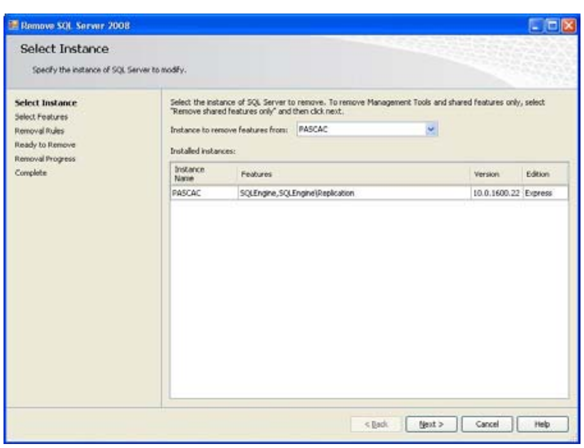

Figure 2-28 Select Instance

10) A ‘Select Features’ screen displays as shown in Figure 2-29. Click the ‘SELECT ALL’ button then click ‘NEXT’.

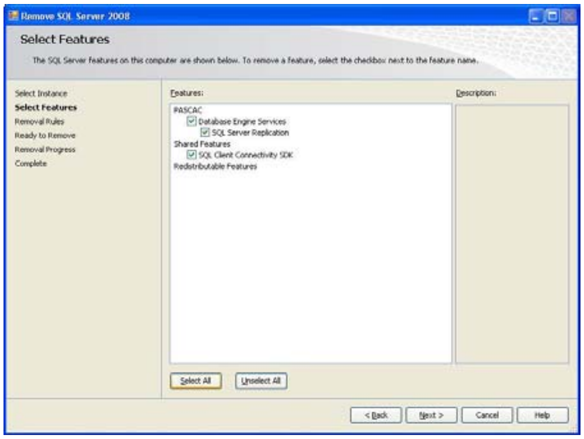

Figure 2-29 Select Features

11) A ‘Removal Rules’ screen appears. Click ‘NEXT’.
12) A ‘Ready to Remove’ screen displays as shown in Figure 2-30. Verify the features to be removed and click ‘REMOVE’.

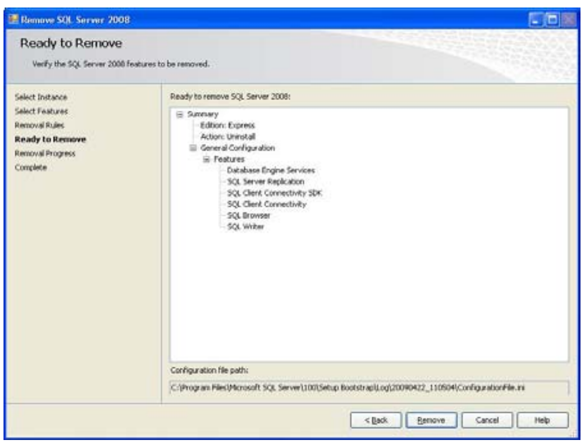

Figure 2-30 Ready to Remove

13) A ‘Removal Progress’ screen displays the status of the removal of selected SQL Server 2008 features. Click ‘NEXT’.
14) A ‘Setup process complete’ message displays showing the successful removal of features. Click “NEXT’.
15) A ‘Complete’ screen displays a statement that your SQL Server 2008 removal completed successfully as shown in Figure 2-31. Click ‘CLOSE’.

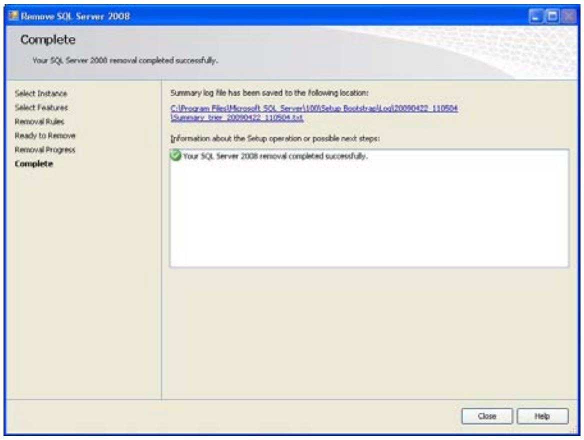

Figure 2-31 SQL Server 2008 Removal Complete

16) From the ‘Add or Remove Programs’ window, remove the following programs:
    a) Microsoft SQL Server 2008 Browser
    b) Microsoft SQL Server 2008 Native Client
    c) Microsoft SQL Server 2008 Setup Support Files (English)
    d) Microsoft SQL Server VSS Writer
17) A message appears stating the removal action is only valid for products that are currently installed for Microsoft SQL Server 2008 Browser, Microsoft SQL Server 2008 Setup Support Files (English), and Microsoft SQL Server VSS Writer. Click ‘OK’.
18) From the Desktop, double click ‘My Computer’ and ‘Local Disk (C:)’. Go to ‘C:\Program Files\Microsoft SQL Server’ and delete the ‘MSSQL10.PASCAC’ folder.

3.0 Login and Logout

The PAS-FA application requires that an Operator/Processor login. The login method is specified in the server settings. Administrators can specify the following login methods:

1) Smartcard (ICC Card)
2) Smartcard with Fingerprints
3) Fingerprint
4) Barcode

This feature provides a measure of system accountability by capturing the following information during the Operator/Processor login process:

1) Location where operator logged in
2) Operator's name
3) Card type
4) Time operator logged in or out
5) Event (logged in or logged out)

3.0.1 Disclaimer Notice

A disclaimer notice will appear each time an individual logs into the PAS-FA application as shown in Figure 3-1. Users must review and acknowledge the disclaimer notice by clicking 'OK'.

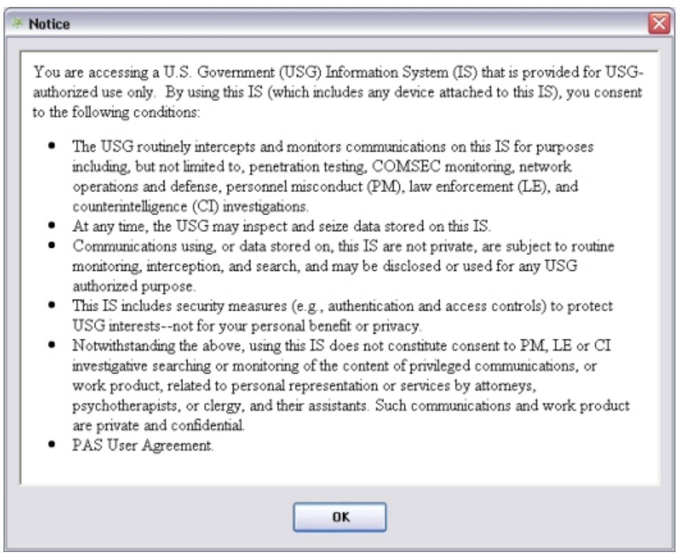

Figure 3-1 Disclaimer notice

3.1 Login with Smartcard (ICC Card)

1) Double-click the PAS-FA icon from the computer desktop.
2) A Fingerprint window will momentarily display with a 'Waiting for device…' message. If a fingerprint scanner is not installed an 'Error initializing Print Reader. Fingerprint capture not available' message displays. Click 'OK'.
   a. If desired (not necessary for Smartcard login), install a fingerprint scanner following scanner manufacturer's instructions and restart PAS-FA.
3) From the main screen, select the login icon on the shortcut toolbar, or select 'Log In' from the 'File' menu at the menu bar located at the top of the screen.
4) Insert ICC card into the card reader.
5) Enter the PIN when prompted.
6) Click 'OK'.
7) Remove the ICC card from the card reader when prompted.

3.2 Login with Smartcard (ICC Card) and Fingerprint

1) Double-click the PAS-FA icon from the computer desktop.
2) The PAS Main Screen displays. A Fingerprint window will momentarily display with a 'Waiting for device…' message. If a fingerprint scanner is not installed an 'Error initializing Print Reader. Fingerprint capture not available' message displays. Click 'OK'.
   a. Install a fingerprint scanner following scanner manufacturer's instructions and restart PAS-FA.
3) From the main screen, select the login icon on the shortcut toolbar, or select 'Log In' from the 'File' menu on the menu bar located at the top of the main screen.
4) Insert the ICC Card into the card reader
5) Enter the PIN when prompted.
6) Click 'OK'.
7) A 'Scan a Fingerprint' message window displays. Place index finger on the fingerprint scanner. The Fingerprint Capture box may display a notice to 'Press Harder' to ensure the quality of the captured print. A notification and color change from red to green on the Fingerprint Capture box indicates a 'Good' fingerprint image capture.
8) When prompted, remove index finger from the fingerprint scanner and the ICC card from the card reader.

3.3 Login with Fingerprint

1) Double-click the PAS-FA icon from the computer desktop.
2) The PAS Main Screen displays. A Fingerprint window will momentarily display with a 'Waiting for device…' message. If a fingerprint scanner is not installed an 'Error initializing Print Reader. Fingerprint capture not available' message displays. Click 'OK'.
   a. Install a fingerprint scanner following scanner manufacturer's instructions and restart PAS-FA.
3) From the main screen, select the login icon on the shortcut toolbar, or select 'Log In' from the 'File' menu on the menu bar located at the top of the main screen.
4) A 'Scan a Fingerprint' message window displays. Place index finger on the fingerprint scanner. The Fingerprint Capture box may display a notice to 'Press Harder' to ensure the quality of the captured print. A notification and color change from red to green on the Fingerprint Capture box indicates a 'Good' fingerprint image capture.
5) When prompted, remove index finger from the fingerprint scanner.

3.4 Login with Barcode

Operators may log into PAS-FA by scanning the barcodes of their ICC cards. Administrators who login using barcodes are not permitted access to administrative features of the Admin menu. Administrators must login with an ICC card, a fingerprint, or an ICC card and a fingerprint to edit settings, import data, archive data, and export reports.

a. Double-click the PAS-FA icon from the computer desktop.
b. The PAS Main Screen displays. A Fingerprint window will momentarily display with a 'Waiting for device…' message. If a fingerprint scanner is not installed an 'Error initializing Print Reader. Fingerprint capture not available' message displays. Click 'OK'.

a. If desired (not necessary for Barcode login), install a fingerprint scanner following scanner manufacturer's instructions and restart PAS-FA.

c. From the main screen, select the login icon from the shortcut toolbar, or select 'Log In' from the 'File' menu.
d. Scan the 3x9 barcode on the back of ICC card or Teslin ID card to log the user into PAS-FA. (Note: Use of barcodes may not be permitted with some ICC cards if SSNs are not allowed).

3.5 Logout

1) From the shortcut tool bar on the main screen, click the 'LOGOUT' icon, or select 'Log Out' from the 'File' menu.
2) If a fingerprint scanner is installed, the operator may alternately scan their fingerprint to log out.
3) PAS-FA terminates the session and records the log out in the user log.

4.0 Administrator Functions

An Administrator is responsible for PAS system maintenance. This function is typically performed by an IT staff member with knowledge of operating systems and databases.

5) Database administration knowledge may be required for system backups and recovery.
6) In addition to the management of user roles and specific reporting abilities, the Administrator role includes all permissions and access rights that an Operator is granted.

4.1 Edit Settings

Users with administrative rights can modify PAS-FA application settings to provide desired functionality for local requirements. To view or modify application settings:

1) Select ‘Edit Settings’ from the Admin menu as shown in Figure 4-1.

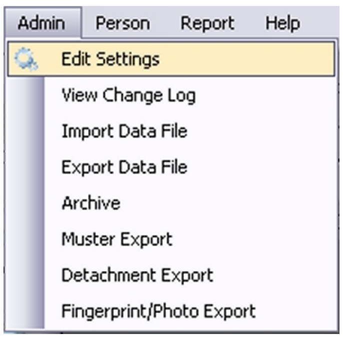

Figure 4-1 Admin, Edit Settings

2) From the Settings screen (see Figure 4-2), modify settings as explained in the following sections. Once all desired changes have been made, click ‘APPLY’ then ‘OK’ to save your changes. A ‘Saving Settings, Please Wait…’ message window appears until the settings are saved.

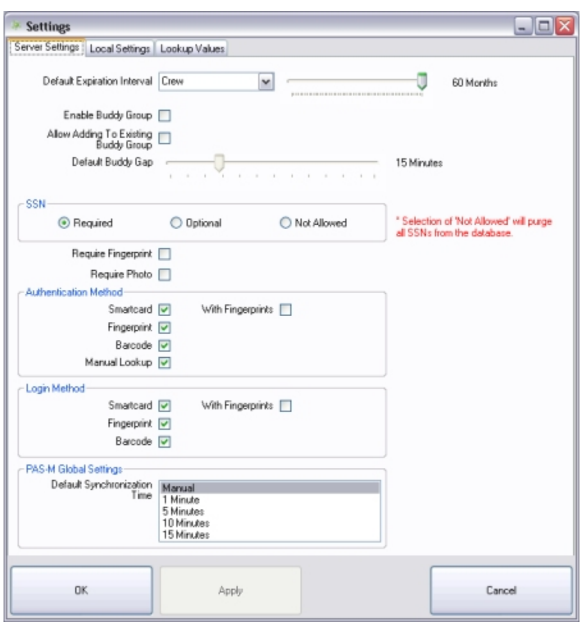

Figure 4-2 Settings

4.1.1 Server Settings

4.1.1.1 Default Expiration Interval

The default expiration interval assigns an expiration date to a cardholder's access privileges when the cardholder record is individually added to the database. For example, if the maximum assignment to a vessel is less than 60 months, the default expiration interval should be modified to reflect that standard. The default expiration interval is set for crew, detachment, and visitors. To set the Default Expiration Interval:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, Click the 'Admin' menu.
3) Select 'Edit Settings' from the Admin menu.
4) The 'Settings' screen opens. Click the combo-box next to Default Expiration Interval to select one of the following person types:
   a. Crew
   b. Detachment
   c. Visitor
5) The interval defaults to the maximum of 60 months. Move the slider next to the person type left or right to uniquely configure the number of months for the specified person type (the slider adjusts in one month increments from 1-60).
6) Click 'APPLY' at the bottom of the 'Settings' screen to apply the change.
7) Click 'OK' to close the 'Settings' screen and return to the Main Screen.

4.1.1.2 Server Settings - Enable Buddy Group

When the 'Enable Buddy Group' option is selected, all departing personnel must be linked to at least one other person before Check-Out is completed.

Note: Exemptions can be made at time of check out to allow individuals to depart a ship or station without a buddy.

To enable Buddy Groups:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, Click the 'Admin' menu.
3) Select 'Edit Settings' from the Admin menu. The 'Settings' screen opens.
4) Check the 'Enable Buddy Group' box.
5) Click 'APPLY' at the bottom of the 'Settings' screen to apply the change.
6) Click 'OK' to close the 'Settings' screen and return to the Main Screen.

4.1.1.3 Server Settings - Allow Adding to Existing Buddy Group

When the 'Allow Adding to Existing Buddy Group' option is selected, Administrators are allowed to add personnel to existing Buddy Groups after the Buddy Group has departed.

Note: The 'Allow Adding to Existing Buddy Group' option is not available unless the 'Enable Buddy Group' option is first selected (see Section 4.1.1.2, *Enable Buddy Group*).

i. An Administrator logs into PAS-FA.
ii. On the Main Screen, Click the 'Admin' menu.
iii. Select 'Edit Settings' from the Admin menu. The 'Settings' screen opens.
iv. Check the 'Allow Adding to Existing Buddy Group' box.
v. Click 'APPLY' at the bottom of the 'Settings' screen to apply the change.
vi. Click 'OK' to close the 'Settings' screen and return to the Main Screen.

4.1.1.4 Server Settings - Default Buddy Gap

Personnel that have been linked through a buddy grouping must return within a specified interval (Gap) as determined by the 'Buddy Gap' setting. Linked personnel not returning within the specified 'Buddy Gap' interval are identified in the 'Buddy Exception' report. To set the default buddy gap:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, Click the 'Admin' menu.
3) Select 'Edit Settings' from the Admin menu. The 'Settings' screen opens.
4) Move the Default Buddy Gap Slider left or right to set the default buddy gap for the specified person type (the slider adjusts in one minute increments from 1-60).
5) Click 'APPLY' at the bottom of the 'Settings' screen to apply the change.
6) Click 'OK' to close the 'Settings' screen and return to the Main Screen.

4.1.1.5 Server Settings - Social Security Number (SSN) Option

Administrators can require SSNs, make them optional, or not allow their use. Selecting 'Not Allowed' purges all SSNs from the database and may restrict use of some barcodes. When SSNs are required, an individual's record that is open for editing must have an SSN in order to save changes to the record. Also, when SSNs are required, persons must have an SSN in order to check in or out. SSN data fields are encrypted in the database, and cannot be edited once entered. To specify use of SSNs:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the 'Admin' menu.
3) Select 'Edit Settings' from the 'Admin' menu. The 'Settings' screen opens.
4) In the 'SSN' field of the 'Settings' screen, click one of the following options:
   a. Require
   b. Optional
   c. Not Allowed
5) Click 'APPLY' at the bottom of the 'Settings' screen to apply the change.
6) Note: If 'Not Allowed' is selected, *all SSNs will be purged from the database*.
   a. Click 'CANCEL' to keep the 'Settings' screen open.
   b. or click 'OK' to purge PAS-FA of all SSNs.
7) Click 'OK' to close the 'Settings' screen and return to the Main Screen.

4.1.1.6 Server Settings - Require Fingerprints

This option requires anyone without fingerprints stored in the PAS-FA Master Database to provide prints at the next check-in/out or when their record is next edited. When fingerprints are required, the 'Prints' data fields are encrypted in the database. To set the 'Require Fingerprints' option:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, Click the 'Admin' menu.
3) Select 'Edit Settings' from the Admin menu. The 'Settings' screen opens.
4) Check the 'Require Fingerprints' checkbox.
5) Click 'APPLY' at the bottom of the 'Settings' screen to apply the change.
6) Click 'OK' to close the 'Settings' screen and return to the Main Screen.

4.1.1.7 Server Settings - Require Photo

This option requires anyone without a photo stored in the PAS-FA Master Database to provide a photo at the next check-in/out or when their record is next edited. Photos are obtained from ICC Cards if possible. To set the ‘Require Photo’ option:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, Click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) Check the ‘Require Photo’ checkbox.
5) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change.
6) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

4.1.1.8 Server Settings - Authentication Methods

Administrators specify the method PAS-FA uses to authenticate personnel during check-in/out.

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) In the ‘Authentication Methods’ section, check all of the applicable methods:
   a. Smartcard (ICC Card)
   b. With Fingerprints (fingerprints in addition to smartcard)
   c. Fingerprint
   d. Barcode
   e. Manual Lookup
5) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change.
6) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

4.1.1.9 Server Settings - Login Methods

Administrators specify the method PAS-FA uses to login personnel.

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) In the ‘Login Methods’ section, check all of the applicable methods:
   a. Smartcard (ICC)
   b. With Fingerprints (fingerprints in addition to smartcard)
   c. Fingerprint
   d. Barcode
5) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change.
6) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

4.1.2 Local Settings

4.1.2.1 Local Settings - Database Path

The database path defaults to the PAS-FA directory of the local machine unless PAS-FA is pointed to an alternate database during setup. When desired, the PAS-FA application is pointed to an external database residing on another computer in a networked environment. This option allows all access points to communicate with a common database.

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) Click the ‘Local Settings’ tab at the top of the screen.
5) The current database path displays in the ‘Database Path’ text box. To point PAS-FA to another Master Database on the same network:
   a. Click the ‘Find’ button. PAS-FA searches for the database and provides results matching the search criteria
   b. Select the desired database and click ‘OK’, or click ‘CANCEL’ if the desired database is not found on the network.
6) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change.
7) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

4.1.2.2 Local Settings - Location

The location defaults to the computer name when it is initially installed. If multiple access points exist, the location can be edited to reflect where processing occurs. For example, it can be changed to read ‘Quarterdeck’, ‘Flight Deck’, ‘Well Deck’, etc. This allows system reports to indicate where personnel entered and/or exited.

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) Click the ‘Local Settings’ tab at the top of the screen.
5) In the ‘Location’ text box, type the name of the applicable access point where processing occurs.
6) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change.
7) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

4.1.2.3 Local Settings - Mode

A ‘Normal’ mode allows an operator and/or administrator to check personnel in and out. The mode can be set to ‘Normal’ (for Check-In and Check-Out), ‘Incoming’ (for Check-In only processing), or ‘Outgoing’ (for Check-Out only processing) if desired. This allows the user to have separate lanes for incoming or outgoing access.

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) Click the ‘Local Settings’ tab at the top of the screen.
5) Click the ‘MODE’ combo-box and set the mode to one of the following:
   a. Normal
   b. Incoming
   c. Outgoing
6) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change.
7) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

4.1.3 Lookup Values

The Lookup Values setting allows data values to be updated (values referenced by other tables cannot be deleted). The Lookup Values that can be modified include:

1) Command/Battalion
2) Country
3) Department/Company
4) Division/Platoon
5) Duty Section
6) Liberty Risk
7) Person Type
8) Rate/Occupation
9) Type Description
10) UIC

To set the Lookup Values:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘Edit Settings’ from the Admin menu. The ‘Settings’ screen opens.
4) Click the ‘Lookup Values’ tab at the top of the screen.
5) Click the ‘Lookup Table’ combo-box, and select a value.
6) The item name and all possible values appear. Make changes to the values by editing text fields, or add new values to blank text fields.
7) Specify a sort order to display the values on reports and in windows. Values automatically display in alphabetical order if no sort order is specified.
8) Click ‘APPLY’ at the bottom of the ‘Settings’ screen to apply the change
9) Click ‘OK’ to close the ‘Settings’ screen and return to the Main Screen.

Operators and Administrators may enter new text descriptions during Add New User or User Update. The values are added to the Lookup Table if they don’t already exist. Values are also added to the Lookup Table during RADM imports (see Section 4.3, *Import and Export Personnel Records*).

4.2 View Change Log

The View Change Log function allows Administrators to view changes made to PAS-FA personnel data during a specified date range.

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the ‘Admin’ menu.
3) Select ‘View Change Log’ from the Admin menu.
4) A Change Log opens as shown in Figure 4-3. The ‘Start’ date defaults to the previous day and the ‘End’ date to the current day, with corresponding results displayed.

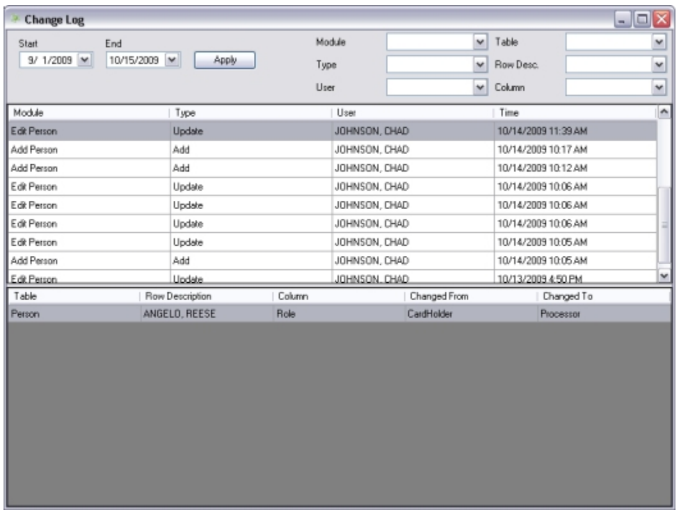

Figure 4-3 Change Log

5) An Administrator can specify a desired date range using the ‘Start’ and ‘End’ drop-down options.
6) Click ‘APPLY’ to see a list of changes for the date range specified.
7) Results can be further searched by using the ‘Module’, ‘Type’, ‘User’, ‘Table’, and ‘Column’ boxes.
    a. Use the down arrows to the right of the categories to select specific search parameters.
    b. Any or all search categories may be used.
    c. Click ‘APPLY’ to see a filtered Change Log.
8) Close out of the Change Log to return to the main screen.

4.3 Import and Export Personnel Records

The PAS-FA application includes import and export options for personnel records.

4.3.1 Import Data File

PAS-FA is based on open technologies to facilitate importing personnel data from other systems in order to populate the system with current and/or updated information about individuals. The feed consists of a file in a standard comma separated value (*.csv) file format. The following data must be included in the extract:

- Last Name
- First Name
- Middle Name
- Social Security Number

- Rank
- Rate
- Paygrade
- UIC
- Department
- Division
- Duty Section
- Expiration Date
- Street1
- Street2
- City
- Region
- Country
- Postal Code
- Phone1
- Phone2
- Email

The following data elements are not included in the data import, but are entered manually by the person reading the import into PAS-FA:

1) Branch
2) Command

Personnel data files can be uploaded from the U.S. Navy's Relational Administrative Data Management System (R-ADM). To use this option, a personnel export file by Duty Section (DS) must be generated by R-ADM in *.csv format (as shown in Figure 4-4) and saved to a directory accessible by PAS-FA (contact the Navy CAC PMO for further information on the proper ad-hoc queries for the RADM export file). Note: R-ADM personnel records imports also update the Lookup Values Tables.

```
lname,fname,mname,rate_rank,dept,div,wc,ssn,deactvtd_dt,prd,eaos,nprt_duty_sect,sect_of,
pay_seq,paygrade,c_uic,c_dept,c_div,c_wc,cmpt_no,bunk_no,street1,street2,city,region,postal
Code,country,phone1,phone2,email,Service,cmd_type
```

Figure 4-4 RADM Export Format

If you create your own *.csv file the column headings must mimic the R-ADM Export Format shown in Figure 4-4

To import a Data File:

1) An Administrator logs into PAS-FA.
2) On the Main Screen, click the 'Admin' menu.

3) Select ‘Import Data File’ from the Admin menu. An ‘Import Data File’ window opens as shown in Figure 4-5.

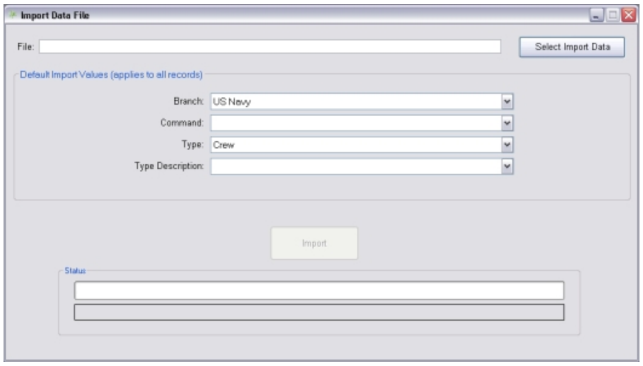

Figure 4-5 Import Data File

4) Select the applicable ‘Branch of Service’, ‘Command’, ‘Type’, and ‘Type Description’.

Note: These settings will be applied to *all* imported records. If these settings vary for personnel, individual records must be edited following import as required. ‘Branch of Service’ and ‘Type’ have default settings (‘US Navy’ and ‘Crew’ respectively, since this information is not included in the imported R-ADM data), but can be modified.

5) Click the ‘SELECT IMPORT FILE’ button (the user can also select a file by typing its name in the ‘File’ box).
6) An ‘Open File’ screen will appear. Select the directory where the import file is located.
7) Select the file to be imported.
8) Click the ‘OPEN’ button.
9) The name of the selected file appears in the ‘Import Data File’ dialog box. If correct, click on the ‘IMPORT’ button.
10) An ‘Import Completed’ dialog box displays upon successful completion of the import. Click ‘OK’ (a user can click ‘CANCEL IMPORT’ at any time).
11) A screen will appear reading ‘The PAS records listed below were not found in the import file’ as shown in Figure 4-6.

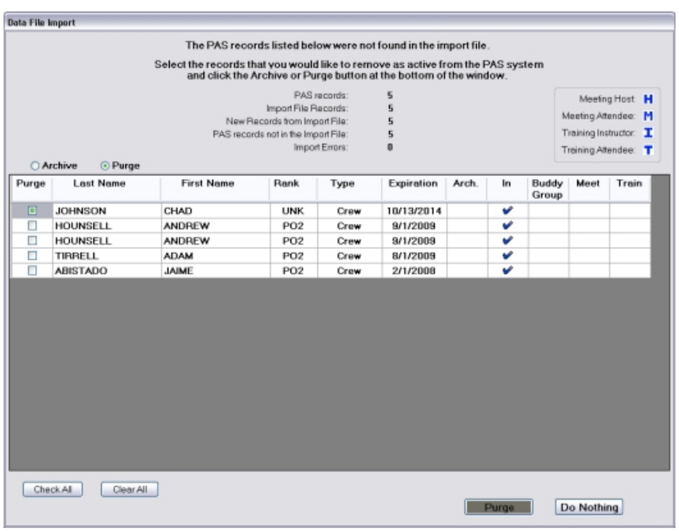

Figure 4-6 Import record screen

12) The Administrator has the option to 1) Archive the records, 2) Purge the records or 3) Do Nothing.

13) To Archive the Records:

a. Choose the Archive radio button on the left hand side of the screen.
b. Select the records to be archived by clicking on the box to the lefty of the entries (users may also use the 'CHECK ALL' or 'CLEAR ALL' buttons).
c. Click 'ARCHIVE'.
d. A screen appears reading 'Are you sure you wish to archive?'. Click 'YES'.
e. A screen appears reading 'The selected records were archived'. Click 'OK'.
f. Click the 'FINISH' button when finished. The Import Data File screen will appear. Continue to import data or close the window to return to the main screen.

To Purge the Records:

- Choose the Purge radio button on the left hand side of the screen.
- Select the records to be purged by clicking on the box to the left of the entries (users may also use the 'CHECK ALL' or 'CLEAR ALL' buttons).
- Click 'PURGE'.
- A screen appears reading 'Are you sure you wish to purge?'. Click 'YES'.
- A screen appears reading 'Are you REALLY sure you wish to purge? Purging will PERMANENTLY DELETE records'. Click 'YES'.
- A screen appears reading 'The selected records were purged'. Click 'OK'.
- Click the 'FINISH' button when finished. The Import Data File screen will appear. Continue to import data or close the window to return to the main screen.

14) To Do Nothing:

1) Click 'Do Nothing'.
2) The Import Data File screen will appear. Continue to import data or close the window to return to the main screen.

4.3.2 Export Data File

To Export a Data File:

3) An Administrator logs into PAS-FA.
4) On the Main Screen, click the 'Admin' menu.
5) Select 'Export Data File' from the Admin menu. An 'Export Data File' window opens as shown in Figure 4-7

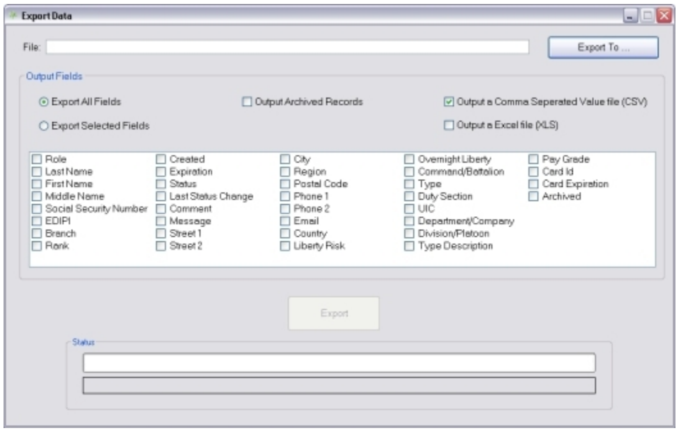

Figure 4-7 Export Data File

6) Users have several output options:
6) Choose ‘Export All Fields’ or ‘Export Selected Fields’ by clicking either field.
    i. If ‘Export Selected Fields’ is chosen, click on the desired export fields displayed: ‘Role’, Last Name’, ‘First Name’ etc.
7) Choose to Output Archived Records by clicking the ‘OUTPUT ARCHIVED RECORDS’ field.
8) Choose to ‘Output a Comma Separated Value File (CSV)’ or ‘Output an Excel File’ by clicking either field.
7) When finished selecting output options, click the ‘EXPORT TO’ button.
8) A ‘Save As’ window will appear. A default file name is automatically generated in the ‘File Name’ field (a new name can be typed in its place).
9) Chose the location where the file is to be saved in the ‘Save In’ field.
10) Click ‘SAVE’.
11) Close out of the screen to return to the ‘Export Person Data’ window. Continue to export data or close the window to return to the main screen.

4.4 Archive and Purge Database Records

The option to Archive and Purge database records enables Administrators to manage active database tables and maintain PAS-FA’s processing speed and efficiency.

4.4.1 Archiving Records

The Archive process moves events that occurred prior to a specified date from the active database tables to archive tables. The Archive option is only available to Administrators on the PAS-FA Master Database.

- Archived personnel can be in a checked-in or out status.
    - Date selection defaults to data more than 90 days old but can be modified.
- Archiving a Person includes all the Person’s Images and Fingerprints. Personnel are archived by UIC, Command, and Person Types other than ‘Crew’.

These options archive selected personnel regardless of the archive date selected:

- Archive Events - Archives all events that are older than the selected date.

- Archive Buddy Groups - Archives all Buddy Groups that have an end date that is older than the selected date.
- Archived Expired Personnel - Archives expired personnel, along with their event and closed Buddy Group entries, whose expiration date is older than the selected date.
- Archive Selected Personnel - Archives selected personnel, along with their events and Buddy Group entries.

To Archive Records:

1) Select ‘Archive’ from the Admin menu.
2) Select the ‘Archive’ tab as shown in Figure 4-8.
3) Select the desired date from the ‘Selected Date’ combo-box menu. Data preceding that date will be archived.

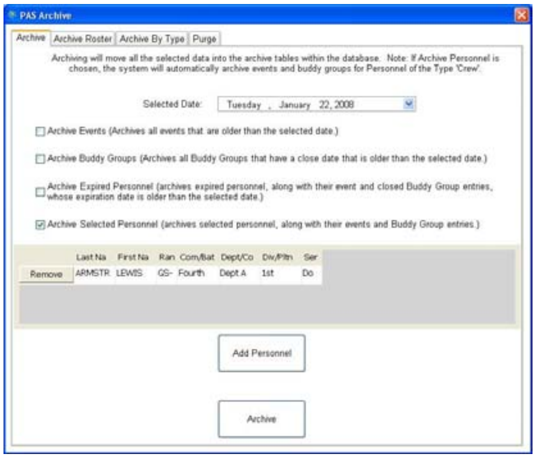

Figure 4-8 PAS Archive screen

4) Select the data to be archived by checking the applicable check boxes that correspond to the following data:
   a. Archive Events
   b. Archive Buddy Groups
   c. Archive Expired Personnel
   d. Archive Selected Personnel

   If the ‘Archiving Selected Personnel’ check box is checked, an ‘ADD PERSONNEL’ button appears. Click the ‘ADD PERSONNEL’ button to display a ‘Find Person’ screen, and search for personnel to archive. Click the display bar of the person to be archived on the ‘Find Person’ screen to add them to the list of personnel to be archived. Click the ‘REMOVE’ button to remove erroneous personnel from the archive list. Multiple data sets may be selected and archived simultaneously.

5) Click the ‘ARCHIVE’ button.
6) A ‘Confirm Archive’ dialog box displays. Click ‘YES’ to archive, or ‘NO’ to cancel.

4.4.2 Archiving Rosters

1) Select ‘Archive’ from the Admin menu.
2) Select the ‘Archive Roster’ tab as shown in Figure 4-9.
3) Select the date (from the ‘Selected Date’ combo-box menu) for which all records with preceding activity are to be permanently moved to the archives.

4) Select the data to be archived (e.g. Meeting Rosters, Training Rosters). Multiple data sets may be selected and archived simultaneously.
5) Click the ‘ARCHIVE’ button.
6) A ‘Confirm Archive’ message displays asking, “Are you sure you wish to archive?” Click ‘YES’ to continue with the archive process.
7) An ‘Archive Complete’ message displays after selected rosters have been moved to the archive tables. Click ‘OK.’
8) Close the ‘PAS Archive’ screen.

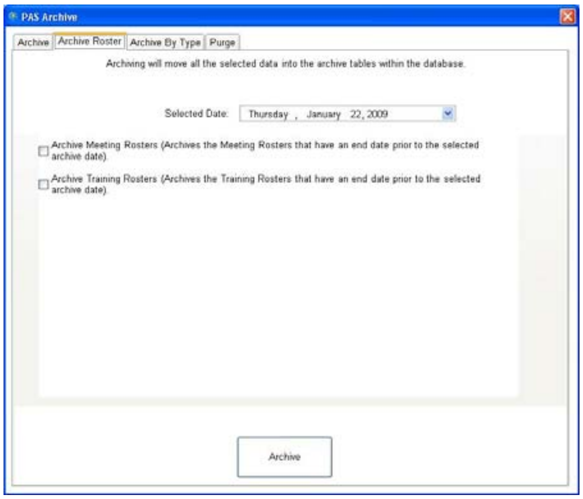

Figure 4-9 PAS Archive screen

4.4.3 Archive By Type

1) Select ‘Archive’ from the Admin menu.
2) Select the ‘Archive By Type’ tab as shown in Figure 4-10.
3) Select the Date, Type, and Type Description from the applicable combo-boxes.
4) Click the ‘ARCHIVE’ button to archive personnel.

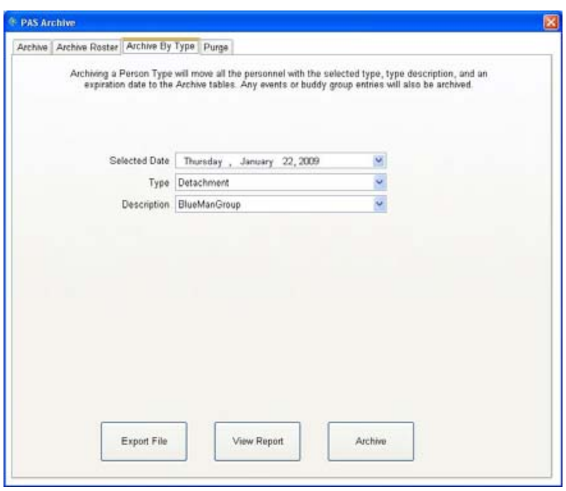

Figure 4-10 PAS Archive screen

5) Click the ‘VIEW REPORT’ button to view PAS reports of personnel archived.
6) Click the ‘EXPORT FILE’ button to export a ‘Detachment Export’ report of personnel archived.

7) Close the 'PAS Archive' screen.

4.4.4 Purging Records

The option to purge database records allows Administrators to manage the volume of the PAS-FA database by reducing the size of the archives.

1) Select 'Archive' from the Admin menu.
2) Archive data (see Sections 4.41, *Archiving Records*; 4.42, *Archiving Rosters*; and 4.43, *Archiving by Type*).
3) Select the 'Purge' tab from the 'Archive' screen as shown in Figure 4-11.

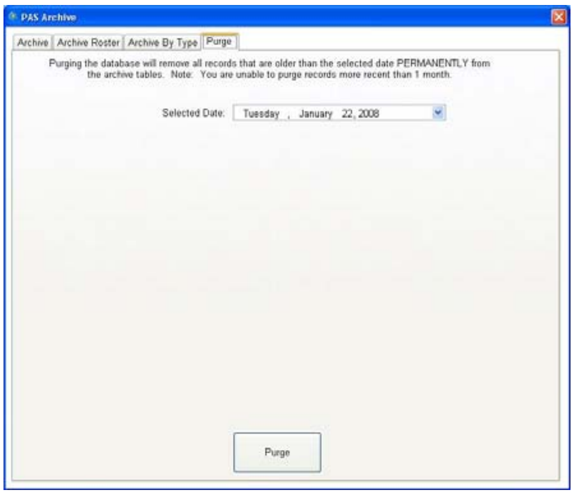

Figure 4-11 PAS Archive screen

4) Click the 'PURGE' button.
5) A 'Confirm Purge' message displays asking, "Are you sure you wish to purge? Purging will PERMANENTLY DELETE records." Click 'YES' to continue the purge process.
6) A second 'Confirm Purge' message displays (see Figure 4-12) asking, "Are you REALLY sure you wish to purge? Purging will *PERMANENTLY DELETE* records."

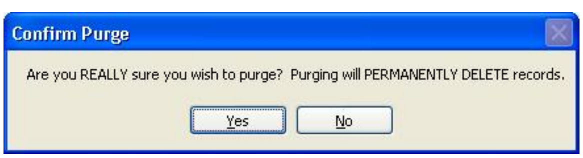

Figure 4-12 Second Confirm Purge

7) This is the final notice before archived records are *permanently* deleted from PAS. Click 'YES' to purge data.

8) A ‘Purge complete’ message displays after archived records are permanently deleted as shown in Figure 4-13.

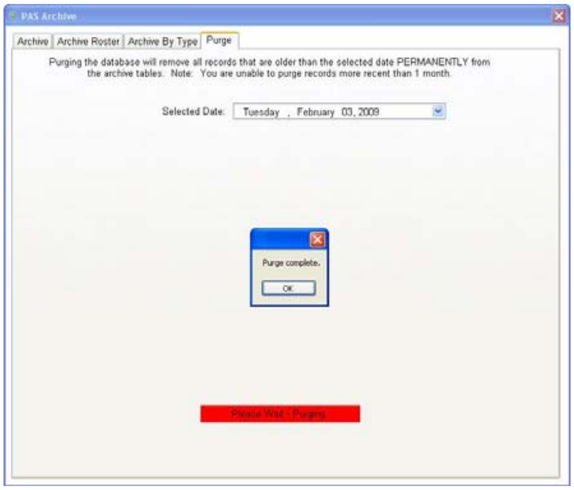

Figure 4-13 Purge complete

9) Click ‘OK’ on the ‘Purge complete’ message.
10) Close the ‘PAS Archive’ screen.

4.5 Exports

4.5.1 Muster Export

The ‘Muster Export’ displays the total number of cardholders checked in and total number of cardholders checked out of each department at a specified time. The muster report exports to a spreadsheet.

a. Click ‘MUSTER EXPORT’ on the ‘Admin’ menu. A ‘Department Muster Export’ window displays as shown in Figure 4-14.

Figure 4-14 Department Muster Export window

b. Use the combo boxes to specify a date and time for the export.
c. Click the ‘EXPORT FILE’ button. A ‘Save As’ dialog box displays.
d. Specify a location to save the file.
e. Click the ‘SAVE’ button. The export is saved to the location indicated in the ‘Save As’ dialog.

4.5.2 Detachment Export

The ‘Detachment Export’ displays selected person types and descriptions for a specified date. The report exports to a spreadsheet and has worksheets for ‘Demographics’, ‘Accountability’, and ‘Rosters’. It can be generated prior to archiving data by type or through the following:

- Click ‘DETACHMENT EXPORT’ on the ‘Admin’ menu. A ‘Detachment Export’ window displays as shown in Figure 4-15.

Figure 4-15 Detachment Export window

- Use the combo boxes to specify a ‘Type’, and ‘Description’.
- Click the ‘EXPORT FILE’ button. A ‘Save As’ dialog box displays.
- Specify a location to save the file
- Click the ‘SAVE’ button. The export is saved to the location indicated in the ‘Save As’ dialog.

4.5.3 Fingerprint/Photo Export

The ‘Fingerprint/Photo Export’ displays personnel who have not enrolled fingerprints or captured photos. Both reports export to a spreadsheet.

1) Click ‘FINGERPRINT/PHOTO EXPORT’ on the ‘Admin’ menu. A ‘Fingerprint/Photo Export’ window displays as shown in Figure 4-16.

Figure 4-16 Fingerprint/Photo Export window

2) Use the combo box to select either the ‘Fingerprint’ or the ‘Photo’ export type.
3) Click the ‘EXPORT FILE’ button. A ‘Save As’ dialog box displays.
4) Specify a location to save the file
5) Click the ‘SAVE’ button. The export is saved to the location indicated in the ‘Save As’ dialog.

5.0 User Management

5.1 Add Personnel

Personnel added to PAS-FA are assigned a role and a type. The four user roles are:

1) Cardholder
2) Processor - Allows check in/out of persons, and management of meeting/training data (people with this role cannot edit cardholder records i.e. liberty risk, messages, comments, etc.).
3) Operator - Responsible for general operation of PAS-FA (i.e. enrolling users, check-in, check-out).
4) Administrator - Assigns or removes a user's role and changes security authentication methods of the application.

The three person types are:

1) Crew - Primary group of personnel.
2) Detachment - Temporary group of persons that are not part of the primary group.
3) Visitor - Individual that is not part of the crew or detachment.

5.1.1 Adding a Person Not Registered in the Database

The 'Add Person' function adds records of personnel not previously registered in the PAS-FA database. Personnel are added using manual data entry, ICC Card, ICC Card barcode, or fingerprint.

5.1.1.1 Add a Person, Manual Entry

1) Click the Add shortcut on the shortcut toolbar on the main screen, or click 'New' on the 'Person' menu.
2) The 'Add Person' screen appears as shown in Figure 5-1.

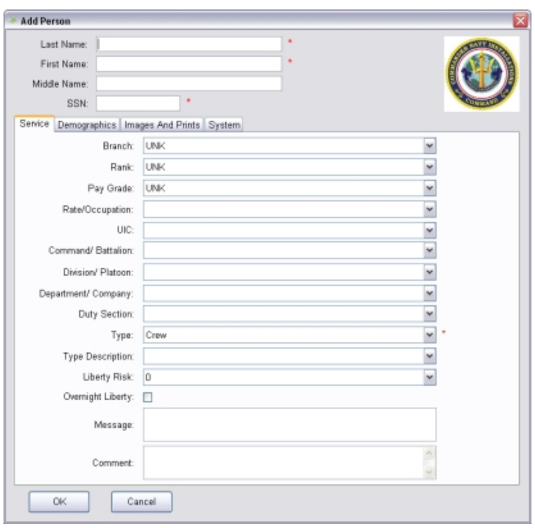

Figure 5-1 Add Person screen

3) Add data using the applicable text fields and combo-boxes (required fields are denoted by a red asterisk next to the field).
   a. First Name
   b. Middle Name
   c. Last Name

d. SSN (mandatory if required in the settings, but not editable if not allowed in the settings).

4) Use the ‘Service’ tab to enter personnel data:
   a. Branch
   b. Rank
   c. Pay Grade
   d. Rate/Occupation
   e. UIC
   f. Command/Battalion
   g. Division/Platoon
   h. Department/Company
   i. Duty Section
   j. Type
   k. Type Description
   l. Liberty Risk
   m. Click the ‘OVERNIGHT LIBERTY’ box to allow overnight liberty privileges.
   n. Message
   o. Comment
5) Use the ‘Demographics’ tab text and combo-boxes to enter data:
   a. Street
   b. City
   c. Zip/Postal Code
   d. Country
   e. State / Region
   f. E-mail
   g. Phone 1
   h. Phone 2
6) Click the ‘IMAGES AND PRINTS’ tab (see Section 5.1.4, *Adding Digital Photos*).
   a. Click the ‘ADD PHOTO’ button. Since the PAS-FA does not yet support a camera option, the user must select a picture image from the ICC Card or a file on the computer.
   b. A ‘Select Input Location’ dialog displays (see Figure 5-2) with options to extract an image from an ICC Card or manually add an image.

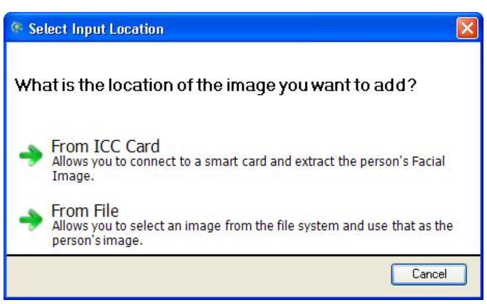

Figure 5-2 Select Input Location

c. If ‘From ICC Card’ is selected, insert ICC card and enter PIN when prompted.
d. If ‘From File’ is selected, an Open file dialog displays allowing the user to browse for the image file.
   i. The ‘From Card’ check-box is checked if an image was imported from the ICC Card. The ‘From Card’ check-box is disabled for manual entry.

    ii. The ‘Add Photo’ button is disabled if the image was imported from an ICC Card.

7) Click the ‘IMAGES AND PRINTS’ tab.
8) Click the ‘ENROLL PRINTS’ button.
9) Capture fingerprint images using the PAS Fingerprint Wizard (see Section 5.1.5, *Enrolling Print Images*).
10) Select the ‘System’ tab.
11) Click the ‘ROLE’ combo-box to designate the person’s role as Cardholder, Processor, Operator or Administrator.
12) Click the ‘Expiration Date’ combo-box to select the person’s expiration date. The expiration date will display the current date plus the default expiration interval designated in the settings.
13) Click ‘SAVE’ to add the person, or ‘CANCEL’ to close and return to the Main screen.

5.1.1.2 Add a Person with an ICC Card or Barcode

1) To add a new person with an ICC Card or barcode, either:
    a. Insert the person’s ICC card into the reader and when prompted, instruct the person enter their PIN,
    b. Scan the barcode from the person’s ICC card (if SSNs are not allowed, barcodes from some ICC cards may not be used).
    c. Insert the person’s ICC Card into the reader. Instruct the person to enter their PIN when prompted, and then scan their index finger.
2) PAS-FA performs a search of the master database. If the person is found, their record displays for check in/check out. If the person is not found, an audible alert sounds, and a ‘Select Action’ dialog box appears (see Figure 5-3) with options to add a new person or match the ICC card with a person already in the database.

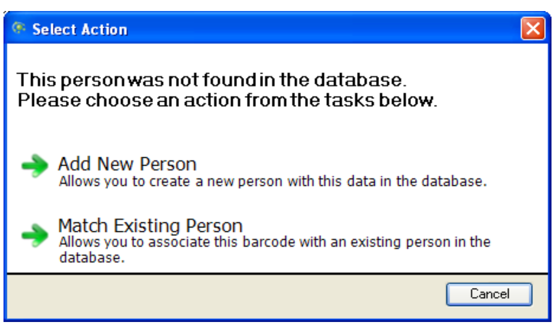

Figure 5-3 Select Action dialog box

3) Select ‘Add New Person’.
4) The ‘Add Person’ screen appears with the person’s name and SSN pre-populated. Edit the person’s service, demographics, images and prints, and system data.
5) Click ‘OK’ to add the person, or ‘CANCEL’ to return to main screen.

5.1.1.3 Match Existing Person

If ‘Match Existing Person’ is selected on the ‘Select Action’ dialog, the ‘Find Person’ screen will display.

1) Perform a user search (see Section 5.1.2, *User Search*).
2) The Check In/Out screen displays. Click ‘CHECK IN,’ ‘CHECK OUT,’ or ‘CANCEL’.
3) The ICC card is matched to the individual’s record in the database.

5.1.1.4 Add a User with Fingerprint Scan

1) Scan the person’s index finger.
2) PAS-FA performs a search of the master database. If the person is found, their record displays for check in/check out. If the person is not found, an audible alert sounds, and a ‘Select Action’ dialog box displays (see Figure 5-4) with an option to add a new person.

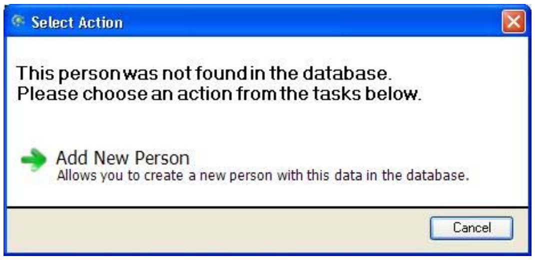

Figure 5-4 Select Action for fingerprint scan

3) Select ‘Add New Person’.
4) The ‘Add Person’ screen appears. Add the person’s name, SSN (if required), service, demographics, images and prints, and system data.
5) Click ‘OK’ to add the person, or ‘CANCEL’ to return to main screen.

5.1.2 User Search

Use any of these methods to perform a user search:

1) From the main screen (see Figure 5-5), filter the list of cardholders by clicking the ‘SEARCH’ combo box, and selecting one of the following filter criteria:
   a. Last Name
   b. SSN (Last 4 digits)
   c. Rank
   d. Command/Battalion
   e. Department/Company
   f. Division/Platoon

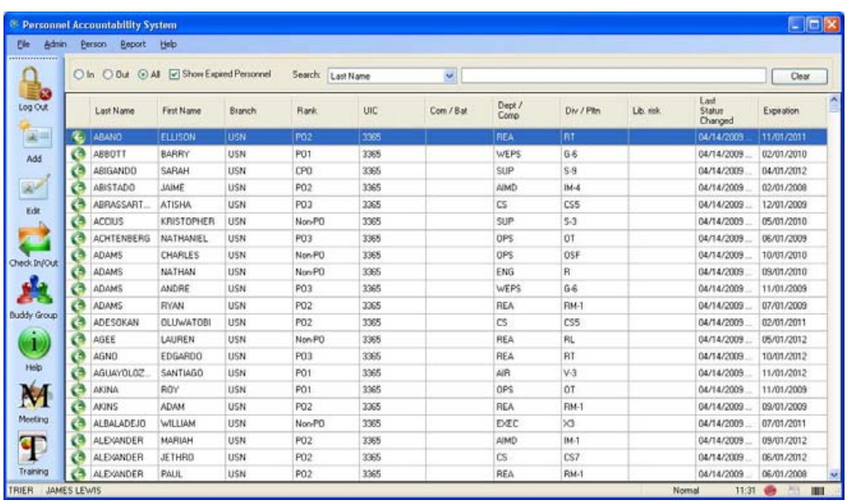

Figure 5-5 PAS main screen

The text box to the right of the ‘Search’ combo box activates when an option is selected so that a selection criteria can be typed (the cardholder list auto-filters as criteria is entered). Click the ‘CLEAR’ button to the right of the text box to remove typed criteria.

2) Select the ‘IN’ or ‘OUT’ radio buttons to filter the cardholder list by check in/check out status. The default ‘ALL’ radio button displays all cardholders regardless of status.
3) Click column headers to sort (ascending or descending) by heading.
4) Open the cardholder’s record in one of the following ways:
    a. Double-click the cardholder row to open the ‘Edit Person’ screen.
    b. Highlight the cardholder row and click the ‘Edit’ icon from the vertical toolbar on the left of the main screen to open the ‘Edit Person’ screen.
    c. Highlight the cardholder row and click the ‘CHECK IN/OUT’ icon from the vertical toolbar on the left of the main screen to open the ‘Check In/Out’ screen.
    d. Right-click the cardholder row to display a shortcut menu as shown in Figure 5-6. Select ‘Edit’ to open the ‘Edit Person’ screen, or ‘Check In/Check Out’ to change the cardholder’s status.

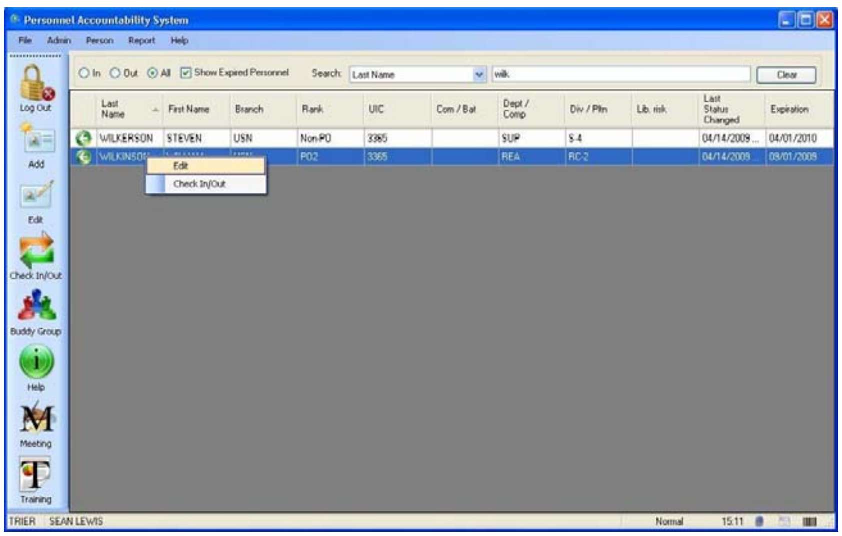

Figure 5-6 Shortcut menu

5.1.3 Assigning User Privileges to Existing Cardholders

1) Perform a search for a cardholder's record in any manner previously described (see Section 5.1.2, *User Search*).
2) From the 'Edit Person' screen, select the 'System' tab as shown in Figure 5-7.

Figure 5-7 Edit Person

3) Click the 'ROLE' combo box.
4) Select Cardholder, Processor, Operator or Administrator as the person's new role.
5) Click 'OK' to save changes and close the 'Edit Person' screen.

5.1.4 Adding Digital Photos

Digital photos of cardholders are displayed each time a Cardholder checks in or out, or whenever the 'Edit Person' dialog of the Cardholder is active. Photos are displayed from the images stored on the person's ICC Card or from stored images. *Image deletion from ICC Cards is not permitted*. To add an image:

1) From the 'Edit Person' screen, select the 'Images' tab.
2) Click the 'ADD PHOTO' button

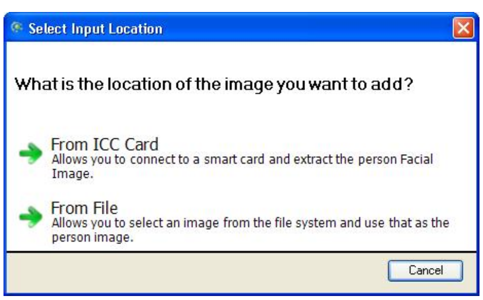

Figure 5-8 Select Input Location, Images

3) A 'Select Input Location' window displays as shown in Figure 5-8. Click to obtain an image from either an ICC Card or from a file.
4) If the image is from an ICC Card, insert the card and have the person enter their PIN when prompted to obtain the photo.

5) If the image is from the file system, an 'Open-file' dialog box appears. Select the image file that contains the person's photo.
6) Click 'OPEN' to import the image to the PAS-FA photo table.
7) Click 'OK' on the 'Edit Person' screen to add the image to the cardholder's record.

Important: During upgrades from PAS/CAC to PAS-FA, photos are copied from the directory located in the 'Picture Path' to a photo table in the PAS-FA database. Once copied, users are given the option to delete the photo file in the Picture Path.

5.1.5 Enrolling Print Images

If the 'Require Fingerprints' check-box in the server settings is checked, each person in PAS-FA is required to have fingerprint images stored in the database. Fingerprints must be captured from a scanning device. Captured prints are matched against fingerprint minutia collected and/or against fingerprint minutia stored on ICC Cards. Fingerprints will be scanned a minimum of two times (2X) during enrollment in order to store a composite print for enhanced matching capabilities of future scans.

1) From the either the 'Add Person' or the 'Edit Person' screens, click the 'Image and Prints' tab.
2) Click the 'Enroll Prints' button to launch the PAS Fingerprint Wizard, and capture prints (*Note: Old print records cannot be deleted. New print records are created and over-write the old prints*).

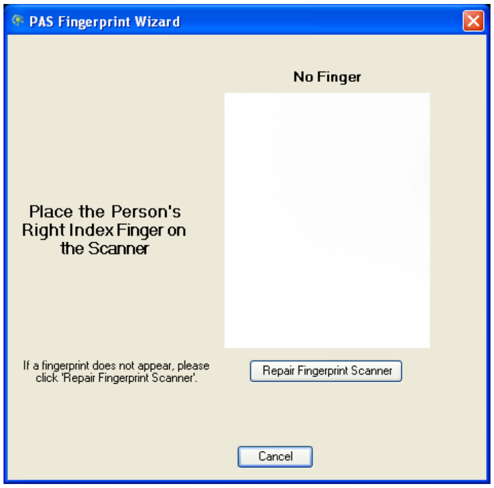

Figure 5-9 PAS Fingerprint Wizard

3) Place the person's right index finger on the scanner as prompted by the PAS Fingerprint Wizard as shown in Figure 5-9. If a fingerprint scanner is installed, but a fingerprint does not appear in the white field of the wizard, click the 'Repair Fingerprint Scanner' button (see Section 8.2, *Repair Fingerprint Scanner*).
4) The fingerprint image will appear on the Fingerprint Wizard and in a Fingerprint Capture box. The Fingerprint Capture box may display a notice to 'Press Harder' to ensure the quality of the captured print. A notification and color change from red to green on the Fingerprint Capture box indicates a 'Good' fingerprint image capture as shown in Figure 5-10.

Figure 5-10 Fingerprint Capture box

5) Instruct the individual to remove their finger from the scanner when prompted (the Fingerprint Wizard requires at least one additional scan of the fingerprint).
6) Place the person's left index finger on the scanner when prompted. The PAS Fingerprint Wizard and the Fingerprint Capture box close when images of both the left and right index fingerprints are successfully captured.
7) A Print Capture date displays next to the 'Enroll Prints' button.

5.2 Edit Personnel

i. Click the 'Edit' shortcut on the shortcut toolbar on the main screen, or click 'Edit' on the 'Person' menu.
ii. The 'Edit Person' screen appears. Administrators can edit personnel information contained in any of the tabs:

Service
Demographics
Images and Prints
System

5.3 Import and Export Personnel Records

For information on Importing and Exporting Data Files, refer to Section 4.3, *Import and Export Personnel Records.*

5.4 Archive and Purge Database Records

For information on Archiving and Purging Records and Rosters, refer to Section 4.4, *Archive and Purge Database Records.*

6.0 Operator/Processor Functions

This section provides Users an overview of PAS-FA functionality and guides the Operator/Processor through the steps typically encountered during routine use of PAS-FA in effectively managing personnel accountability.

6.1 Main Screen (Records Display)

The main screen displays the active (un-archived) records of all personnel stored in the PAS-FA database as shown in Figure 6-1.

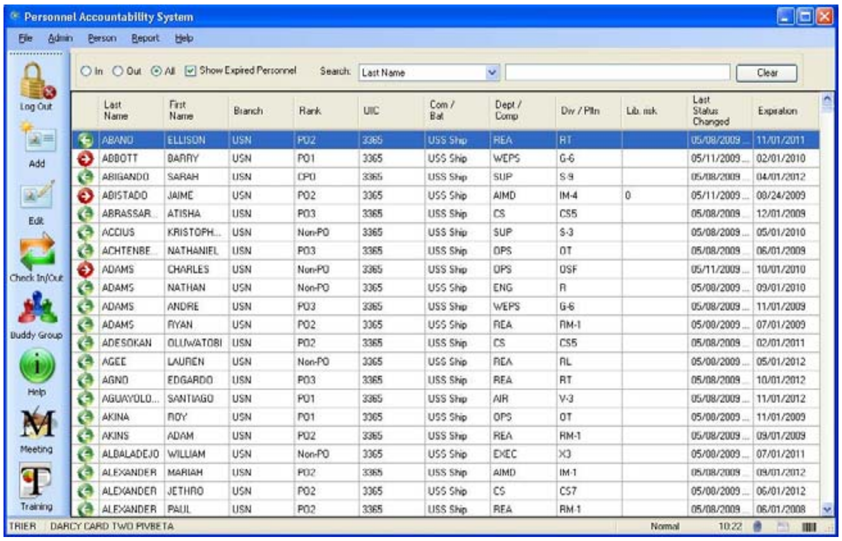

Figure 6-1 Main Screen (Records Display)

The main screen displays information for each individual database record (records may be sorted by any field by clicking on the field title at the top of each column):

1) Current Status indicator in front of each name.

    A green bullet with a white left arrow indicates the cardholder is checked in.

    A red bullet with a white right arrow indicates the cardholder is checked out.

2) Cardholder's name.
3) Branch of Service.
4) Rank.
5) Duty assignment information (e.g., UIC, Command or Battalion, Department or Company and Division or Platoon).
6) Liberty Risk assignment code.
7) Last Status Change (When an individual last checked in or out).
8) Expiration date (Date when the individual is no longer expected to require access).

PAS-FA status appears on a status bar at the bottom of the main screen. The following information is displayed:

1) Location
2) Operator's Name
3) Mode of Operation (Normal, Incoming, or Outgoing)
4) Time clock
5) Symbols for authentication methods (fingerprint, smartcard, barcode)

6.1.1 Alter Main Screen Appearance

All of the shortcut icons on the vertical tool bar on the left side of the main screen may not appear if PAS-FA is not maximized.

- Click the right arrow below the last visible icon on the tool bar to display and use the remainder of the icons as shown in Figure 6-2.

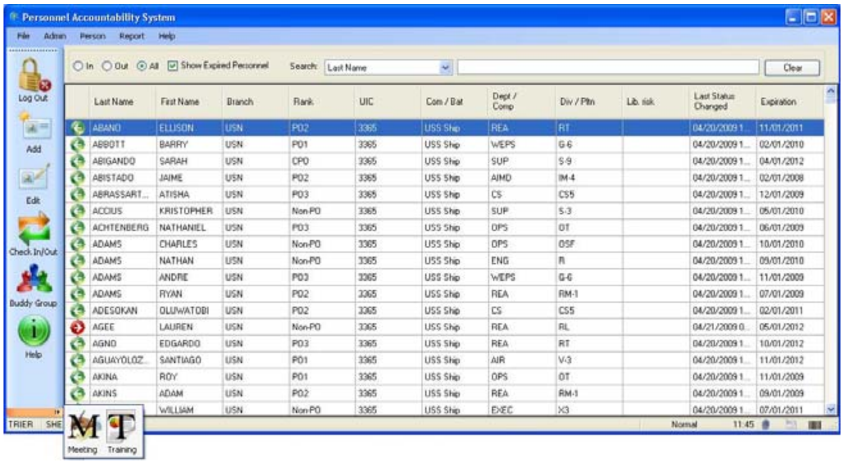

Figure 6-2 Vertical Toolbar Icons

- The vertical shortcut toolbar can be repositioned horizontally above the filters on the main screen by clicking, holding, dragging, and dropping the handle above the icons as shown in Figure 6-3.

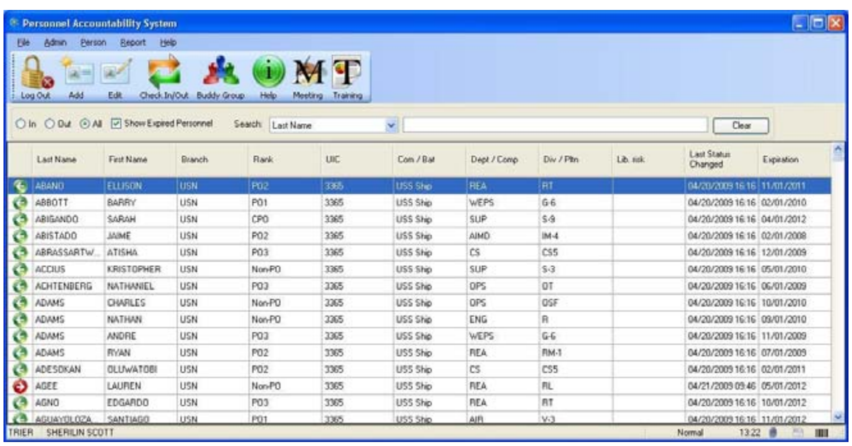

Figure 6-3 Shortcut Toolbar Repositioned

- The size of the toolbar can be changed by right-clicking on it and selecting or deselecting the ‘Large Icons’ and/or ‘Show Text’ items as shown in Figure 6-4.

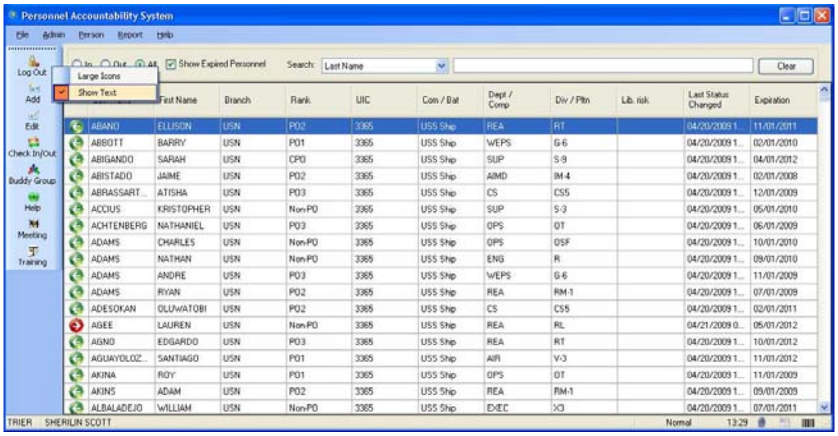

Figure 6-4 Shortcut Toolbar small icons

6.1.2 Searching and Filtering Records

There are two methods to narrow or expand the displayed list of cardholder records through the use of the search field at the top of the main screen (these methods can be used separately or together).

1) Select a button to filter Cardholder records by current status.

Displays only the personnel that are currently checked in.

Displays only the personnel that are currently checked out.

Displays all personnel, regardless of their in/out status.

2) To filter or search cardholder records by name, in the Search text box, type the cardholder's last name in the 'Search' box shown in Figure 6-5.

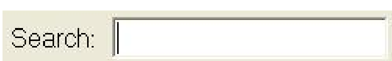

Figure 6-5 Search Box

The main screen immediately displays only those cardholders whose last names begin with the letters typed. If the entire last name is typed in, only the record(s) of Cardholders with that last name are displayed.

3) To clear the search box, click the 'Clear' button to the right of the Search Box.

6.2 Check Personnel In and Out

The Check In/Out functions are used to check personnel in and out as they board and exit a designated ship or facility. The following procedures assume the PAS station is set to 'Normal' (see Section 6.2.6, *Rapid Check In/Out* for other options).

6.2.1 Check In and Check Out Using the ICC Card

Operators can check a cardholder in or out by inserting the individual's ICC Card into a card reader. The cardholder's database record is then displayed. This method of processing provides an additional level of security since it requires correct ICC Card PIN entry for enhanced cardholder identity verification.

1) Starting at the main screen, insert the ICC Card of the processing cardholder into the card reader.
2) When prompted, the cardholder enters their assigned PIN.
3) The cardholder or operator presses the 'Enter' or 'Return' key of the keyboard, or the operator clicks on the 'OK' button of the 'Enter PIN' dialog box.

4) Remove the ICC Card from the reader when prompted.
5) If the person has a liberty risk, an audible alert sounds and a ‘Liberty Risk’ dialog box displays as shown in Figure 6-6. Click ‘OK’ to proceed.

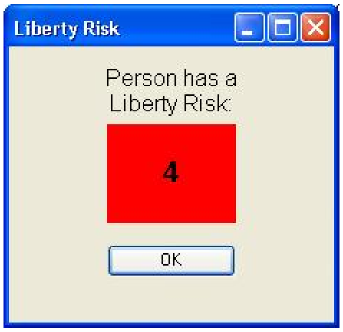

Figure 6-6 Liberty Risk dialog box

6) The ‘Check In/Out’ dialog appears displaying (as applicable):
   a. The person’s name and rank
   b. A red ‘Liberty Risk’ notification box
   c. Service information
   d. A photo of the person if one exists on file
   e. Comments
   f. Messages in a yellow message text box with a ‘Clear Message’ button as shown in Figure 6-7. Click the ‘Clear Message’ button to remove messages from the Message field on both the ‘Check In/Out’ dialog and the ‘Edit Person’ screen.

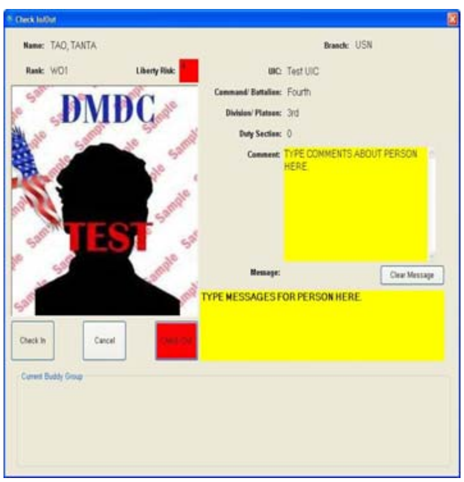

Figure 6-7 Check In/Out dialog

7) The current status of the person dictates the active buttons for checking in and checking out. If the person’s current status is checked in, then a red ‘Check Out’ button is enabled. If the person’s current status is checked out, then a green ‘Check In’ button is enabled. A white ‘Cancel’ button is permanently enabled on the ‘Check In/Out’ dialog. Click one of the following:
   a. ‘CHECK IN’ to check the person in from liberty
   b. ‘CHECK OUT’ to check the person out on liberty
      i. If ‘Enable Buddy Group’ is selected in ‘Settings’ (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*) a ‘Create New Buddy Group’ screen containing the person’s name appears. Add to or check out the

Buddy Group following the instructions found in Section 6.3.1, *Create Buddy Groups*.

ii. If 'Enable Buddy Group' *and* 'Allow Adding to Existing Buddy Group' are selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, A*llow Adding to Existing Buddy Group*), an 'Add to Buddy Group' screen appears displaying existing Buddy Groups. Continue with the instructions found in Section 6.3.5.1, *Add Persons to Existing Buddy Group*s.

c. 'CANCEL' to quit the process and leave the person's status unchanged.

6.2.2 Check-In and Check-Out Using the Barcode

Operators can check cardholders in and out by scanning the 3x9 barcode located on the back of the cardholder's ICC Card or Teslin ID card. This method expedites processing by eliminating cardholder PIN entry requirements.

1) Starting at the main screen, scan the barcode of the processing cardholder's ICC Card or Teslin ID.
2) If the person has a liberty risk, an audible alert sounds and a 'Liberty Risk' dialog box displays. Click 'OK' to proceed.
3) The 'Check In/Out' dialog appears displaying (as applicable):
   a. The person's name and rank
   b. A red 'Liberty Risk' notification box
   c. Service information
   d. A photo of the person if one exists on file
   e. Comments
   f. Messages in a yellow message text box with a 'Clear Message' button. Click the 'CLEAR MESSAGE' button to remove messages from the Message field on both the 'Check In/Out' dialog and the 'Edit Person' screen.
4) The current status of the person dictates the active buttons for checking in and checking out. If the person's current status is checked in, then a red 'Check Out' button is enabled. If the person's current status is checked out, then a green 'Check In' button is enabled. A white 'Cancel' button is permanently enabled on the 'Check In/Out' dialog. Click one of the following:

1) 'CHECK IN' to check the person in from liberty
2) 'CHECK OUT' to check the person out on liberty
   i. If 'Enable Buddy Group' is selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*) a 'Create New Buddy Group' screen containing the person's name appears. Continue to add to or check out the Buddy Group following the instructions found in Section 6.3.1, *Create Buddy Groups*.
   ii. If 'Enable Buddy Group' *and* 'Allow Adding to Existing Buddy Group' are selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, A*llow Adding to Existing Buddy Group*), an 'Add to Buddy Group' screen appears displaying existing Buddy Groups. Continue with the instructions found in Section 6.3.5.1, *Add Person's to Existing Buddy Group*s.
3) 'CANCEL' to quit the process and leave the person's status unchanged.

6.2.3 Fingerprint Check-In and Check-Out

Operators can check cardholders in and out by scanning their fingerprints. This method expedites processing by eliminating cardholder PIN entry requirements.

Starting at the main screen, scan the cardholder's index finger using the fingerprint scanner (refer to fingerprint scanning instructions in Section 5.1.5, Enrolling Print Images).

1) If the fingerprint does not match any fingerprints in PAS, a message displays stating the person is not in the database, and asks if you wish to add them. Click 'YES' to add the person or 'NO' to cancel the process and remove the person's index finger from the scanner (note: processors cannot add new people to the database).
   - If the fingerprint matches, remove index finger from the scanner and proceed with check in/out.
   - If the person has a liberty risk, an audible alert sounds and a 'Liberty Risk' dialog box displays. Click 'OK' to proceed.
2) The 'Check-In/Out' dialog appears displaying the following (as applicable):
   - The person's name and rank
   - A red 'Liberty Risk' notification box
   - Service information
   - A photo of the person if one exists on file
   - Comments in a yellow box
   - Messages in a yellow text box with a 'Clear Message' button. Click the 'Clear Message' button to remove messages from the Message field on both the 'Check In/Out' dialog and the 'Edit Person' screen.

3) The current status of the person dictates the active buttons for checking in and checking out. If the person's current status is checked in, then a red 'Check Out' button is enabled. If the person's current status is checked out, then a green 'Check In' button is enabled. A white 'Cancel' button is permanently enabled on the 'Check In/Out' dialog. Click one of the following:
   5) 'CHECK IN' to check the person in from liberty
   6) 'CHECK OUT' to check the person out on liberty
   1) If 'Enable Buddy Group' is selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*) a 'Create New Buddy Group' screen containing the person's name appears. Continue to add to or check out the Buddy Group following the instructions found in Section 6.3.1, *Create Buddy Groups*.
   2) If 'Enable Buddy Group' *and* 'Allow Adding to Existing Buddy Group' are selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, A*llow Adding to Existing Buddy Group*), an 'Add to Buddy Group' screen appears displaying existing Buddy Groups. Continue with the instructions found in Section 6.3.5.1, *Add Person's to Existing Buddy Group*s.
   7) 'CANCEL' to quit the process and leave the person's status unchanged.

6.2.4 Check-In and Check-Out using ICC Card with Fingerprint

Operators can check a cardholder in and out by inserting the person's ICC Card into a card reader and scanning their index fingerprint. This method of processing provides an additional level of security since it requires correct ICC Card PIN entry and a matched fingerprint.

1) Starting at the main screen, insert the cardholder ICC Card in the card reader.
2) When prompted, the cardholder enters their assigned PIN.
3) The Cardholder or Operator presses the 'Enter' or 'Return' key of the keyboard, or the Operator clicks the 'OK' button on the 'Enter PIN' dialog box.

4) When prompted, instruct the cardholder to place their index finger on the fingerprint scanner.
5) If the fingerprint does not match, a message displays stating the fingerprint does not match the ICC Card. Remove the index finger and card when prompted. If the fingerprint matches, remove the index finger and card and proceed with check in/out.
6) If the person has a liberty risk, an audible alert sounds and a 'Liberty Risk' dialog box displays. Click 'OK' to proceed.
7) The 'Check-In/Out' dialog appears displaying the following (as applicable):
   a. The person's name and rank
   b. A red 'Liberty Risk' notification box
   c. Service information
   d. A photo of the person if one exists on file
   e. Comments
   f. Messages in a yellow message text box with a 'Clear Message' button. Click the 'CLEAR MESSAGE' button to remove messages from the Message field on both the 'Check In/Out' dialog and the 'Edit Person' person's name and rank.
8) The current status of the person dictates the active buttons for checking in and checking out. If the person's current status is checked in, then a red 'Check Out' button is enabled. If the person's current status is checked out, then a green 'Check In' button is enabled. A white 'Cancel' button is permanently enabled on the 'Check In/Out' dialog. Click one of the following as applicable:
1) 'CHECK IN' to check the person in from liberty
2) 'CHECK OUT' to check the person out on liberty
5) If 'Enable Buddy Group' is selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*) a 'Create New Buddy Group' screen containing the person's name appears. Continue to add to or check out the Buddy Group following the instructions found in Section 6.3.1, *Create Buddy Groups*.
6) If 'Enable Buddy Group' *and* 'Allow Adding to Existing Buddy Group' are selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, A*llow Adding to Existing Buddy Group*), an 'Add to Buddy Group' screen appears displaying existing Buddy Groups. Continue with the instructions found in Section 6.3.5.1, *Add Person's to Existing Buddy Group*s.
3) 'CANCEL' to quit the process and leave the person's status unchanged.

6.2.5 Manual Check-In and Check-Out

In the event the cardholder's ICC card fails, is lost or is stolen, Operators search for and check cardholders in and out manually.

6.2.5.1 Using the Search Function on the Main Screen

1) From the main screen, filter the cardholders list to search for a user (see Section 5.1.2, *User Search*).
2) Double click on the 'Status Indicator' to the left of the person's name.
   If the person has a liberty risk, an audible alert sounds and a 'Liberty Risk' dialog box displays. Click 'OK' to proceed.
3) The 'Check In/Out' dialog appears displaying the following (as applicable):
   a. The person's name and rank
   b. A red 'Liberty Risk' notification box
   c. Service information
   d. A photo of the person if one exists on file

e. Comments in a yellow box
f. Messages in a yellow text box with a ‘Clear Message’ button. Click the ‘CLEAR MESSAGE’ button to remove messages from the Message field on both the ‘Check In/Out’ dialog and the ‘Edit Person’ person’s name and rank.

4) The current status of the person dictates the active buttons for checking in and checking out. If the person’s current status is checked in, a red ‘Check Out’ button is enabled. If the current status is checked out, a green ‘Check In’ button is enabled. A white ‘Cancel’ button is permanently enabled on the ‘Check In/Out’ dialog. Click one of the following:
1) ‘CHECK IN’ to check the person in from liberty
2) ‘CHECK OUT’ to check the person out on liberty
1) If ‘Enable Buddy Group’ is selected in ‘Settings’ (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*) a ‘Create New Buddy Group’ screen containing the person’s name appears. Continue to add to or check out the Buddy Group following the instructions found in Section 6.3.1, *Create Buddy Groups*.
2) If ‘Enable Buddy Group’ *and* ‘Allow Adding to Existing Buddy Group’ are selected in ‘Settings’ (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, A*llow Adding to Existing Buddy Group*), an ‘Add to Buddy Group’ screen appears displaying existing Buddy Groups. Continue with the instructions found in Section 6.3.5.1, *Add Person’s to Existing Buddy Group*s.
3) ‘CANCEL’ to quit the process and leave the person’s status unchanged.

6.2.5.2 Using the Check In/Out Menu item or Shortcut Button

1) From the main screen, filter the cardholders list to search for a user (see Section 5.1.2, *User Search*).
2) Single click the row of the cardholder to highlight it.
3) Select ‘Check In/Out’ on the ‘Person’ menu. Or, click the Check In/Out shortcut button from the vertical tool bar on the left side of the main screen.

   If the person has a liberty risk, an audible alert plays and a ‘Liberty Risk’ dialog box displays. Click ‘OK’ to proceed.
4) The ‘Check In/Out’ dialog appears displaying the following as applicable:
   a. The person’s name and rank
   b. A red ‘Liberty Risk’ notification box
   c. Service information
   d. A photo of the person if one exists on file
   e. Comments in a yellow box
   f. Messages in a yellow text box with a ‘Clear Message’ button. Click the ‘CLEAR MESSAGE’ button to remove messages from the Message field on both the ‘Check In/Out’ dialog and the ‘Edit Person’ person’s name and rank.
5) The current status of the person dictates the active buttons for checking in and checking out. If the person’s current status is checked in, then a red ‘Check Out’ button is enabled. If the person’s current status is checked out, then a green ‘Check In’ button is enabled. A white ‘Cancel’ button is permanently enabled on the ‘Check In/Out’ dialog. Click one of the following as applicable:
   1) ‘CHECK IN’ to check the person in from liberty
   2) ‘CHECK OUT’ to check the person out on liberty
   1) If ‘Enable Buddy Group’ is selected in ‘Settings’ (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*) a ‘Create New Buddy Group’ screen containing

the person's name appears. Continue to add to or check out the Buddy Group following the instructions found in Section 6.3.1, *Create Buddy Groups*.

2) If 'Enable Buddy Group' *and* 'Allow Adding to Existing Buddy Group' are selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, A*llow Adding to Existing Buddy Group*), an 'Add to Buddy Group' screen appears displaying existing Buddy Groups. Continue with the instructions found in Section 6.3.5.1, *Add Person's to Existing Buddy Group*s.
3) 'CANCEL' to quit the process and leave the person's status unchanged.

6.2.6 Rapid Check In/Out

Administrators can designate a PAS workstation as 'Rapid In', 'Rapid Out', or 'Normal' through the settings. The application is set to 'Normal' (Check In and Check Out), 'Incoming' (Check In only), or 'Outgoing' (Check Out only) modes (the previous sections describe checking in and checking out in Normal mode).

1) When the mode is set to 'Incoming', the 'Rapid Out' button on the Main Screen is disabled and the list of cardholders displays only those who are currently in a checked-out status.
2) When the mode is set to 'Outgoing', the 'Rapid In' button on the Main Screen is disabled and the list of cardholders displays only those who are currently in a checked-in status.
3) Checking personnel in or out in either mode requires the display of their 'Check In/Out' screen.

Operators/Processors and administrators may rapidly check personnel in or out without the interaction of the 'Check In/Out' screen by clicking the 'Rapid In' or 'Rapid Out' icons on the shortcut menu.

6.2.6.1 Rapid Check-Out

1) Click the 'Rapid Out' icon on the Main Screen. A 'Rapid Check Out' screen displays over the list of cardholders as shown in Figure 6-8. The 'Person' menu is disabled, and the 'Add' and 'Edit' shortcuts are hidden on the shortcut menu.

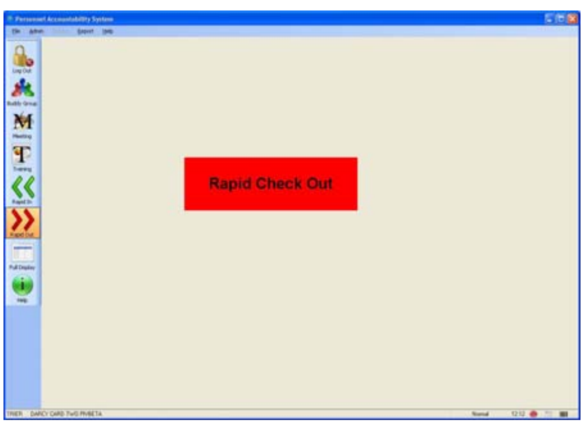

Figure 6-8 Rapid Check Out Screen

2) Check personnel out in one of the following ways:
   a. Scan a barcode from an ICC card.
   b. Scan a fingerprint
   c. Insert an ICC card and enter PIN when prompted.

3) A 'Rapid Check Out' box momentarily displays indicating a status change to checked-out as shown in Figure 6-9.

Figure 6-9 Rapid Check Out box

4) If the person has a liberty risk, an audible alert sounds and a 'Liberty Risk' box displays.
   a. Click 'OK' on the 'Liberty Risk' box.
   b. The 'Check In/Out' screen for the person displays.
   c. Click 'CHECK OUT' to check the person out on liberty or
   d. Click 'CANCEL' to cancel the check out process for the person.
5) Process additional personnel.
6) Click the 'FULL DISPLAY' icon to discontinue rapid check out.

6.2.6.2 Rapid Check-In

- Click the 'Rapid In' icon on the shortcut menu. A 'Rapid Check In' screen displays over the list of cardholders as shown in Figure 6-10. The 'Person' menu is disabled, and the 'Add' and 'Edit' shortcuts are hidden on the shortcut menu.

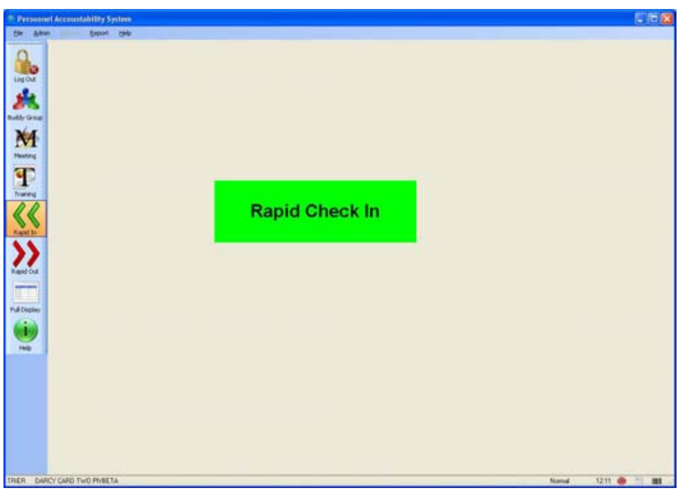

Figure 6-10 Rapid Check In screen

- Check in personnel in one of the following ways:
  - o Scan a barcode from an ICC card.
  - o Scan a fingerprint
  - o Insert an ICC card and enter PIN when prompted.
- A 'Rapid Check In' box momentarily displays indicating a status change to checked-in as shown in Figure 6-11.

Figure 6-11 Rapid Check In box

- If the person has a liberty risk, an audible alert sounds and a 'Liberty Risk' box displays. Click 'OK' on the 'Liberty Risk' box to proceed with check in.
- Process additional personnel.
- Click the 'FULL DISPLAY' icon to discontinue rapid check in.

6.3 Buddy Group Processing

The Liberty policies of various Commands (commonly referred to as 'Buddy Policies') require that individuals granted liberty or pass privileges be accompanied by at least one other member of that individual's command while on liberty outside the continental United States (OCONUS). When the Buddy Groups feature is enabled, it enforces this policy and requires all departing personnel be linked to at least one other individual before the Check Out transaction is accepted (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups*).

Personnel that have been linked through buddy grouping must return within a predetermined time specified by the PAS Administrator (see Section 4.1.1.4, Server Settings - *Default Buddy Gap*). If this does not occur, an exception is recorded by PAS. *Exemptions from the Buddy Policy are made to allow operators and administrators to permit personnel to depart the ship or station without a Buddy Group.*

Note: Current buddy group members are checked in during 'Rapid In' processing; however, if buddy groups are enabled the 'Rapid Out' processing feature is not available.

6.3.1 Create Buddy Groups

Note: 'Enable Buddy Group' must first be selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups).*

- Select 'Create Buddy Group' on the 'Person' menu.
- The 'Create New Buddy Group' screen appears as shown in Figure 6-12. From this screen, click on the 'ADD' button.

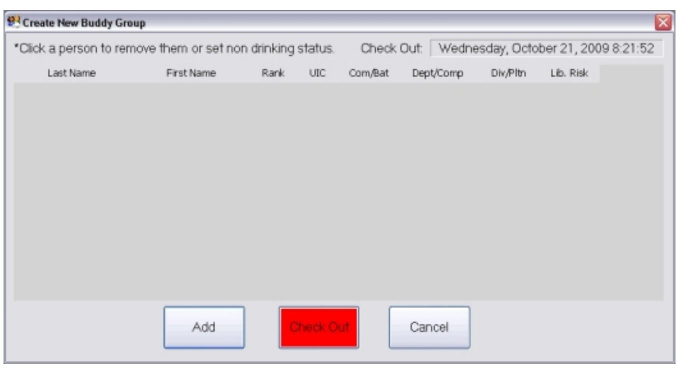

Figure 6-12 Create New Buddy Group

- A ‘Find Person to Add to Buddy Group’ screen appears.
    a. Personnel can be displayed by clicking on the ‘OUT’, ‘IN’ or “ALL’ buttons at the top of the screen.
    b. Use the ‘Select By’ pull-down menu to filter further by ‘Last Name’, ‘Rank’ etc.
- Double click on a name in the list to add that person to the Buddy Group.
    a. If an alert appears reading “This person is expired and the system is unable to check them in or out. Do you wish to edit this person’s expirations’ click ‘YES’ or “NO’. If ‘YES’ is chosen, the person’s ‘Edit Person’ screen will appear. Edit the person’s expiration information in the ‘System’ tab.
- The person’s Check In/Check Out screen will appear. Click ‘CHECK OUT’.
- Continue until all buddy group members are added to the Buddy Group list.

  Note: A minimum of two personnel are required for a Buddy Group (an exemption can be made at check out for a single person).
- Members will appear on the ‘Create Buddy Group’ screen as shown in Figure 6-13.

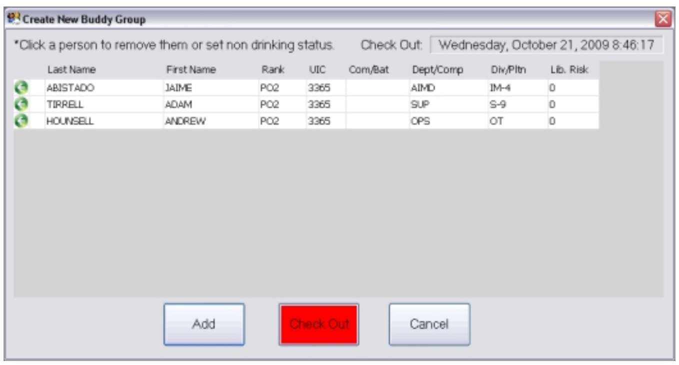

Figure 6-13 Create New Buddy Group

6.3.1.1 Set Non-Drinking Flag

Before checking out a Buddy Group, at least one member of each group must be set to ‘Non Drinking’ status.

a. Click on the Buddy Group member to set as ‘Non Drinking’. A window will appear as shown in Figure 6-14. Select ‘Set Non Drinking’.

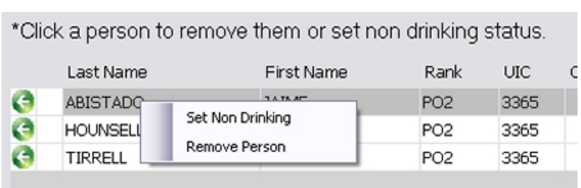

Figure 6-14 Set Non Drinking

b. A Non Drinking icon appears beside the person’s name 

(the icon will also appear next to the person’s name in other related fields including ‘Buddy Group’).

Note: If an attempt is made to check out a Buddy Group before at least one member is set to ‘Non Drinking’, an alert will appear reading ‘You must have a non drinking-member in the buddy group. Do you wish to make an exception?’.

a. Click ‘NO’, then follow the Set Non Drinking Flag directions above.
b. Click ‘YES’ and the group will be checked out.

6.3.1.2 Remove Person from Buddy Group

While creating a Buddy Group, a person can be removed from the Buddy Group List.

a. Click on the Buddy Group member to be removed. A window will appear as shown in Figure 6-14. Select 'Remove Person' and the person will be removed from the Buddy Group list.

6.3.2 Check Out Buddy Groups

To Check Out a completed Buddy Group:

- Click the 'Check Out' button from the 'Create New Buddy Group' screen to check out all members of the group.
- Click on the 'Cancel' button to cancel check out, and leave the cardholder's current status unchanged.

6.3.2.1 Check Out Exception - Buddy Group Members

If an attempt is made to check out a Buddy Group with only one member, an alert will appear reading 'You must have at least two people in a buddy group. Do you wish to make an exception?'

1) Click 'NO' and add personnel to the Buddy Group as described in Section 6.3.1, *Create Buddy Groups*.
2) Click 'YES' and the group will be checked out.

6.3.2.2 Check Out Exception - Non Drinking Buddy Group Member

If an attempt is made to check out a Buddy Group before at least one member is set to 'Non Drinking', an alert will appear reading 'You must have a non drinking-member in the buddy group. Do you wish to make an exception?'.

1) Click 'NO' and follow the Set Non Drinking Flag directions in Section 6.3.1.1, *Set Non-Drinking Flag*.
2) Click 'YES' and the group will be checked out.

6.3.3 Add Persons to Existing Buddy Groups

An individual can be added to an existing Buddy Group during check out if both 'Enable Buddy Group' *and* 'Allow Adding to Existing Buddy Group' are selected in 'Settings' (see Section 4.1.1.2, *Server Settings - Enable Buddy Groups* and 4.1.1.3, *Allow Adding to Existing Buddy Group*).

1) Highlight the individual to be checked out from the list of personnel on the main screen and click on the 'CHECK IN/OUT' icon, or right-click and chose 'Check In/Out'.
2) A screen will display existing Buddy Groups as shown in Figure 6-15.

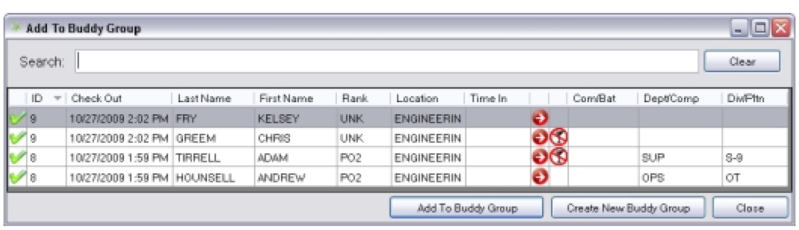

Figure 6-15 Add to Buddy Group

3) Highlight a member of the existing Buddy Group to which the new person will be added.
    a. To filter results, type a person's name in the 'Search' box at the top of the screen.
    b. Use the 'CLEAR' button to clear search parameters and display all names.

4) Click ‘ADD TO BUDDY GROUP’.
5) The person will be added to the existing Buddy Group and the main screen will appear.

Note: A user may also use the ‘Add to Buddy Group’ screen shown in figure 6-15 to create a new Buddy Group for the individual rather than adding them to an existing group. Click ‘CREATE NEW BUDDY GROUP’ and follow the instructions found in Section 6.3.1, *Create Buddy Groups*.

6.3.4 Check In a Buddy Group

Returning members of a buddy group are checked-in in the same manner as any method previously described. As buddy group members check in, the ‘Check In/Out’ screen of each Cardholder displays the current status of all remaining members of that group as shown in Figure 6-16.

Figure 6-16 Check In Buddy Group

6.3.5 View Buddy Groups

Buddy Groups remain current until all members of that group have been checked in.

1) View current buddy groups by clicking on the ‘BUDDY GROUP’ icon on the left side of the main screen or selecting ‘View Buddy Groups’ in the ‘Person’ menu.
2) The ‘View Buddy Groups’ screen appears (see Figure 6-17) with a Buddy Group ID number next to each member of that Buddy Group.

Figure 6-17 View Buddy Groups

6.3.6 Checking In/Out Totals

Administrators are able to check the totals of personnel in the PAS-FA database.

1) From the main screen, click the 'PERSON' menu on the menu bar.
2) Select 'Check In/Out Totals'. The totals for personnel checked in and check out in the PAS-FA database are displayed as shown in Figure 6-18.

Figure 6-18 Check In/Out Totals

7.0 Meeting and Training Rosters

Meeting and Training (Event) rosters are used to track attendance at meeting and training events.

7.1 Create New Meeting/Training Rosters

- Click either the ‘MEETING’ or ‘TRAINING’ icon on the vertical toolbar on the left side of the main screen, or from the ‘File’ menu, select either the ‘Meeting Roster’ or ‘Training Roster’ menu item. The ‘Meeting Roster’ or ‘Training Roster’ window displays scheduled meetings, an option to create new rosters, and an option to remove meeting rosters as shown in Figure 7-1

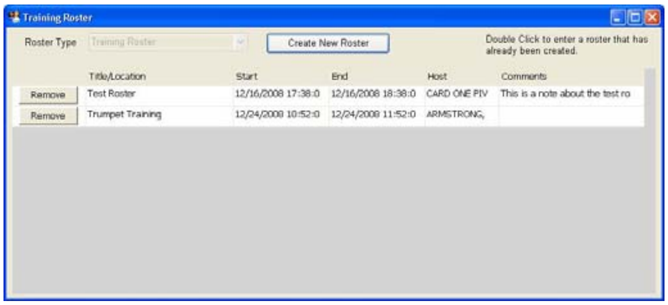

Figure 7-1 Training Roster

- To create a new roster, click the ‘CREATE NEW ROSTER’ button. The ‘Create Roster’ dialog box opens as shown in Figure 7-2.
- Enter the title/location of the event. *The Title/Location field is required and cannot be left blank.*
- The event host defaults to the Operator creating the event in PAS-FA. The host can be changed to another user in the PAS-FA database by clicking the ‘CHANGE SELECTION’ button.

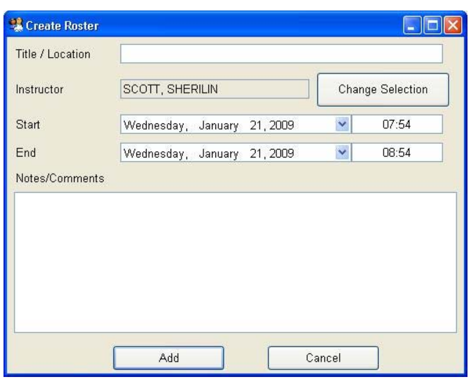

Figure 7-2 Create Roster dialog box

- The ‘Start’ date and time defaults to the time the ‘Create Roster’ dialog box opens. The ‘End’ date and time defaults to one hour from the time the ‘Create Roster’ dialog box opens. Both time blocks can be changed if applicable.
- Enter any notes or comments for the event in the ‘Notes/Comments’ field.
- Click the ‘ADD’ button to create the meeting or training event and close the ‘Create Roster’ dialog box, or click the ‘CANCEL’ button to quit and close the ‘Create Roster’ dialog box without saving training or meeting data.

7.1.1 Sign-In Meeting/Training Attendees

- Click either the ‘MEETING’ or ‘TRAINING’ icon on the vertical toolbar on the left side of the main screen, or from the ‘File’ menu, select either the ‘Meeting Roster’ or ‘Training Roster’ menu item. The ‘Meeting Roster’ or ‘Training Roster’ window displays scheduled events and an option to create new rosters.
- From the event roster window (see Figure 7-3), double-click an event title to begin capturing attendance.
- Log meeting/training attendance can be logged through these methods:
    - o Click the ‘ADD’ button and manually search for attendees in the database.
    - o Scan the barcode of an ICC card.
    - o Insert an ICC card into a reader and request the attendee enter their PIN when prompted.
    - o Scan the index fingerprint of an attendee.
- The attendee’s name, rank, military assignment information, service, and current check in date and time are added to the roster.

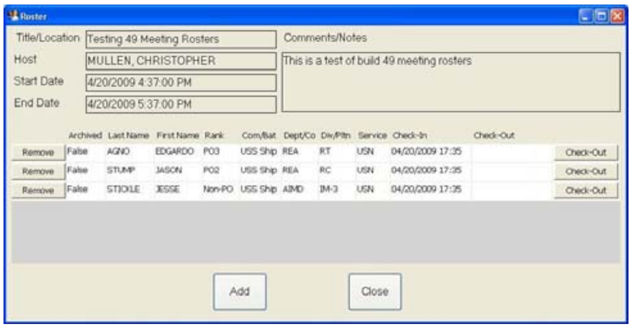

Figure 7-3 Roster, Check In Attendees

7.1.2 Sign-Out Meeting/Training Attendees

1) Select either the ‘MEETING’ or ‘TRAINING’ shortcut icon from the vertical toolbar on the left side of the main screen.
2) From the applicable event roster window (see Figure 7-4), double-click a meeting or training title to open the roster.
3) Attendees are signed out from meetings or training events from the ‘Roster’ window through these methods:
    a. Click the ‘CHECK-OUT’ button corresponding to each attendee.
    b. Scan the barcodes from the attendees’ ICC cards.
    c. Insert the attendees’ ICC cards and request they enter their PINs when prompted.
    d. Scan the index fingerprints of attendees.

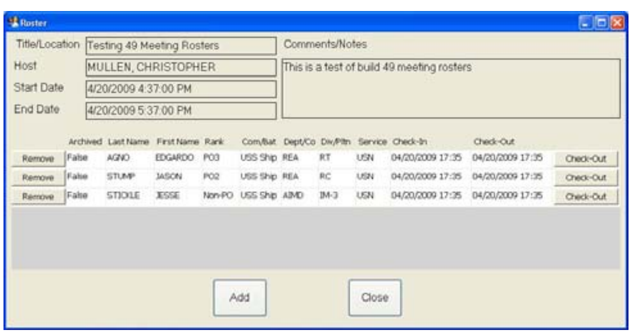

Figure 7-4 Roster, Check Out Attendees

4) Sign-Out times for attendees appear in the ‘Check-Out’ column. The current date and time of sign out displays and cannot be altered.

7.1.3 Remove Meeting/Training Attendees

a. Select either the ‘MEETING’ or ‘TRAINING’ shortcut icon on the vertical toolbar on the left side of the main screen.
b. From the applicable event roster window, double-click an event title to open the roster.
c. Click the ‘REMOVE’ button to remove attendees from rosters.

7.1.4 Removing Meeting/Training Rosters

Note: Operators cannot remove rosters.

a. Click either the ‘MEETING’ or ‘TRAINING’ icon on the shortcut toolbar on the main screen, or from the ‘File’ menu, select either the ‘Meeting Roster’ or ‘Training Roster’ menu item. The ‘Meeting Roster’ or ‘Training Roster’ window displays scheduled events and an option to create new rosters.
b. Click the ‘REMOVE’ button to remove a meeting or training event.
c. Rosters are archived (see Section 4.4.2, *Archiving Rosters*).
d. Rosters can also be permanently purged from the PAS-FA database (see Section 4.4.4, *Purging Records*).

8.0 Help Menu

The Help' menu contains a several features to assist users with the PAS-FA application. Access the 'PAS Help System' function through the shortcut icon on the vertical toolbar on the left side of the main screen, or additional features through the pull down menu at the top of the main screen.

8.1 Display Administrators

To display a list of all PAS administrators, click the 'DISPLAY ADMINISTRATORS' item on the 'Help' menu. All PAS cardholders with administrator rights are displayed.

Figure 8-1 Display Administrators

8.2 Repair Fingerprint Scanner

To repair the connection from PAS-FA to the fingerprint scanner:

a. Select 'REPAIR FINGERPRINT SCANNER' from the 'Help' menu. The repair fingerprint scanner feature is also available when enrolling prints (see Section 5.1.5, *Enrolling Print Images*).
b. A 'Calibrate' dialog box appears (see Figure 8-2) with the following instructions for repairing the connection:
a. Clean the scanner's sensor.
b. Do not place anything on the sensor after cleaning.
c. Click 'Start' to initialize calibration.

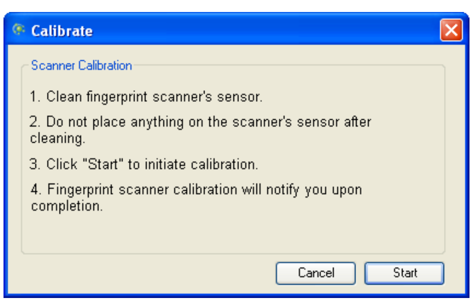

Figure 8-2 Calibration dialog box

c. A 'Calibration Complete' message displays when calibration is done. Click 'OK' to close the message box.
d. If a fingerprint scanner is not installed, an error message appears stating that fingerprint capture is unavailable as shown in Figure 8-3)
a. Click 'OK' .
b. Install a fingerprint scanner following the scanner manufacturer's instructions.

Figure 8-3 Repair Fingerprint Scanner message

Note: PAS-FA attempts to initialize the fingerprint scanner to login and accomplish searches for assigning hosts and attendees to rosters even if a scanner is not installed. PAS-FA will not attempt to initialize the scanner if the 'Fingerprint' checkboxes in the Authentication and Login sections of the 'Settings' screen are not checked (see Section 4.1.4.8, *Server Settings - Authentication Methods* and 4.1.1.9, *Server Settings - Login Methods*).

8.3 Activate Fingerprint Match License

If the PAS-FA application is installed on a computer by means other than a new installation (see Section 2.2.1, *New Installations*), the Fingerprint Match License must be activated.

1) Select 'Activate Fingerprint Match License' from the 'Help' menu.
2) A screen will display 'Activation Succeeded'. Click 'OK'

8.4 PAS Help System

The PAS-FA application includes a Help System that allows users to view and search contents of the *Personnel Accountability System - Full Application (PAS-FA) User's Guide*.

a. Access the 'Help System' through the shortcut icon on the vertical toolbar on the left side of the main screen or through the pull down 'Help' menu at the top of the main screen.
b. Click the 'Contents' tab to view the *Personnel Accountability System - Full Application (PAS-FA) User's Guide* Table of Contents.
   o Click on any section in the Table of Contents to view that section.
c. Click the 'Search' tab to search the document for specific words or phrases.
1) Type in keywords and click the 'LIST TOPICS' button.
   a. Click on any topic displayed to view that section.

8.5 About PAS

To view information on the version of PAS installed, select 'ABOUT PAS' from the 'Help' menu.

9.0 Reports

The PAS-FA 'Reports' function provides varying search and sort options that allow users to produce detailed reports of cardholder and user activity.

9.1 Run Existing PAS Reports

a. Click 'RUN REPORTS' on the 'Report' menu. A 'PAS Reports' window displays as shown in Figure 9-1.

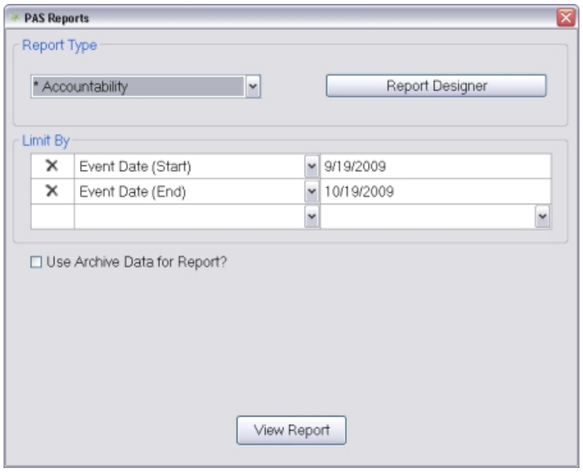

Figure 9-1 PAS Reports window

b. Select the desired report from the 'Report Type' combo box on the left. Existing reports include:

a. Accountability Report - Displays both the Operator Log-in/Log-Out events and manual Check-In/Check-Out events entered by a user within the specified date and time range.
b. Buddy Exception Report - Displays all of the personnel information for Buddy Groups currently in violation of the local buddy policy.
c. Change Log – Displays changes made to PAS-FA personnel data during a specified date range.
d. Comments Report - Displays all personnel comments.
e. Department Muster Report - Displays the total number of cardholders checked-in and total number of cardholders checked-out of each department at a specified time.
f. Error Report - Displays all of the errors logged by the application within the specified date and time range.
g. Event Report - Displays all events that have taken place at a given location within a specified date and time range.
h. History Report - Displays all personnel and their check in status history.
i. Meeting Roster Report - Displays all personnel checked into a meeting.
j. Restricted Personnel Report - Displays all personnel that have a liberty restriction.
k. Snapshot Report - Displays all personnel and their current check in status.
l. Training Roster Report - Displays all personnel checked into a training course.

9.1.1 The Limit By Field

The ‘Limit By’ function allows a user to define what limits to apply to report data as shown in Figure 9-2.

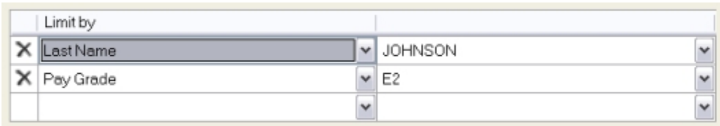

Figure 9-2 Limit By Field

1) In the ‘Limit By’ column, use the down arrow to select the limits for the report (Branch, City, Command/Battalion etc.). In Figure 9-2, ‘Last Name’ and ‘Pay Grade’ were selected.
   a. After a new limit is selected, a new blank field will display allowing the inclusion of an additional limit. Repeat until all desired limits are included
   b. In the column to the right of the limits, select the specific limit to be applied to the report. In Figure 9-7, the name ‘Johnson’ was used as a specific limit for ‘Last Name’, and ‘E2’ as a specific limit for ‘Pay Grade’.
   c. Select all desired ‘Limit By’ Options.

9.1.2 Use Archive Data

Click the ‘USE ARCHIVE DATA FOR REPORT?’ box to run the report using archived data.

9.1.3 View or Print the Report

Click the ‘VIEW REPORT’ button to display the report.

1) Using the tools at the top of the report, a user can:
   1) Scroll through the document by page number
   2) Refresh
   3) Print
   4) View Print Layout
   5) View Page Setup
   6) Export as an Excel or Acrobat file
   7) Adjust document view (zoom).
2) Close out of the report to return to the ‘PAS Reports’ screen.

9.2 Customize an Existing PAS Report

(also see Section 9.3, *Design a New PAS Report*).

1) Click 'RUN REPORTS' on the 'Report' menu. A 'PAS Reports' window displays as shown in Figure 9-1.
2) In the 'Report Type' combo box, select the existing report to be customized and click the 'REPORT DESIGNER' button (if the 'Report Type' combo box was not changed, the screen will alphabetically default to the 'Accountability' report options).
3) A 'Report Designer' screen appears as shown in Figure 9-3.

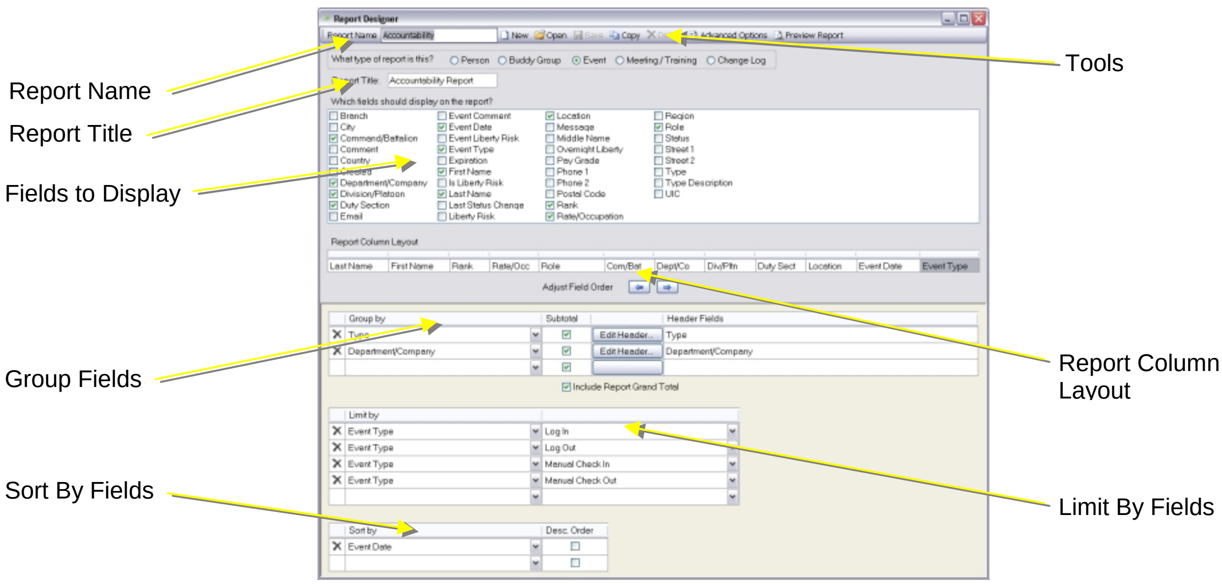

Figure 9-3 Report Designer

4) Make a copy of the existing report using the 'Copy' tool at the top of the screen. A screen will appear reading 'Report Copied. Enter a new name and save the changes.' Click 'OK' and rename the report in the 'Report Name' field.

Important: Attempting to modify the settings for any existing report without first making a copy will result in an alert reading 'System reports cannot be modified. You can make a copy of the report and modify the copy'. Click 'OK' to return to the 'Report Designer' screen.

5) Click 'SAVE' using the tool at the top of the screen (the new report name will populate the 'Report Type' combo box and can be selected from that field during subsequent PAS report sessions).
6) Type a new report title in the 'Report Title' box.

9.2.1 The Display Field

The ‘Which fields should display in the report’ field indicates (with a GREEN checkmark) the default fields included in the existing report. Check fields on or off to include or exclude from the custom report as shown in Figure 9-4.

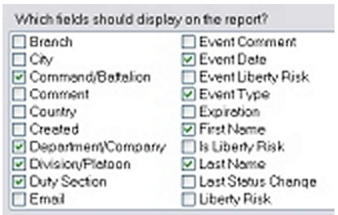

Figure 9-4 Display Field

9.2.2 Report Column Layout

The ‘Report Column Layout’ feature allows a user to adjust the field order for the custom report.

1) Click on any column name displayed under ‘Report Column Layout’ (it will become highlighted).
2) Click the BLUE Left and Right ‘Adjust Field Order’ arrows to move that column to left or right of other columns in the report as shown in Figure 9-5.

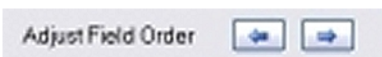

Figure 9-5 Adjust Field Order

3) Repeat for any additional column adjustments.

9.2.3 The Group Field

The ‘Group By’ function allows a user to customize how the report fields are grouped as shown in Figure 9-6.

Figure 9-6 Group By Field

1) In the ‘Group By’ column, use the down arrow to select the group categories for the report (Branch, City, Command/Battalion etc.). In Figure 9-5, ‘Type’ and ‘Department/Company’ were selected.
   a. After a new group is selected, a new blank field will display below the last group entered to allow for the inclusion of an additional group. Repeat until all desired groups are included
2) In the ‘Subtotal’ column, click on or off the groups that are to be subtotaled in the report.
3) Click the ‘Include Report Grand Total’ box if a group Grand Total is desired in the report.
4) Default Header Fields will appear to the right of the group name under the ‘Header Fields’ column as shown in Figure 9-6. To edit the Header Fields, click the ‘EDIT HEADER’ button to the right of the group name. An ‘Edit Header Branch’ screen will display as shown in Figure 9-7 asking ‘Which fields should display on this group header?’

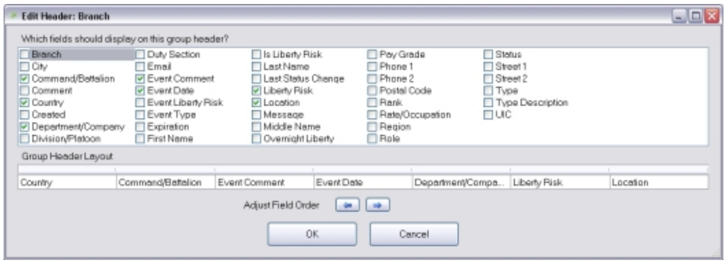

Figure 9-7 Edit Header Branch

a. Click on or off the desired fields for that group header.
b. Adjust the ‘Group Header Layout’ columns using the same techniques used in Section 9.2.2, *Report Column Layout*.
c. When finished click ‘OK’ (or click ‘CANCEL’ at any time) to return to the ‘Report Designer’ screen.
d. Continue to edit additional Header Fields as desired.

9.2.4 The Limit By Fields

The ‘Limit By’ function allows a user to define what limits to apply to report data as shown in Figure 9-8.

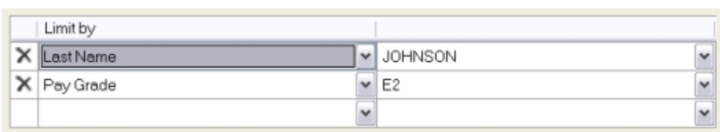

Figure 9-8 Limit By Field

1) In the ‘Limit By’ column, use the down arrow to select the limits for the report (Branch, City, Command/Battalion etc.). In Figure 9-8, ‘Last Name and ‘Pay Grade’ were selected.
   a. After a new limit is selected, a new blank field will display below the last limit entered to allow for the inclusion of an additional limit. Repeat until all desired limits are included
2) In the column to the right of the limits, select the specific limit to be applied to the report. In Figure 9-8, the name ‘Johnson’ was used as a specific limit for ‘Last Name’, and ‘E2’ as a specific limit for ‘Pay Grade’.

9.2.5 The Sort By Fields

The ‘Sort By’ function allows a user to sort the report by specific categories as shown in Figure 9-9.

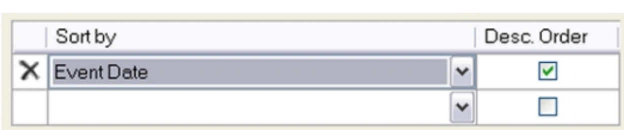

Figure 9-9 Sort By Field

1) In the ‘Sort By’ column, use the down arrow to select the sort category for the report (Branch, City, Command/Battalion etc.). In Figure 9-9, ‘Event Date’ was selected.
   a. After a new sort category is selected, a new blank field will display below the last sort category entered to allow for the inclusion of an additional sort category. Repeat until all desired sort categories are included.

2) Check the ‘Desc. Order’ box to the right of the sort category to sort that category in descending order.

9.2.6 View or Print Custom Reports
Click the ‘PREVIEW REPORT’ tool at the top of the ‘Report Designer’ screen.

i. Using the tools at the top of the preview window, a user can:

8) Scroll through the document by page number
9) Refresh
10) Print
11) View Print Layout
12) View Page Setup
13) Export as an Excel or Acrobat file
14) Adjust document view (zoom).

9.2.7 Advanced Options
Click the ‘ADVANCED OPTIONS’ tool at the top of the ‘Report Designer’ screen. A window appears (see Figure 9-10) allowing a user to define report formatting options including:

1) Paper Size/Width/Height
2) Portrait/Landscape Orientation
3) Font
4) Margins

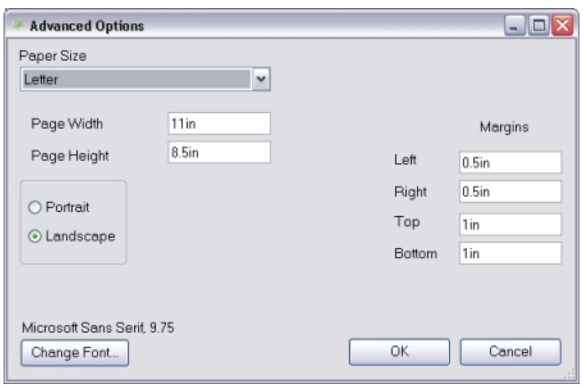

Figure 9-10 Advanced Options

9.2.8 Delete a Custom Report
Users may delete a custom report by clicking the ‘DELETE’ tool at the top of the ‘Report Designer’ screen while a report is open.

1) A screen appears asking ‘Are you sure you want to delete this report?’. Click ‘YES’, ‘NO’ or ‘CANCEL’ to return to the report in the ‘Report Designer’ screen.
2) Custom reports that are in progress (not saved) are not allowed to be deleted.
3) Existing Reports (see Section 9.1, *Run Existing PAS Reports*) can not be deleted.

9.3 Design a New PAS Report

(also see Section 9.1, *Design a PAS Report Based on Existing Report Types*).

1) Click ‘RUN REPORTS’ on the ‘Report’ menu. A ‘PAS Reports’ window displays as shown in Figure 9-1.
2) Click the ‘REPORT DESIGNER’ button. A ‘Report Designer’ screen appears as shown in Figure 9-11.

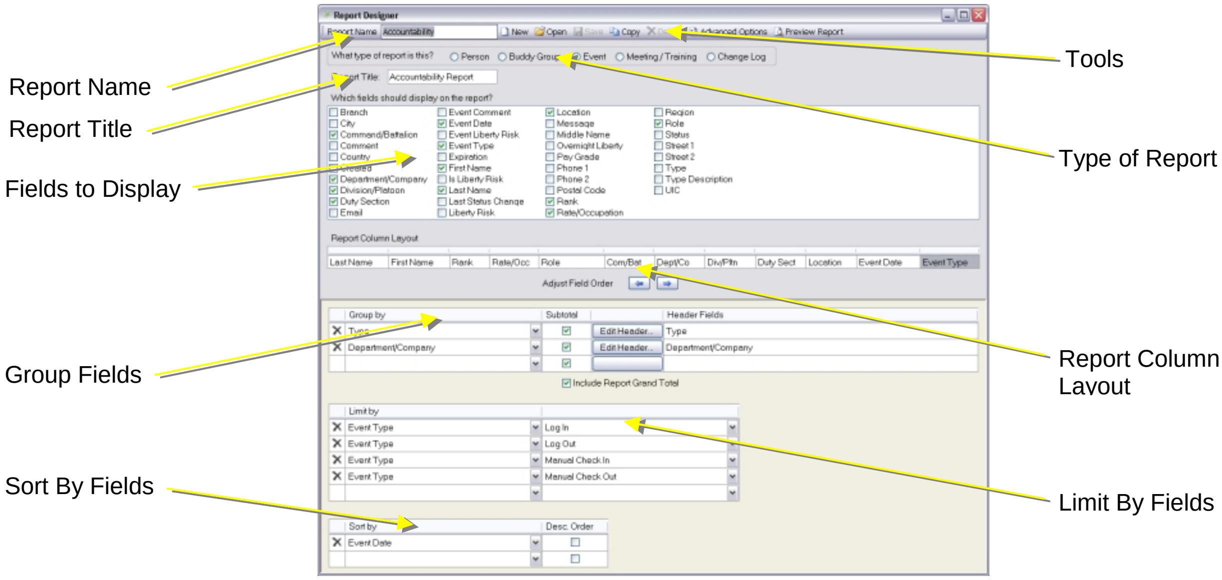

Figure 9-11 Report Designer

a. Click the ‘NEW’ tool at the top of the screen.
b. Enter a report name in the ‘Report Name’ field.
c. Click on the type of custom report from the options in the ‘What type of report is this?’ field. Options include:
   1) Person (check the ‘Include Status History’ box for person-specific information to be included the report).
   2) Buddy Group
   3) Event
   4) Meeting/Training
   5) Change Log

a. Click ‘SAVE’
b. Continue with the instructions beginning in Section 9.2.1, *The Display Field* through Section 9.2.7, *Delete a Custom Report*.