

Appendix F

Standalone Procedures

F.1 Standalone Concept

GCSS-A/T software provides for operation both in garrison and field environments. The GCSS-A/T concept involves a centralized data storage and retrieval system. Users connect to the central database via application software that operates within the domain of the Army Knowledge Online (AKO) website. Since the software is web-based, many functions that once required user intervention, such as creating asset visibility reports, running catalog updates, or backing-up user data, can now be generated automatically without end-user support. While users should operate in connected mode whenever possible, there may occasionally be a need to operate in an environment where a reliable network connection to AKO is not available. For this period of time, the user will need to operate in Standalone mode.

The Standalone concept provides the ability for a user to transfer all or a portion of his database into database that operates on the user's laptop computer. The Standalone interface is identical to the software interface on AKO; however, the automated features of connected operation are not available in Standalone mode. Of primary concern is the protection of the user's data. While in Standalone mode, it is the user's responsibility to ensure that data is properly protected and backed-up.

Standalone Process Concept

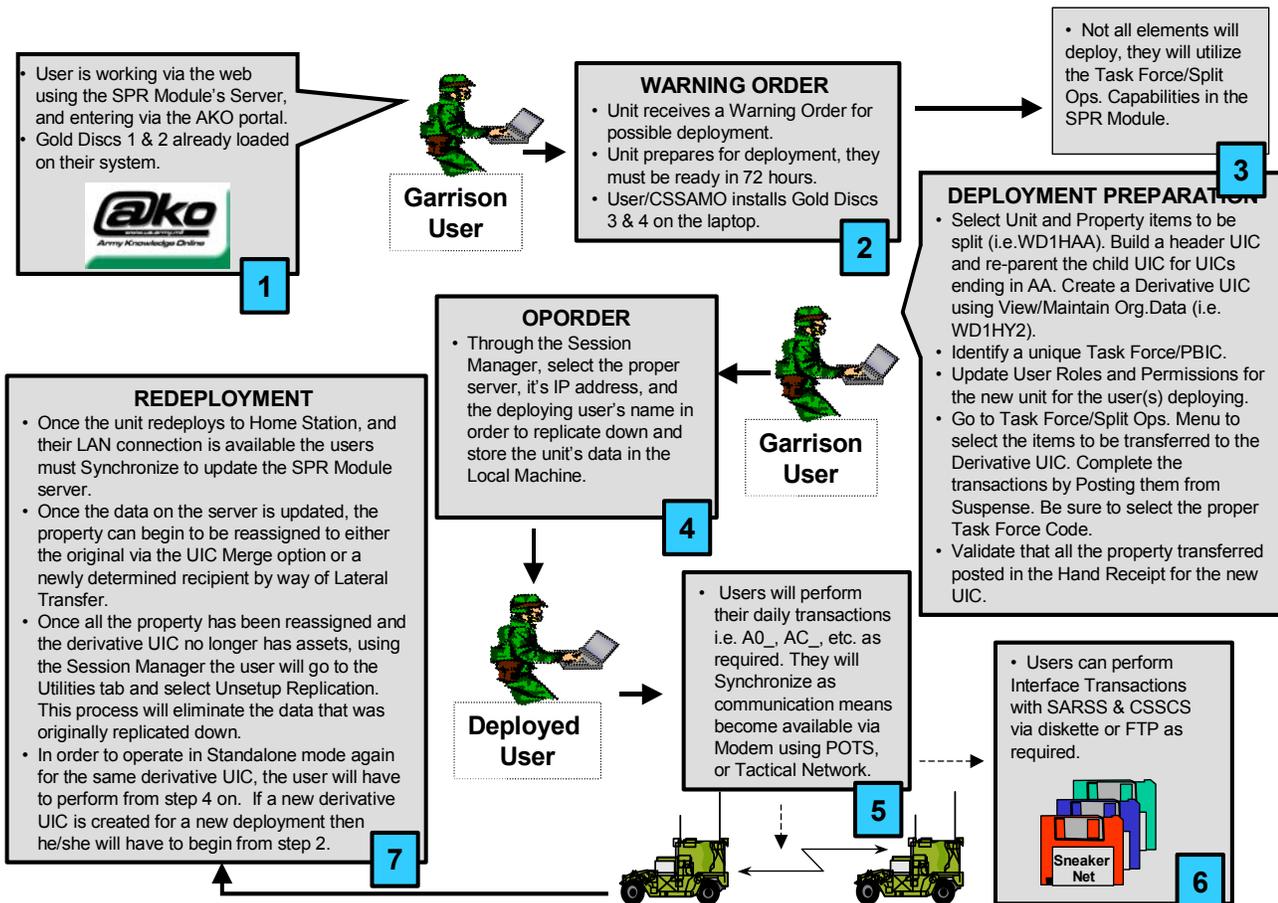


Figure F.1-1. Standalone Concept.

If only a portion of the user's unit and property items will be deploying, it is advantageous for the user to create a derivative UIC and only replicate data for the equipment that is assigned to the deploying element. In this way, the user can maintain an operation in garrison for units and equipment that are not deploying while providing the deploying users exclusive access to data for deploying equipment. By customizing a user's roles and permissions, PBO's can ensure that users have appropriate access to deployed and non-deployed data.

F.1.1 Create a derivative UIC.

In accordance with the Standalone concept, a user should create a derivative UIC before deploying part of a unit's assets. This will allow the property book office to maintain operations in Garrison while simultaneously providing direct support for deployed elements. For some units, creating a derivative UIC will require first building a "header UIC" and then making this header UIC a parent UIC for the original UIC.

For divisional units, a four-position parent UIC is appended with AA to represent the top level or branch. Other UICs in this structure are represented with the same four-position parent UIC appended with other alphanumeric characters, typically A0, B0, T0 etc., each representing a specific company or unit. In this example, all property is held at the unit level and therefore, the AA UIC does not hold property. When a derivative UIC is made from one of the property holding UICs, it is created within this same UIC structure as another node or leaf. In this way, asset visibility of all property is preserved.

Some units do not have this same UIC structure. This is primarily true of non-divisional units that use UICs ending in AA to hold property. In many of these UIC hierarchies, the AA UIC is assigned to a parent UIC in which the first four positions of the UICs do not match. This can be illustrated using an example from the Army Reserve. Consider this subsection of units that fall within the 90th Regional Support Command:

```
WZZZFF U.S. ARMY INS = 00AA (HEADER)
  W47AFF USARC (HEADER)
    W8B2FF 90TH Regional Support Command (HEADER)
      WS6NFF 694th Maint Bn. (HEADER)
        WS6NAA 694th Maint Bn
        WQ8TAA 887TH QM Co.
        WS65AA 238TH Maint Co.
        WTYZAA 340TH QM Co.
```

Note that WS6NFF serves as the parent UIC for three company UICs and one battalion UIC. Each of these child UICs is assigned property. In a situation like this, a derivative UIC could not be directly created from the child UIC since the first four positions of the child UIC and the first four positions of its parent UIC do not match.

In order to create a derivative UIC for WS65AA, then a new header UIC needs to be created in which the first four positions are "WS65" and the last two positions are "FF." When this UIC is created, it is assigned as a child to WS6NFF and a parent to WS65AA. Once this is accomplished, a derivative UIC, such as WS65Y1, can be created.

F.1.2 Build a header UIC (if required).

This step is required when first four positions of the parent UIC do not match the first four positions of the child UIC as in the example of UIC WS65AA used above. This example will use the UIC structure listed in section F.1.1. Throughout this section, the original UIC will be WS65AA (238th Maint Co.) and the original parent UIC, WS6NFF.

- a. From the Administrative Menu, select Build Organization. (Fig. F.1-2).
- b. In the UIC: text block, enter the desired name for the header UIC. This name will be made up from the first four positions of the child UIC along with the suffix characters "FF." For this example, the header UIC is WS65FF.
- c. Select the parent UIC from the LOV. This will assign the new header UIC as a child to the original parent UIC.
- d. Enter the Ins Cd as appropriate for the child UIC.
- e. Add other descriptive data as desired.
- f. Click <Apply> to create the header UIC.

The screenshot shows a software interface titled "Organization Data" with four tabs: "View / Maintain Organization VORG-1", "Build Organization BORG-2", "Create Derivative UIC BORG-3", and "DODAAC Functions BORG-4". The "Build Organization BORG-2" tab is active. Below the tabs is a "Search..." button and an "ACL Request" button. The main form area contains several fields and dropdown menus:

- UIC: WS65FF
- Parent UIC: WS6NFF (dropdown)
- Ins Cd: 80S
- TOC: 1 (dropdown)
- MACOM: (dropdown)
- DSSC: (dropdown)
- Commander: (text)
- HR Holder: (text)
- Next Projected EDate: (text)
- Unit Name: (text)
- Parent Unit Name: (text)
- Task Force Cd: (text)
- MTOE/TDA: (text)
- Rank: (dropdown)
- HR Phone: (text)
- Station Name: (text)
- Reporting UIC: (dropdown)
- Task Force PBIC: (text)
- Effective Date: 13 JUL 2002
- UAT: (dropdown)
- UAC: (dropdown)
- ALO: (dropdown)
- HR Email: (text)

At the bottom of the form, there is a row of buttons: "Search...", "Apply", "Refresh", "Undo", "Insert", "Delete", "Print...", "Coach...", and "Help...".

Figure F.1-2. Create a header UIC.

F.1.3 Re-parent the child UIC (if required).

When this step is completed, the header UIC will be the parent of the original child UIC as well as a child of the original parent UIC.

- a. From the Administrative Menu, select the View/Maintain Organization tab. (Fig. F.1-3).
- b. In the UIC text box at the top of the screen, enter the name of the child UIC and click <GO>.
- c. Select the newly created header UIC from the Parent UIC LOV.
- d. Click <Apply> to save the changes.

Organization Data

View / Maintain Organization VORG-1 Build Organization BORG-2 Create Derivative UIC BORG-3 DODAAC Functions BORG-4

UIC:

UIC: WS65AA	Unit Name: CS CO MA	Station Name: SAN ANTON	
Parent UIC: <input type="text" value="WS65FF"/>	Parent Name: 694TH MAIN	Reporting UIC: <input type="text" value="WS6NAA"/>	
INS Cd: 80S	Task Force Cd: <input type="text"/>	Task Force PBIC: <input type="text"/>	
TOC: 1	MTOE/TDA: 43649LAR03	Effective Date: 11 DEC 1971	
MACOM: FORSCOM	CAC: DU	UAT: GENERAL	
DSSC: D	Comp Cd: 3	UAC: <input type="text"/>	
Commander: GIRARD SEI	Rank: LTC	ALO: 1	
Hr Holder: CPT MARK E.	BHr Phone: 210-922-6395	Hr Email: <input type="text"/>	

DODAAC	FAD	Mail To	Bill To	Ship To	Unit Type
W45B86	3	238TH MAINTENANCE CO GS,432 BOSWELL STREET,, SAN ANTONIO,782142499	90 RSC, 8000 CAMP ROBINSON RD, N. LITTLE ROCK, AR 72118-2205		P

DSU DODAAC	DSU Name	DSU Phone	DSU Address	DSU Email	DSU Ric	SC
W45LGC	812TH QUARTERMASTER C	956-423-4571	1300 TEEGE AVE	CORTEZ@USARC-EMH2.ARMY.MIL	WMH	2,4,7

Figure F.1-3. Re-parent the child UIC.

F.1.4 Complete derivative UIC.

- a. From the Administrative Menu, select View/Maintain Organizational Data.
- b. {View/Maintain Organizational Data screen} opens (Fig. F.1-4).
- c. In the UIC text box, (next to the <Go> button) enter the UIC (for example, WQNAAA) that will be split to create the derivative UIC.
- d. Click <Go> to bring up information about this UIC.

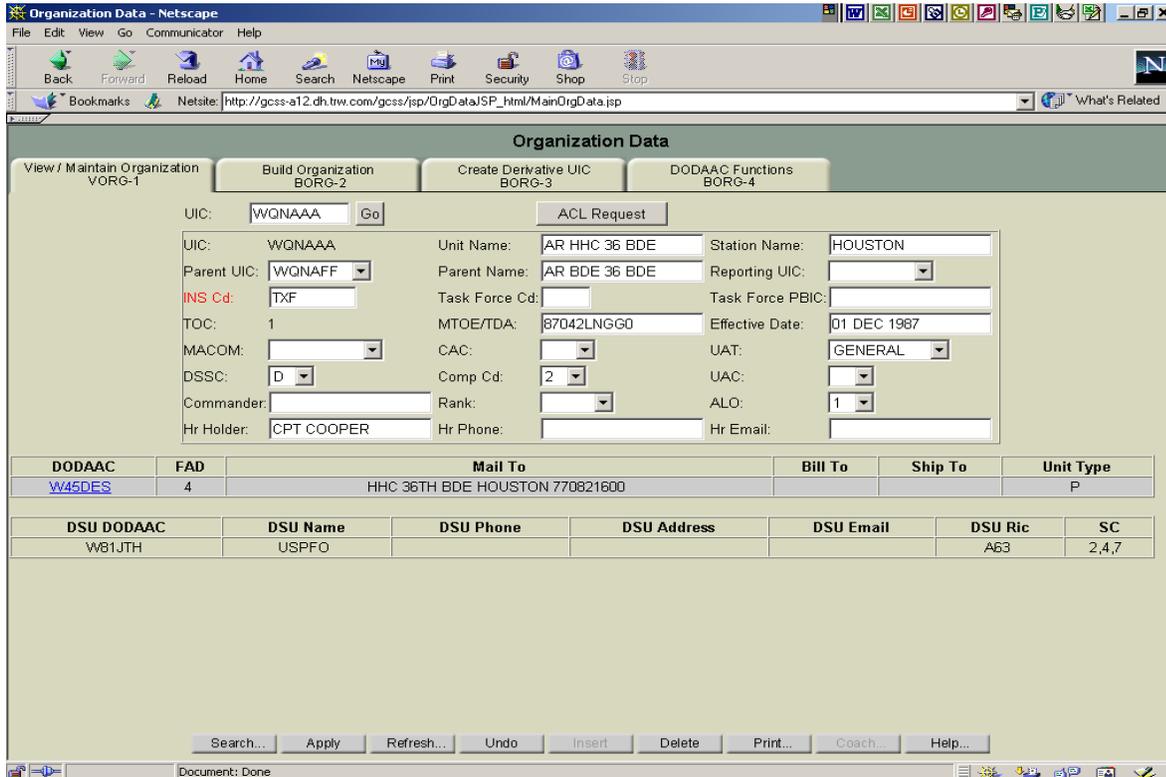


Figure F.1-4. View/Maintain Organization screen with sample UIC information.

- e. Record the Parent UIC. It will be needed in following steps.
- f. Click on the Create Derivative UIC tab (Fig. F.1-5).
- g. Verify that the UIC listed on this tab is the same as the Parent UIC from the View/Maintain Organization tab (recorded in Step 1.1e above). If the UIC is different from the Parent UIC recorded in 1.1e above, change it to the Parent UIC referred to in Step 1.1e and click <Go>.
- h. The four-position Parent UIC for the UIC that was entered will be listed next to the text box for the Derivative UIC. Enter the last two digits to complete the derivative UIC. In this example, "Y2" is entered to create the derivative UIC "WQNAY2".

NOTE: Both the original UIC and the Derivative UIC have the same Parent UIC.

- i. Add other descriptive unit information as is appropriate. Note that all text boxes labeled in red are mandatory fields.

NOTE: To expedite data transfer between the UIC and its Derivative UIC, ensure that the Task Force Cd: box is given a value (Fig. F.1-5). The derivative UIC must have a Task Force Code in order to be selected as a property recipient in the Unit Transfer/Task Force/Split Operations process (Section F.1.4).

- j. Click <Apply> to save the changes.

AIS Manual GCSS-A/T PBUSE EM
1 January 2003

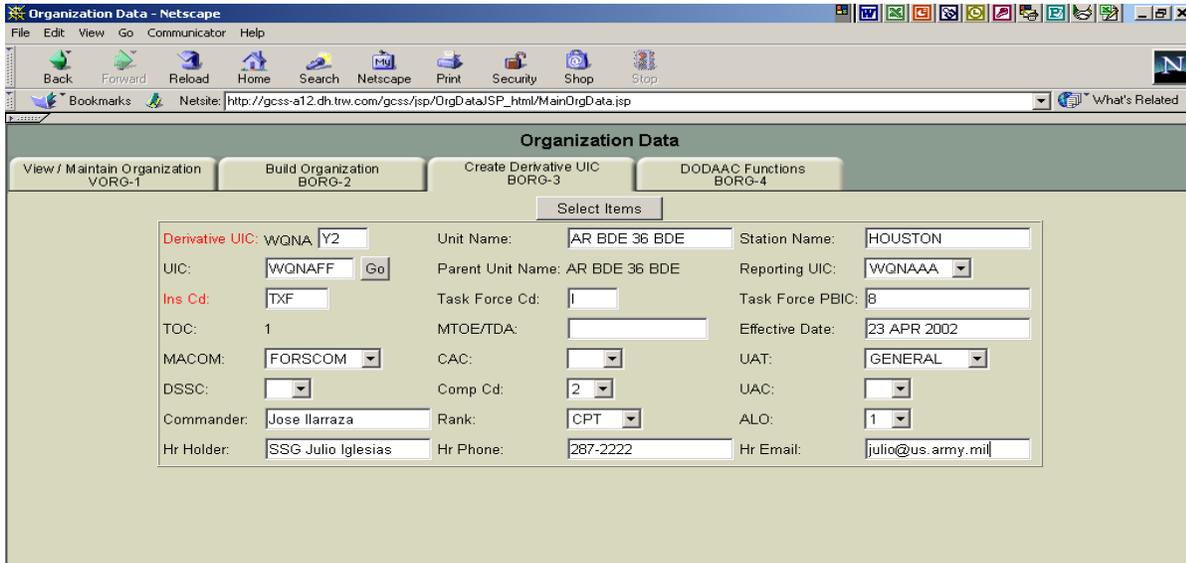


Figure F.1-5. Create Derivative UIC tab.

- k. If the new UIC is not found in the DODAAF table, the system will ask if you would like to build it. Click <OK> to complete the build of the Derivative UIC (Fig. F.1-6).



Figure F.1-6. Message box indicating that the derivative UIC is not in the ARMY DODAAF table.

- l. Once the UIC is created, the system will alert the user with a message box (Fig. F.1-7). Click <OK>.



Figure F.1-7. Message box showing successful creation of derivative UIC.

F.1.5 Add DODAAC information for the derivative UIC.

- a. Select the DODAAC Functions tab (Fig. F.1-8).

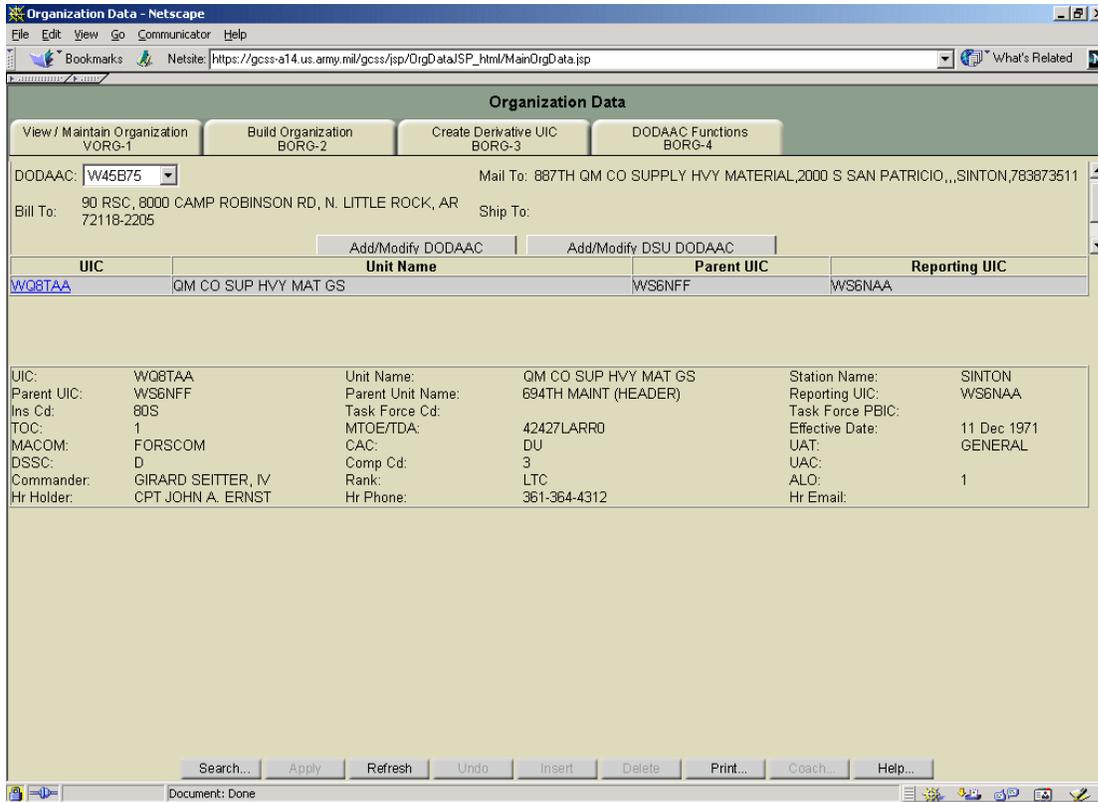


Figure F.1-8. DODAAC Functions tab.

- b. If the **<Add/Modify DODAAC>** button and the **<Add/Modify DSU DODAAC>** button do not appear, use the scroll bar on the right hand side of the screen to show these buttons. Click the **<Add/Modify DODAAC>** button to enter the DODAAC for the derivative UIC. This will open a link to the Reference Lookup Tables and open the Milstrip Property Book Code Table VMPT-40 (Fig. F.1-9).

- c. Click the <Insert> button at the bottom of this window to add a new record (Fig. F.1-10).

Delete	INS Code	UIC	DODAAC	Ship Bill Supad DODAAC	FAD	Unit Type	Cmdr Except Threshold	Mailing Address	Billing Address
<input type="checkbox"/>	41B	W1HDA1	W90N2H	W81F5M	3	P		21ST CAV BDE ACFT MAINT FORT HOOD 765445060	
<input type="checkbox"/>	41B	W1HDAA	W81D4T	W81F5M	3	P		21 CAV BDE FORT HOOD 765445060	
<input type="checkbox"/>	41B	W1HDB1	W90N2J	W81F5M	3	P		21ST CAV BDE 1 SQDN APACHE FORT HOOD 765445060	
<input type="checkbox"/>	41B	W1HDC1	W90N2K	W81F5M	3	P		21ST CAV BDE 2 SQDN KIOWA FORT HOOD 765445060	
<input type="checkbox"/>	41B	W1HDD1	W90N2L	W81F5M	3	P		21ST CAV BDE PBO OPFOR FORT HOOD 765445060	
<input type="checkbox"/>	41B	WC43AA	W81CB9	W81F5M	3	P		1ST BN 158TH AVN REG CO B AIR WHSE BLDG 49015 SANTA FE AVE FT HOOD 765445060	
<input type="checkbox"/>	80S	WQ8TAA	W45B75		2	P		887TH QM CO SUPPLY HVY MATERIAL, 2000 S SAN PATRICIO,,,SINTON,763873511	90 RSC, 8000 CAMP ROBINSON RD, N. L ROCK, AR 72118-22
<input type="checkbox"/>	80S	WS65AA	W45B86		3	P		238TH MAINTENANCE CO GS, 432 BOSWELL STREET,,,SAN ANTONIO,782142499	90 RSC, 8000 CAMP ROBINSON RD, N. L ROCK, AR 72118-22

Figure F.1-9. Milstrip Property Book Code Table for entering derivative UIC/DODAAC information.

Figure F.1-10. Milstrip Property Book Insert window.

- d. Fill in data values as appropriate to add a new DODAAC for the Derivative UIC. Remember that all text boxes with red labels require information.
- e. Click the <Apply> button to save the information and create a new record and close the window. Click the <Close> button to close the window without saving.
- f. Click <Add/Modify DSU DODAAC> to add a supporting DSU (Fig. F.1-10).
- g. {DSU DODAAC Code Table} is displayed (Fig. F.1-11).
- h. To insert new information, click the <Insert> button at the bottom of the screen. {DSU DODAAC Insert} window opens (Fig. F.1-12).

The screenshot shows a web browser window titled "View/Maintain Parameter Tables - Netscape". The main content area is titled "View/Maintain Parameter Tables" and contains a dropdown menu set to "DSU DODAAC Code Table VMPT-4H". Below the menu is a table with the following columns: Delete, DSU DODAAC, DODAAC, INS Cd, SC, DSU Address, DSU Name, DSU Phone, and DSU Email. The table contains seven rows of data, each with a checkbox in the "Delete" column.

Delete	DSU DODAAC	DODAAC	INS Cd	SC	DSU Address	DSU Name	DSU Phone	DSU Email
<input type="checkbox"/>	W45LGC	W45B75	80S	2,4,7	1300 TEEGE AVE	812TH QUARTERMASTER C	956-423-4571	CORTEZN@USARC-EMH2.ARMY.MI
<input type="checkbox"/>	W45LGC	W45V44	80S	2,4,7	1300 TEEGE AVE	812TH QUARTERMASTER C	956-423-4571	CORTEZN@USARC-EMH2.ARMY.MI
<input type="checkbox"/>	W45LGC	W45B86	80S	2,4,7	1300 TEEGE AVE	812TH QUARTERMASTER C	956-423-4571	CORTEZN@USARC-EMH2.ARMY.MI
<input type="checkbox"/>	W45LGC	W45B84	80S	2,4,7	1300 TEEGE AVE	812TH QUARTERMASTER C	956-423-4571	CORTEZN@USARC-EMH2.ARMY.MI
<input type="checkbox"/>	W45NQZ	W81CB9	41B	2,4,7	FORT HOOD TX.	DOL	254-7790	
<input type="checkbox"/>	W45NQZ	W90N2L	41B	2,4,7	FORT HOOD TX.	DOL	254-7790	
<input type="checkbox"/>	W45NQZ	W90N2K	41B	2,4,7	FORT HOOD TX.	DOL	254-7790	

At the bottom of the window, there is a navigation bar with buttons: Search..., Apply, Refresh, Undo, Insert..., Delete, Print..., Coach..., and Help....

Figure F.1-11. DSU DODAAC Code Table for entering derivative UIC supporting unit information.

The screenshot shows a web browser window titled "DSU DODAAC Insert - Netscape". The main content area is titled "DSU DODAAC Insert" and contains a form with the following fields:

- DSU DODAAC:
- DODAAC:
- INS Cd:
- Supply Class: 1 2 3 4 5 6 7 8 9 10
- DSU Name:
- DSU Address:
- DSU Phone:
- DSU Email:
- DSU RIC:

At the bottom of the form, there are two buttons: "Apply" and "Close".

Figure F.1-12. DSU DODAAC Insert window.

- i. Insert data as appropriate (Fig. F.1-12).
- j. Click **<Apply>** to save the data or **<Close>** to close the window without saving.
- k. Exit the Organizational Data screen and return to the main menu.

F.1.6 Assign user access for the derivative UIC.

It is important to ensure that while unit data is being modified in Standalone mode the same unit data is not being changed in enterprise databases on AKO. When a unit synchronizes data from a Standalone laptop to the AKO enterprise database, the laptop data that has changed overwrites data on the main server. If unit data changes are made to the enterprise database and then data for the same unit operating in Standalone mode is synchronized with the enterprise database, changes that were made to the enterprise database will be overwritten by data that has changed on the Standalone computer. By carefully assigning specific UICs to individual users, it is possible to ensure that only certain individuals have access to a particular unit's data and thereby eliminates the risk of accidentally overwriting unit transactions during a re-sync operation. Furthermore, the replication operation, referenced in Section F.3, will copy unit data to the laptop for all of the units that are assigned to the user performing replication. For those users that are deploying with a Standalone laptop, user roles and permissions should be modified to limit user visibility to those specific units that will be supported in Standalone mode.

NOTE: The Assign User Roles task is covered in detail in Section 5.4 of the End User Manual (EUM). The EUM is always available on the left hand side of the SPR Main Menu screen. It is recommended that users download the EUM when time permits, for use offline.

- a. From the Administrative Menu, select **<User Roles-View/Status/Modify/Add>**.
- b. {User Roles - View window} opens.
- c. Click the **<Modify>** button at the top of the screen to open the User Roles-Modify screen (Fig. F.1-13).
- d. In the left hand pane, select the user account to be modified. If the user account is not displayed in the left-hand pane, use the Next button to scroll through the panes, or use the Search button to find the user directly.
- e. Once a user is selected, the user role information will be displayed in the right hand pane.
- f. Update the list of UIC's to display only those that the user should now access. Remove all UIC's that the user should not access. Figure F.1-13 shows a sample User Roles - Modify screen where the UIC list has been changed to limit access to one UIC.
- g. Slide the locator bar in the right-hand pane to the top. Click the **<Action>** list of values (LOV) and select **<Modify>** to add the new UIC to the selected individual. Click the **<Authorizing ISSO>** LOV and select the appropriate ISSO.

NOTE: Once the User Roles changes are submitted, the changes must be approved by ISSO that was selected. The PBUSE program will automatically notify the ISSO of the User Role modification request.

- h. Exit to Main Menu.

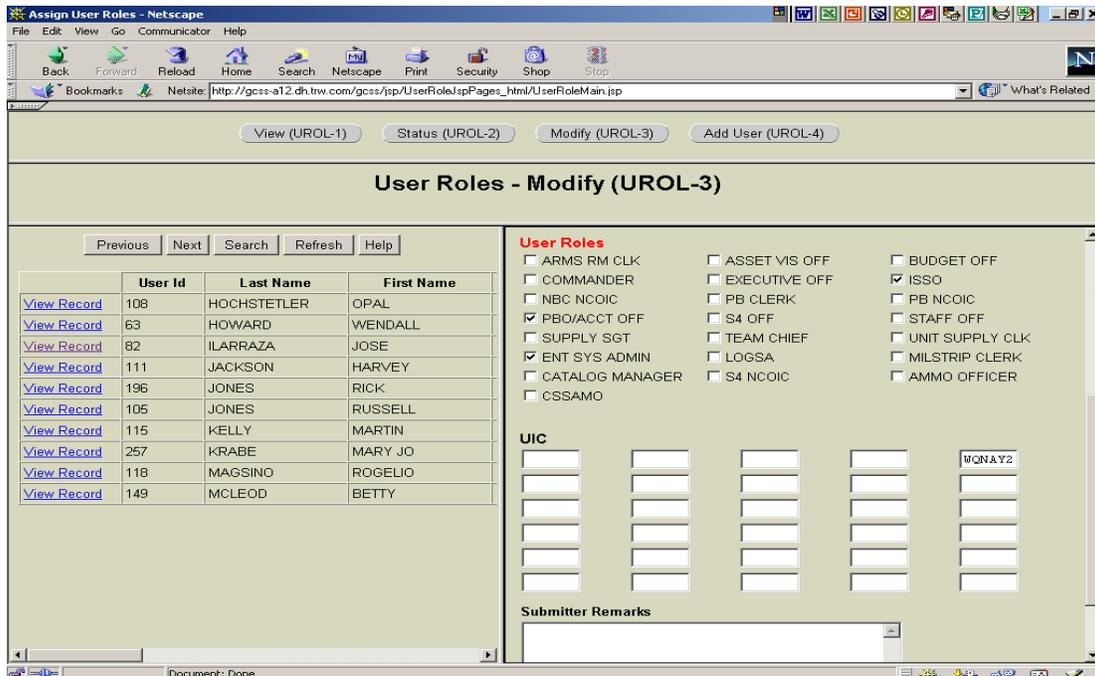


Figure F.1-13. User Roles - Modify screen.

F.1.7 Assign property to the derivative UIC.

The derivative UIC has been created and assigned to the user, but the derivative UIC has no property assigned to it. Unlike regular Lateral Transfers, authorizations are not required for a Task Force UIC/DUIC. The authorization TAC will automatically have a TAC of 9 for all derivative UIC property assignments. Follow the steps below to assign property from the host UIC to the derivative UIC.

- a. From the Main Menu, select **<Property Book>**.
- b. From the Property Book menu select **<Unit Transfer/Task Force/ Split Operations>**.
- c. Click the **<Task Force/Split Operations>** tab at the top of the screen (Fig. F.1-14).
- d. Select the **<Material Items>** tab.
- e. Select the **<Losing UIC>** from the LOV on the left hand side of the screen.
- f. Select the **<Task Force CD>**, and then select the **<Gaining UIC>** on the right hand side of the screen.

NOTE: During this property transfer operation, the user will have visibility of Army-wide (PBUSE) Task Forces. This visibility allows units to move equipment outside of their INS.

- g. Select property to transfer on the left hand side of the screen. Use the **<SELECT>** button to move property from the left hand side of the screen to the right hand side of the screen. Use the **<DELETE>** button to remove highlighted items from the right hand side of the screen.
- h. After selecting all property for transfer, click **<Apply>** to create an internal transfer document and generate a document number.
- i. When the transaction has been accepted, a message box will open and indicate the document number (Fig. F.1-15).

AIS Manual GCSS-A/T PBUSE EM
1 January 2003

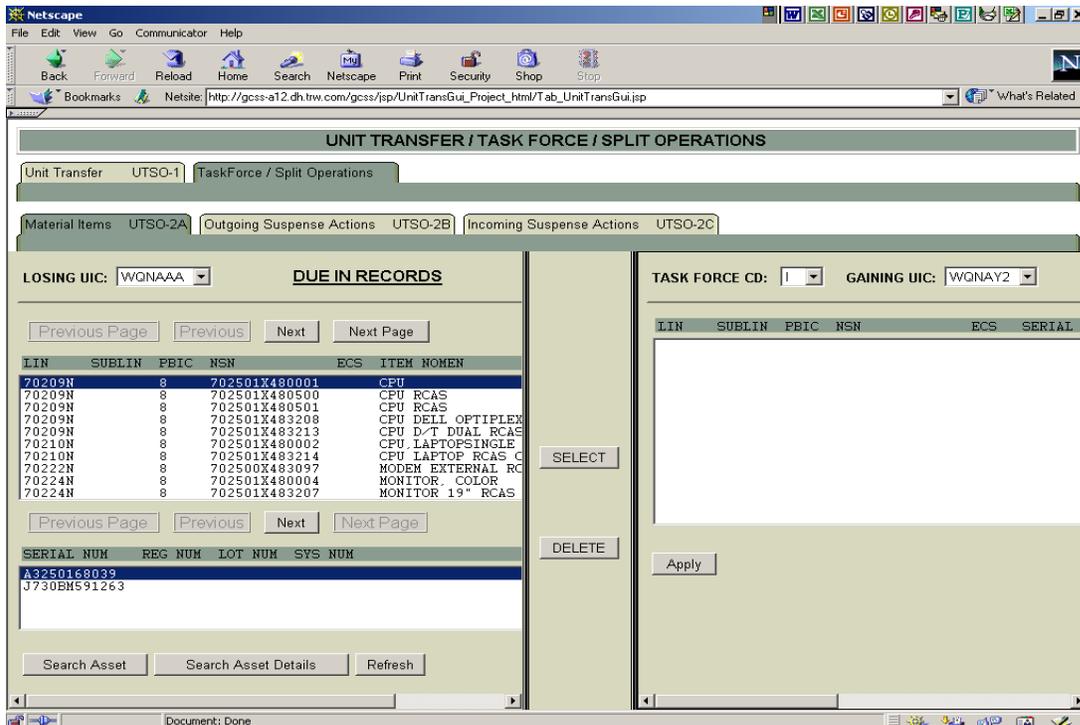


Figure F.1-14. Unit Transfer / Task Force / Split Operations screen.

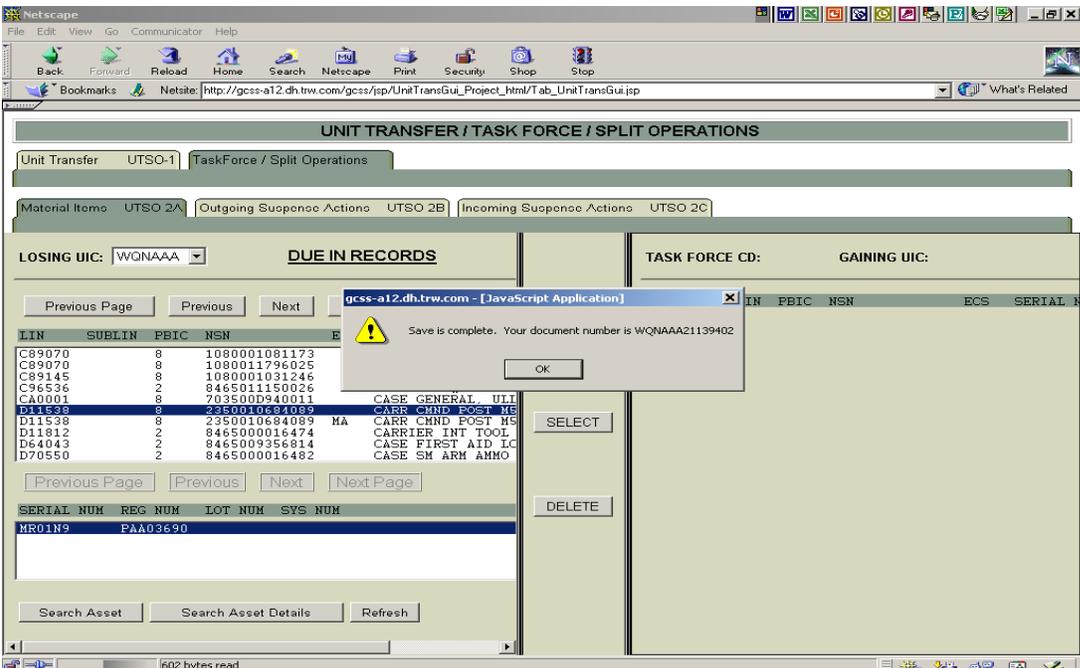


Figure F.1-15. Document number message box indicating that property transfer has been initiated.

- j. Click the **<Outgoing Suspense Actions>** tab (Fig. F.1-16).
- k. Select the document number that was just generated from the **<DOC NUM>** LOV. If the document number does not appear in the LOV, click the Refresh button to prompt the system to save recent document number changes.
- l. Click the **<Generate Form>** button to print a copy of the property transfer form.

- m. Click the **<Notify the Gaining PBO>** button. This will notify the gaining PBO of all the items that are a part of this document. A message box will indicate when this step is complete (Fig. F.1-17).
- n. If more than one document was used to transfer property to the derivative UIC, repeat steps g - h as appropriate.

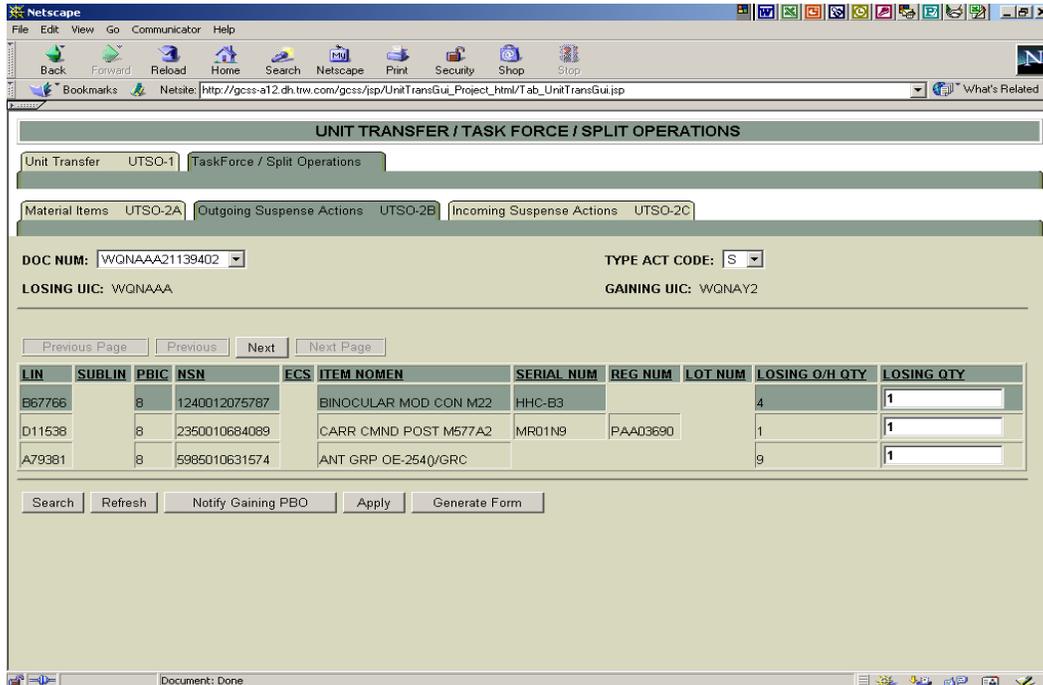


Figure F.1-16. Outgoing Suspense Actions tab awaiting PBO verification of transferred items.

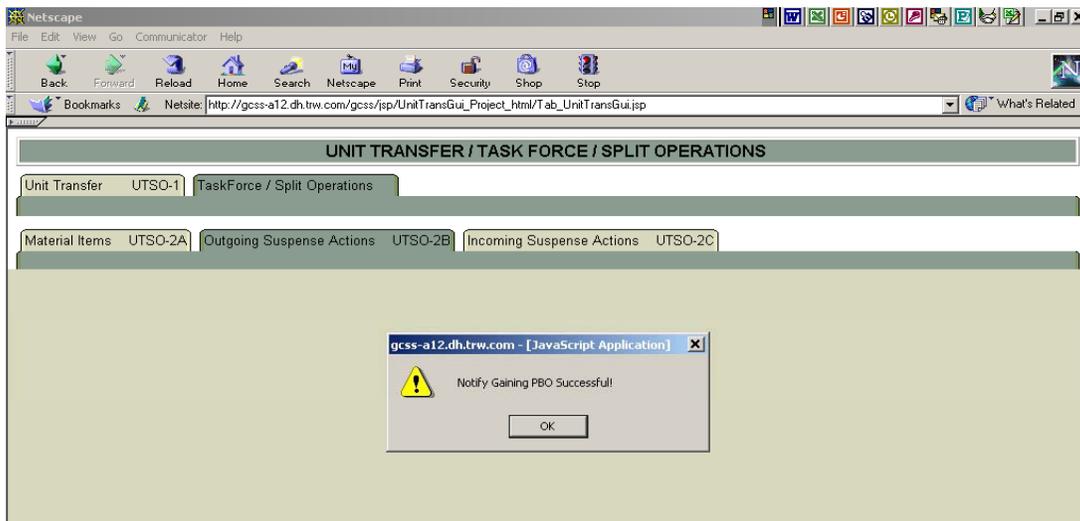


Figure F.1-17. Message box indicating Derivative PBO notification is successful.

F.1.8 Receive incoming property to the derivative UIC.

Once property has been assigned to the derivative UIC, it must be accepted just as with any Lateral Transfer operation.

- a. Click on the **<Incoming Suspense Actions>** Tab (Fig. F.1-18).
- b. Select the document number from the **<DOC NUM>** LOV.
- c. Select **<TYPE ACT CODE>** of P to post the transaction and accept the property transfer.
- d. Click **<Apply>** to complete the property transfer and accept all of the items transferred on this document. A message box will list a new document number from the derivative UIC to indicate that the transfer is complete (Fig. F.1-19).
- e. If multiple document numbers were used, repeat steps l - n as appropriate.
- f. Close the screen and return to the main menu.

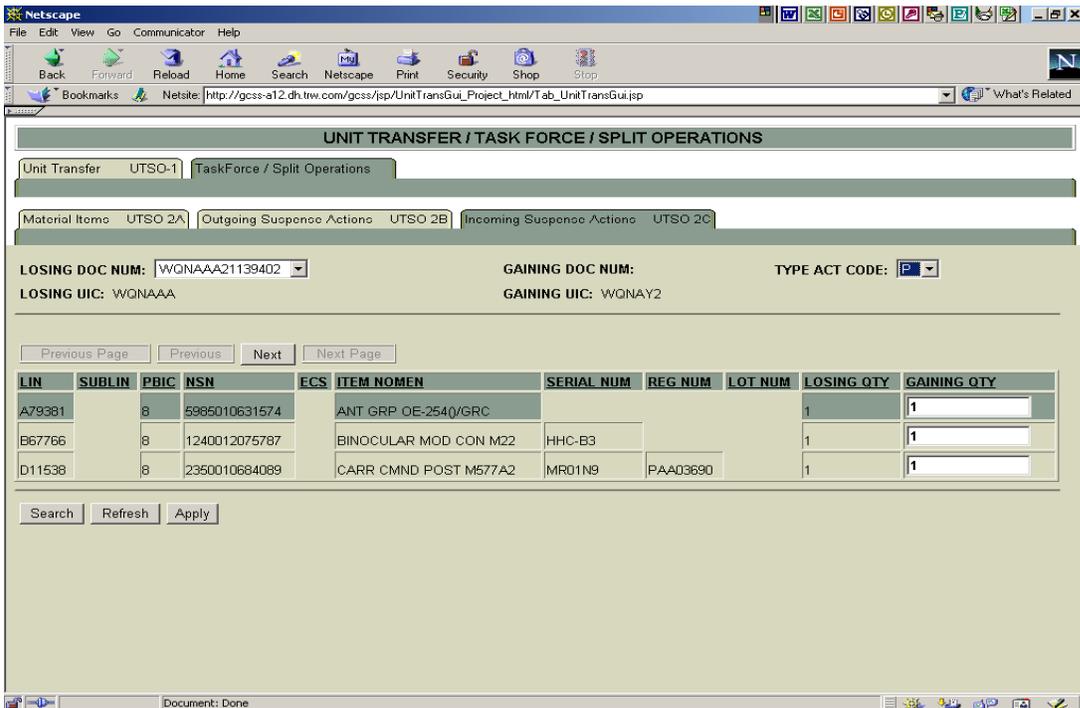


Figure F.1-18. Incoming Suspense Actions tab.

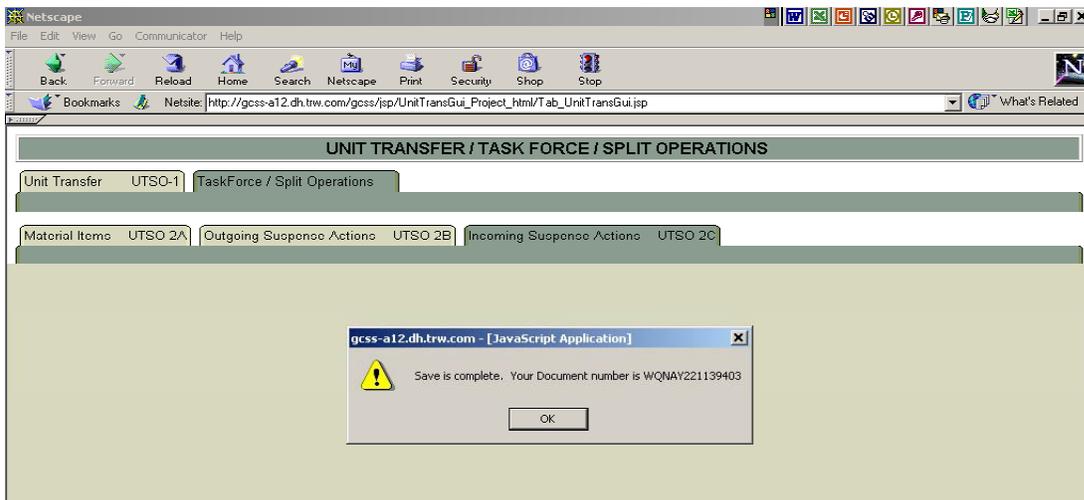


Figure F.1-19. Message box showing property transfer document number indicating that the process is complete.

F.1.9 Verify property transfer.

To ensure that all property transfers completed as expected, validate the property transfer using the primary hand receipts of the original UIC and the derivative UIC.

- a. From the Main Menu, select <**Hand Receipt**>, and then select <**Primary Hand Receipts**>.
- b. Compare items on the derivative UIC hand receipt with the desired items to ensure all items have been processed (Fig. F.1-20).
- c. Compare items on the derivative UIC hand receipt with the original UIC Hand receipt to ensure that equipment has transferred as desired. Depending on the type of property that was transferred, the user may need to compare items on the Organization Hand Receipts tab, Installation Hand Receipts tab or both.
- d. Close the screen and return to the main menu.

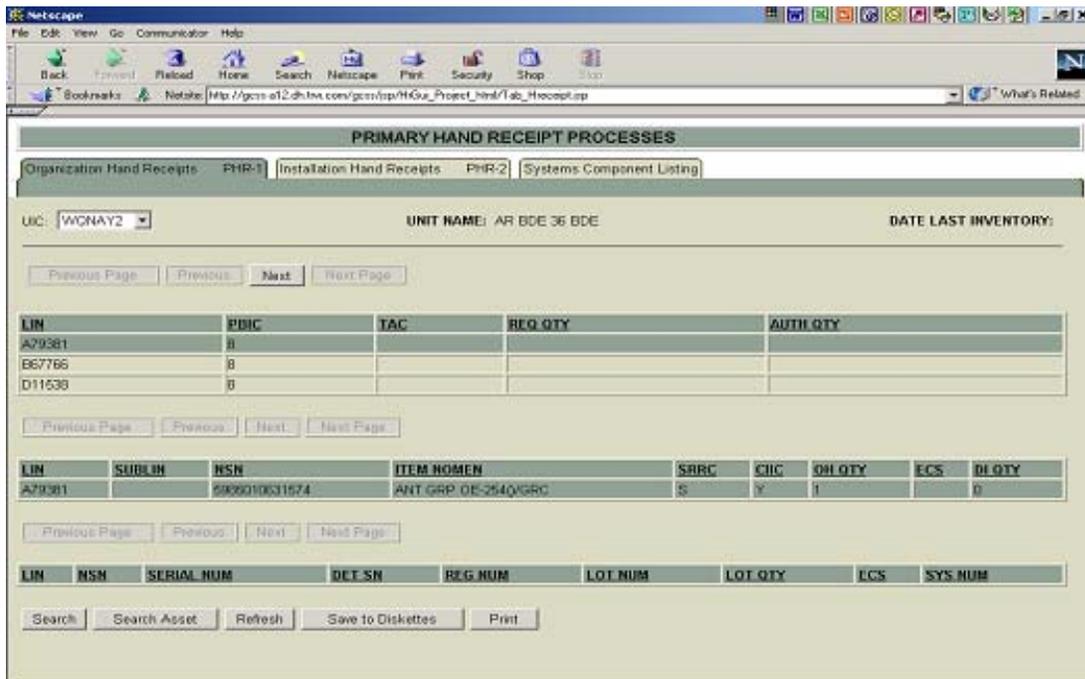


Figure F.1-20. Organization Hand Receipt property verification.

F.1.10 Complete the derivative UIC by modifying the remaining parameter tables.

Update the remainder of the Parameter Tables (if information is available) as required, before replicating the data to build the Standalone. From the SPR Administration Menu, select <**View/Maintain Parameter Tables**>. When the window opens select <**Reference Lookup table**> tab (Fig. F.1-21).

NOTE: In order to maintain data integrity between a Standalone computer and the enterprise database, some unit configurations, such as DODAAC changes, cannot be performed in Standalone mode. For this reason, it is desirable to update the derivative UIC as completely as possible prior to performing the replication process.

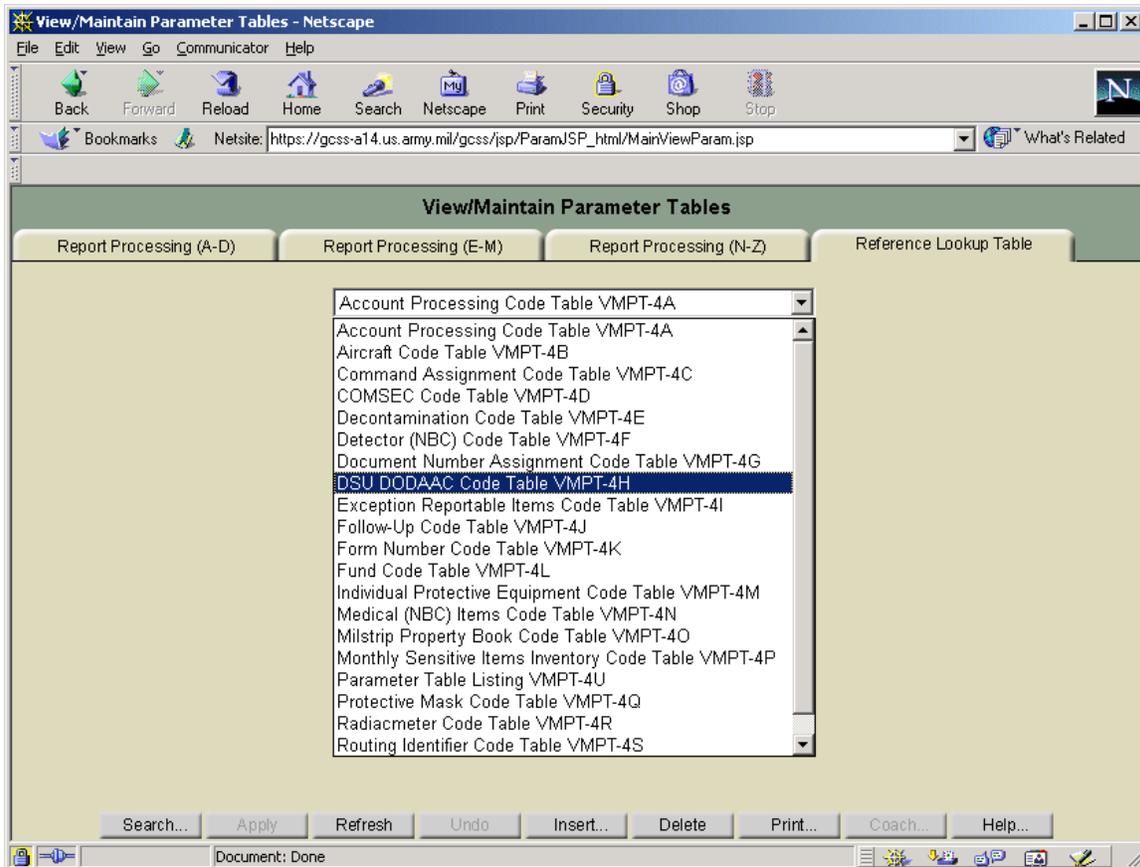


Figure F.1-21. Reference Lookup Table with LOV expanded.

- a. On the <**Reference Lookup Table**> tab, select the LOV to display tables that may be altered.
- b. Highlight the table of choice, and allow the table to display on the screen.
- c. Make alterations to tables in the same manner used to alter the DSU DODAAC Code Table and the Milstrip Property Book Code Table in Section F.1.2.

F.2 Load Standalone Module

See Appendix I – Loading for Standalone Operations section.

F.3 Replication – Server to Laptop

This process contains the steps necessary to download data, for a designated user, to a laptop. This must be done prior to working in a standalone manner. In order to perform these steps, the user must be a member of the Power Users group. For information on how to add users to the Power Users group, see Section F.6.

F.3.1 Identify the AKO Server

Prior to running the replication process, users must identify the AKO server that holds their data. The server information will be largely static and will not change often. However, large database servers such as those used by AKO are regularly cycled offline for maintenance purposes to ensure server functionality and data integrity. During the server maintenance process, the primary server is taken offline and seamlessly replaced with a redundant server that has the same unit data. This process will be transparent to users logging onto AKO to access their GCSS-A/T application data.

In order to complete the data replication process, users will need to know the fully qualified domain name of the database server on which the data to be replicated resides. A fully qualified domain name is also commonly known as the WWW address. This information is listed on the SPR module Main Menu screen.

- a. Login to AKO using normal PBUSE access methods.
- b. Login to the PBUSE application.
- c. {SPR Module Main Menu} window opens (Fig. F.3-1).
- d. At the top of the web page an information bar is displayed that shows the current PBUSE software build information (Build-2.8), the date of the build (25 February 2002), the Rapid Application Development (RAD) tool used to develop the software (Jdev 3.2.2, JDK 1.2.2), and the name of the database where the unit data is stored (gcss-a14.us.army.mil).
- e. Identify the name of the database where the unit data is stored. In this example, the unit data is stored on database **gcss-a14.us.army.mil** (Fig. F.3-1). The ":1521:gcss" is specific port information that the user does not need to specify in order to replicate data.

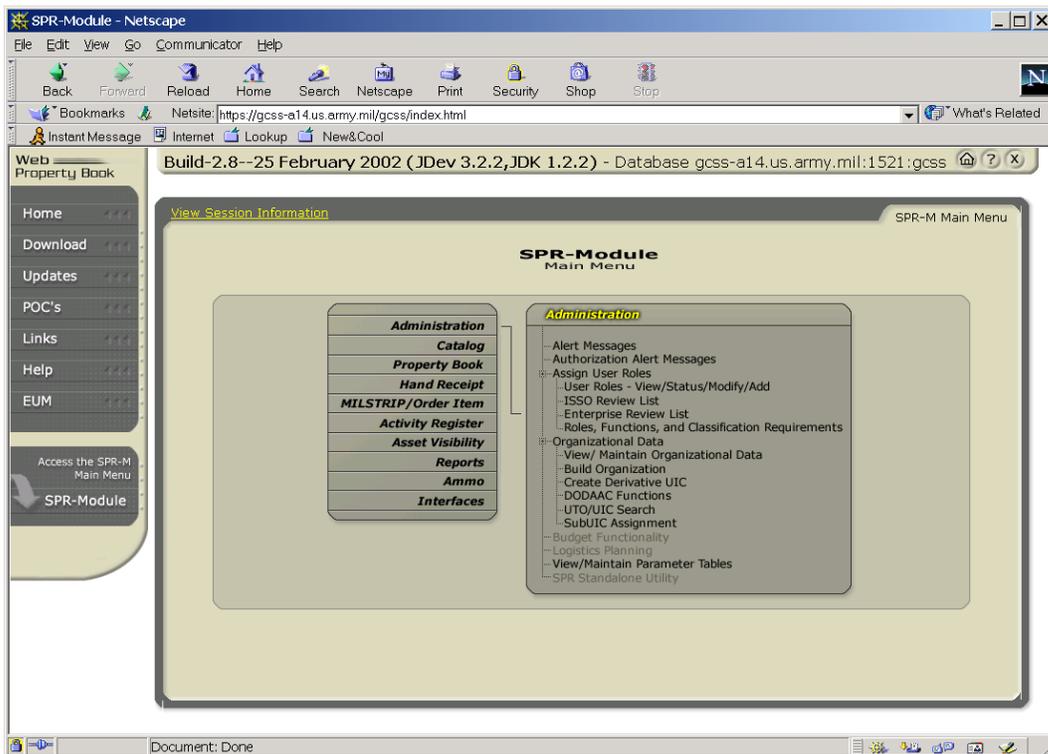


Figure F.3-1. SPR Module Main Menu in connected mode displaying database information.

NOTE: The web server that controls the PBUSE application and the database server that holds user data are usually on separate machines. These machines may have different names and different IP addresses. The database name that is listed on the information bar is the database name that users need to select from the **SERVER NAME** LOV shown at the top of Figure F.3-2. The fully qualified domain name for the server will then appear in the next block: **DB HOST NAME**. In this example, the SERVER NAME is GCSS_A1 and its fully qualified domain name is gcss-a1.dh.trw.com.

F.3.2 Verify Power Properties.

Because the replication process is lengthy, it is imperative that the Power Properties for the PBUSE Standalone are properly configured. See Step 2.2 for information on completing Power Properties update and validation.

F.3.3 Open Session Manager.

- a. Double click the SPR Session Manager desktop icon.
- b. {USER LOGIN} window opens (Fig. F.3-2).

The image shows a 'USER LOGIN' dialog box with the following fields and values:

Field Label	Value
SERVER NAME:	GCSS_A14
DB HOST NAME:	gcss-a14.us.army.mil
APPLICATION SERVER NAME:	gcss-a14.us.army.mil
USER NAME:	
USER PASSWD:	

Figure F.3-2. User Login window with sample database server name selected.

F.3.4 Select database server and login.

- a. **SERVER NAME:** select the server name from the LOV matches the database server name.
- b. **DB HOST NAME:** verify that the DB Host Name matches the database host name that was identified in Step 3.1 above.
- c. **USER NAME:** AKO login name of appropriate user for replication.
- d. **User PASSWD:** AKO password for the USER NAME.
- e. Click <OK> to attempt to login with this information.

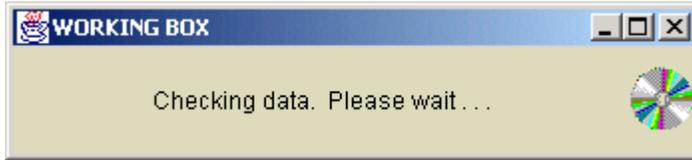


Figure F.3-3. Message box indicating that user authentication is taking place.

- f. A message box will open (Fig. F.3-3) indicating that the Session Manager is verifying the USER NAME and PASSWORD with the list of appropriate users for the SERVER NAME and DB HOST NAME selected.
- g. If the USER NAME is properly verified, the session manager will return showing the first tab, "Replication Setup REP-1". All options are available to the user. No buttons are grayed out (Fig. F.3-4).

NOTE: If the USER NAME is not authenticated, the PBUSE Standalone Session Manager window will open with information for the previous validated user. However, since the login attempt was unsuccessful, options requiring AKO validation will be unavailable. This is a key security component of the replication process. Only those users with the appropriate permissions will be allowed to replicate unit data and operate in Standalone Mode.

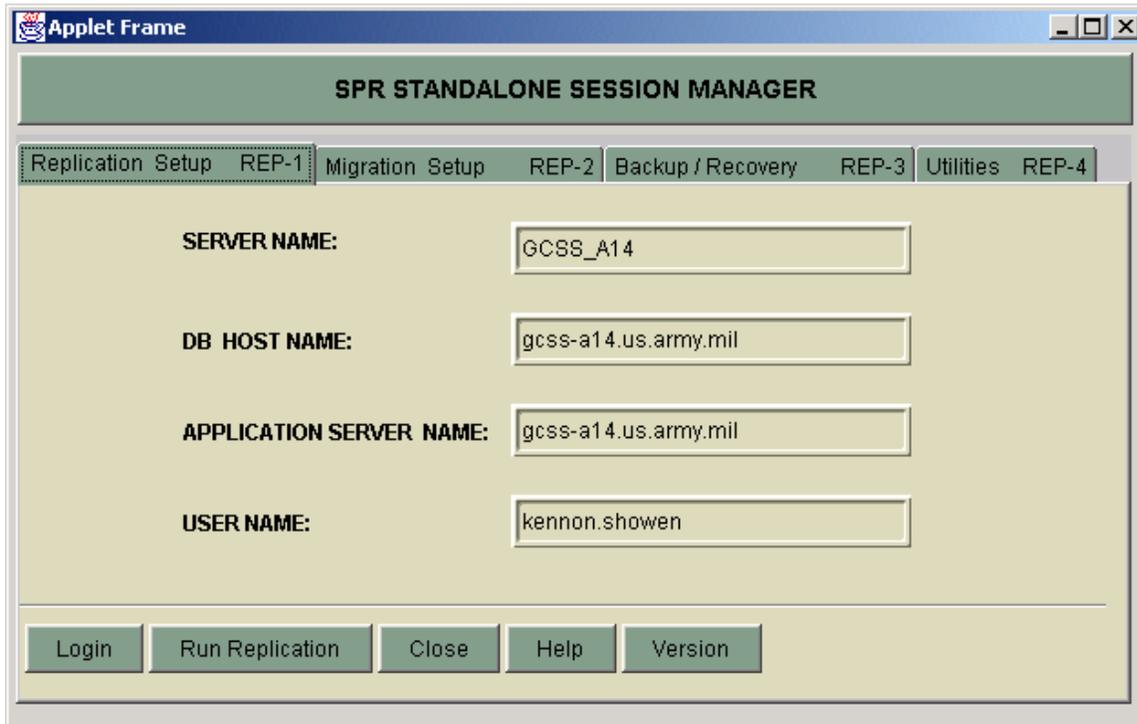


Figure F.3-4. SPR Standalone Session Manager tab 1 after validating user information.

F.3.5 Start replication.

Once the user name has been authenticated, the user may replicate data from the PBUSE server. The data that will be transferred will be the same data that the user has access to when the user is operating in connected mode.

- a. Click <Run Replication>.
- b. {Info} window is displayed (Fig. F.3-5).

NOTE: The system will replicate only those UICs related to the validated user.

NOTE: For Split-Based operations, a user's roles and UIC access may require changing.

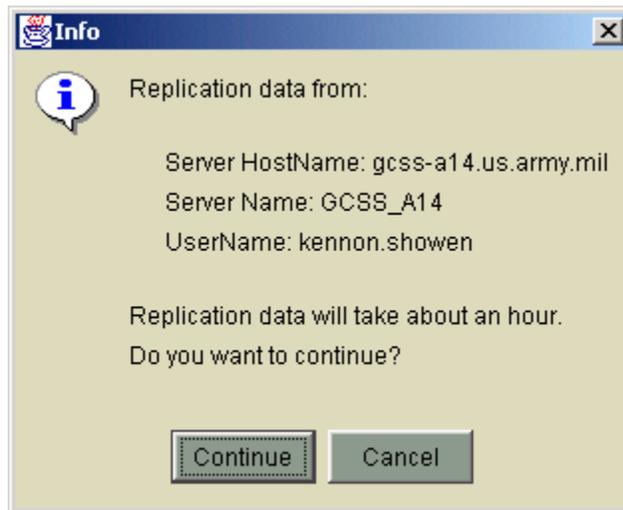


Figure F.3-5. Info window with sample values.

F.3.6 Confirm login data.

- a. Verify replication information entered is ok.
- b. If ok, click<**Continue**>.
If not ok, click <**Cancel**> and go to Section F.3.3.

F.3.7 Wait for replication to complete.

The time required for data transmission depends on several factors, including the quantity of data that to be transmitted and the quality of the communications link that is being used. Tests have shown that transmission of data for a typical battalion sized element with one parent UIC and four company UICs over a typical military LAN may take between one and three hours. If performing this operation via modem, transmission time may double. Your actual results may vary.

- a. While data replication is ongoing, a message box will be displayed (Fig. F.3-6). For best results, user's should refrain from other computer activity during the replication process.



Figure F.3-6. Replication in progress message.

- b. {MSG} displayed when replication finished (Fig. F.3-7).



Figure F.3-7. Replication complete message.

- c. Click <Ok> to acknowledge completion.
d. The {PBUSE STANDALONE SESSION MANAGER} window becomes active. Click <Close> to exit.
e. The replication process is complete – user data has been loaded on the PBUSE Standalone computer.

NOTE: The computer should be shutdown daily. When the computer restarts, an automated script is run that sets system variables and restarts the automated document number sequence. This script will require approximately five minutes to execute. It will be displayed as a command window at the bottom of the screen. If the computer is not restarted or if the script is not allowed to run to completion, then the document numbers will continue in sequence from the previous day.

F.4 Data Sync – Laptop to Server

This process contains the steps necessary to upload data from a laptop to the server. This will synchronize the laptop and the server. In order to perform these steps, the user must be a member of the Power Users group. For information on how to add users to the Power Users group, see Section F.6.

F.4.1 Perform Data Sync.

- Double click the **<SPR Standalone Applications>** desktop icon.
- Click **<Continue>** on {*Security Warning*}.
- {*SPR Module Home Page*} displayed.
- Select **<SPR-Module>**.
- {*SPR Module Main Menu*} displayed (Figure F.4-1).

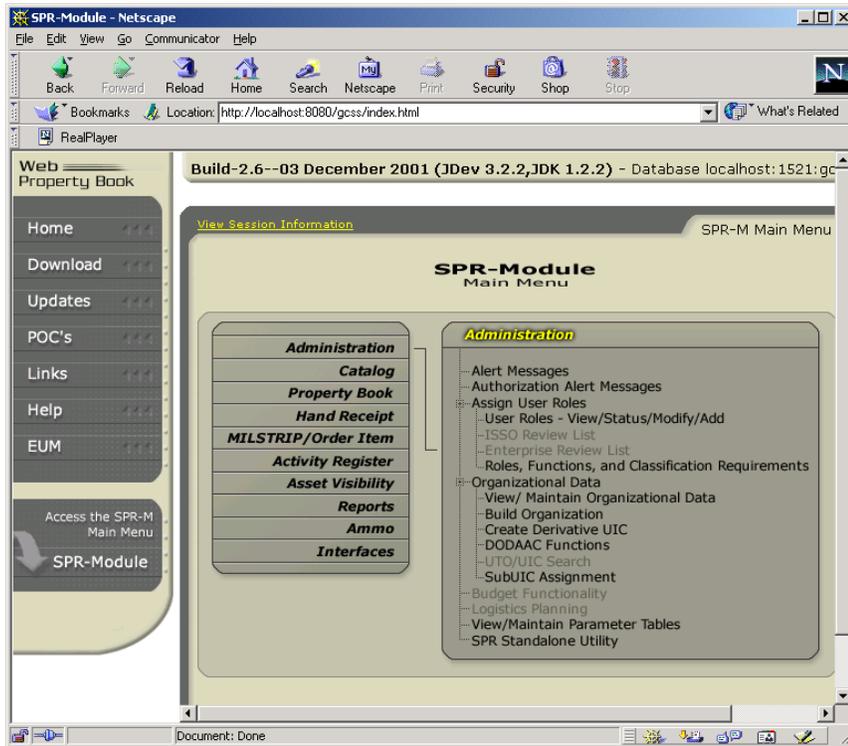


Figure F.4-1. SPR Module Main Menu

- Select **<SPR Standalone Utility>** from the Administration menu.
- {*Replication Utilities*} displayed (Figure F.4-2).

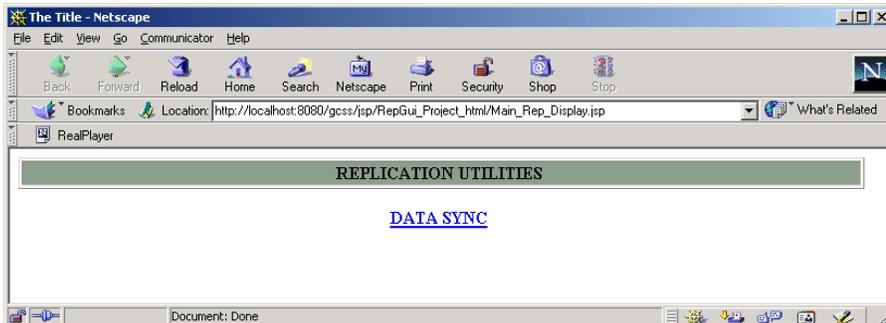


Figure F.4-2. Data Sync link.

- h. Select <Data Sync>.
- i. Information box displayed indicating server is loading. (Fig. F.4-3).
- j. Dialog box displayed when sync is complete (Fig. F.4-4).

NOTE: The Data Sync process does not take as long as the initial Replication process. During a Data Sync, only records that have been modified while in Standalone Mode are transmitted back to AKO to overwrite unit data on the Enterprise database. Typically, this process will take between 15 and 20 minutes the first time it is performed. Subsequent Data Sync operations are much faster, often taking only a minute or two.

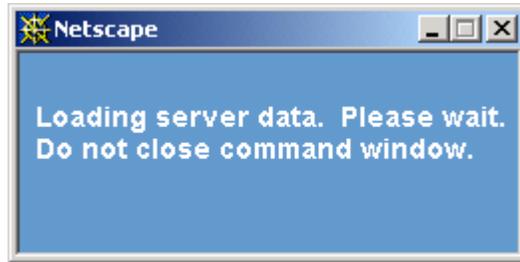


Figure F.4-3. Data Sync in progress message.



Figure F.4-4. Data Sync complete message.

- k. Click <OK>.
- l. Click <File><Close> on Netscape taskbar to close {Replication Utilities}. The replication process is complete – laptop data has been synchronized with the server.

NOTE: The Data Sync process should be repeated as frequently as communications capability is available until the unit returns to home station and the Standalone operation is complete. Performing data sync provides an extra measure of data surety for the Standalone user and provides for current DA asset visibility for the unit.

F.4.2 Unsetup Replication

When the need for operating in Standalone Mode has passed and the user has performed a Data Sync, the user should remove the Standalone Mode data from the laptop and return to operating completely in connected mode. The data is removed from a Standalone Mode computer using the Unsetup Replication process on the Utilities tab of the Session Manager. By performing Unsetup Replication, all PBUSE Standalone Mode application data will be completely erased. This operation will protect a unit's Enterprise-level data from being overwritten by outdated Standalone Mode data.

NOTE: After operating in Standalone Mode, users must perform the Data Sync operation prior to performing Unsetup Replication. Once the Unsetup Replication operation has started, users will not be able to access data in the Standalone Mode without again performing the Replication operation discussed in Step 3.

- a. Double click on the <Session Manager> icon on the desktop.
- b. Enter user information as described in Step 3 or click <Cancel> to bypass the login screen.
- c. Click on the <Utilities REP-4> tab (Fig. F.4-5).
- d. Click on <UNSETUP REPLICATION> button.

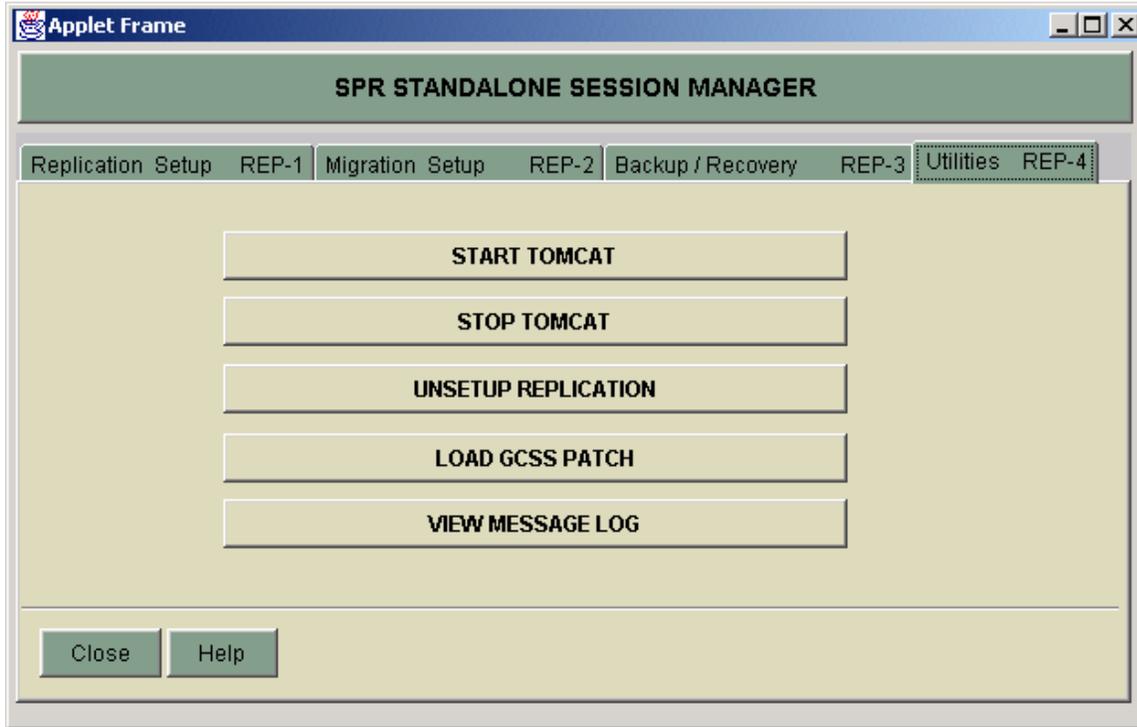


Figure F.4-5. SPR Standalone Session Manager Utilities tab.

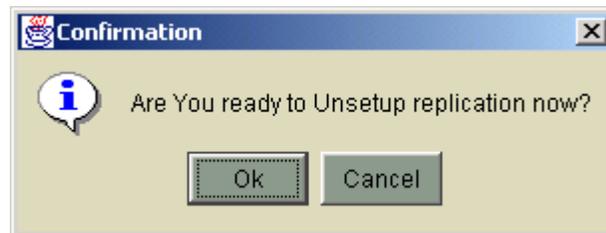


Figure F.4-6. Unsetup replication confirmation window.

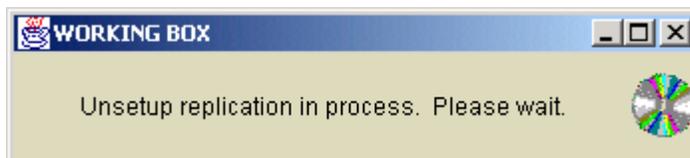


Figure F.4-7. Unsetup replication in progress message.

- e. {Confirmation} window will open. Click <OK> to continue the Unsetup Replication process (Fig. F.4-6).
- f. {Working Box} window will open during the Unsetup Replication process (Fig. F.4-7).
- g. When the Unsetup replication process is complete, a message window will open to inform the user (Fig. F.4-8). Click <OK> to complete the process.
- h. Click <Close> to exit the PBUSE Standalone Session Manager (Fig. F.4-5).



Figure F.4-8. Unsetup replication complete message.

F.5 FTP to SARSS-1

In order to successfully transfer data to SARSS-1 via FTP, several configuration steps have to take place, both on the SARSS-1 and on the PBUSE Standalone computer.

F.5.1 Fixed IP address requirement.

SARSS-1 computer systems have strict data reception rules that govern all incoming FTP transmissions. One of the primary sources of protection against false transmissions, both real and accidental, is the requirement that each customer computer have an IP address previously known to the SARSS-1. This address is entered in a table within the SARSS-1 so that all incoming transmissions can be validated. Using this information, SARSS-1 will receive only those transmissions from known customers. This effectively forces all SARSS-1 customers to have a fixed IP address, since all changes to an IP address must be updated within the SARSS-1.

F.5.2 Obtain a fixed IP address.

All IP address information is network specific. In most Army networks, the organization that provides network support can also distribute a fixed IP address. This information should always be coordinated with the network administrator, as failing to do so will likely cause an IP conflict which will render both computers incapable of transmitting data until the situation is resolved. When contacting the network support organization, request the following information:

- IP Address:
- Default Gateway:
- Subnet Mask:
- DNS Server Address: (if available).

Each number will be a series of four numbers between 0 and 255, in a dotted decimal format. For example, the following could be legitimate values for a local network.

- IP: 192.138.53.100
- Gateway: 192.138.53.1
- Subnet Mask: 255.255.255.0
- DNS Server: 192. 138.2 20.

F.5.3 Loading a fixed IP address.

- a. Obtain a fixed IP address from the network's governing body.
- b. Right-click on the **<My Network Places>** icon on the desktop.
- c. Select **<Properties>** from the menu that opens.
- d. Right-Click on the **<Local Area Network Connection>** icon and select **<Properties>**.
- e. {Local Area Connection Properties} window will open (Fig. F.5-1).

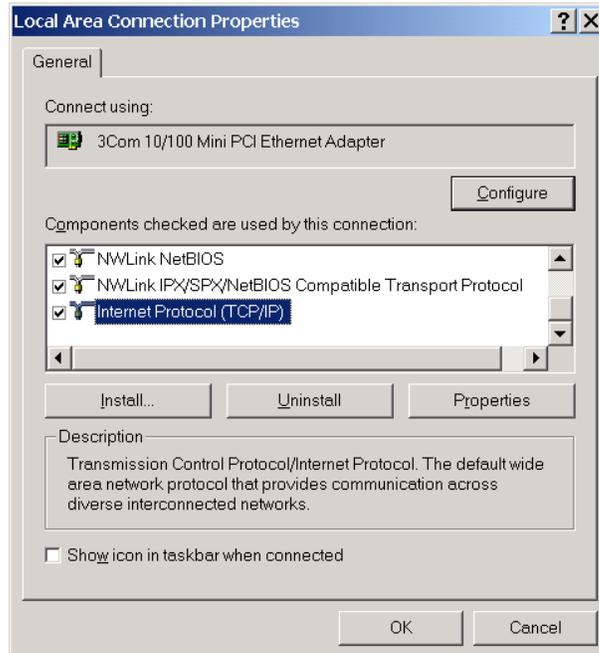


Figure F.5-1. Local Area Connection Properties with Internet Protocol Selected.

- f. Select **<Internet Protocol (TCP/IP)>** from the list of values.
- g. Click the **<Properties>** button (Fig. F.5-1).
- h. {Internet Protocol TCP/IP Properties} window will open (Fig. F.5-2).

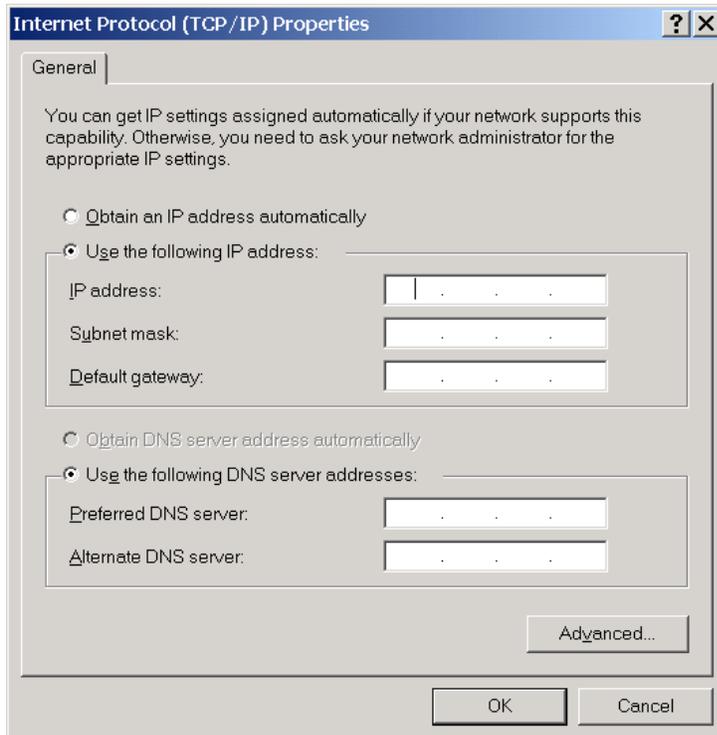


Figure F.5-2. Internet Protocol (TCP/IP) Properties ready for IP address input.

- i. Click the radio button in front of **<Use the following IP address>**:
- j. Enter values for IP Address, Subnet Mask, and Default Gateway and for the Preferred DNS Server, if available.
- k. Click **<OK>** to accept the input values.
- l. Close all open windows.

F.5.4 Getting a SARSS-1 FTP account

- a. Once the fixed IP address is loaded in the PBUSE Standalone computer, the same information must be given to the SARSS-1 operator to be loaded so that account information can be generated.
- b. The SARSS-1 operator will create an account name and password for each DODAAC that will be ordering supplies through the SARSS-1.
- c. The SARSS-1 operator will also provide the customer with an IP address for the SARSS-1.
- d. The Account Name, Password, and SARSS-1 IP Address will be entered into the Interfaces module as shown in Figure F.5-6.

F.5.5 Sending transactions to SARSS-1

- a. From the SPR Main Menu, select the **<Interfaces>** module (Fig. F.5-3).

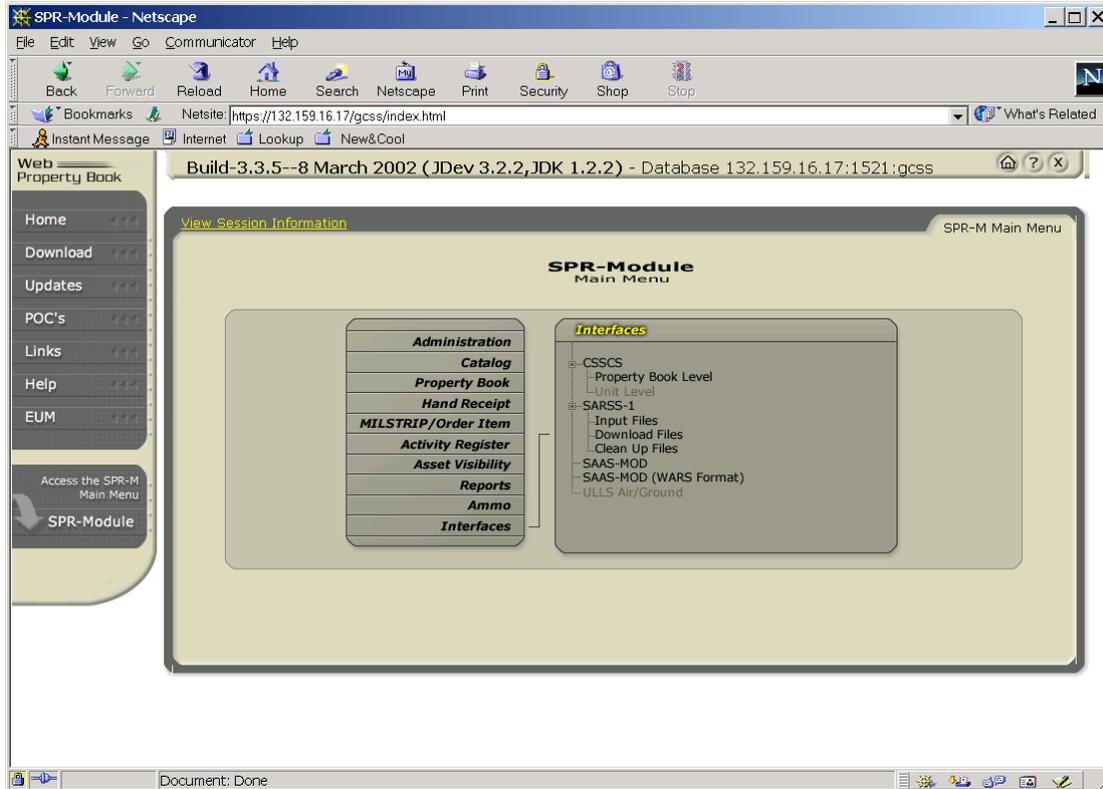


Figure F.5-3. Interfaces option selected from the main menu.

- b. Select **<Download Files>** from the Interfaces menu. (Fig. F.5-3, right-hand menu).
c. {WebPB Interfaces} window opens prompting the user to select the appropriate RIC from a LOV (Fig. F.5-4).
d. Select a **<RIC>** from the LOV and Click **<Continue>**
e. A transmission options window opens (Fig. F.5-5).

AIS Manual GCSS-A/T PBUSE EM
1 January 2003

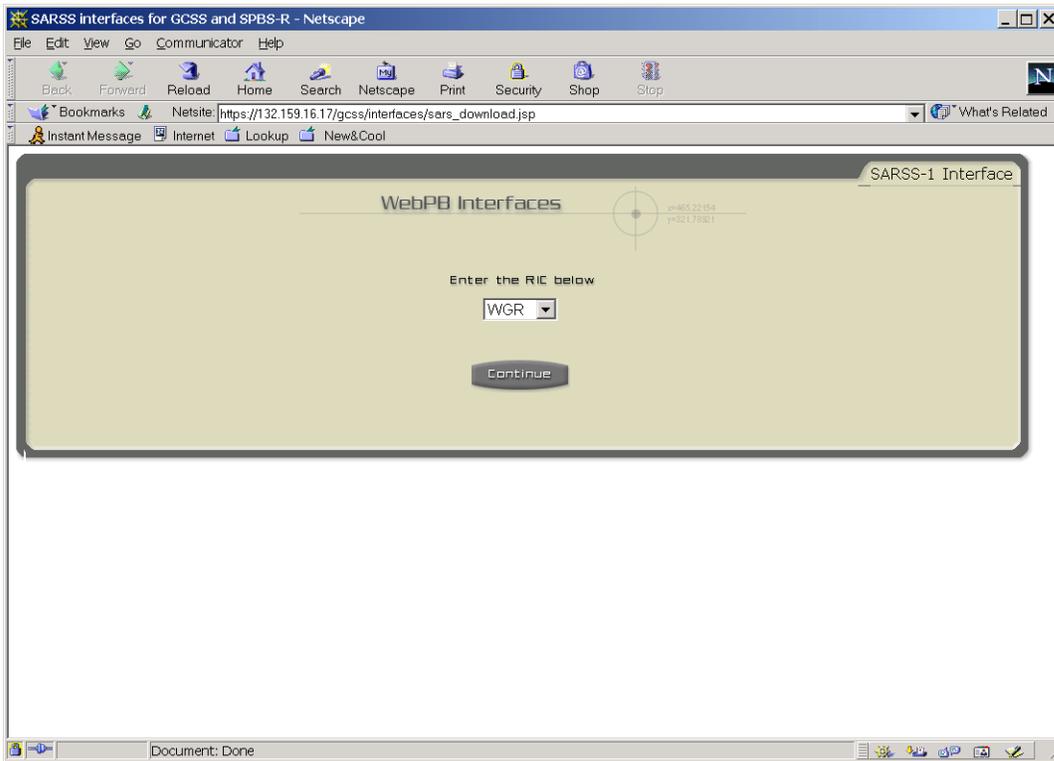


Figure F.5-4. WebPB Interfaces screen with RIC LOV.

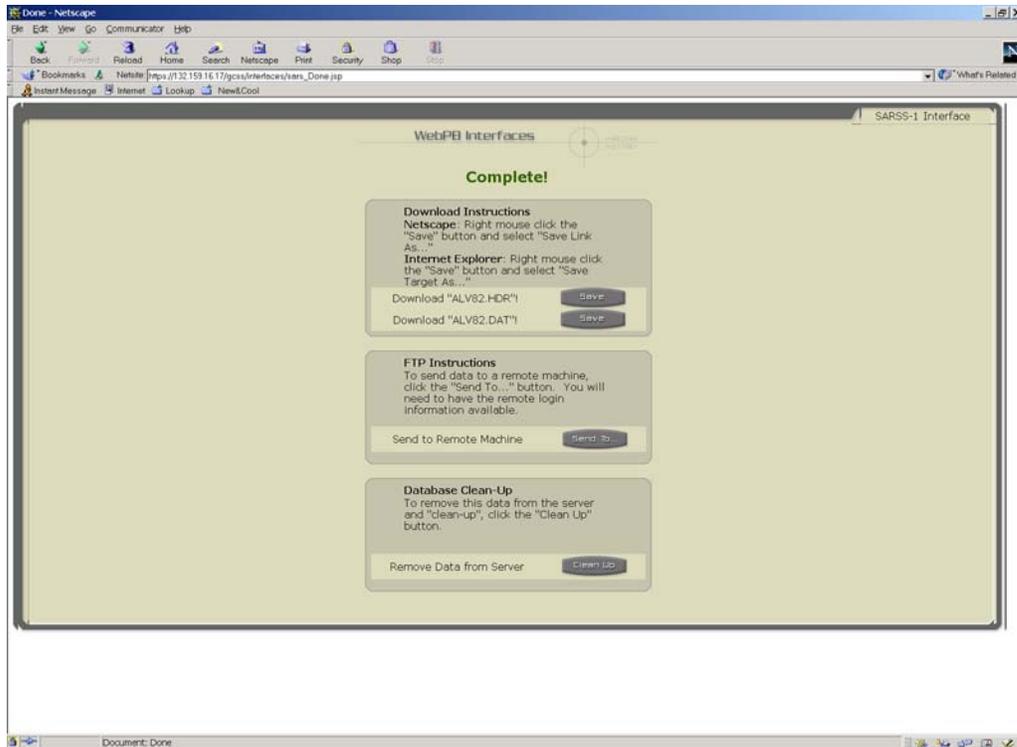


Figure F.5-5. WebPB Interfaces options: Diskette transfer, FTP and Database Clean-Up options.

- f. In the section marked FTP Instructions, Click the <**Send To...**> button to open the SARSS-1 Electronic Transfer window (Fig. F.5-6).

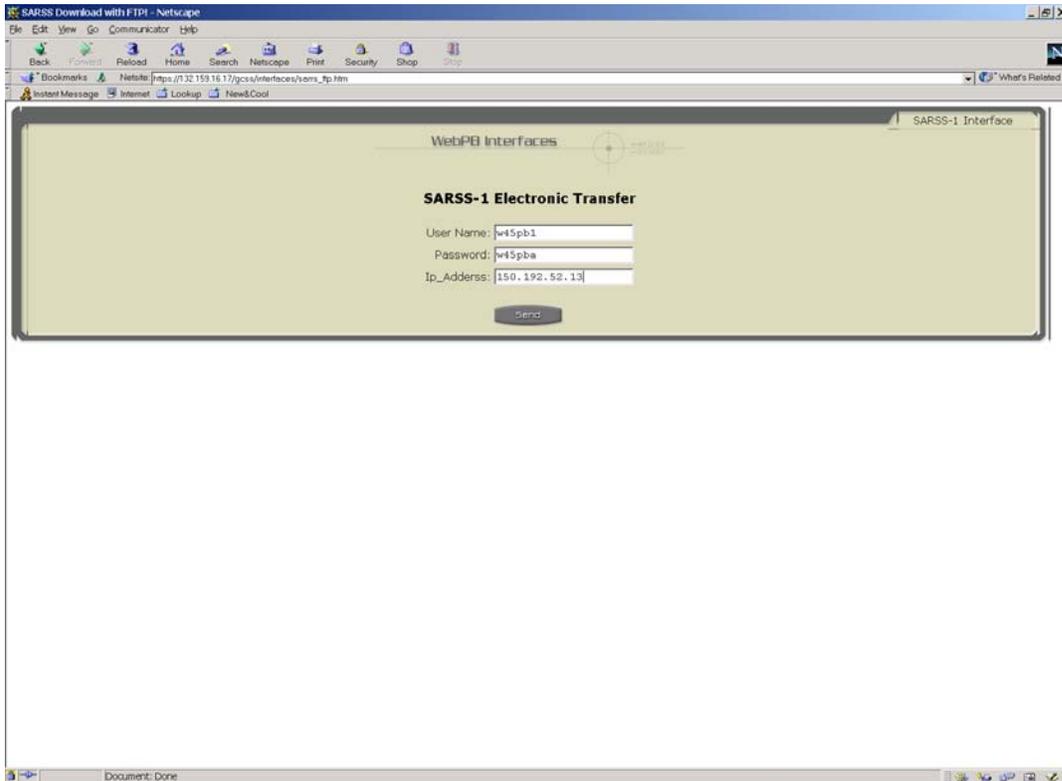


Figure F.5-6. SARSS-1 User name, password and IP Address input.

- g. Enter the account information provided by the SARSS-1 Operator, along with the IP address for the SARSS-1.
h. Click <**Send**>.

F.5.6 SARSS-1 operator instructions

The operator instructions for setting-up an PBUSE Standalone computer customer are no different than for setting up any regular SARSS-1 FTP customer. PBUSE conforms to legacy SARSS-1 FTP transmission standards. These instructions are provided in Section F.7 for operator review.

F.6 Managing User Accounts

F.6.1 Default Security Settings

Three primary groups are used to define the permissions given to user accounts on the PBUSE Standalone computer. These three groups are the Administrators, Power Users and Users groups. A short discussion of the intended use of each group will be followed by a recommended method for managing these users and groups.

F.6.2 Administrators Group

Members of the Administrators group can perform all functions supported by the operating system. The default security settings do not restrict administrative access to any registry or file system object. Administrators can grant themselves any rights that they do not have by default.

Microsoft recommends that administrative access only be used to:

- Install the operating system and components (such as hardware drivers, system services, and so on).
- Install Service Packs and Windows Packs.
- Upgrade the operating system.
- Repair the operating system.
- Configure critical operating system parameters (such as password policy, access control, audit policy, kernel mode driver configuration, and so on).
- Take ownership of files that have become inaccessible.
- Manage the security and auditing logs.
- Back up and restore the system.

F.6.3 Users Group

The Users group provides the most secure environment in which to run programs. The default security settings are designed to prevent members of this group from compromising the integrity of the operating system and installed programs. Users cannot modify system-wide registry settings, operating system files, or program files. Users cannot install programs that can be run by other Users. They also cannot access other Users' private data or desktop settings.

F.6.4 Power Users Group

Members of the Power Users group have more permissions than members of the Users group and fewer than members of the Administrators group. Power Users can perform any operating system task except tasks reserved for the Administrators group. Power Users do not have permission to add themselves to the Administrators group. Power Users do not have access to the data of other users on an NTFS volume, unless those users grant them permission.

Power Users can:

- Install programs that do not modify operating system files or install system services.
- Customize system-wide resources including Printers, Date/Time, Power Options, and other Control Panel resources.
- Create and manage local user accounts and groups.
- Stop and start system services that are not started by default.

Warning: Since Power Users can install or modify programs, running as a Power User when connected to the Internet could make the system vulnerable to Trojan horse programs and other security risks.

F.6.5 Viewing User Account Properties in Windows 2000

- a. Right-Click on the <My Computer> icon on the desktop to bring up an options menu.
- b. Select <Manage>.
- c. {Computer Management} window opens (Fig. F.6-1).

NOTE: Within all Microsoft Windows operating systems, important system-level processes often have many access methods. The method used above, for example is an alternate way to access the Computer Management console. Alternately, users can follow the menu path:

- a. <Start> → <Settings> → <Control Panel>
- b. Inside the Control Panel, click on the <Administrative Tools> icon.
- c. Inside the Administrative Tools folder, click on the <Computer Management> icon.
- d. {Computer Management} window opens (Fig. F.6-1).

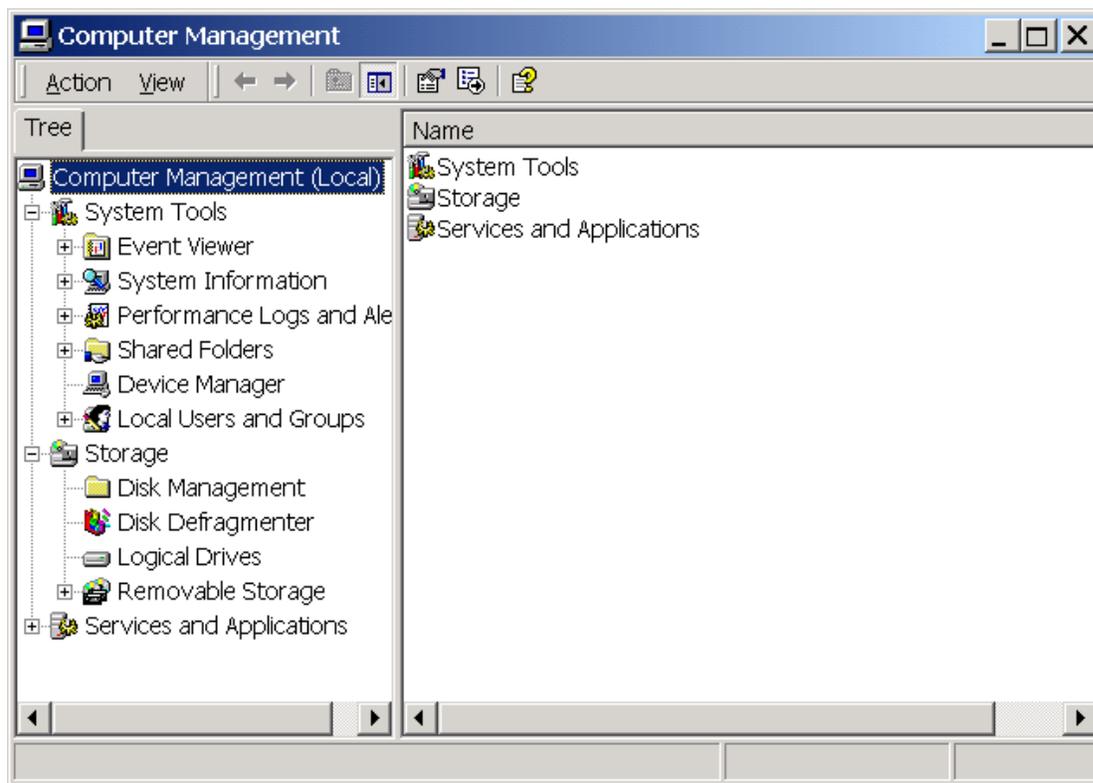


Figure F.6-1. The Computer Management console.

- d. Click the plus sign beside <Local Users and Groups> to show the **Users** and **Groups** folders.
- e. Click on the Users folder.
- f. The {Computer Management} window will now show all of the User accounts that are currently configured to login to this machine (Fig. F.6-2).
- g. To find out more information about a particular user, double click on the <user account> in the right-hand pane of the Computer Management console.
- h. This will open a {User Properties} window such as the sample window displayed in Figure F.6-3 for the example account, PBUSE_user.

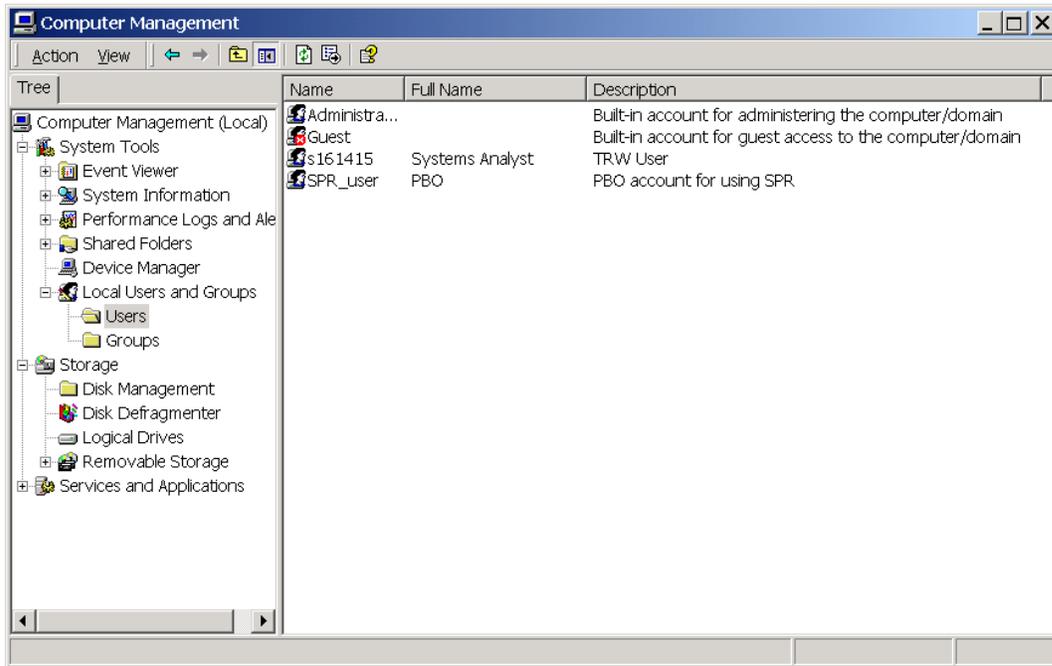


Figure F.6-2. Local Users configured on a sample computer.

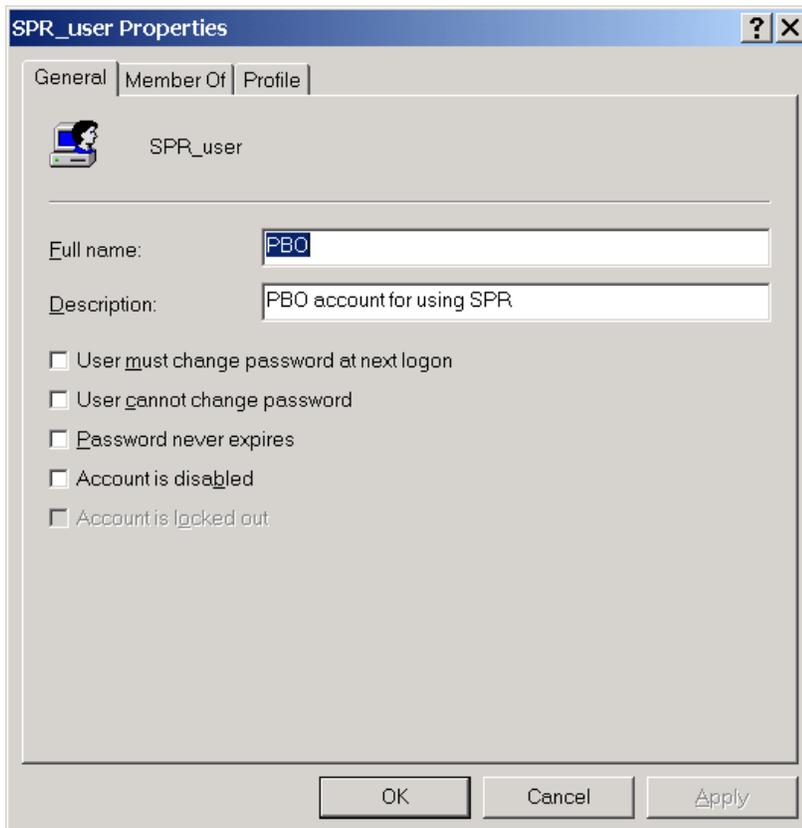


Figure F.6-3. Sample User properties.

- I To view the group memberships of a user, select the **<Member Of>** tab of the {User Properties} window (Fig F.6-4).

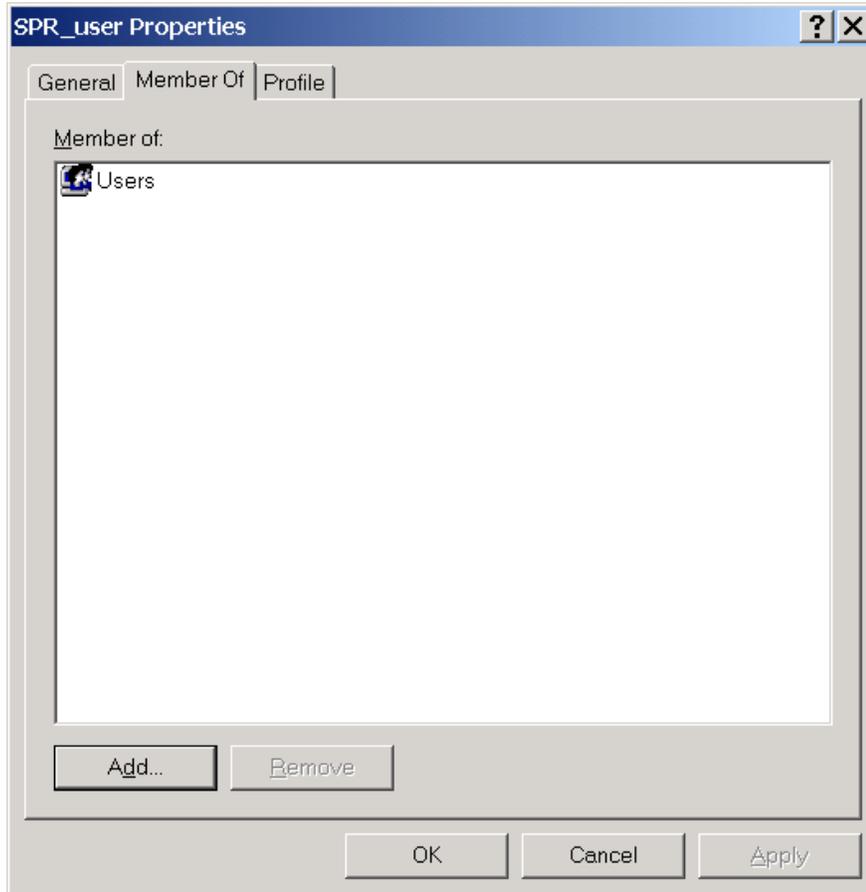


Figure F.6-4. Group membership window for a sample User.

NOTE: In order to login to the PBUSE laptop in Standalone mode and perform Standalone operations, a user's login account, must be a member of the Power User's group. The Power User's group will provide all of the necessary permissions to allow a user to use the Session Manager, Replicate data from the AKO server to the PBUSE Standalone laptop and operate the PBUSE Standalone module.

F.6.6 Adding a new User Account in Windows 2000

- a. Complete Steps **A.5 a - f** above.
- b. From the **<Action>** menu of the {Computer Management} console, select **<New User...>**
- c. {New User} window opens (Fig. F.6-5).
- d. Fill in the provided fields.

NOTE: A User name cannot be identical to any other user or group name on the computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:
"/\ [] : ; | = , + * ? < >

NOTE: A user name cannot consist solely of periods (.) or spaces.

NOTE: The **Password** and **Confirm password** fields must contain the same information. Because of security considerations, Passwords must contain at least one character from three of these four types of characters

- Alphabetic (a,B) characters, uppercase and lowercase, compose two types (passwords are case sensitive).
- Numbers (0,1,2,3...)
- Special characters such as punctuation ` ~ @ # \$ % ^ & * () _ + - = | \ [] : " ; ' < > ? , . /

NOTE: If the default check mark is left besides **User must change password at next logon**. Then at the new User's first attempted logon, a change password notification will be displayed, forcing the User to change his or her password.

- d. Click **<Create>** to add a new User.
- e. To add another user, repeat **b - d** above.
- f. Click **<Close>** to finish adding new Users.

The screenshot shows a 'New User' dialog box with the following elements:

- Title bar: 'New User' with a help icon (?) and a close icon (X).
- Fields: 'User name:', 'Full name:', 'Description:', 'Password:', and 'Confirm password:'.
- Checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires', and 'Account is disabled'.
- Buttons: 'Create' and 'Close'.

Figure F.6-5. New User creation window.

F.6.7 Adding a User Account to a Group in Windows 2000

- a. From the User Properties window shown in Figure F.6-4, Click the <Add> button.
- b. {Select Groups} window opens (Fig. F.6-6).

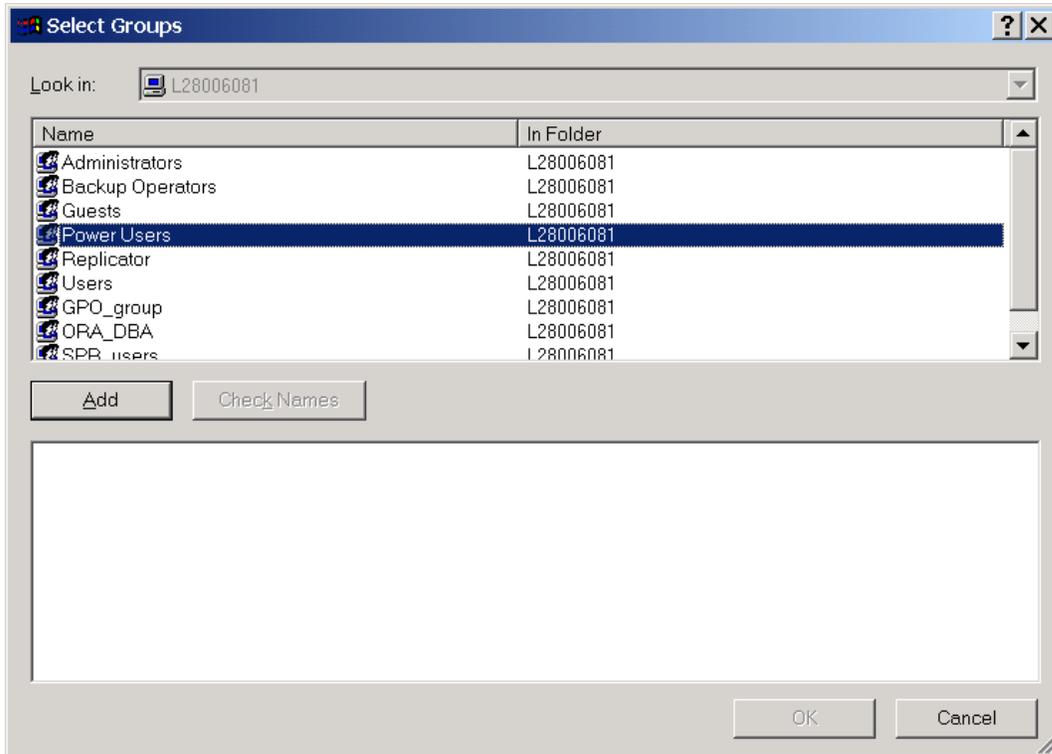


Figure F.6-6. Select Groups window showing Power Users selected.

- c. Highlight the Power User's group by clicking on it.
- d. Click on the <Power Users> group
- e. Select the <Power Users> group by double-clicking on the desired line, or single-clicking on the line and then clicking the <Add> button.

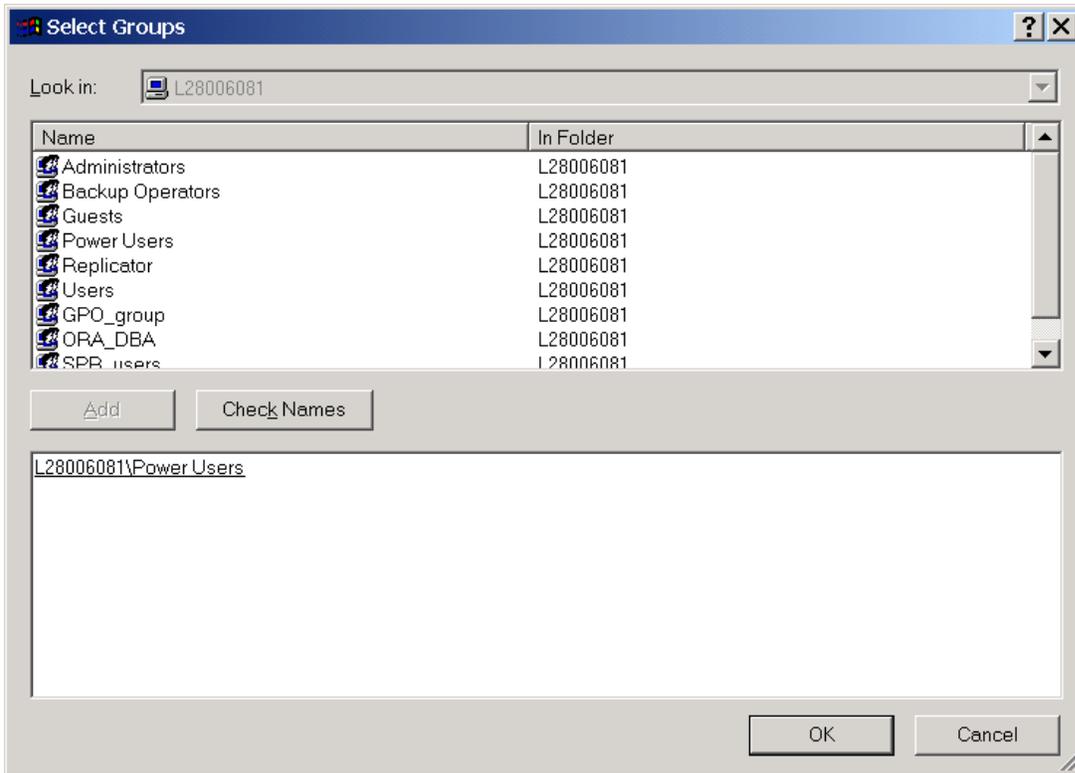


Figure F.6-7. Select Groups window showing Power Users group added.

- f. Click **<OK>** to close the {Select Groups} window.
- g. {User Properties} window becomes active.
- h. Click **<OK>** to finish the group selection process.
- i. Click the **<X>** in the top right corner of the {Computer Management} window to finish altering the User account.

F.6.8 Removing a User Account from a Group in Windows 2000

- a. Repeat Step **A.5** above.
- b. Select the Group access to be removed from a User's account. (Fig. F.6-8).
- c. Click **<Remove>** to remove the User account from the Group.
- d. Click **<OK>** or **<Apply>** followed by **<Close>** to confirm the process.

NOTE: A User must belong to at least one Group. If a User is removed from all Groups, the User will have no access to the system and will not be able to login.

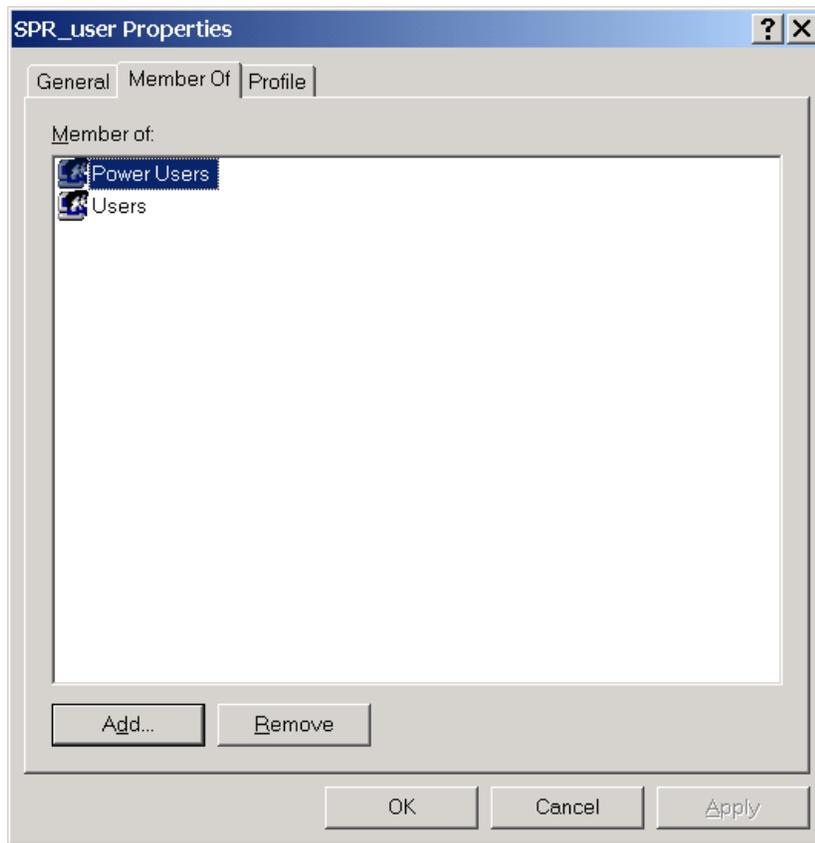


Figure F.6-8. Group selected for removal.

- e. Click the **<X>** in the top right corner of the {Computer Management} window to finish altering the User account

F.7 SARSS-1 Parameter Setup for FTP with PBUSE

1. Logon to SARSS-1 and at the ACTION line Type: **ACCESS**. The ACCESS command is used to maintain the TCP Wrapper /etc/hosts.allow file. This will allow PBUSE to connect with SARSS-1.

DATE:03/2/01	SARSS HOSTS/DENY EDITS	TIME:15:24:18					
IP ADDRESS: 140.183.234.79 (sample user input)							
TYPE OF ENTRY: 2-FTP ONLY (1—FTP AND TCP, 2-FTP ONLY, 3-TCP ONLY)							
NOTE: You may NOT Delete any SARSS-1 Workstation or Server IP'S from the hosts.allow file; you may only modify their IP addresses.							
F1 FIRST ENTRY	F2 LAST ENTRY	F3 QUIT	F4 NEXT ENTRY	F5 PREV ENTRY	F6 ADD IP	F7 DELTE IP	F8 CHANGE IP

Figure F.7-1. SARSS-1 ACCESS command window.

- a. In the space next to IP ADDRESS, enter the IP address for the PBUSE Server or Standalone computer (for example, 140.183.234.79).
- b. Tab the next line TYPE OF ENTRY: Insert the number '2' to indicate FTP Only.
- c. Depress (F6) ADD IP.
- d. Verify that the information has been added correctly by stepping through the list of IP addresses. Depress (F1) to select the first IP Address in the list, then Depress (F4) to cycle through the list until the IP Address that was just added appears. Ensure the TYPE OF ENTRY reads: 2.
- e. (F3) QUIT

2. At the ACTION Line Type: **FTPPASS**. The FTTPASS command allows you to add, change, or delete user login, password, and IP address information for each activity that will need access to your SARSS-1 system for file transfer. The process displays the below screen.

DATE: MM/DD/YY HH:MM:SS	FTP LOGIN/PASSWORD MAINT	TIME:
ENTER DESTINATION RIC/DODAAC		
ENTER DESTINATION IP ADDRESS		
PRESS <Esc> TO CONTINUE		
Screen 1758		
<F1> Clear Screen	<F2> Add Login	<F3> Quit Menu
<F4> Delete Login	<F5> Change Login	<Home> Help/ Info

Figure F.7-2. SARSS-1 FTTPASS command window.

- a. (F2) ADD LOGIN
 - b. Enter the DODAAC of the Property Book that is a customer of your SARSS-1 at the ENTER DESTINATION RIC/DODAAC.
 - c. Next enter the IP of PBUSE Server or Standalone computer (for example, 140.183.234.79) at the ENTER DESTINATION IP ADDRESS then press <Esc>.
 - d. Next enter a PASSWORD and reconfirm the password.
 - e. (F3) QUIT MENU
3. Make sure that the Property Book DODAAC is set as Communication Type of FTP at the Update Routing Table Screen. You can access this screen by typing at the ACTION line: **UPDRT**. The below screen will be displayed.
 - a. Type the Property Book DODAAC in at DESTINATION then press (F8) FIND DESTINATION.
 - b. If COMMUNICATION TYPE: is not FTP (F) then enter F and press (F5) CHANGE ENTRY.
 - c. Double-check to ensure the change did take effect.
 - d. Press (F3) QUIT MENU.

AIS Manual GCSS-A/T PBUSE EM
1 January 2003

DATE: MM/DD/YY HH:MM:S	SARSS1 UPDATE ROUTING TABLE	TIME:
SOURCEAIR DESTINATIONS2B FILEIDAJTS9A		
COMMUNICATION TYPE: DISKETTE (D) /POINT TO POINT (P) /CAISI-VEE (V) /FTP (F)		
FOR POINT TO POINT (PTP) ENTER:		
TELEPHONE NUMBER OR M FOR MANUAL PTP:		
MAX ATTEMPTS: START TIME:		
IF CAISI-VEE WAS SELECTED ENTER:		
DESTINATION ADDRESS OR (M) FOR MANUAL:		
<F1> Clear Screen	_____	<F3> Quit/ Menu
<F4> Delete Entry	Screen 1707 <F5> Change Entry	<F6> Next Entry
_____	<F8> Find Destination	_____
		<Home> Help/ Info

Figure F.7-3. SARSS-1 UPDRT command window.

F.8 Backup the PBUSE Database onto a CD

1. Double click the **PBUSE Standalone Session Manager** desktop icon. Then, select the **Backup/Recovery** tab from the PBUSE Standalone Session Manager window. The window will be displayed. (See Figure F.8.1)



Figure F.8.1 PBUSE Standalone Session Manger (Backup/Recovery Rep-4)

NOTE: If the CD has not been formatted, select **FORMAT DIRECTCD**, and then follow the steps below. Otherwise, skip to step 7.

2. After you select **FORMAT DIRECTCD** on the Backup/Recovery tab, the Welcome window will be displayed. (See Figure F.8.2)



Figure F.8.2 Welcome Window

3. Select **Next** to go to the Drive Information window. (See Figure F.8.3)



Figure F.8.3 Drive Information Window

4. Select **Next** to continue. The **Welcome** window will be displayed. (See Figure F.8.4)



Figure F.8.4 Welcome Window

5. Select **Next** to configure the CD. The 'Name Your Disc' window is displayed. (See Figure F.8.5)



Figure F.8.5 Name Your Disk Window

6. Enter the name for the CD and then select Finish to continue. A confirmation message will be displayed. (See Figure F.8.6)



Figure F.8.6 Information Window

7. Select **Ok** to start formatting the CD.
8. From the Backup/Recovery tab, select **BACKUP PBUSE DATABASE**. (Make sure the formatted DIRECTCD is in the CD–RW drive). A confirmation message will be displayed. (See Figure F.8.7)



Figure F.8.7 Confirmation Window

NOTE: If a non–formatted disc is inserted in the CD–RW drive, an error message will be displayed. (See Figure F.8.8)

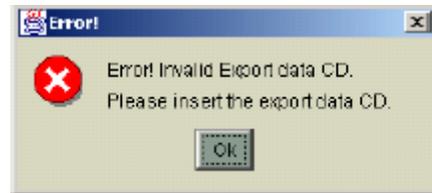


Figure F.8.8 Error Window

9. Select **Ok** to start the backup PBUSE database process. Once the backup is finished, an information message will be displayed. (See Figure F.8.9)



Figure F.8.9 MSG Window

10. Select **Ok** to complete the backup PBUSE database process.
11. Select **Close** to exit.

F.9 Restore the PBUSE Database from the CD

1. Double click the **PBUSE Standalone Session Manager** desktop icon. Select the **Backup/Recovery** tab from PBUSE STAND ALONE SESSION MANAGER window. (See Figure F.9.1)



Figure F.9.1 PBUSE Standalone Window

2. Select **RESTORE PBUSE DATABASE**. Make sure the Backup PBUSE Database DIRECTCD is in the CD-RW drive. The Backup PBUSE DB List window will be displayed. (See Figure F.9.2)

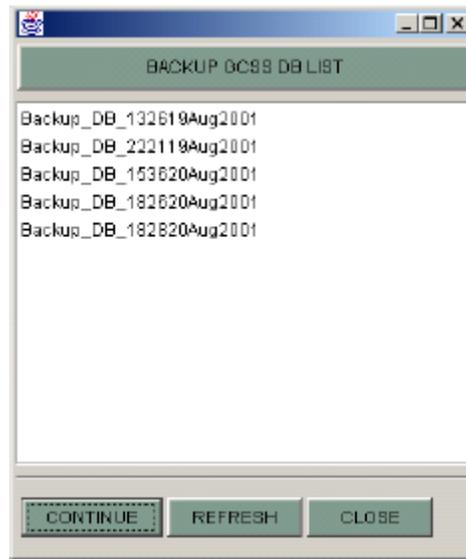


Figure F.9.2 Backup PBUSE DB List Window

NOTE: If an invalid CD is inserted an error message will be displayed. (See Figure F.9.3)



Figure F.9.3 Error Window

3. Select any of the database backups from the list. Select **Continue**. A confirmation message will be displayed. (See Figure F.9.4)

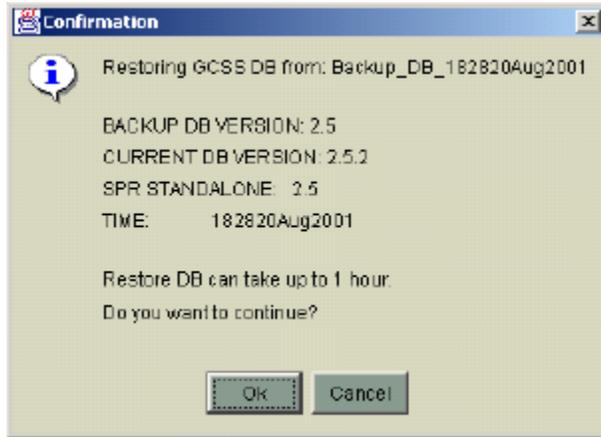


Figure F.9.4 Confirmation Window

4. Select **Ok**. If the Backup DB Version and the Current DB Version are different, a confirmation message will be displayed. (See Figure F.9.5)

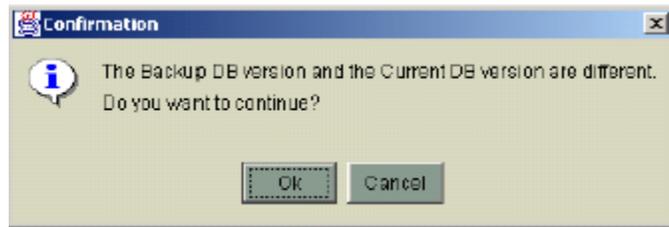


Figure F.9.5 Confirmation Window

5. Select **Ok** to start restoring the DB. Wait until the restore of the PBUSE database is complete. An information message will be displayed. (See Figure F.9.6)

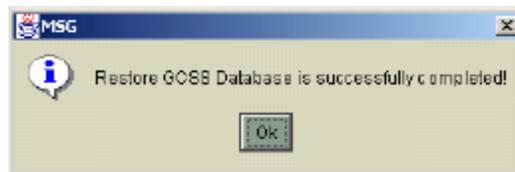


Figure F.9.6 MSG Window

6. Then, select **Ok** to finish the restore of the PBUSE database.
7. Click **Close** to exit.