U.S. Department of the Treasury

Financial Management Service (FMS)

OTC Channel

Paper Check Conversion Over the Counter (PCC OTC)

User Manual

Chapter 3
System Administration Tool- SAT

January,2009
Document Version 1.0

Change/Revision History

Date	Section/Chapter	Revision/Change Description	Page/Section Affected
01/2009		Original Citibank Release	

Table of Contents

POS SAT – System Administration Tool

What is the SAT?

The System Administration Tool or SAT is used by POC's (Point of Contact) to setup configurations for the POS. The PCC OTC POC (Point of Contact) can also use this tool to set up/change/delete users and their permissions, set certain defaults within the POS and other administrative duties. Once setup is complete, this module is typically not used on a daily basis.

The SAT application consists of the following components: (Figure 3.1)

- Configuration
- Users
- Activity Log
- Batch Recovery
- Reset LVD (Optional – may be made inactive if not used)

A complete description of each of these components can be found later in this chapter.

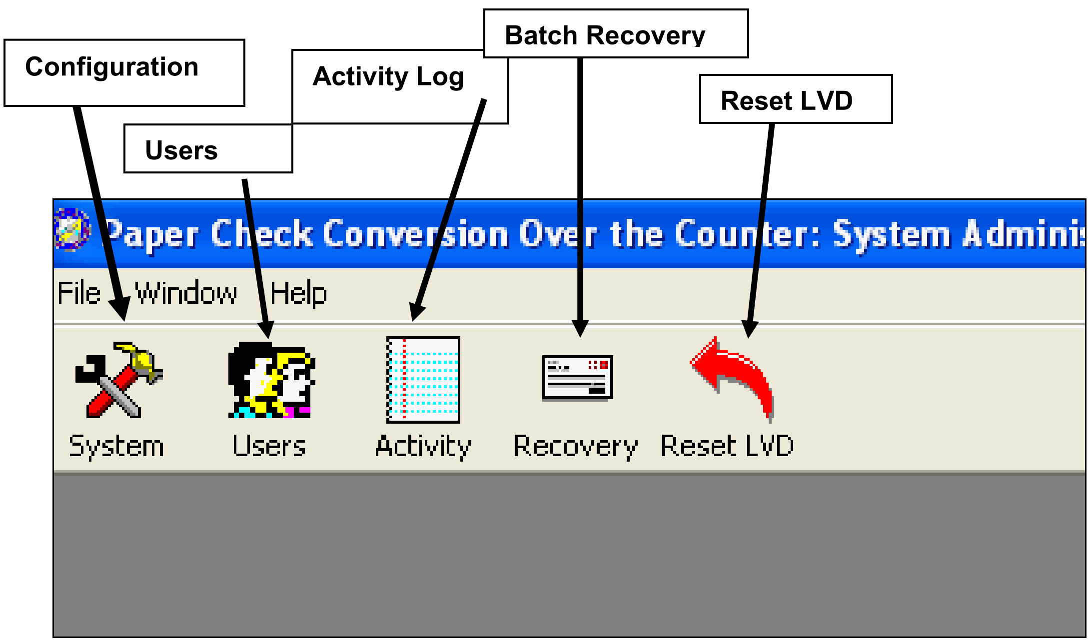


Figure 3.1

Note: The SAT steps described in this chapter need to be performed on each computer that is setup for PCC OTC processing. Since the application is not networked, all users need to remember passwords for each computer.

SAT Access

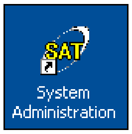
Only an authorized System Administrator, IT Support, designated Point(s) of Contact (POC), or someone with the 'administrator' role should be accessing the POS SAT application. For the initial installation, the Treasury OTC - Deployment Specialist (i.e. Treasury/FMS, or designated agency personnel) launches the POS SAT icon to complete security and application configuration setup, or assists with this step. If the Deployment Specialist is not present at the location site, call Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com. Authorized users are issued Login names and temporary passwords. Upon initial login, the password must be changed to a unique password and known only to that user.

The Built-In SAT Administrative Login name

The SAT comes with a built-in administrative login. This login name is given to people who are authorized to access the SAT by the Treasury OTC Support Center. The password for the administrative login needs to be changed upon initial login. This login and password should only be known to those who share administrative rights for the PCC OTC software. It does not replace a person's own login and password and cannot be deleted from the system. The only way to recover the administration login is to uninstall and to reinstall the software. This is a security safeguard. For more information, please refer to *Appendix M* of this User Manual.

Note: Once the administrative password has been changed, it should be written down and locked up for future use. The administrative password will expire every 90 calendar days and a new password will need to be chosen. If, at any time, the POS SAT system cannot be accessed via the administrative logon because the password is not known, the only way to recover the administrative password is to uninstall and reinstall the POS software. Keeping track (and tight security) of the administrative password is crucial.

Accessing the Application

The SAT icon 

representing the SAT application is placed on the desktop after the installation of the software. A login window controls access to the application. Only authorized users are allowed access.

To open the application:

1. Double click the SAT icon on the desktop. The login window opens. (Figure 3.3)

Figure 3.3

2. Type your Login name in the Login field.
3. In the Password box, type your password.
4. Click OK.
5. The login window closes and access is provided to the application.

First Time Users

If this is the first time the user is signing on to any of the PCC OTC modules, POS, SAT or BM, the user is required to change their password. The Agency's POC assigns each user a login name and initial, temporary password. After typing the login name in the login field, and the temporary password in the password field, the system prompts the user to change their password (see *Changing a Password* section below). For complete specifics regarding password requirements, please see *Appendix R – Password Requirements* in the Appendix chapter of this User Manual, or contact the Treasury OTC Support Center.

Changing a Password/Password Expiration

Users are required to change their password upon initial login. Passwords expire thereafter every 90 days. Passwords should also be changed if the user feels that their password has been compromised.

Note: When the password is changed in one of the modules (SAT, Batch Manager, or POS), it is also automatically changed across all modules.

To change a password:

1. In the Login window, enter your login name and password and click the **'Change Password'** button.
2. The Change Password window opens. (Figure 3.4)
3. In the 'Old Password' field, type your current password.
4. In the 'New Password' field, type your new password
5. In the 'Confirm' field, type the new password again.
6. Click **'OK'**.
7. The Change Password dialog window closes and access is provided to the application.

Figure 3.4

Logging out of the SAT Application

To log out of the application, select **'File'** from the menu at the top of the main SAT screen, then choose **'Logout'**. The Login window appears for another user to login.

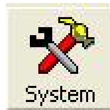
Exiting the SAT Application

To exit the application:

Click the **'X'** at the upper right of the screen or select **'File'** from the menu at the top of the screen. Select **'Exit'** from the dropdown menu. The application closes and the computer returns to the desktop.

System Configuration

The system configuration module is used to configure the POS system to operate in an environment that fits each location's needs. Only authorized users can configure the system. The System Configuration contains three tabs: General, Data Entry Screens, and Tasks.

Select the System Configuration icon 

from the main SAT screen, or click **'File'**, **'Configuration…'** from the menu at the top of the screen. The following window appears: (Figure 3.5)

<u>Warning: The PCC OTC security settings displayed in Figure 3.5 (right side - Login, Batch, and Activity Log) are defaulted to the most restrictive mode and should not be changed.</u>

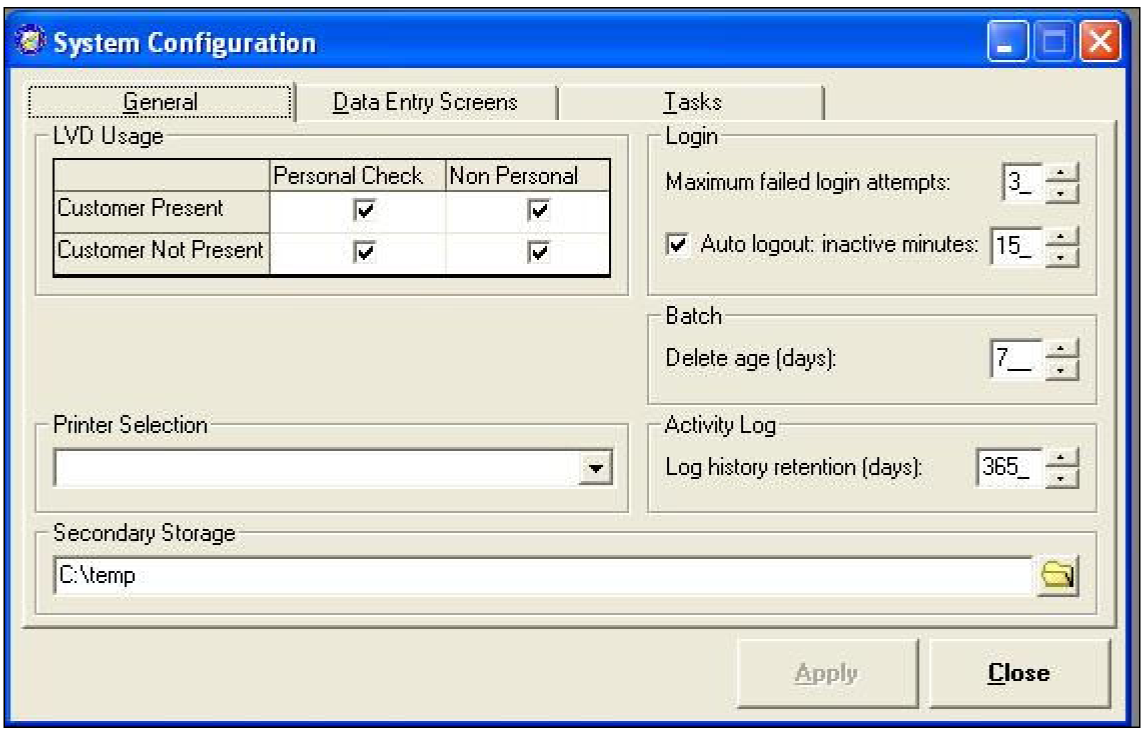


Figure 3.5

There are three tabs on this screen and they are described below.

Note: All configurations settings described below are per computer. Each PCC OTC computer must have configuration settings individually applied.

General Tab

LVD Usage - set the options for using the LVD, or turn off the LVD function.
Select the appropriate choice for which the system should perform check validation. Choices in this section can be set for Personal and/or Non Personal checks and for Customer Present and/or Customer Not Present. The LVD (Local Verification Database) is an optional feature. If none of the options are checked, the LVD becomes disabled provided it is also unchecked in the 'Task Selection' field of the 'Tasks' tab (see the 'Task' tab section for additional information).

Printer Selection – select SAT default printer
Use this section to specify the default printer for the SAT. The SAT printer can be setup to be a different printer from the one used for the POS if so required. If the printer selection is left blank, the system uses the Windows default printer. A font can also be specified by clicking on the 'Print' button and choosing an alternate font. The font name and font sample is displayed to the right of the font button.
Note: This printer defaults to the Windows default printer and cannot be customized at this time.

Secondary Storage – Select the drive to be used for backup
The secondary storage is used to save a temporary backup copy of batches gathered by the application. It is recommended that the secondary storage be on a removable or different network drive from the working POS storage. The backup data remains on the secondary storage drive until it is deleted from the primary location which is set in the 'Batch Delete Age' SAT configuration setting. The 'Secondary storage' field was configured during installation. If a LAN drive is used for secondary storage, and multiple computers use the POS software to scan items, it is recommended that a separate folder is created on the LAN drive for each PC. This keeps the activity separate. The drive displayed should be the same drive that was selected during installation. If it is not correct, this field can be used to navigate to the correct drive specification to change the drive reflected in the secondary storage field. Refer to the 'New Installation' section in the *Installation and Configuration* chapter of this User Manual, if needed. If the Secondary Image Storage fails while in the POS application, refer to the *Troubleshooting* chapter of this User Manual. To change the secondary storage, click the folder icon to the right of the field and choose the correct drive from the 'browse for folder' window. For more information on the types of secondary storage options available, see the *Mirror Image – Backup Device Installation* section of the 'Installation and Configuration' chapter of this User Manual.
Note: If the secondary storage path is changed in the middle of processing batches, the system is not able to find those batches and serious problems can occur.
Also, If the secondary storage location exists outside of the RDM directory (as is the recommendation), it is not removed during an uninstall.

Login – various login settings – This section contains configurable settings that apply to logins for users. <u>The settings in this section are set to the most restrictive mode and should not be changed.</u>

The **'Maximum Failed Login Attempts'** field is used to specify how many bad login attempts a user can have before they become suspended in the system. Once a user has become suspended, he/she must seek the help of an authorized person to have their password reset. <u>The default number of failed login attempts is 3 and should not be changed (see warning box above Figure 3.5).</u>

Note: Upon installation, the agency POC (Point of Contact) should confirm that all settings are in compliance with the agency's guidelines.

The **'Auto Logout: inactive minutes'** setting is used to set the number of minutes of inactivity before the system logs off the user. <u>The default is 15 minutes and should not be changed. (see warning box above Figure 3.5).</u>

Batch – set the default days for batch retention
This section allows an authorized user to set the number of days before acknowledged or deactivated batches are deleted from the system. This setting removes batches from the primary and secondary locations.<u> The default setting is 7 calendar days and should not be changed. (see warning box above Figure 3.5). Only 7 days of batches should be retained to reduce the amount of personal information stored on the hard drive of the POS computer and its secondary storage device. Higher amounts of stored P I I data equates to higher risk of accidental disclosure in the event of unauthorized access to the system, or malicious code.)</u>

Activity Log – set the length of time the log is retained.
The Log History Retention setting defines the length of time the system activity log is retained in days. <u>The default is set to 365 days and should not be changed (see warning box above Figure 3.5, and the System Activity Log section of this chapter).</u>

If changes have been made to any fields on the General tab, click the '**Apply**' button. The system states that the POS application has to restart to use these changes.

Note: the POS should always be closed prior to making changes in the SAT.

Data Entry Screens Tab

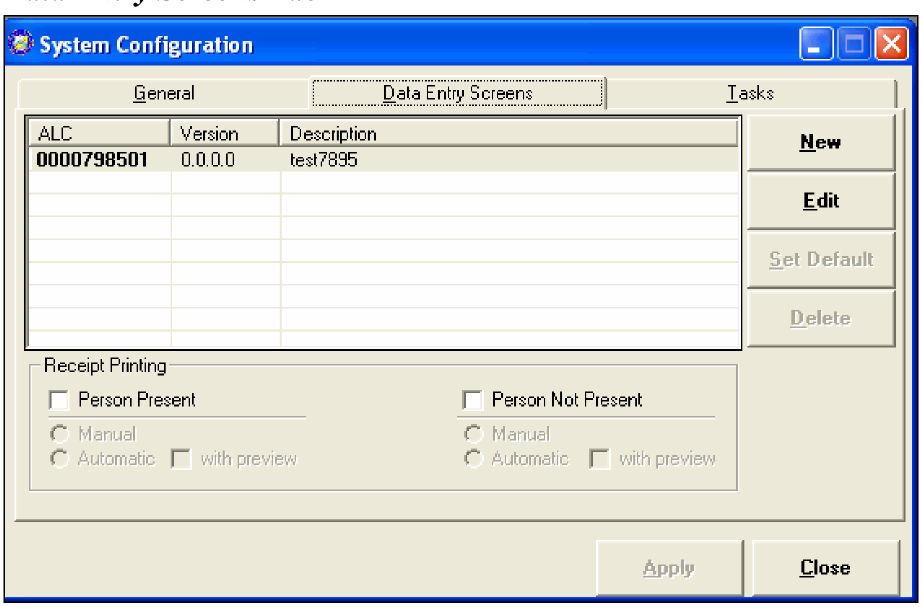


Figure 3.6

The purpose of the Data Entry Screens tab is to configure and manage the POS with the number of ALC+2's that are used by the POS computer. This screen is also used to configure receipt printing. (See Figure 3.6) This feature would be used by Agencies who provide services on behalf of other ALC's.

New – Add new ALC+2's

Clicking the **'New'** button opens a window that allows a new ALC+2 to be added. The ALC+2 and description need to be typed. The description field is an internal field intended only as a means of identifying the ALC+2. It is mandatory only when adding the first ALC +2. Additional ALC+2's do not require a description but it is recommended. Adding the description makes it easier for the operator to identity the ALC+2 during data entry. The version column lists the version number of the most recent data entry screen upgrades downloaded from ELVIS (see tasks tab, task selection section for information on downloading data entry screen upgrades). ***Note: The first ALC+2 that was added becomes the default and is indicated as such with an asterisk and bolded type face on the 'Data Entry Screens' tab. The default ALC+2 determines which ALC+2 is the owner of the POS terminal and can be changed (see Set Default ALC+2 below).***

Note: An Agency Participation Agreement (APA) and an Agency Site Profile (ASP) must be submitted to participate in the PCC OTC program. Do not add an ALC+2 until approval has been granted for that ALC+2 from the Treasury OTC Support Center. Please advise the Treasury OTC Support Center if multiple locations are consolidated into a single location.

Edit – edit the ALC+2's description

The data entry screens listing may be edited by clicking the **'Edit'** button. This allows the user to change the description of a location.

Set Default ALC+2

The 'Set Default' button allows an authorized user to choose which ALC+2 should be setup as the owner of the POS terminal. When the POS is accessed for the first time, the default ALC+2 is defaulted to the data entry screen. Once another ALC+2 is chosen for a transaction, that ALC+2 remains active as the processing ALC+2 until the operator chooses another ALC+2. Users choose the ALC+2 on the data entry screen from a multiple choice field, based on the transaction. When viewing the listing of ALC's on the 'Data Entry Screens' tab, the default ALC+2 is indicated with an asterisk and bolded type face.

Delete – allows the deletion of the ALC+2

The 'Delete' button allows an authorized user to delete the ALC+2 by clicking on the ALC+2 to be deleted, then clicking the **'Delete'** button. It is recommended that ALC+2's be deleted only after all activity for that ALC+2 have been sent.

Note: The default ALC+2 cannot be deleted. If it is necessary to delete an ALC+2 that has been designated as the default ALC+2, change the default to another ALC+2 then delete the former default ALC+2.

Receipt Printing – setup whether or not to use receipt printing function

The bottom portion of this screen is used to setup receipt printing. Receipts can be created and printed to be handed to a person who is cashing a check or making a payment in person, or to be mailed for payments received via mail (person not present). These receipts are generated during the actual

transaction, but default settings for those receipts are setup here. Leaving both the ‘Person Present’ and ‘Person (Customer) Not Present’ fields unchecked results in the disabling of this option. If receipts are desired, click to check the appropriate box(es). The choices of ‘Manual’, ‘Automatic’ or ‘With preview’ can then be chosen. Choosing ‘Manual’ requires that the operator take additional steps to print the receipt. Choosing ‘Automatic’ results in a receipt printout each time a transaction has been entered, and choosing the ‘With Preview’ option allows the operator to see the receipt on the screen prior to the generation of the printout. When the ‘Person Present’ and/or ‘Person Not Present’ fields are clicked, the default setting is manual.
Note: Receipts are printed on a full sheet of paper.

When all changes have been made to the Data Entry Screens window, click the **‘Apply’** button. The system responds with the message that the POS application must be restarted to use these changes.

Tasks Tab

The fields should be set exactly as displayed below (Figure 3.7) (URL and values are case-sensitive) and should only be changed with the direction and guidance of the Treasury OTC Support Center. The exception to this is the Task selection choices at the bottom of the window which can be customized. **Upon deployment or re-installation, these settings are confirmed. A change to any of these settings prevents a successful transmission of batches.**

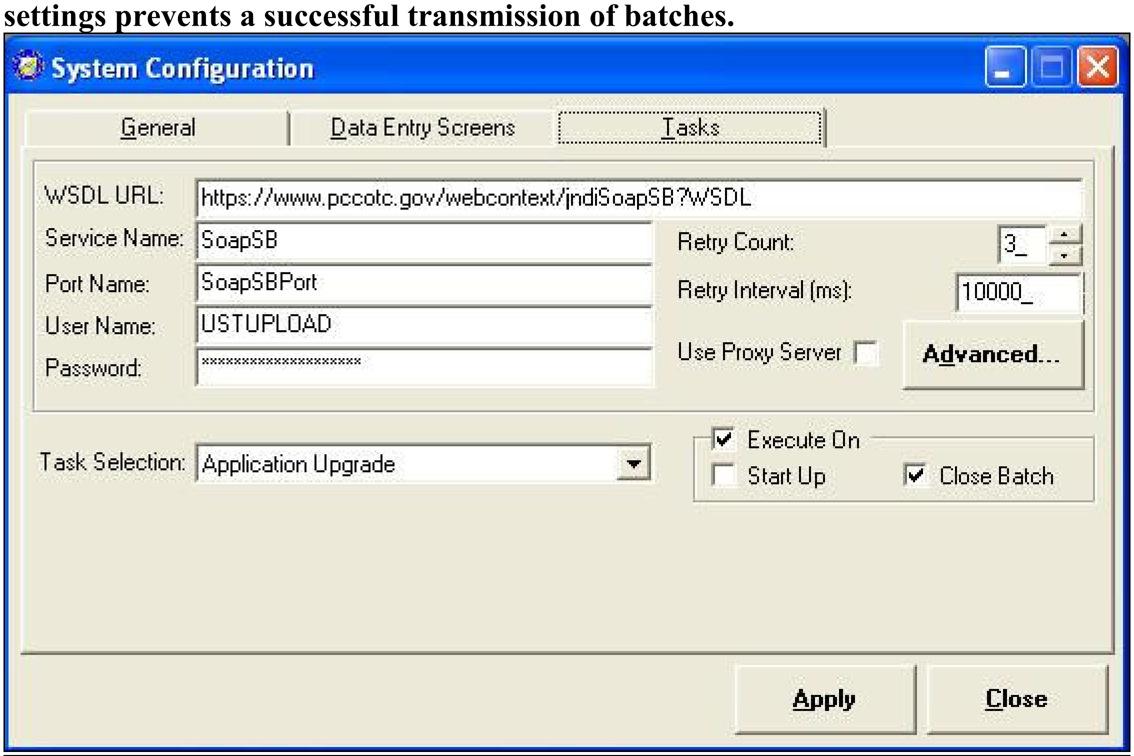


Figure 3.7

Note: The ‘Password’ field on this screen should not be changed unless under the direction and guidance of the Treasury OTC Support Center. If the Deployment Specialist is not present, call Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com.

Retry Count and Retry Interval
These fields are defaulted to work with our ELVIS system as pictured in Figure 3.7. The defaults are set to the 'Retry Count' of 3 and the 'Retry Interval' of 10000 when the POS software is installed. Do not change these settings unless instructed to by the Treasury OTC Support Center.

Use Proxy Server
This field is available for agencies to insert their internal proxy settings if proxy servers are used to grant access to the internet. To use the Proxy Server options, click to check the **'Use Proxy Server'** box then click the **'Advanced'** button to the right of the box. The following fields are available for setup: (Figure 3.7.1)

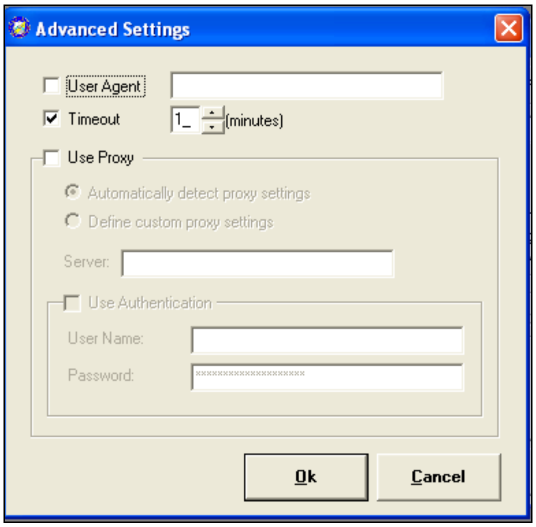


Figure 3.7.1

User Agent – Click the checkbox to activate the field. Type the name of the User Agent if a user agent is required.
Timeout – Click the checkbox to activate the field. Type the number of minutes the application waits for a response from the host before it times out (for all communications). The default setting is 1 minute with a maximum setting of 30 minutes.

Note: Work with your I T staff if more information is needed regarding proxy servers.

Use Proxy – Click the checkbox to activate the fields beneath. Choose one of the two options:

- Automatically detect proxy settings. Click the check box to have the system automatically detect proxy settings.

- Define custom proxy settings. Click the check box to define the proxy setting manually and type the name of the proxy server

- Use Authentication. Click the check box if the application needs a user name and password to connect to the proxy server. When this choice is used, a user name and password is required to access the internet.

Note: The POS software is proxy aware. If your agency is proxy aware, you need to enable the use of the Proxy Server by placing a check in the box for 'Use Proxy Server'. The associated proxy server's IP address and/or port numbers need to be specified in the 'Server' field. Any required user authentication parameters needed for internet access need to be set in the 'Use Authentication' field. Your central network infrastructure staff can assist you by providing the required values needed for this screen. Use of this screen depends upon your firewall rules. Contact your Firewall Administrator for further information.

Task Selection – Automate tasks

The bottom portion of the screen includes Task Selection. This field is used to automate certain tasks that are performed by the POS computer. Using the dropdown arrow to the right of the field, the choices are:

Application upgrade – POS allows for automatic downloads of application upgrades to the POS computer including firmware. Once the upgrade is transmitted to the POS, an authorized user needs to execute the upgrade. The download can be setup to require that upgrades to the POS application be performed at either 'Start up' or 'Close Batch' by clicking to check the appropriate box. The default is set so upgrades download on 'Close Batch'. It is vitally important to ensure that at least one box is checked.

Note: Firewalls can block the download of updates or files sent with an .exe extension. Your firewall may need to allow anything from our IP in order to receive the upgrade. If application downloads are not practical or permissible for your Agency, a CD with the upgrade can be sent via mail, or the upgrade can be placed on a server on your end and POS terminals can access the upgrade from that server.

Batch acknowledgement – A batch acknowledge is sent to the POS computer once a batch is received and processed by the ELVIS system. Larger batches can take longer for our system to process so the batch acknowledgement may not be sent immediately after transmission. This system task can be setup to execute an acknowledgement to a batch at either 'Start up' or 'Close Batch'. The default is set to execute on 'Start Up' and 'Close Batch'. It is vitally important to ensure that at least one box is checked.

Batch upload – The Batch Upload task determines when the closed batch is transmitted to ELVIS. This task can be setup to execute a batch transmission at either 'Start up' or 'Close Batch'. The default is set to execute on 'Close Batch'. It is vitally important to ensure that at least one box is checked.

Data Entry Screen Update - The Data Screen Update task allows new data screens, sometimes called forms, to be transmitted from ELVIS to the POS computer. The data entry screens need to be updated immediately after an install or upgrade, and thereafter only when changes to the unique configurable fields are needed. This task can be setup to require that upgrades to the data entry screens be performed at either 'Start up' or 'Close Batch'. The default is set to execute on 'Close Batch'. It is vitally important to ensure that at least one box is checked.

LVD Download - The LVD Download task allows updates to the Local Verification Database, if the agency uses this optional feature. This task can be setup to execute an LVD download (update to the

Local Verification Database) at either 'Start up' or 'Close Batch'. The default is set to execute on 'Close Batch'. When the LVD Download task selection is active, an additional field appears. This field allows the Agency to choose the number of days the old LVD is allowed to become before an override is required from a supervisor. (See Figure 3.8) The default is 30 days. After the LVD has reached its override age, it is considered to be stale and a new LVD needs to be downloaded. The operator is prompted to download an updated LVD. If the operator chooses to use the existing LVD without an update, the system requires a supervisor to approve (override) by supplying their login and password each time the POS application is launched. The default is set to execute on 'Close Batch'. It is vitally important to ensure that at least one box is checked.

Note: The LVD is an optional feature that can be disabled. To disable the LVD download feature, please make sure that that the 'Execute on' box is unchecked. This along with the 'General' tab settings for LVD download makes the LVD optional (see 'General' Tab settings).

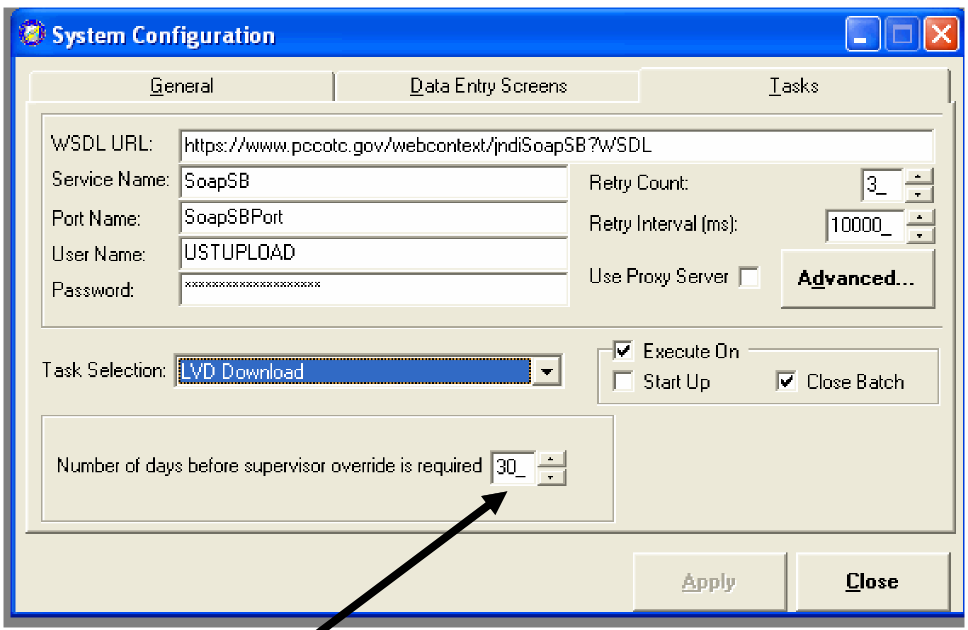


Figure 3.8

When all changes have been made within the Tasks Tab window, click the 'Apply' button. The system responds with the message that the POS application must be restarted to use these changes.

Note: It is strongly recommend that these settings be left at the default settings.

Override

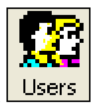
The section above mentions a setting for a supervisor override. An override occurs when an operator encounters a situation that requires higher approval, such as overriding the existing Local Verification Database, or overriding a blocked or suspended item. The action calls for a one-time approval from a person with supervisory or higher access. A window appears requesting a login and password for authorization. Once the approver types their login and password, the system checks the login to ensure proper permissions. If the login is accepted, the process can continue. The operator remains logged on during the entire process and can continue with their work.

User Administration

This section covers the granting of access to the POS system only. If access needs to be granted to the web-based system called ELVIS, please refer to the *ELVIS* chapter of this User Manual.

New users of the POS must first be set up in the SAT user administration and be assigned roles and permissions before accessing the POS application. New permissions have been added so existing user's roles must be reviewed to make certain they have all of the necessary permissions to perform their work.

Users that are added to the POS are controlled solely by the Agency. Action from the Treasury OTC Support Center is not needed to grant access to the POS component for user administration. The Agency controls access on who uses the POS software and their level of access on the computer in your location.

Select the User Administration icon 

from the main SAT screen to access the following user administration screen. (Figure 3.9), or using the menu at the top of the screen, click **'File'**, then **'Users…'**. This screen displays a list of all users including their Login name, full name, the date they were created in the system, the date that they last accessed the system and their role.

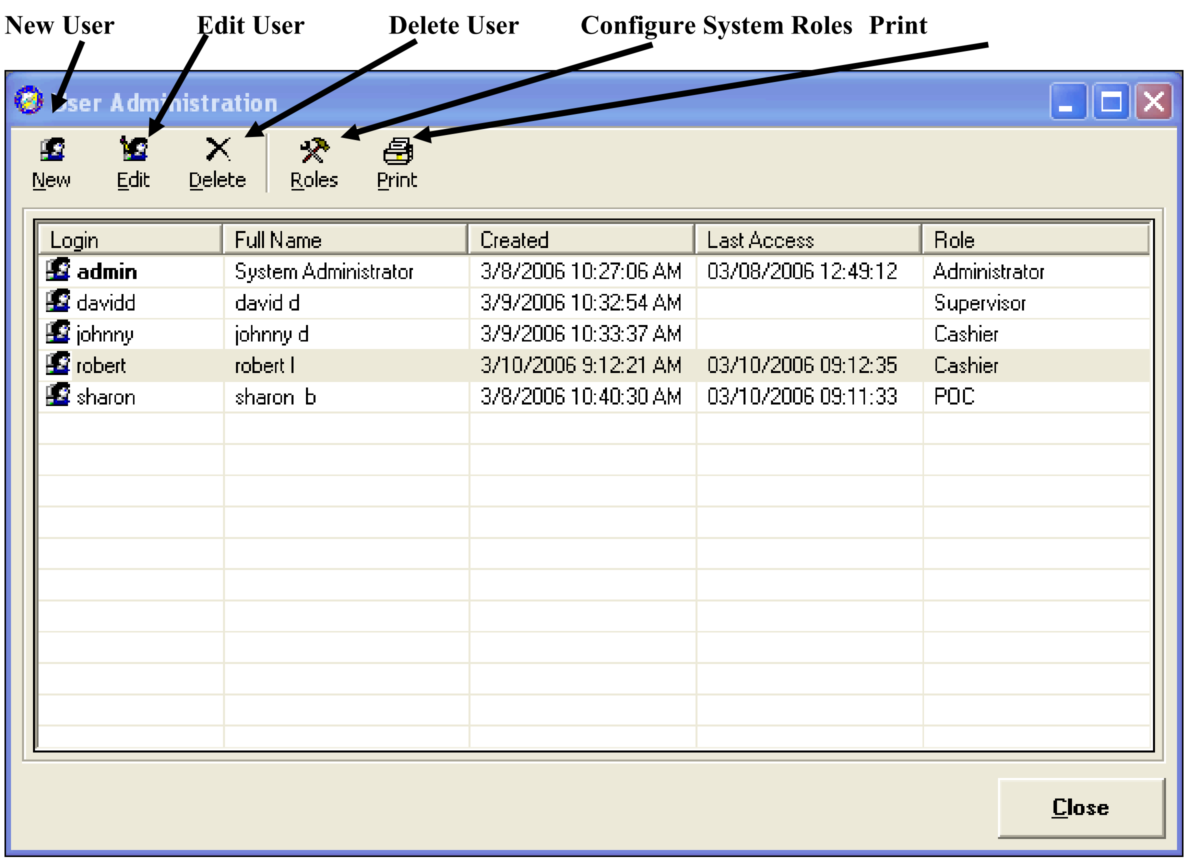


Figure 3.9

User Administration consists of five primary functions: (as displayed in Figure 3.9)

- Add New User
- Edit User
- Delete Users
- Configure System Roles
- Print out a list of system users

Further explanations of these functions are covered on the next pages.

Adding a New User

From the main SAT screen, select the 'Users' icon 

then select the 'New User' icon 

from the User Administration screen. Users can only be added by an authorized user. The following screen appears: (Figure 3.10)

At the first login after the software installation, the admin user must add the Point Of Contact (POC). The POC needs to be setup as a user and assigned the POC role. The POC has the highest level of authority within the POS.

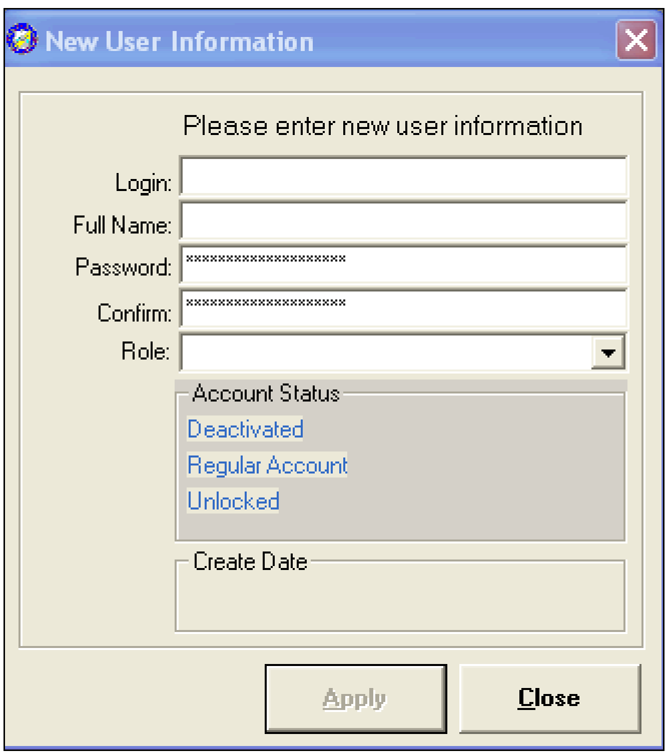


Figure 3.10

Enter the new user information including the Login, Full Name, and default Password. The default password is typed twice, once in the 'Password' field and then again in the 'Confirm' field.

- The Login is not case sensitive and must be between 6 and 20 characters. The login should be identifiable by the user, for example the user's first initial and last name. The Login can be all numeric, all alpha, or a combination of alpha-numeric and should not include commas, spaces, or apostrophes. The login does allow the use of a hyphen in the login ID.
- The Full Name field must be between 4 & 20 characters and should be the first and last name of the user. The Full Name should not include special characters such as commas, apostrophes or periods..

Users are assigned a default user password and are required to establish a new password upon their initial login. For complete specifics regarding password requirements, please see *Appendix R – Password Requirements* in the Appendix chapter of this User Manual, or contact the Treasury OTC Support Center.

Note: Users should be aware that 3 unsuccessful login attempts (or the configurable number of attempts that are set in the System Configuration) results in a locked account. Once an account is locked, the POC (or a user with the 'administrator' role) must sign into the SAT and unlock the user and reset the password if necessary.

Select the appropriate role by using the dropdown arrow, then click **'Apply'**. Once a user has been added, an administrator can view the user's information, which would include the status of their account and the date that the user was added to the system.

Account Status

The 'Account Status' portion of the screen displays information pertaining to each user (See Figure 3.11)

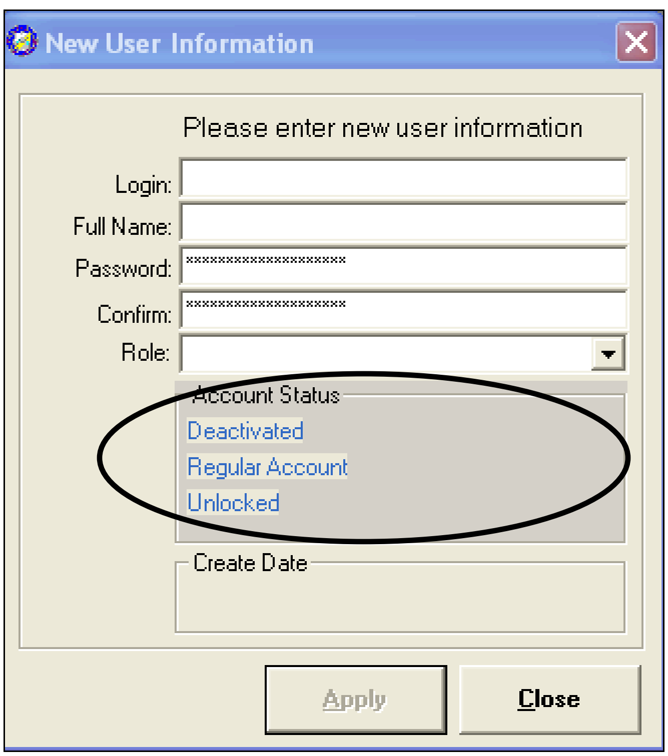


Figure 3.11

Active/Deactivated - Until the apply button is clicked, the new user is displayed as 'Deactivated'. After the 'Apply' button is clicked and the user is successfully added, the new user's account status can be displayed by double-clicking on the new user from the User Administration screen. The user's status now reflects 'Active'. Also, a user's status displays 'Deactivated' if that person has been intentionally deactivated by an authorized user.

Regular/System Account - All users account status display 'Regular Account' unless the user has the Administrator role. Administrator accounts display 'System Account'.

Locked/Unlocked – The normal status for a user is 'Unlocked'. If a user should exceed their maximum sign-on attempts (as defined in the SAT configuration settings) by typing an incorrect password, their account becomes 'Locked'. That user is not able to sign back into the POS, SAT or Batch Manager until their account has been changed to 'unlocked' by an authorized user.

Edit User

A user's account can be edited by an authorized user. A user's Login, Full name, password and role can be edited. To edit a user's account:

1. From the main SAT screen, select the 'User's icon 
.

2. The screen displays all of the users as seen in Figure 3.12. Click to highlight the user to be edited then click the edit user button, or right-click on the user to be edited and choose 'edit'.

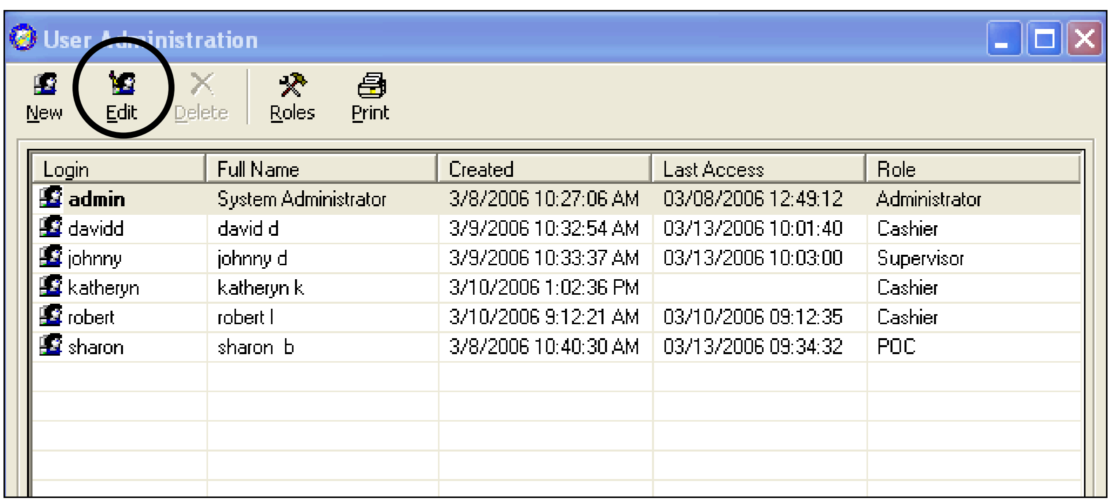


Figure 3.12

3. A 'Modify User Information' screen appears: (Figure 3.13).

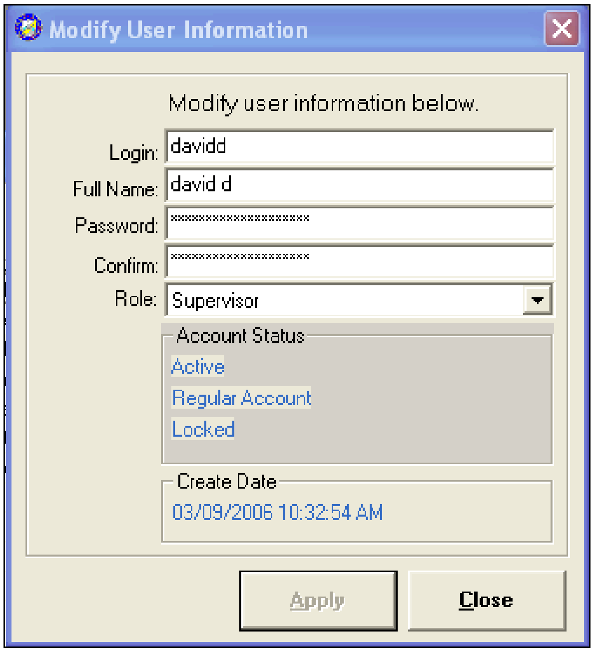


Figure 3.13

4. Key in the updated information or click to choose a different role, then click the **'Apply'** button at the bottom of the window. The screen returns to the User Administration Window. Click **'Close'** when finished.

Unlock

A user's account becomes 'locked' if their unsuccessful login attempts exceed the 'maximum failed login attempts' as set in the System Configuration. The POC, or a user with the 'administrator' role, can 'Unlock' a user account. ***(Note: The user's password may also need to be reset if the user does not remember their password – see Reset Password).*** This function can only be performed from the User Administration screen. There are no menu options for unlocking a user's account.

To unlock a user's account:

1. From the main SAT screen, select the 'Users' icon 
.

The screen displays all users . When a user account is locked, a red 'lock' appears as seen in Figure 3.14

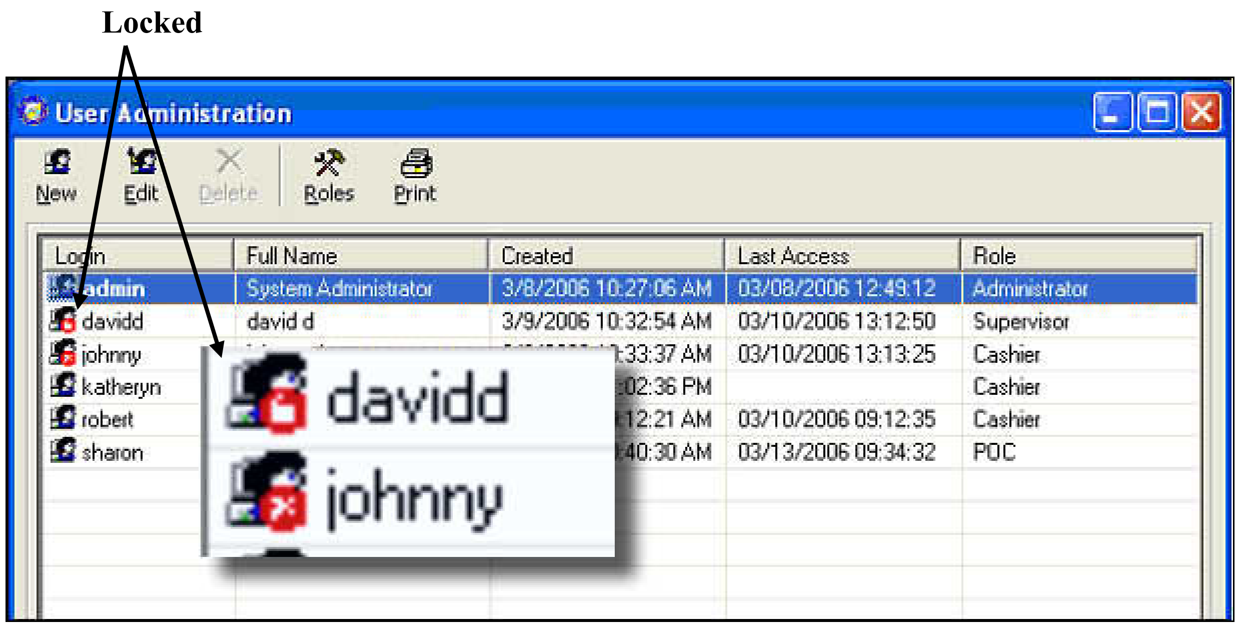


Figure 3.14

2. To unlock, a user's account, right-click on the user's login. A drop down menu appears with choices as seen in Figure 3.15.

3. If the user has forgotten their password, the next step is to reset their password. Please see the next section, 'Reset Password'.

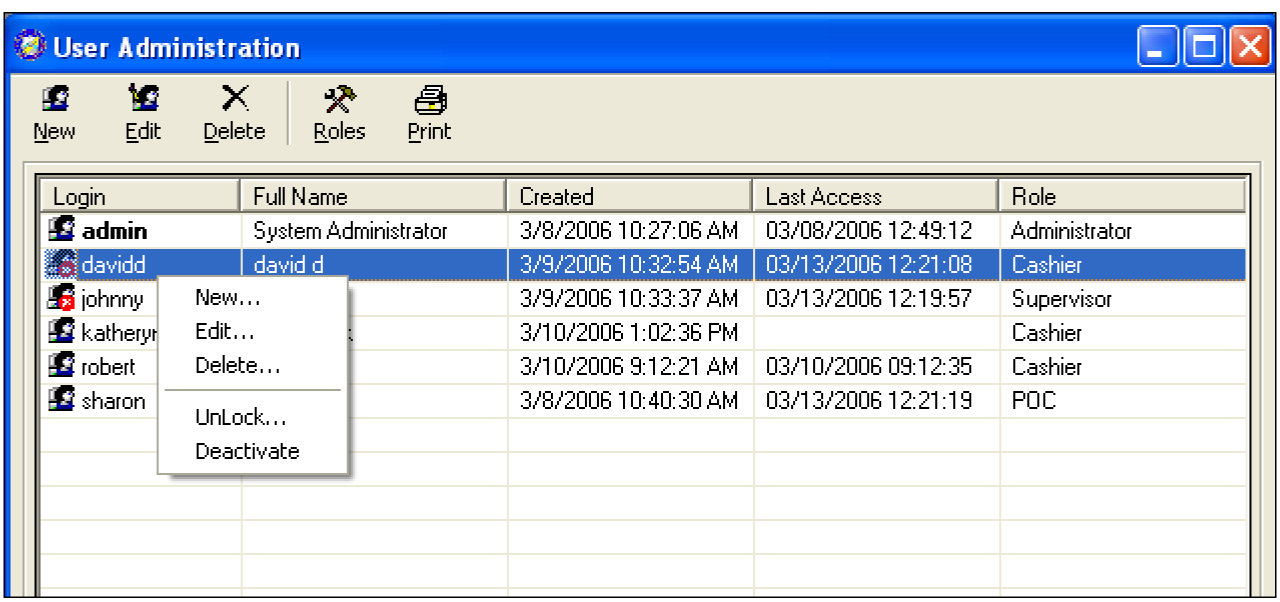


Figure 3.15

4. Click the 'UnLock' action and the user's account is immediately updated.

5. If the user forgets their password, it is necessary to reset the user's password (see the 'Reset Password section of this chapter).

Reset Password

If a user has become locked because they cannot remember their password, the POC or a user with the 'administrator' role needs to reset the user's password by assigning a new, temporary password. The user is required to change their temporarily assigned password to their own unique password.

To reset a user's password:

1. Click the 'Users' icon 

from the main SAT screen. A window appears that displays all user accounts. Double-click the user login whose password needs to be reset. Type a new password in the 'Password' and 'Confirm Password' fields as displayed below in Figure 3.16. Password requirements mandate that the password have a minimum of 8 alphanumeric characters. The password is also case sensitive.
2. When complete, click **'Apply'** and **'Close'** to exit.

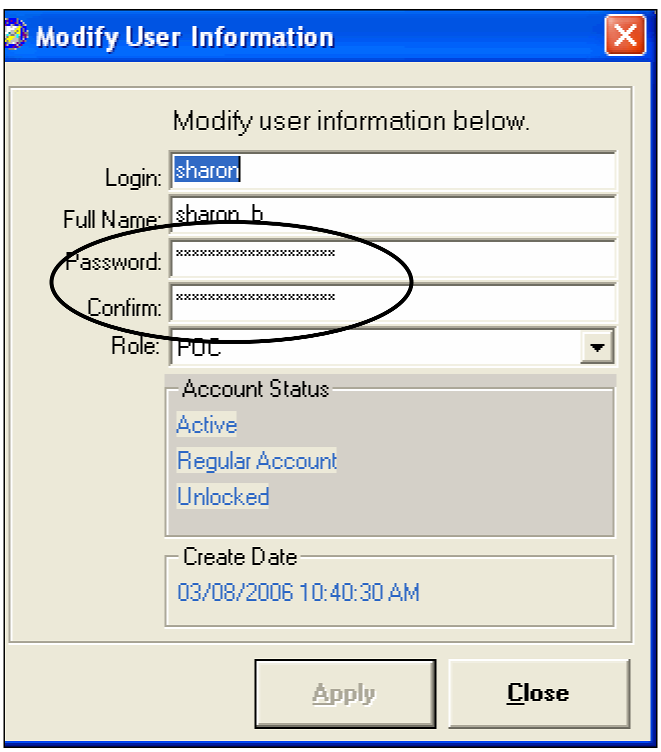


Figure 3.16

Note: Resetting a user's password automatically unlocks the account.

Activate or Deactivate User Account

A user account can be intentionally ‘Deactivated’ if, for example, a user is on vacation or medical leave. Upon their return, their account can be ‘Reactivated’. These functions can only be performed from the User Administration screen by the POC or a user with the ‘administrator’ role. There are no menu options for these functions.

To Deactivate a user’s account

1. From the main SAT screen, select the ‘Users’ icon 

.

2. The screen displays all users as seen in Figure 3.18.

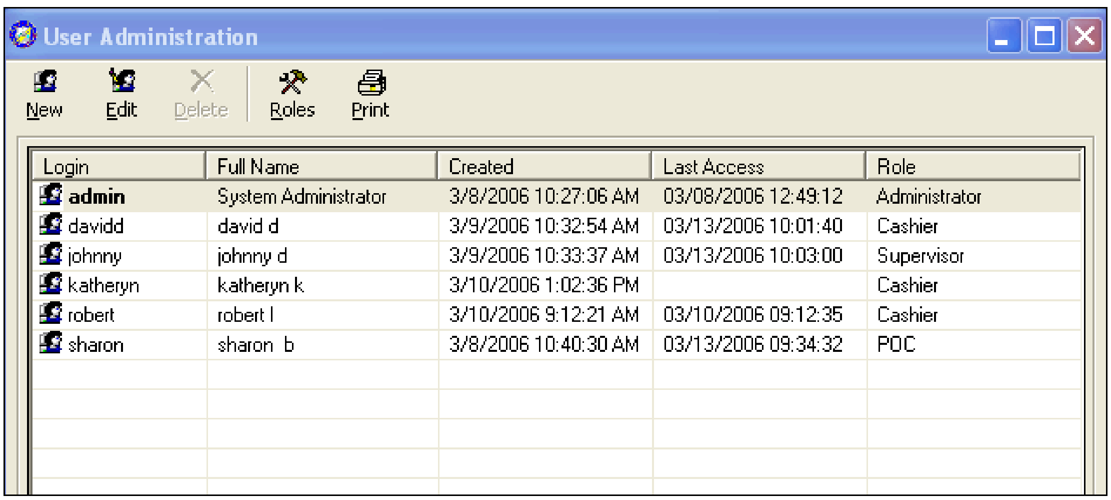


Figure 3.18

3. Right click on the Login to deactivate. A drop down menu appears with choices, as displayed in Figure 3.19.

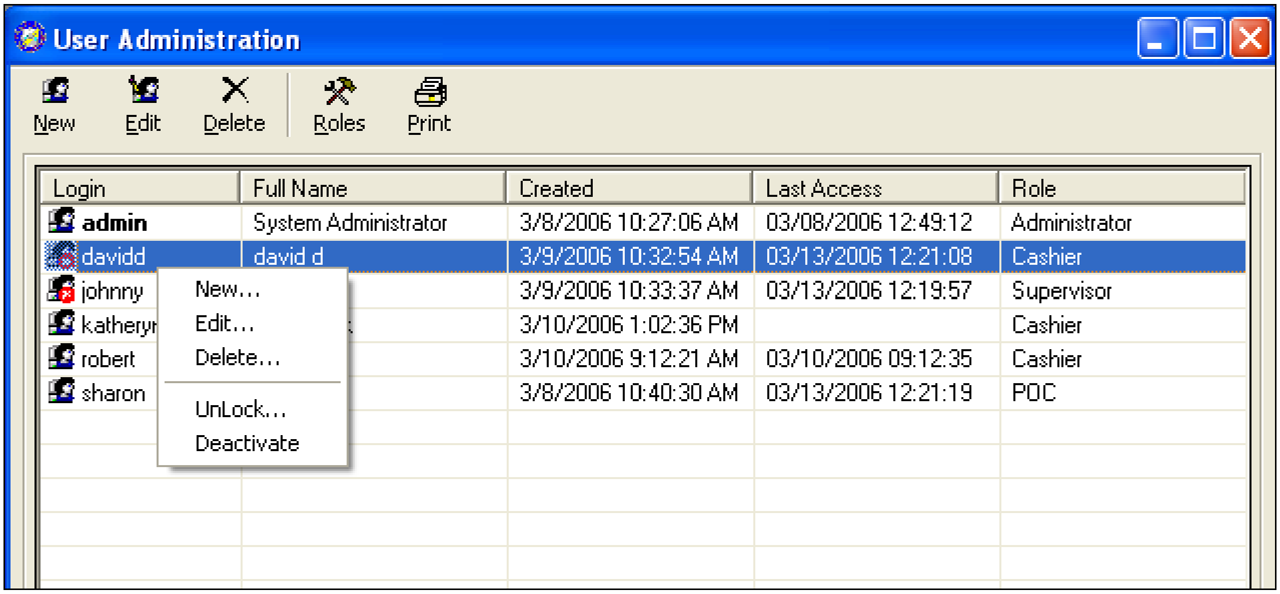


Figure 3.19

4. Click the 'Deactivate' action. The user's login now appears with a red 'X', as displayed in Figure 3.20.

Deactivated

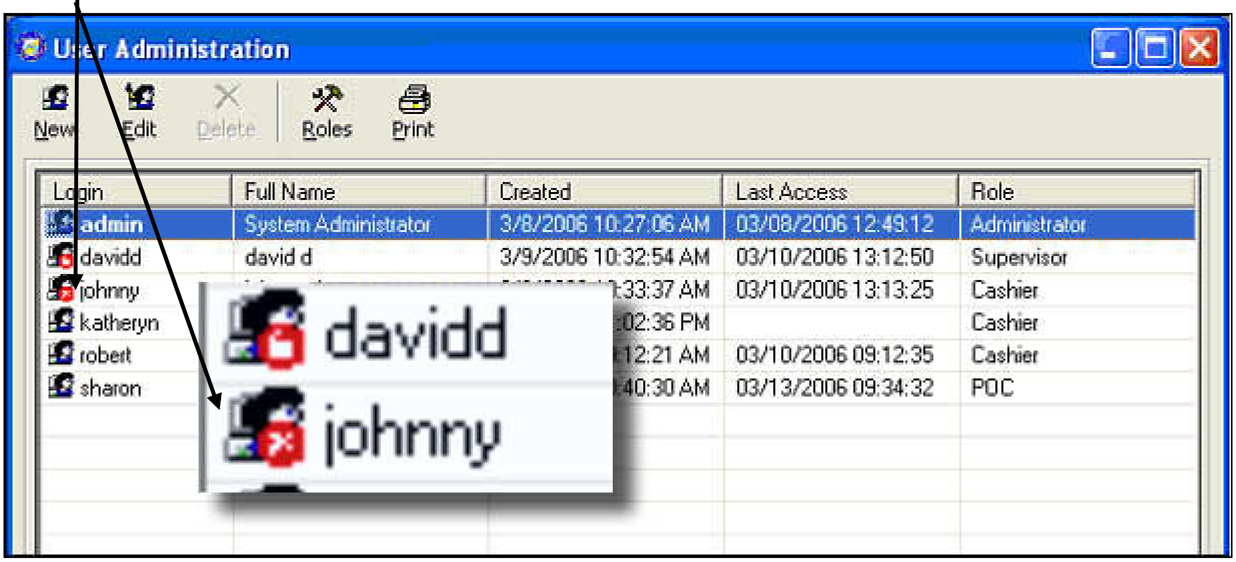


Figure 3.20

To Activate a user's account

1. From the main SAT screen, select the 'Users' icon 

.

2. The screen displays all users as seen in Figure 3.21.

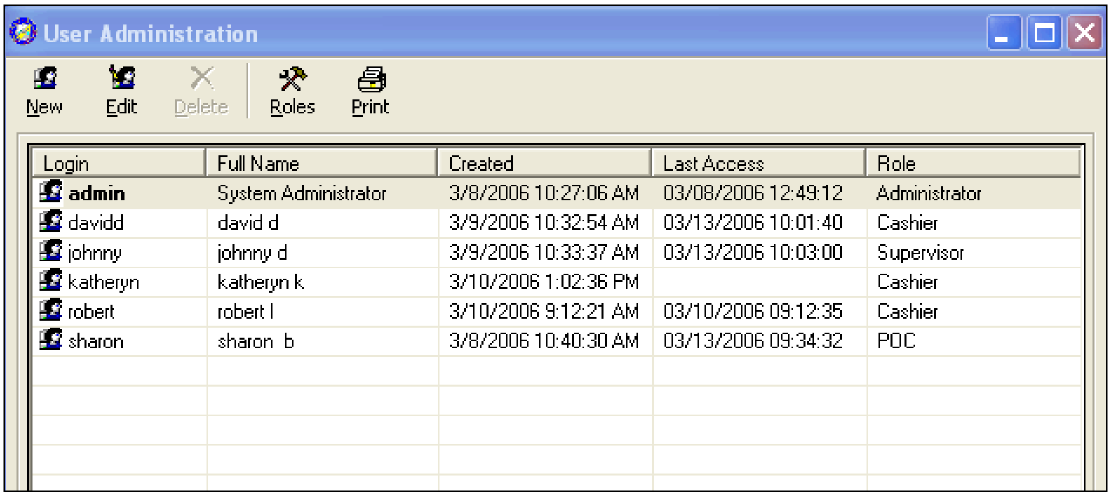


Figure 3.21

3. Right click the row of the Login to activate. A drop down menu appears with choices, as displayed in Figure 3.22.

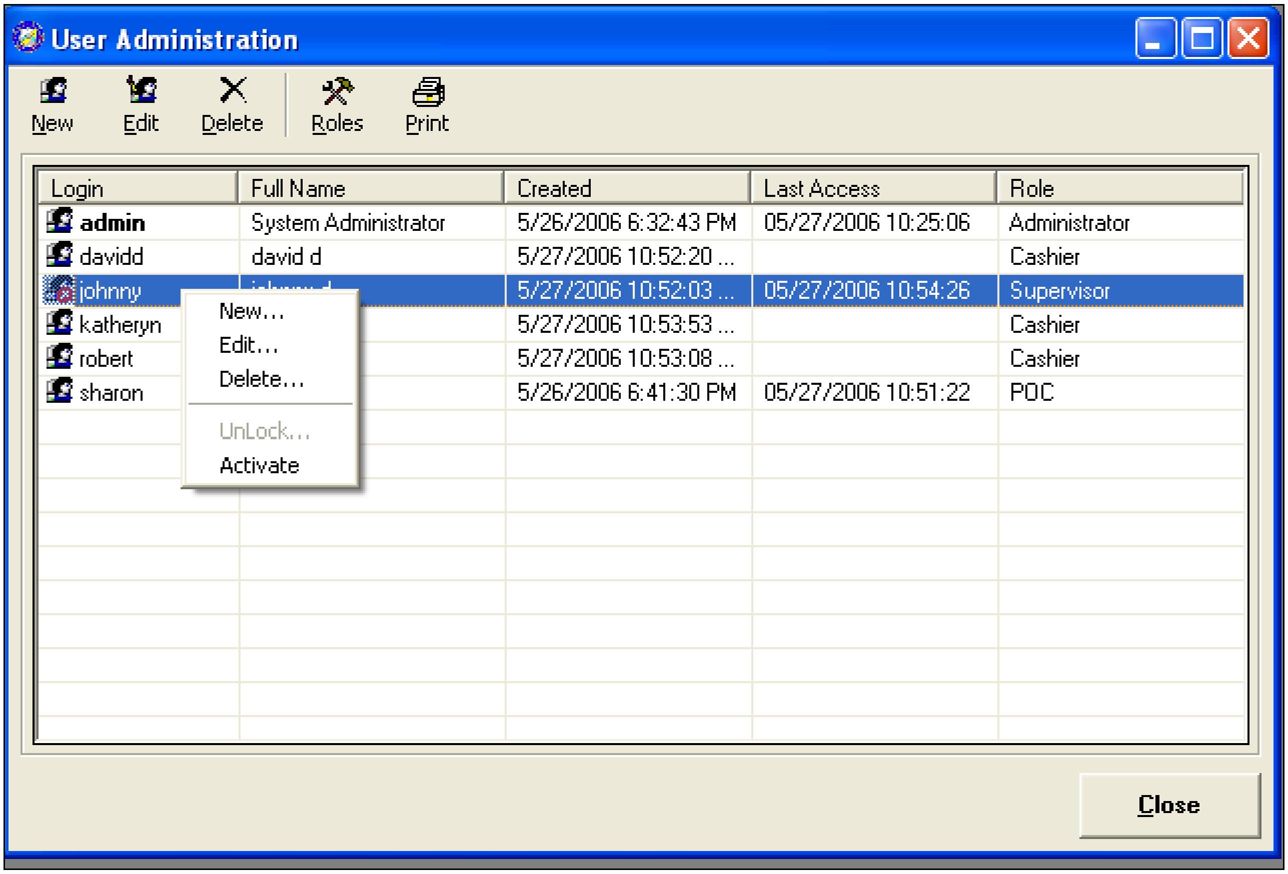


Figure 3.22

4. Click the 'Activate' action. The red 'X' that appeared on the user's login is now removed.

5. If the user forgets their password, the user's password must be reset (see the 'Reset Password' section of this chapter).

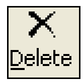
Delete Users

An authorized user has the ability to delete a selected user.

1. From the main SAT screen, select the ‘Users’ icon 

.

2. Click on the user to be deleted.

3. Select the **‘Delete User’** icon 

from the User Administration screen. The user can also be deleted by selecting the user and right-clicking. Click **‘Delete’** to delete the user.

4. A prompt appears on the screen asking, “Delete user ‘nnnn’, Are you sure?” Click **‘Yes’**. The user account is removed from the system and no longer appears on the User Administration screen.

Configure System Roles

System Roles are assigned specific system permissions to indicate the access levels of each role. Administrator, Cashier, POC (Point of Contact), and Supervisor are provided as system default roles. These roles can be changed according to the agency's needs. Additional system roles required by an agency can be added or edited by an authorized user. Each user is assigned one of the four system default roles, or an Agency created role. Roles should be consistent across an agency, and not be location specific. Highlight the specific role to determine the role permissions. For example, if the user is logged in as a Supervisor, and the Supervisor role has the System Permission to configure users, the Supervisor user is able to perform user configuration functions. Review the accuracy and completeness of the role permissions to agency requirements prior to assigning users.

To configure system roles, click the 'Users' icon 

, from the main SAT screen, then click the 'Configure System Roles' icon 

, from the User Administration screen. The following screen appears: (Figure 3.25)

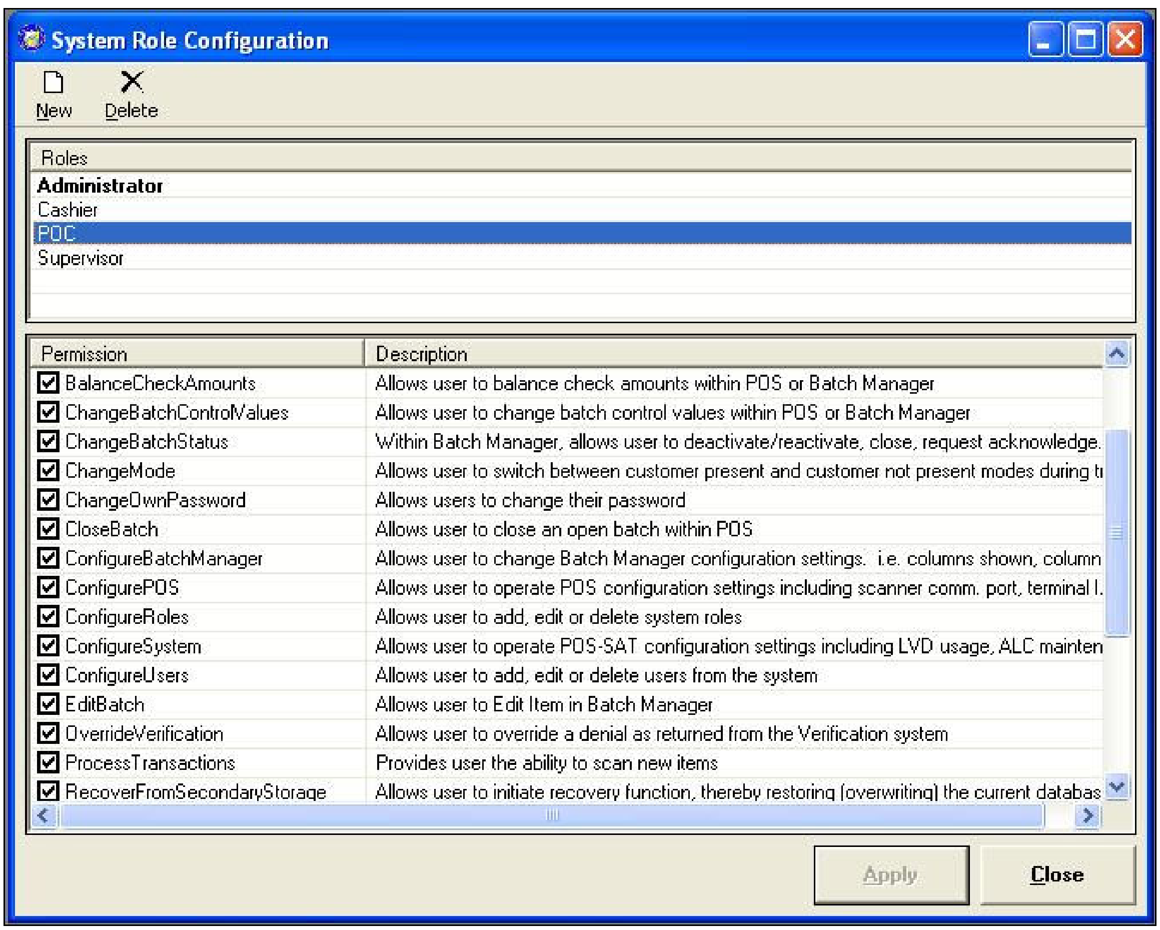


Figure 3.25

The system default roles can be edited by clicking to check or uncheck specific permissions.

Permissions

The table below describes the meaning and use of each of the permissions. These permissions can be assigned to new or predefined system roles.

Predefined permissions

Permission Name	Used to…
AuthorizeDuplicates	Allows a user to accept a duplicate within POS.
AuthorizeMICRCorrection	Allows a user to make MICR corrections within POS.
AuthorizeOldVerification	Allows user to authorize the use of an out-of-date LVD.
AuthorizePoorImageQuality	Allows a user to accept items whose images are of poor quality within POS.
BalanceCheckAmounts	Allows a user to balance check amounts within POS or Batch Manager.
ChangeBatchControlValues	Allows a user to change batch control values within POS or Batch Manager.
ChangeBatchStatus	Within Batch Manger, allows uers to deactivate/reactivate, close, request acknowledgement, or upload a batch.
ChangeMode	Allows a user to switch between customer present and customer not present modes during transaction entry.
ChangeOwnPassword	Allows users to change their password.
CloseBatch	Allows a user to close an open batch within the POS.
ConfigureBatchManager	Allows a user to change Batch Manager configuration settings i.e. columns shown, column order and column move.
ConfigurePOS	Allows user to operate POS configuration settings including scanner comm. port, terminal ID, and enable/disable Yes/No Keypad.
ConfigureQueueInterface	Allows user to configure the Queue Interface in the SAT.
ConfigureRoles	Allows a user to add, edit or delete system roles
ConfigureSystem	Allows user to operate POS- SAT configuration settings including LVD usage, ALC maintenance, and receipt printing.
ConfigureUsers	Allows a user to add, edit, or delete users from the system.
EditBatch	Allows editing an item in Batch Manager.
OverrideVerification	Allows a user to override a denial as returned from the Verification system
ProcessTransactions	Allows a user the ability to scan new items..
RecoverFromSecondaryStorage	Allows a user to initiate the recover function, thereby restoring (overwriting) the current database from the secondary storage location.
ResetLVD	Allows a user to clear all of the records from the LVD (to be re-populated through a subsequent update LVD operation)
Setup Printer	Allows a user to setup a default printer for the POS or SAT operations. Printers will only print to the Windows default printer. Will be corrected in the next Release)
UpdateLVD	Allows a user to request updates (or entire database if LVD reset has occurred) of verification records to the LVD from the MVD.
UpgradeApplication	Allows a user to extract an upgraded application from the local database (once it has been downloaded from the host) and launch the installation procedure.
ViewActivityLog	Allows a user to view activity log entries of the completed audit trail within the system.
ViewBatchList	Allows a user to launch the View Batch List function within the POS or Batch Manager.
VoidItems DuringBalancing	Allows a user to void items during balancing within the POS or Batch Manager
Void Transaction	Allows a user to void a previously processed transaction within the POS or Batch Manager. (Prior to transmission)

Predefined System Roles

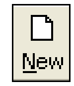
The following roles are the defaulted roles when the POS is first installed. When upgrading from a previous version, any changes that were made to these predefined roles in the previous version are carried over to the upgrade.

Note: The predefined system roles can be deleted and unique roles can be created in their place. Only the 'Admin' role cannot deleted.

Predefined roles and their default permissions

Name	POC	Supervisor	Administrator	Cashier
Authorize Duplicates	✓	✓	-	-
Authorize MICR Correction	✓	✓	-	-
Authorize old verification	✓	✓	-	-
Authorize poor image quality	✓	✓	-	-
Balance Check Amounts	✓	✓	-	✓
Change Batch Control Values	✓	✓	-	✓
Change batch status	✓	✓	-	-
Change mode	✓	✓		✓
Change own password	✓	✓	✓	✓
Close batch	✓	✓	-	✓
Configure Batch Manager	✓	✓	-	-
Configure POS	✓	✓	✓	-
Configure Queue Interface	-	-	-	-
Configure roles	✓	-	-	-
Configure system	✓	✓	✓	-
Configure users	✓	✓	✓	-
Edit batch	✓	✓	-	-
Override verification	✓	✓	-	-
Process transactions	✓	✓	-	✓
Recover from secondary storage	✓	✓	-	-
Reset LVD	✓	✓	✓	-
Setup printer	✓	✓	✓	✓
Update LVD	✓	✓	-	✓
Upgrade application	✓	-	✓	-
View activity log	✓	✓	✓	✓
View batch list	✓	✓	✓	✓
Void items during balancing	✓	✓	-	-
Void transaction	✓	✓	-	-

Adding System Roles

Authorized users are able to add system roles by selecting the 'New System Role' icon 

from the System Role Configuration screen. (Figure 3.26) The POS system comes with four predefined system roles. As an alternative to using the predefined roles, a customized system role can be added and assigned the appropriate permissions to suit the Agency's specific needs.

1. Enter the new system role name in the space indicated below, then click **'OK'**. The new role appears on the System Role Configuration screen.

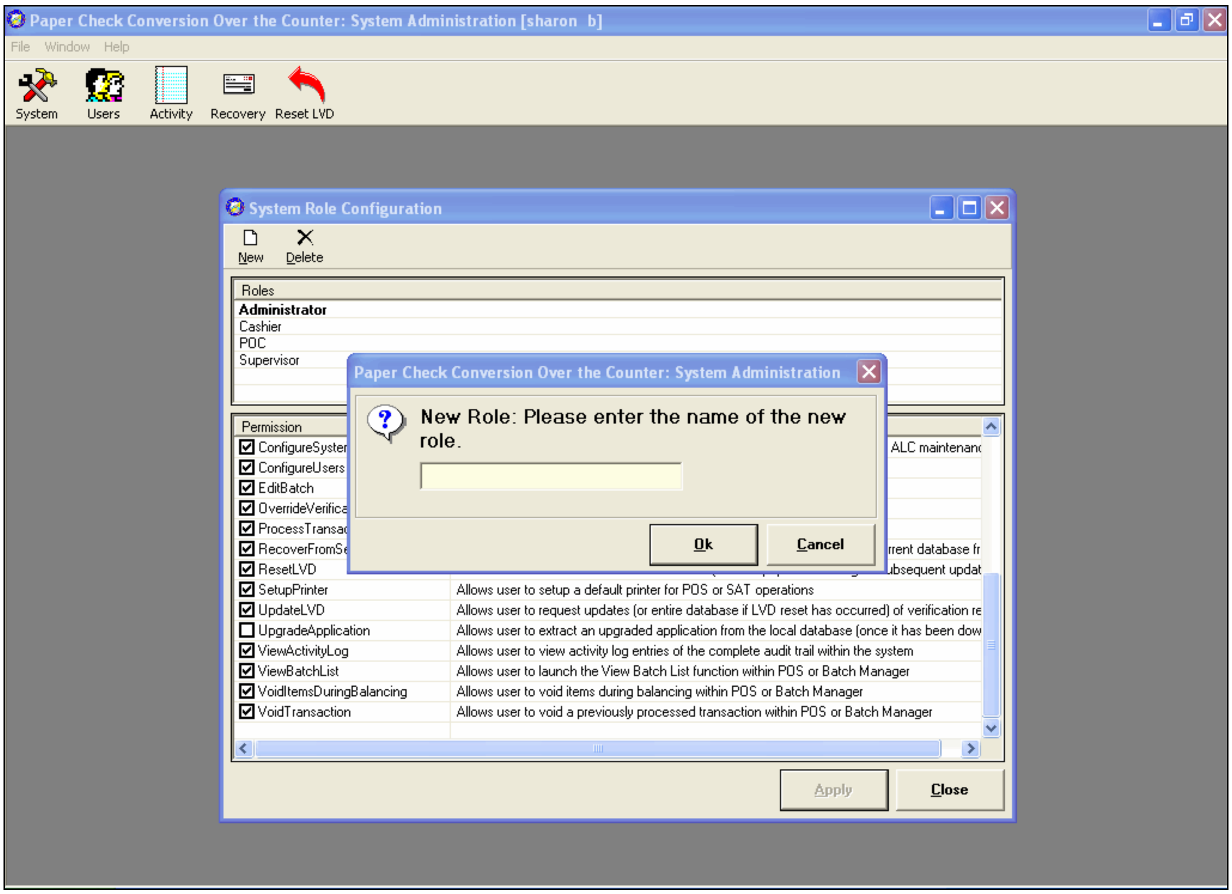


Figure 3.26

2. Click to select the new role, then click to check the System Permissions for that role. The System Permission, ChangeOwnPasword, must be checked for all roles. If it is not selected, the user will not be able to sign on.

3. Click **'Apply'**.

Modify Roles

A user's role can also be modified. This function can be used to add or remove permissions from one or more of the predefined system roles rather than create a new role, or to modify an Agency created role.

Click the 'Users' icon 

from the main SAT screen. A window appears that displays all user accounts.

1. Double-click the user whose role needs to be modified.
2. Change the user's role by clicking the down arrow to the right of the 'Role' field, then clicking on the new role as displayed in Figure 3.27.
3. When complete, click **'Apply'.** Click **'Close'** to exit User Administration.

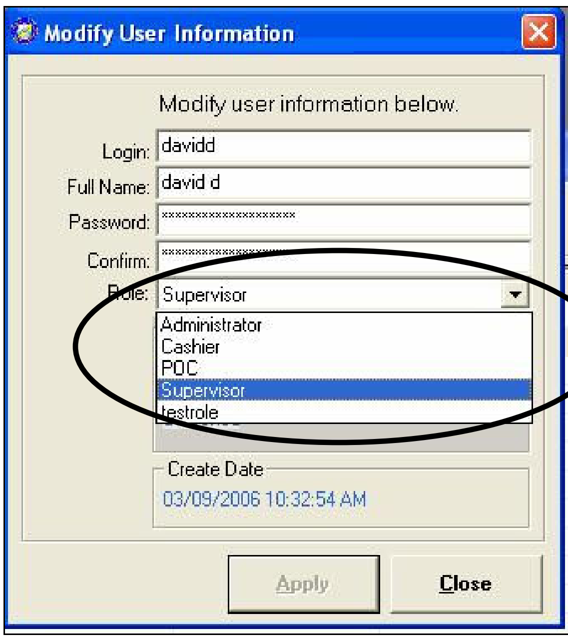
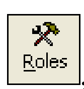


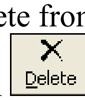
Figure 3.27

Deleting System Roles

Authorized users are able to delete system roles.

1. Click the 'Users' icon 

from the main SAT screen. A window appears that displays all user accounts.
2. Click the 'Configure System Roles' icon 

, from the User Administration screen.
3. Click to highlight the role to delete from the top of the 'System Role Configuration' window. Click the **'Delete System Role'** button 

from the System Role Configuration screen.
4. At the verification message or 'Are you Sure?' click **'Yes'**. The role is removed from the system Role Configuration screen.

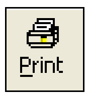
Note: A role cannot be deleted if a user is assigned to that role. Reassign users to new roles before deleting the existing role.

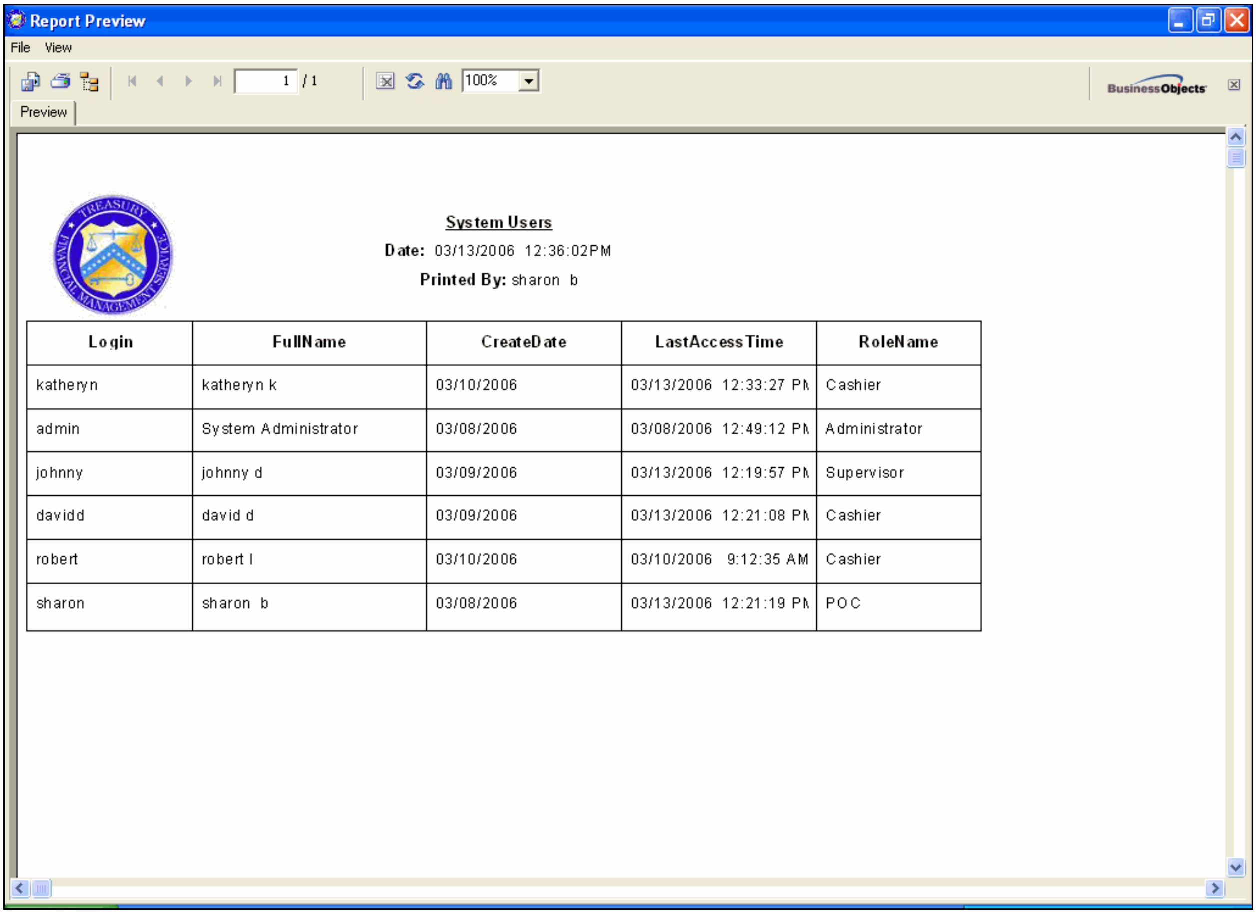
Print User Information

An authorized user has the ability to print the listing of all user information.

1. From the main SAT screen, select the 'Users' icon . A window appears with a listing of all users in the
   POS system.

2. Fields can be sorted by clicking on the heading above each column.

3. Click the 'Print' icon  from the top of the User Administration screen. A preview of the System User Report is displayed on the computer's screen as displayed in Figure 3.27.1. To print the report, click the printer icon at the top of the screen, or click 'File', then 'Print' from the menu at the top of the screen.



System Users

Date: 03/13/2006 12:36:02PM

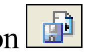
Printed By: sharon b

Login	FullName	CreateDate	LastAccessTime	RoleName
katheryn	katheryn k	03/10/2006	03/13/2006 12:33:27 PM	Cashier
admin	System Administrator	03/08/2006	03/08/2006 12:49:12 PM	Administrator
johnny	johnny d	03/09/2006	03/13/2006 12:19:57 PM	Supervisor
davidd	david d	03/09/2006	03/13/2006 12:21:08 PM	Cashier
robert	robert l	03/10/2006	03/10/2006 9:12:35 AM	Cashier
sharon	sharon b	03/08/2006	03/13/2006 12:21:19 PM	POC

Figure 3.27.1

Other SAT Report Preview Functions

Export Report

The User Information report can be exported by clicking on the 'Export Report' icon  at the top left of the report preview screen. When the icon is clicked, a window appears that allows the user to choose the file format by using the dropdown arrow (Figure 3.28).

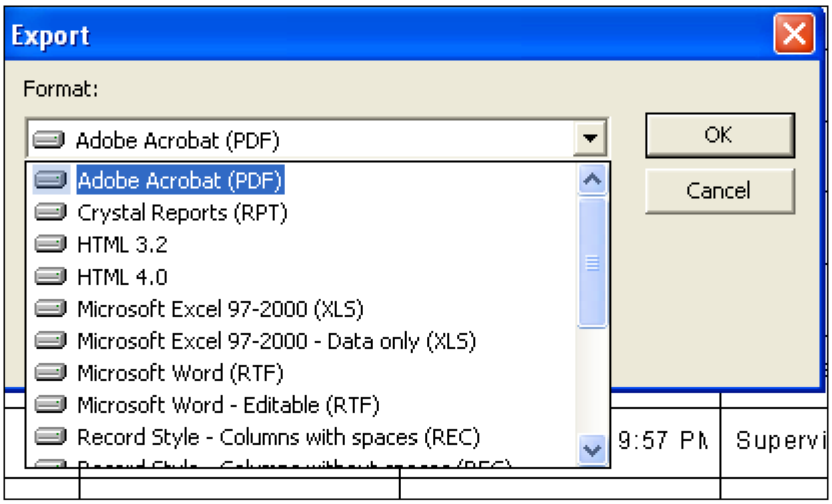


Figure 3.28

Click the appropriate format and the choice is placed in the format field. Click the 'Destination' drop down arrow and choose 'Disk File' as displayed in Figure 3.29.

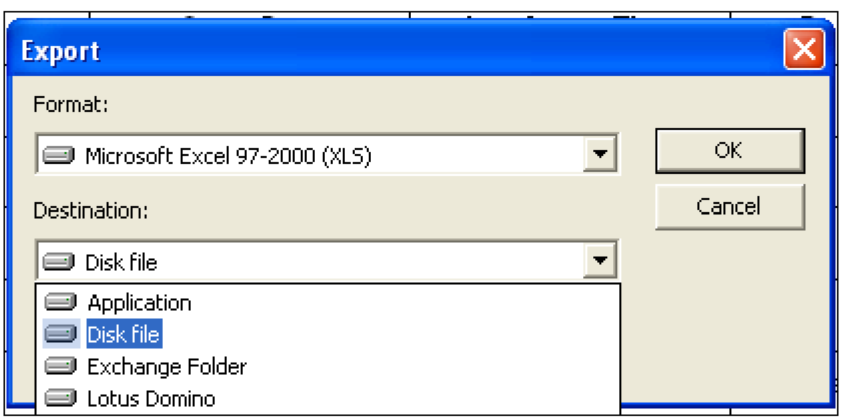


Figure 3.29

Based on the format that was chosen, additional data may need to be keyed regarding the file such as page range, column width (xls format), or delimiter /separator (csv format). If an additional options screen appears, key in the appropriate data or click the appropriate boxes, then click **'OK'**. A 'Choose Export File' screen appears (Figure 3.30).

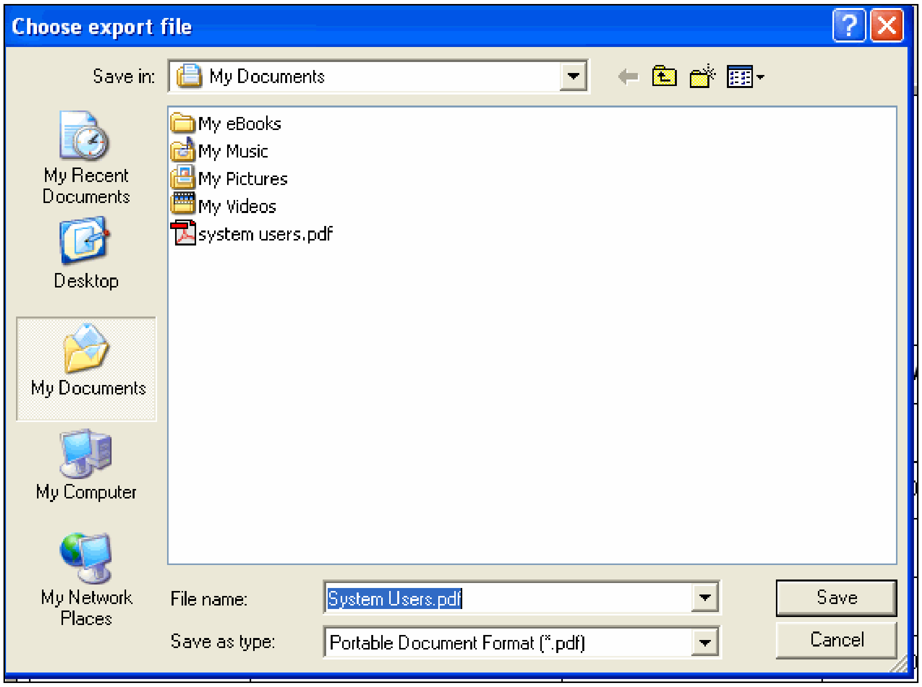
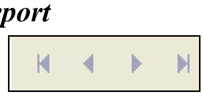


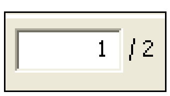
Figure 3.30

In the 'Save in' field at the top of the window, click the down arrow to navigate to the appropriate folder or drive in which to save the file. Near the bottom of the window, type the name of the file in the 'File name' field. Click **'Save'**.

Page through a Report

The 'Arrow' icons  at the top of the screen can be used to page forward and backward in the printout (if more than one page).

Page Display

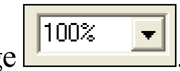
The page display icon 

displays the current page within the box. The total number of pages in the report is displayed after the slash mark.

Search Text

The 'Search Text'  icon is used to pinpoint specific data within the report. When the icon is clicked, a window appears for the user to type the text. Click the 'Find Next' button. If the text is found within the report, the word or words are highlighted. To continue to search for more instances of the text click the 'Find Next' button. When there are no more instances of the text, the system replies with the message, "Search could not find any more instances of the specified text after this page". Click OK.

Increase/Decrease Screen Display

The top right side of the screen displays the screen zoom percentage 

. Use the drop down arrow to the right of the percentage to choose another zoom percentage. The screen display can be increased or decreased.

Exit Report Preview

To exit the Report Preview screen, click the 'X' in the upper right corner of the screen (Figure 3.31).

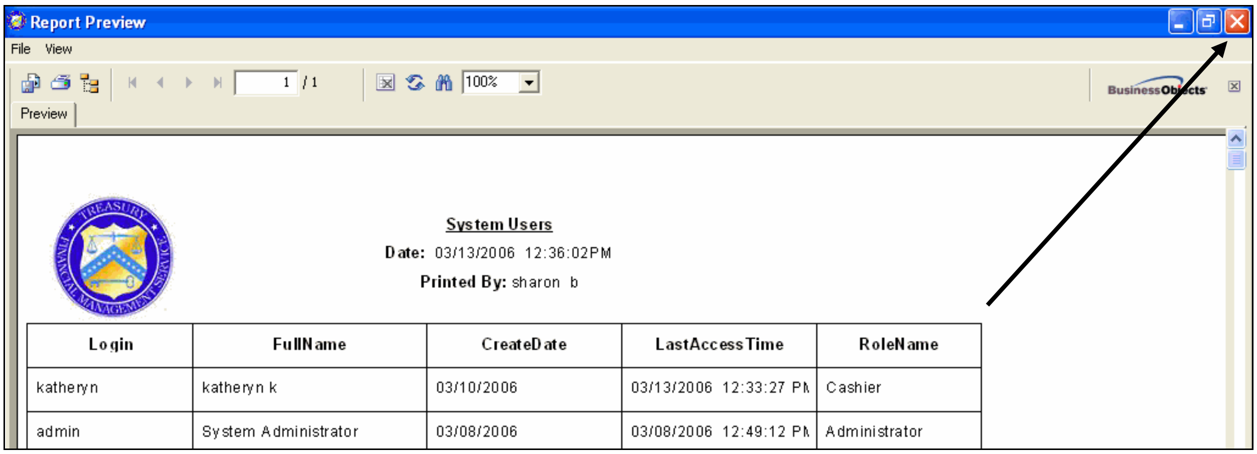
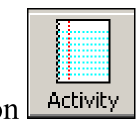


Figure 3.31

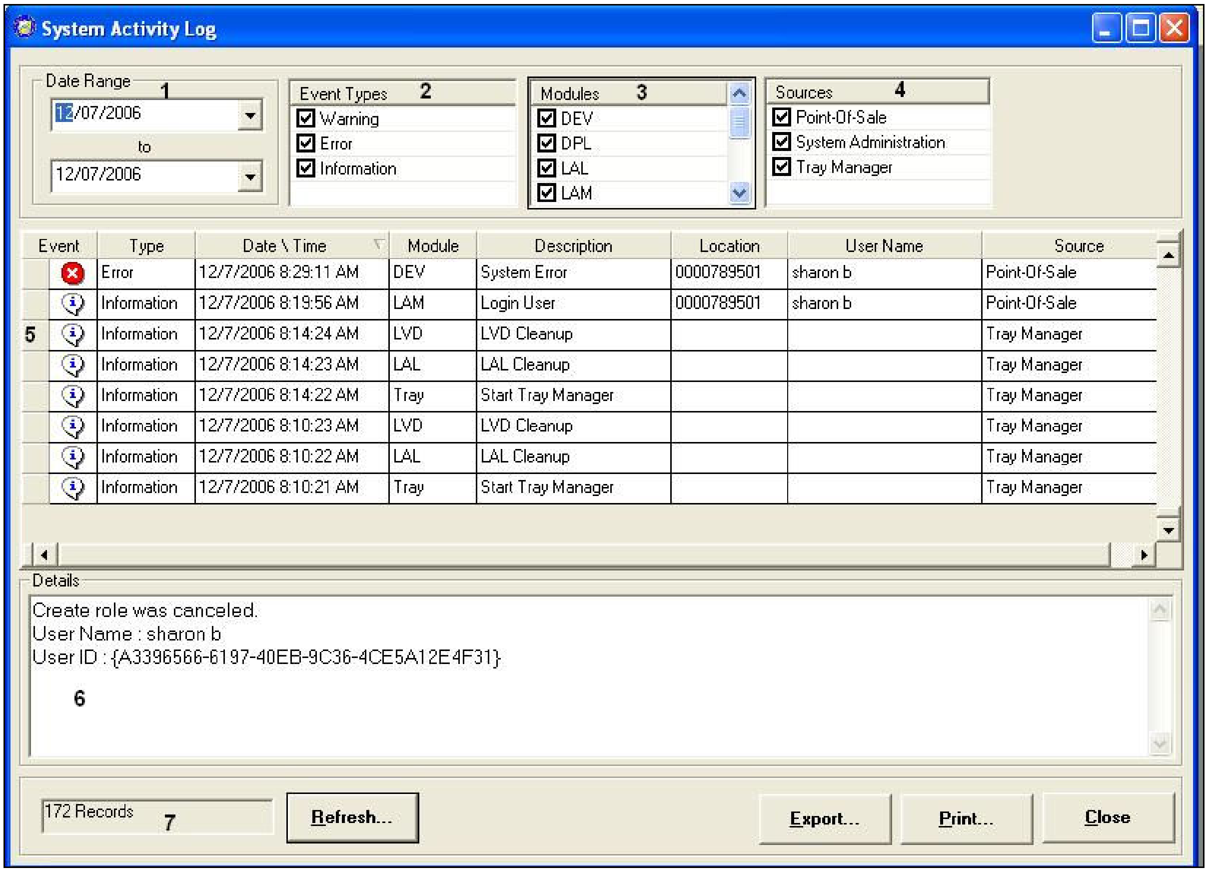
System Activity Log

The system activity log records all interaction between the user and the PCC OTC system. Selecting various settings changes the way that the information is displayed.

> ***Warning: It is recommended that agencies monitor the activity log at least once a month. The POS is configured to save the activity log for 365 days, which is the <u>minimum</u> recommended setting. Entries older than the configured setting will be overwritten. (The activity log can be setup to be automatically retained for as many as 1,095 days but this will use more hard disk space on your computer.) Agencies that wish to keep more than 365 days should print or export the activity log. It can be exported in a .csv format and opened in a spreadsheet program. In the event of a hard drive failure, the activity log will be lost so agencies may wish to export the activity log on a regularly scheduled basis.***

To view the activity log, select the Activity Log icon 

from the main SAT screen, or use the menu at the top of the screen and click '**File**', **'Activity Log…'**. When viewing the activity log, select the appropriate event types, sources, and modules. The user can also check all settings to capture all system activity (Figure 3.32).


System Activity Log
Date Range 1
12/07/2006
to
12/07/2006
Event Types 2
Warning
Error
Information
Modules 3
DEV
DPL
LAL
LAM
Sources 4
Point-Of-Sale
System Administration
Tray Manager
Event Type Date \ Time Module Description Location User Name Source
Error 12/7/2006 8:29:11 AM DEV System Error 0000789501 sharon b Point-Of-Sale
Information 12/7/2006 8:19:56 AM LAM Login User 0000789501 sharon b Point-Of-Sale
5 Information 12/7/2006 8:14:24 AM LVD LVD Cleanup Tray Manager
Information 12/7/2006 8:14:23 AM LAL LAL Cleanup Tray Manager
Information 12/7/2006 8:14:22 AM Tray Start Tray Manager Tray Manager
Information 12/7/2006 8:10:23 AM LVD LVD Cleanup Tray Manager
Information 12/7/2006 8:10:22 AM LAL LAL Cleanup Tray Manager
Information 12/7/2006 8:10:21 AM Tray Start Tray Manager Tray Manager
Details
Create role was canceled.
User Name : sharon b
User ID : {A3396566-6197-40EB-9C36-4CE5A12E4F31}
6
172 Records 7
Refresh...
Export...
Print...
Close
Figure 3.32

Event Types

Event types are categories of events that can be recorded by the audit log. The event types include the following:

Event Type	Description
Warning	Warnings entries are created to inform the user when events of note have taken place. This includes canceling an action, deleting information from the system and inactive users.
Error	Error entries are created when the system is unable to complete an action.
Information	Information entries are general records of the activity that has happened while using the POS.

Modules

The following table identifies the Modules and briefly describes them.

Module	Description
DEV	Hardware integration module.
DPL	Centralized Deployment module.
LAM	Local Access management module.
LID	Local Item storage module.
LVD	Local Check verification module.
SYS	System integration module.
Tray	Service management module.
WKR	Background processing module.

The System Activity Logging consists of several sections:

1. Date Range – User configurable date criteria selection. Use the down arrows to choose the date range .A calendar appears from which to choose the month/day, or simply type the date.
2. Event Types – Types of events logged for viewing include 'Warning', which are indicated in the listing with the symbol ; 'Error', which are indicated in the listing with the symbol ; and 'Information', which are indicated in the listing with the symbol . The type of events that are displayed can be narrowed by clicking to un-check the event types that should be eliminated from view.
3. Modules – Configurable selections. Some examples of these modules are:
   LAM – Administrator; POS – Point of Sale;
   LVD – Local Verification database; LID – batch activity
   The total number of events displayed can be narrowed by clicking to un-check the modules should be eliminated from view..
4. Sources – Current sources available include Batch Manager, Point-of-Sale, System Administration Tool, and Tray Manager
5. Listing – An event listing of selected sources and/or module by date. This listing contains a column for the Event type, Date/Time, Module, Description of the event, Location – which lists the ALC+2, The name of the user who was logged into the system at the time of the event, and the Source – the application in which the event occurred, i.e., POS, SAT, Batch Manager, etc.
6. Details – The details of an event are displayed in the Details portion of the screen when the line for a particular event is clicked.
7. Number of Records – displays the number of records within the requested log.

Additional Functionality
Refresh button – the Refresh button can be used to refresh the system activity log display. Any POS activity that occurs during the SAT session can be reflected on the screen by clicking the Refresh button.
Export button– Allows the log to be exported into a .csv (comma separated value file) which allows the log to be opened in other programs such as spreadsheet software. There may be times when the Treasury OTC Support Center may request an exported activity log for diagnostic purposes.
Print Button – Generates a print preview report and allows the log to be printed. Various other tools are used within the Report Preview window. For a complete explanation of how these tools work, please refer to *'Other SAT Report Preview Functions'* section of this chapter.
Close Button– Exit the System Activity Log listing.

The SAT activity log should be printed before an upgrade. It is also recommended that the SAT activity log be printed monthly, or as the Agency requires. If the location processes high volumes of checks, a more frequent schedule may be appropriate, because activity file data is lost in the event of a hard drive failure.

To print the activity log:

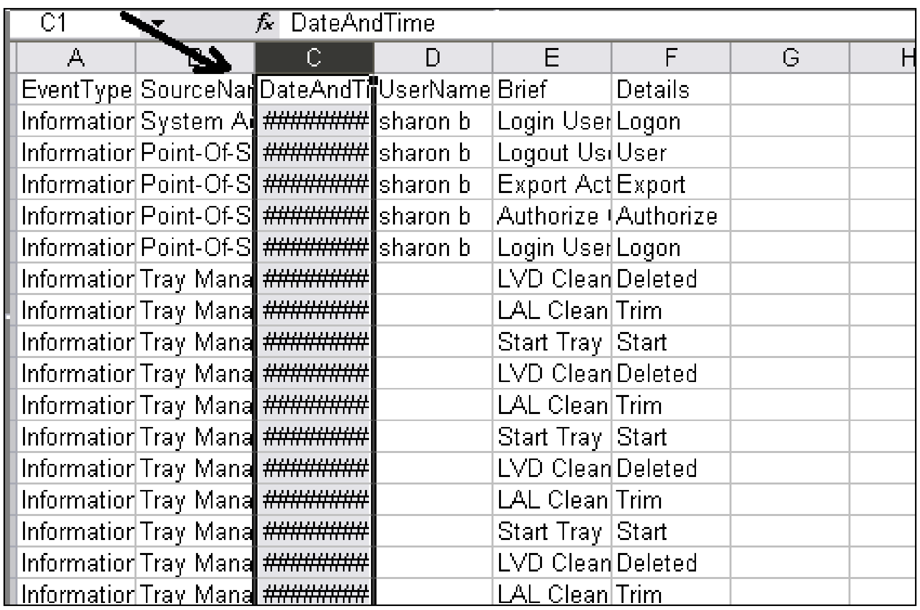
1. Select the event types, modules, and sources desired.
2. Enter the date range.

3. Click **'Print'**. A report preview screen is displayed. Click the printer icon at the top of the screen to print the log.

To export the Activity Log:

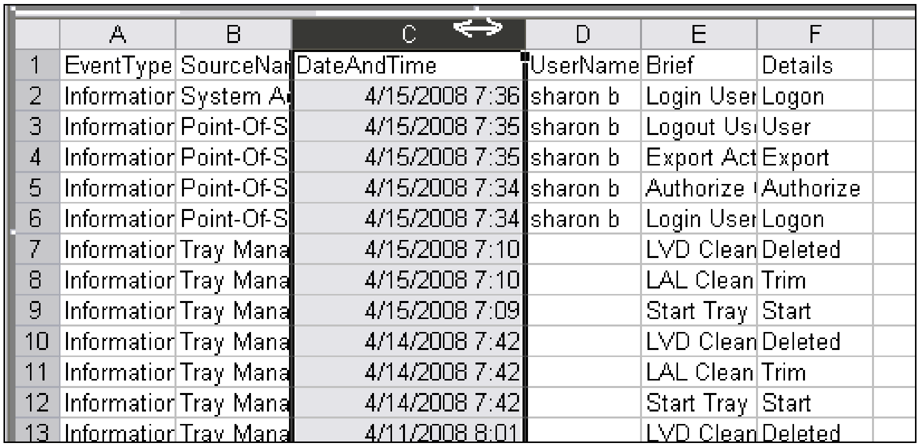
1. Select the event types, modules and sources desired.
2. Enter the date range.
3. Click the **'Export'** button.
4. Name and save the file on the hard drive. The file is saved in a .csv format which is Comma Separated Value and can be read by most spreadsheet software. This file can be sent to the Treasury OT C Support Center.

Note: When the audit log is exported, the date/time column may not display correctly, as pictured below in Figure 3.32.1. To correct the problem, adjust the column width in order to view all of the data (see Figure 3.32.2). Columns may also need to be formatted as general text fields for data to appear correctly. Consult your spreadsheet documentation for complete instruction.


C1 fx DateAndTime

A	B	C	D	E	F	G	H
EventType	SourceNar	DateAndTi	UserName	Brief	Details		
Informatior	System A	########	sharon b	Login User	Logon		
Informatior	Point-Of-S	########	sharon b	Logout Us	User		
Informatior	Point-Of-S	########	sharon b	Export Act	Export		
Informatior	Point-Of-S	########	sharon b	Authorize	Authorize		
Informatior	Point-Of-S	########	sharon b	Login User	Logon		
Informatior	Tray Mana	########		LVD Clean	Deleted		
Informatior	Tray Mana	########		LAL Clean	Trim		
Informatior	Tray Mana	########		Start Tray	Start		
Informatior	Tray Mana	########		LVD Clean	Deleted		
Informatior	Tray Mana	########		LAL Clean	Trim		
Informatior	Tray Mana	########		Start Tray	Start		
Informatior	Tray Mana	########		LVD Clean	Deleted		
Informatior	Tray Mana	########		LAL Clean	Trim		
Informatior	Tray Mana	########		Start Tray	Start		
Informatior	Tray Mana	########		LVD Clean	Deleted		
Informatior	Tray Mana	########		LAL Clean	Trim		

Figure 3.32.1



	A	B	C	D	E	F
1	EventType	SourceNar	DateAndTime	UserName	Brief	Details
2	Informatior	System A	4/15/2008 7:36	sharon b	Login User	Logon
3	Informatior	Point-Of-S	4/15/2008 7:35	sharon b	Logout Us	User
4	Informatior	Point-Of-S	4/15/2008 7:35	sharon b	Export Act	Export
5	Informatior	Point-Of-S	4/15/2008 7:34	sharon b	Authorize	Authorize
6	Informatior	Point-Of-S	4/15/2008 7:34	sharon b	Login User	Logon
7	Informatior	Tray Mana	4/15/2008 7:10		LVD Clean	Deleted
8	Informatior	Tray Mana	4/15/2008 7:10		LAL Clean	Trim
9	Informatior	Tray Mana	4/15/2008 7:09		Start Tray	Start
10	Informatior	Tray Mana	4/14/2008 7:42		LVD Clean	Deleted
11	Informatior	Tray Mana	4/14/2008 7:42		LAL Clean	Trim
12	Informatior	Tray Mana	4/14/2008 7:42		Start Tray	Start
13	Informatior	Tray Mana	4/11/2008 8:01		LVD Clean	Deleted

Figure 3.32.2

Batch Recovery
Authorized users are able to use this feature to recover items from a non-functioning PC to restore items to a backup PC. This would occur when a POS terminal unexpectedly fails prior to batches being transmitted.

Note: The backup or contingency PC must have the same secondary media or a compatible secondary media in order for the batch recovery to work. If the backup or contingency PC is being used to process batches, all batches must be closed and transmitted before using the PC for batch recovery. The primary computer and the contingency computer must both have the same version of the POS installed.

If the Secondary Image Storage fails while in the POS application, a batch recovery cannot be performed. Call the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com for assistance or refer to the *Troubleshooting* chapter of this User Manual.

To initiate a batch recovery and retrieve the unacknowledged, non-transmitted, or open batch from the secondary image storage of the failed PC, **do the following on the backup/contingency PC**:

1. Close all batches in process and exit the POS application.
2. Connect or insert the backup device (USB Flash drive, PCMCIA, zip, etc.) from the non-functioning PC to the backup PC. If the backup PC is only used as backup hardware, check the following:
   - Date and time are accurate.
   - Scanner is connected.
   - Printer driver is installed.
   - POS application version on the backup computer should be 5.4. Refer to the *Help* section in this chapter for instructions on how to display the computer's POS version number.
3. Launch the SAT application and enter the Login and Password. Make sure that the POS is closed before making the following changes.
4. Click **'File'**, then **'Configuration'** from the menu at the top of the screen. Write down or capture a screen print of the current configuration settings under all three tabs (General, Data Entry Screens and Tasks). If these settings need to be altered to accommodate the batch recovery procedure, they will need to be restored once the process is complete (step 19).
5. If the batch to be restored contains ALC+2's that are not currently on the backup PC, they need to be added. Click **'File'**, then **'Configuration'**, from the menu at the top of the screen. Click on the **'Data Entry Screens**' tab and add the ALC+2's as described in the *Data Entry Screens Tab* section of this chapter.
6. Click the 'Tasks' tab at the top of the screen. Click the down arrow in the 'Task Selection' field and click to choose 'Data Entry Screen Upgrade'. Click to add a check mark to the 'Start up' box just to the right of the 'Task Selection' field, then click the **'Apply'** button.
7. A window appears indicating that the changes may affect the POS and a restart to the POS may be necessary. Click the **'Ok'** button. Click **'Close'** to close the System Configuration window.
8. Logout of the SAT and Login to the POS.
9. The Data Entry Screen Upgrade window appears and the new Data Entry Screens are applied.

Note: Verify the configuration information is the same as the failed POS computer's information, if unsure call the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com for assistance.

Verify the secondary image storage drive is accurate by selecting the secondary image drive from Windows Explorer (USB Flash drive, PCMCIA, zip, etc.).
If necessary changes were made, select 'Apply' to apply the changes, and 'Close' to close the System Configuration screen.

10. Launch the POS application on the backup computer and enter the Login and Password.
11. Select **'File'**, then **'Configuration'** from the menu.
Click the **'Application'** tab to change the Terminal ID field, so it matches the non-functioning POS terminal. If unsure of this information contact the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com.
12. Select the correct cashflow as **'Mixed'** or **'Non Personal Only'**.
13. Select **'Apply'** to apply the change), and **'Close'** to close the Configuration window screen.
14. Logon to the SAT. Select the Batch Recovery Icon 

, or from the menu at the top of the screen, select **'File'**, then **'Batch Recovery…'**. The following message appears: (Figure 3.33)

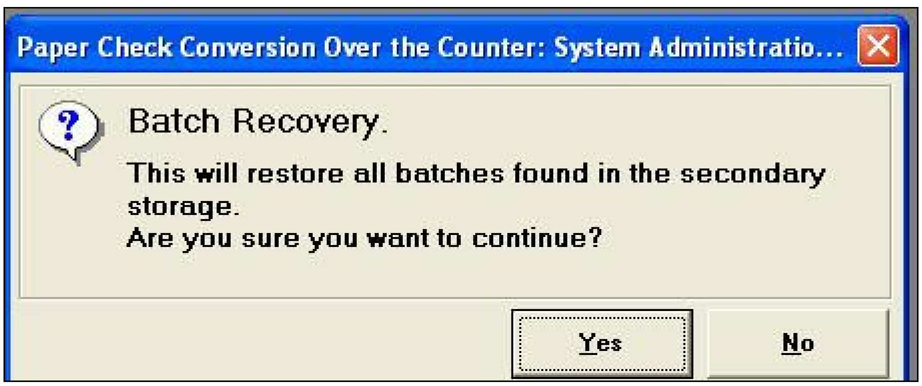


Figure 3.33

15. Click **'Yes'** to accept the batch recovery function. The following window appears and displays the percentage complete (Figure 3.34)

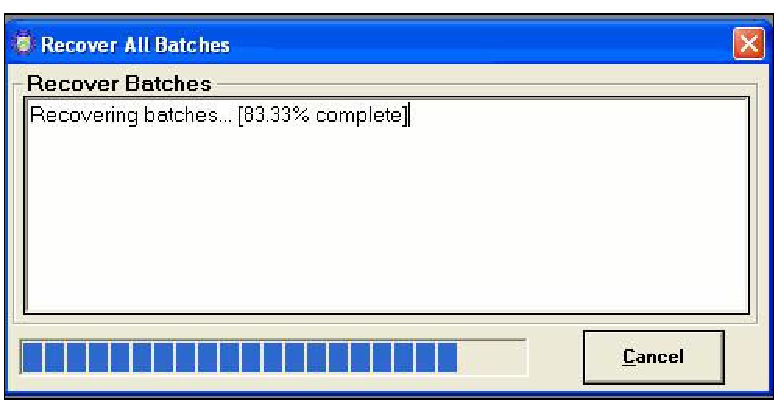


Figure 3.34

16. The following message appears when the batch recovery is complete. (Figure 3.35)

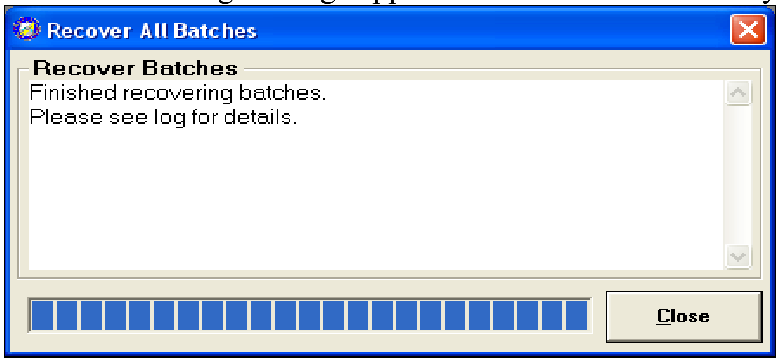


Figure 3.35

17. Check the SAT activity log to verify the batch recovery was successful. If it was unsuccessful, reseat (remove then replace) the backup device (if PCMCIA, zip or flash drive) and reselect Batch Recovery or call the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com.
18. Once complete, the cashier has an active batch list of items that were recovered. Select **'Close'** on the Batch Recovery screen. Follow the regular Batch Close process described in the *Daily Processing* chapter of this User Manual. Balance with item count and dollar amount before transmitting the batch.
19. Once the batch is closed and transmitted, use extreme caution to restore the previous POS terminal configuration to its original configuration prior to further batch processing. Use the information was recorded in step 4 (written or screen print) to restore back to the original configuration if the settings were altered.

Note: The person who created the batch must be added to the PC that is being used for batch recovery since batches are user-specific and only that user can close and transmit the batch. If the person who created the batch is not available, an authorized user can use Batch Manger to close and transmit the batch.

Local Verification Database (LVD) Reset

If an agency is utilizing the check verification process through the LVD download, there will be occasions where a new LVD is required. Daily LVD downloads contain only new items received by the MVD. If there is a change in the location's policy, or if the POS is re-deployed to a new location, an entire new LVD should be obtained and needs to be requested manually. Only people authorized to use the SAT are able to perform an LVD reset.

The LVD reset button erases everything on the LVD in anticipation for a full replacement with new data. **If the LVD reset is selected and a new LVD is not obtained, i.e., user forgets to download a new LVD, verification of checks presented does not occur.** To initiate an LVD reset, select the 'LVD Reset' 

icon from the main SAT screen, or click **'File'**, **'Reset LVD…'** from the menu at the top of the screen. The following window appears: (Figure 3.36)

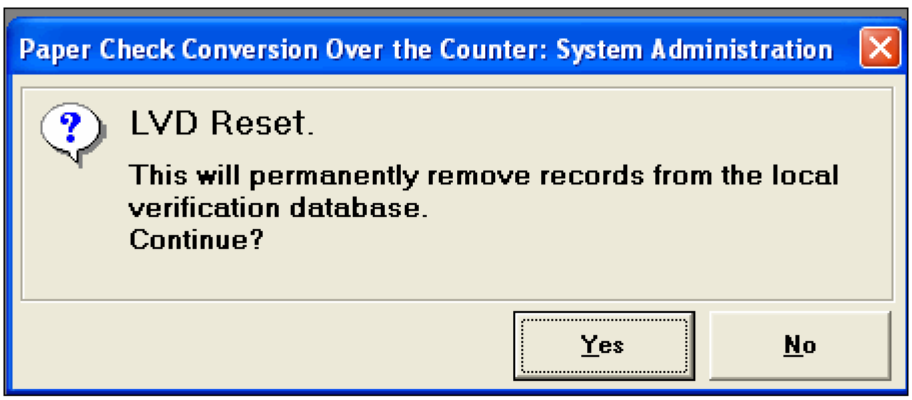


Figure 3.36

Click **'Yes'** to perform the LVD Reset. Click **'No'** to stop the process and return to the main SAT screen.

Additional information on the LVD is located in the 'Master Verification Database' section of the *ELVIS* chapter of the User Manual.

Help – About PCC OTC - SAT

The About 'PCC OTC – SAT' option under the Help menu within the SAT provides the PCC OTC SAT version information, as well as a link to the computer's system information.

1. Login to the SAT application.
2. Select **'Help'**, then **'About PCC OTC – System Administration…'**
3. The screen displays the version number for the SAT (circled). This information may be requested from the Treasury OTC Support Center for troubleshooting purposes.(Figure 3.37).

Figure 3.37

4. The Help window can also be used to obtain information pertaining to the computer. Click on the 'System Info' button to display information regarding the computer. (Figure 3.38)

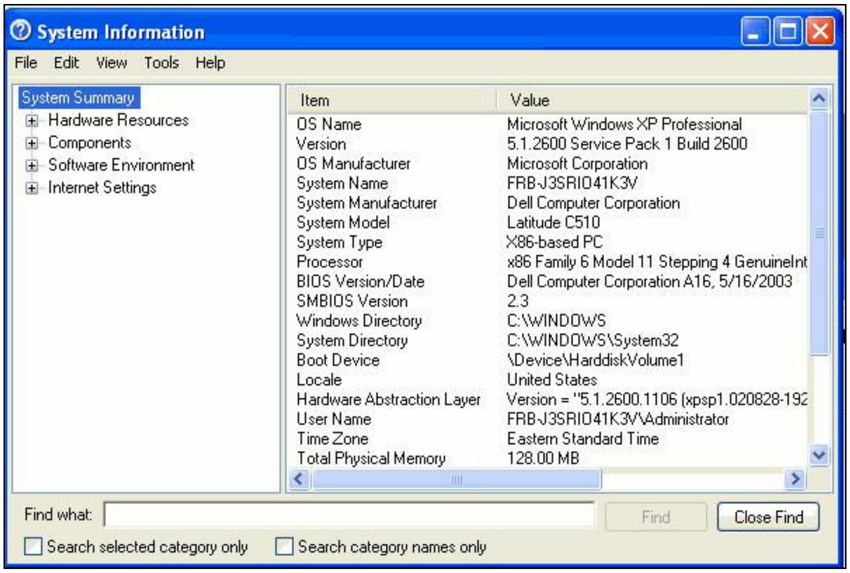


Figure 3.38

Help – other menu options

By clicking on 'Help' from the SAT menu, the system displays three choices; 'Contents', 'Index', or 'Search'.

- Contents – Displays a menu of in the left pane that includes a Welcome screen – Introduction to Batch Manager, the POS and the SAT as displayed below in Figure 3.39. System messages for each application can also be displayed by clicking in the appropriate area of the left pane. The right pane includes links for the Introduction sections, Tray Manager (an application that monitors all of the PCC OTC applications) messages, System Errors, and a table of navigational key strokes to assist in using the software. An example of POS Activity Log Messages is displayed in Figure 3.40.

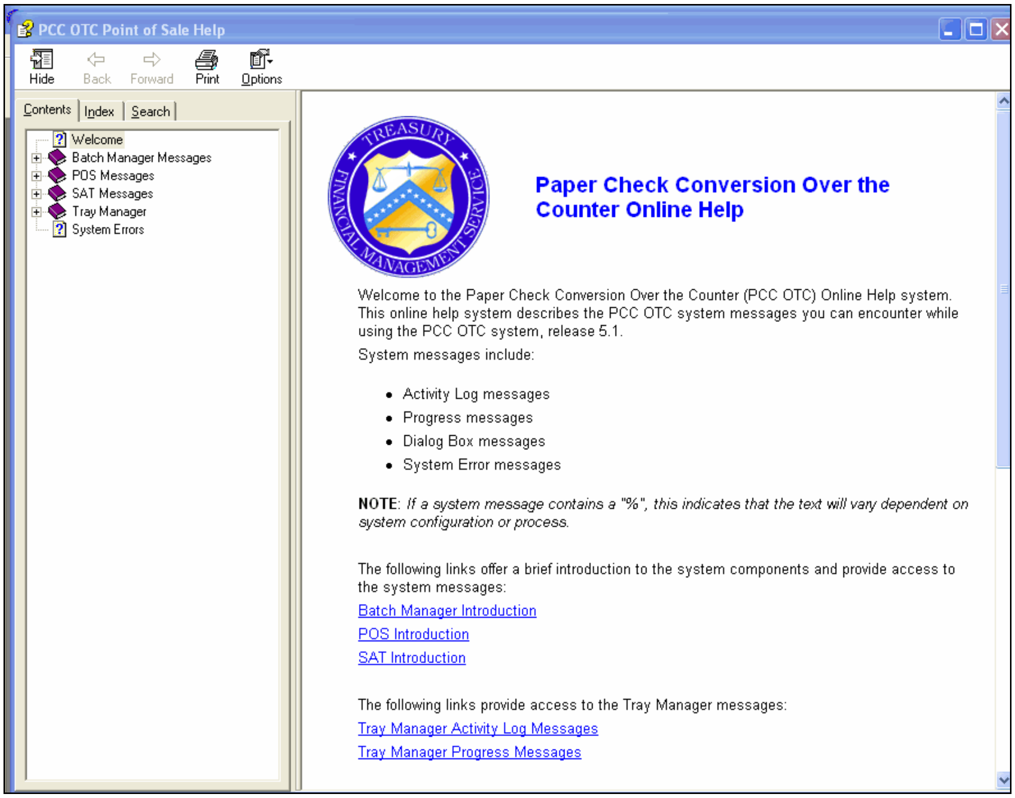


Figure 3.39

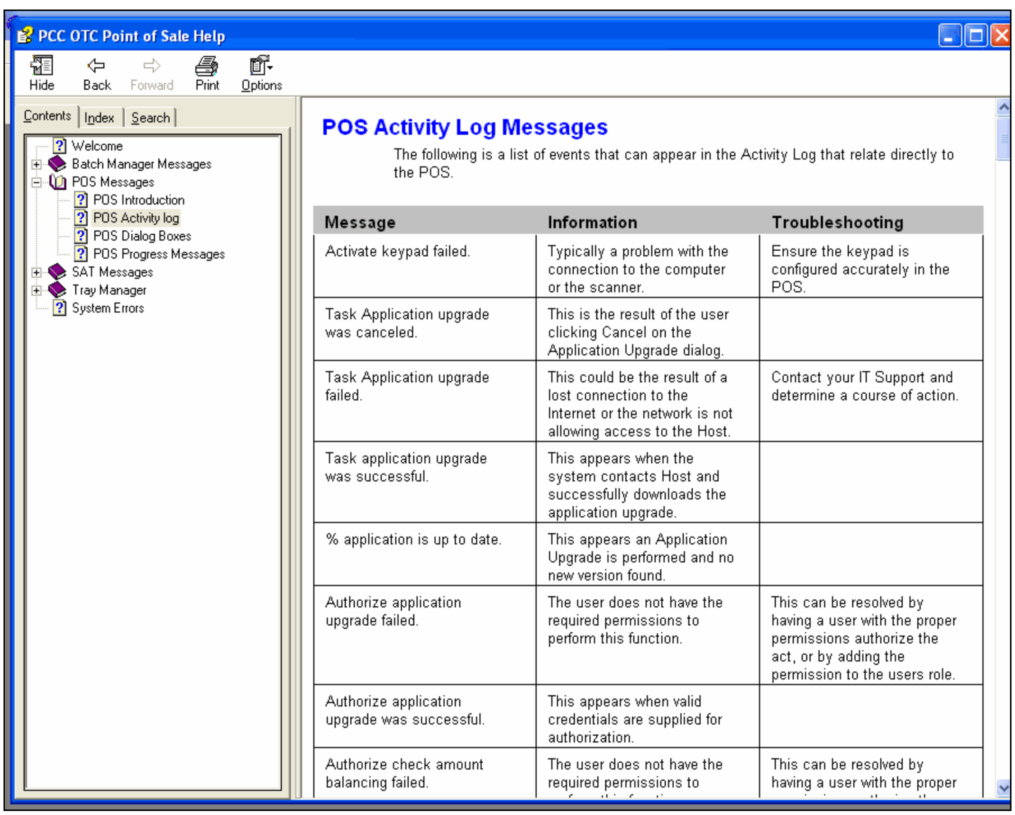


Figure 3.40

- Index – displays an alphabetical index of items on the left side of the screen and the user can click the 'Display' button at the bottom of the window on the left to display the contents of that subject in the window on the right side of the screen. (Figure 3.41)

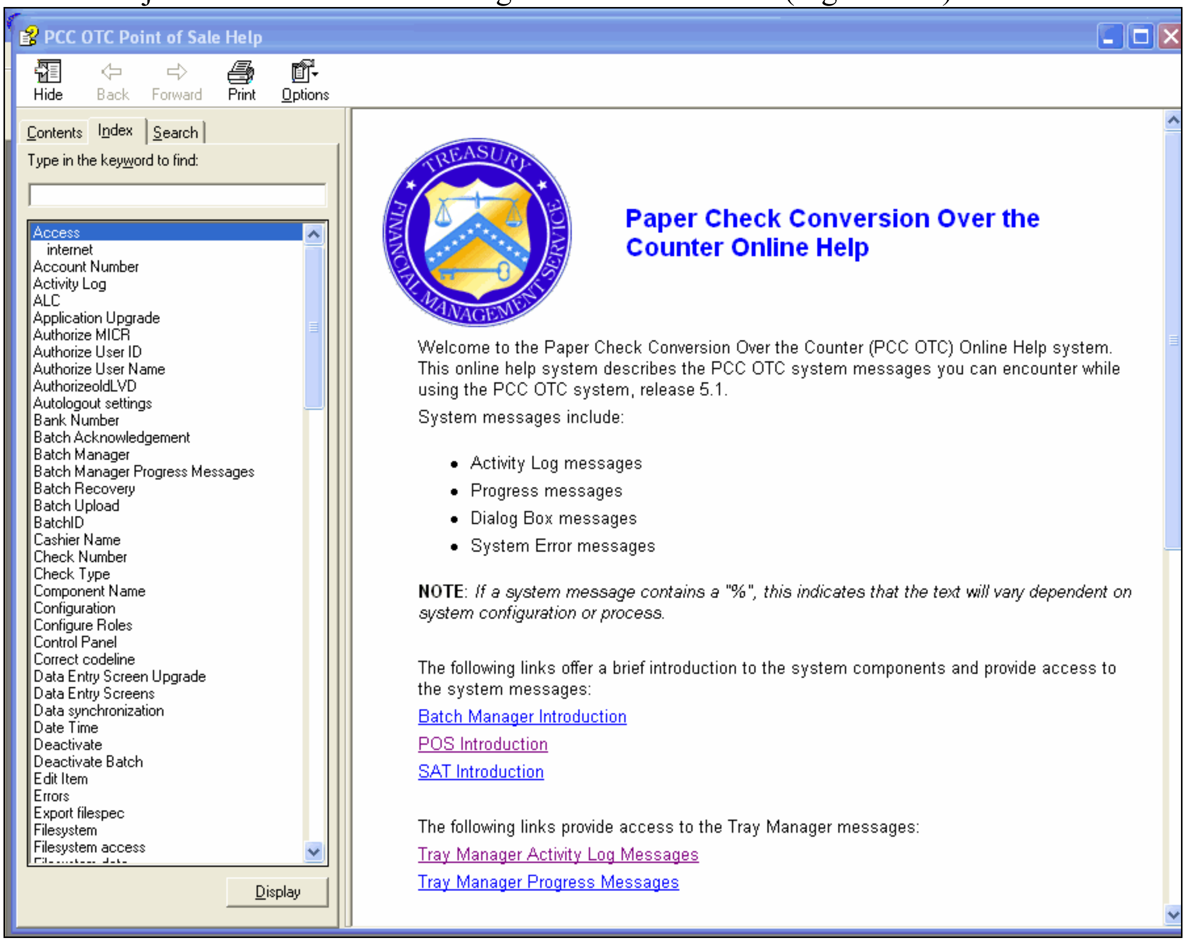


Figure 3.41

- Search – The search function allows the user to type a word or group of words to search for a specific error. An example of the results is displayed in Figure 3.42.

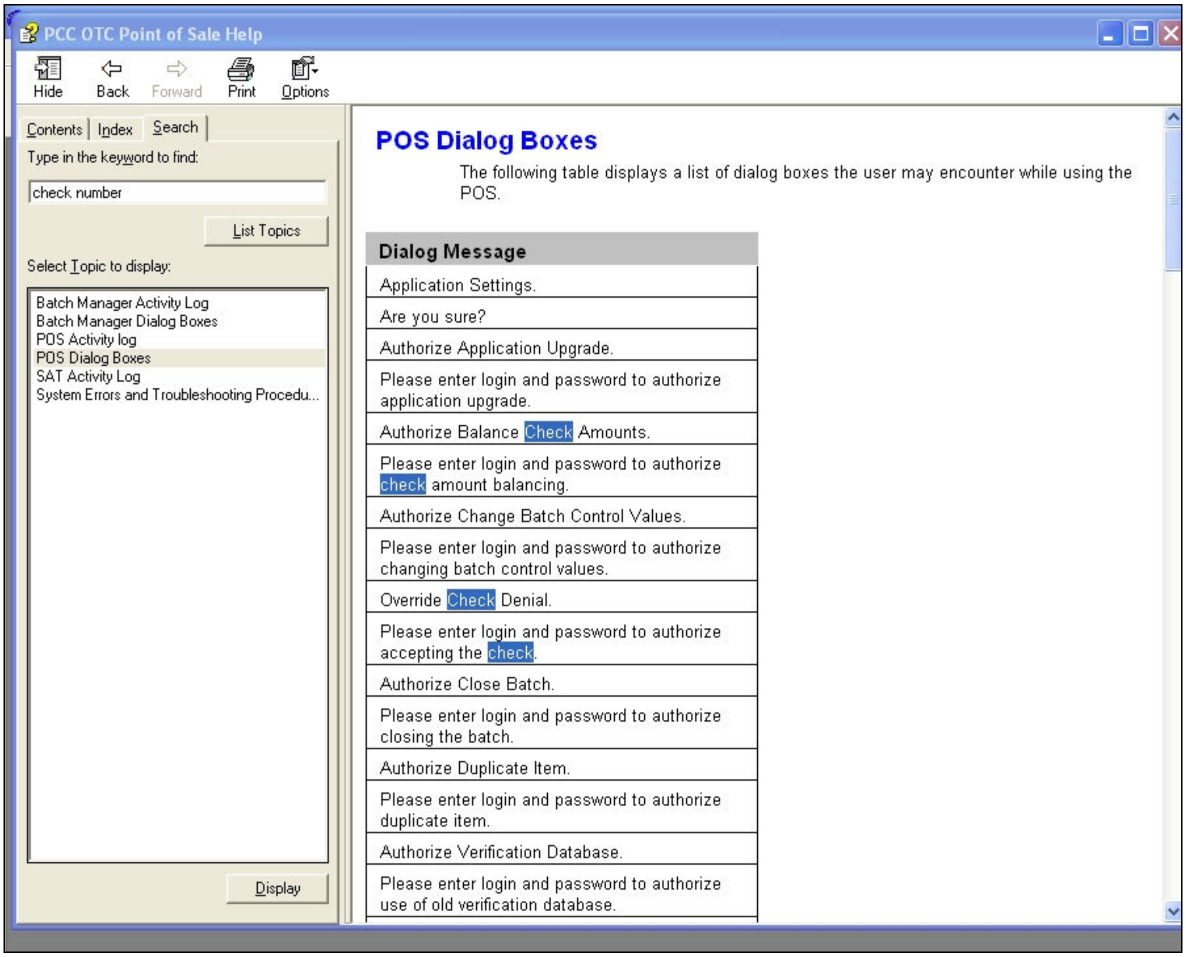
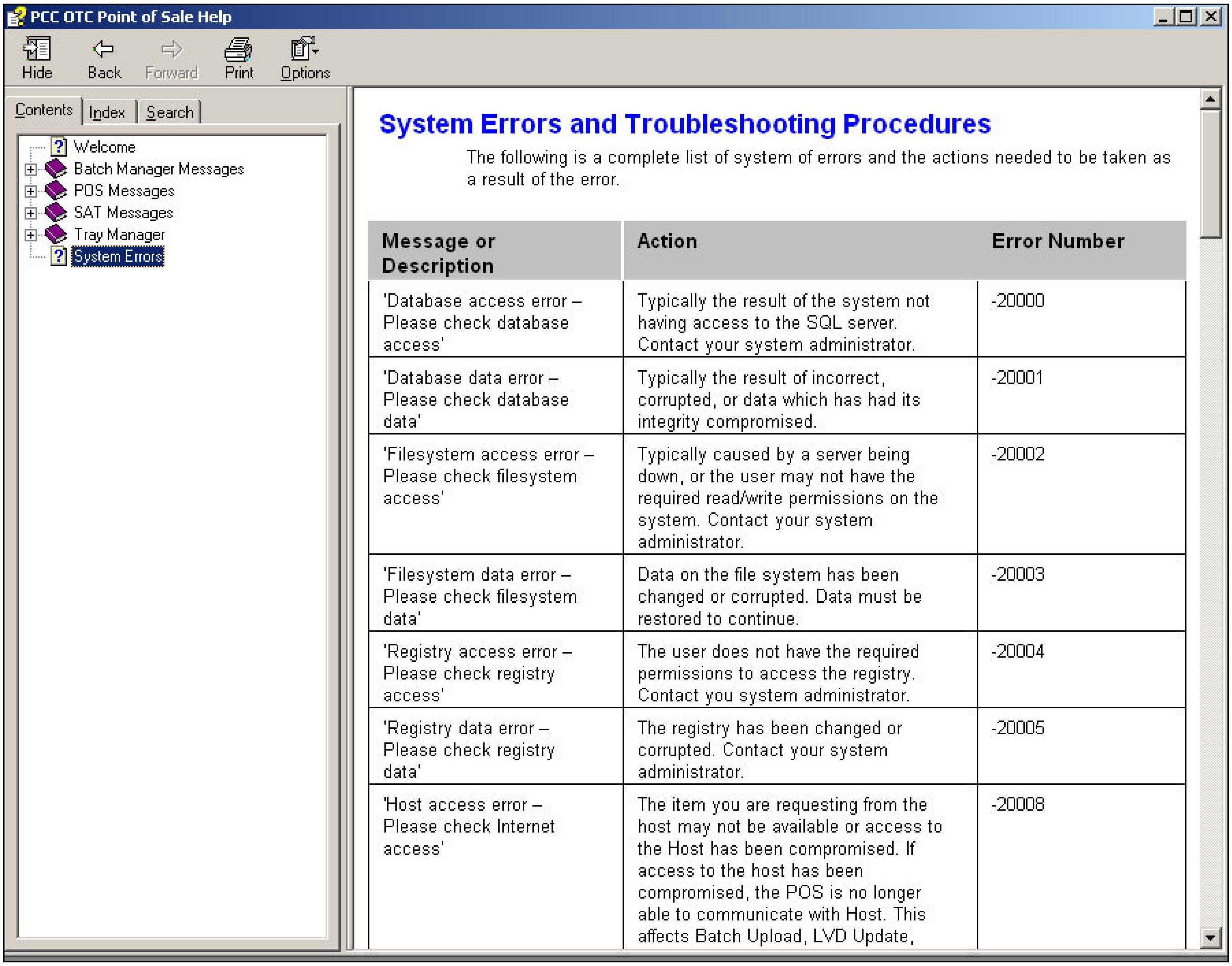


Figure 3.42

POS System Errors

Whenever an error is encountered while using the POS, the operator can check the ‘Help’ screens for an explanation of the error and the action to be taken. To access the System Error help:

1. Click ‘Help’ from the POS menu, then click ‘Contents’.
2. Click the last option in the left window called ‘System Errors’. The following screen appears (Figure 3.43)



System Errors and Troubleshooting Procedures

The following is a complete list of system of errors and the actions needed to be taken as a result of the error.

Message or Description	Action	Error Number
'Database access error – Please check database access'	Typically the result of the system not having access to the SQL server. Contact your system administrator.	-20000
'Database data error – Please check database data'	Typically the result of incorrect, corrupted, or data which has had its integrity compromised.	-20001
'Filesystem access error – Please check filesystem access'	Typically caused by a server being down, or the user may not have the required read/write permissions on the system. Contact your system administrator.	-20002
'Filesystem data error – Please check filesystem data'	Data on the file system has been changed or corrupted. Data must be restored to continue.	-20003
'Registry access error – Please check registry access'	The user does not have the required permissions to access the registry. Contact you system administrator.	-20004
'Registry data error – Please check registry data'	The registry has been changed or corrupted. Contact your system administrator.	-20005
'Host access error – Please check Internet access'	The item you are requesting from the host may not be available or access to the Host has been compromised. If access to the host has been compromised, the POS is no longer able to communicate with Host. This affects Batch Upload, LVD Update,	-20008

Figure 3.43

3. The error numbers appear in sequential order in the far right column. Scroll down to view all errors.