

User Security Reference

Version 4.0 Level U


Copyright 2005 - 2006

Rosebud Management Systems

User Security system overview

Access via Eden Client to Eden Server resources may be configured for individual users by using the Eden User Security system. This system is a CICS based transaction that uses a tabbed display to allow authorized users to manage Eden user login account information.

Access to the Eden User Security system is gained through the Eden Client toolbar button which will appear only when a signed in user has sufficient security, or when the client session is running on the physical Eden Server machine *and* the Windows session is running under an Administrator account.

The toolbar button will appear as follows: 

Note that in terms of the overall security features of Eden Server and Eden Client, the User Security system is but one of a number of features. Additional security features also include the Eden Server Firewall and Windows Authentication, as well as the configuration items on the EManager Security tab.

For information on the Eden Server Firewall and using Windows Authentication, please see the Eden Server Administrators guide.

For information on configuring the security requirements of an Eden CICS region, please see the EManager Reference, Security tab section.

For information on setting individual user rights, please see the remaining pages of this document.

Once access has been granted, the following tabbed display will appear, as shown below in figure 1.

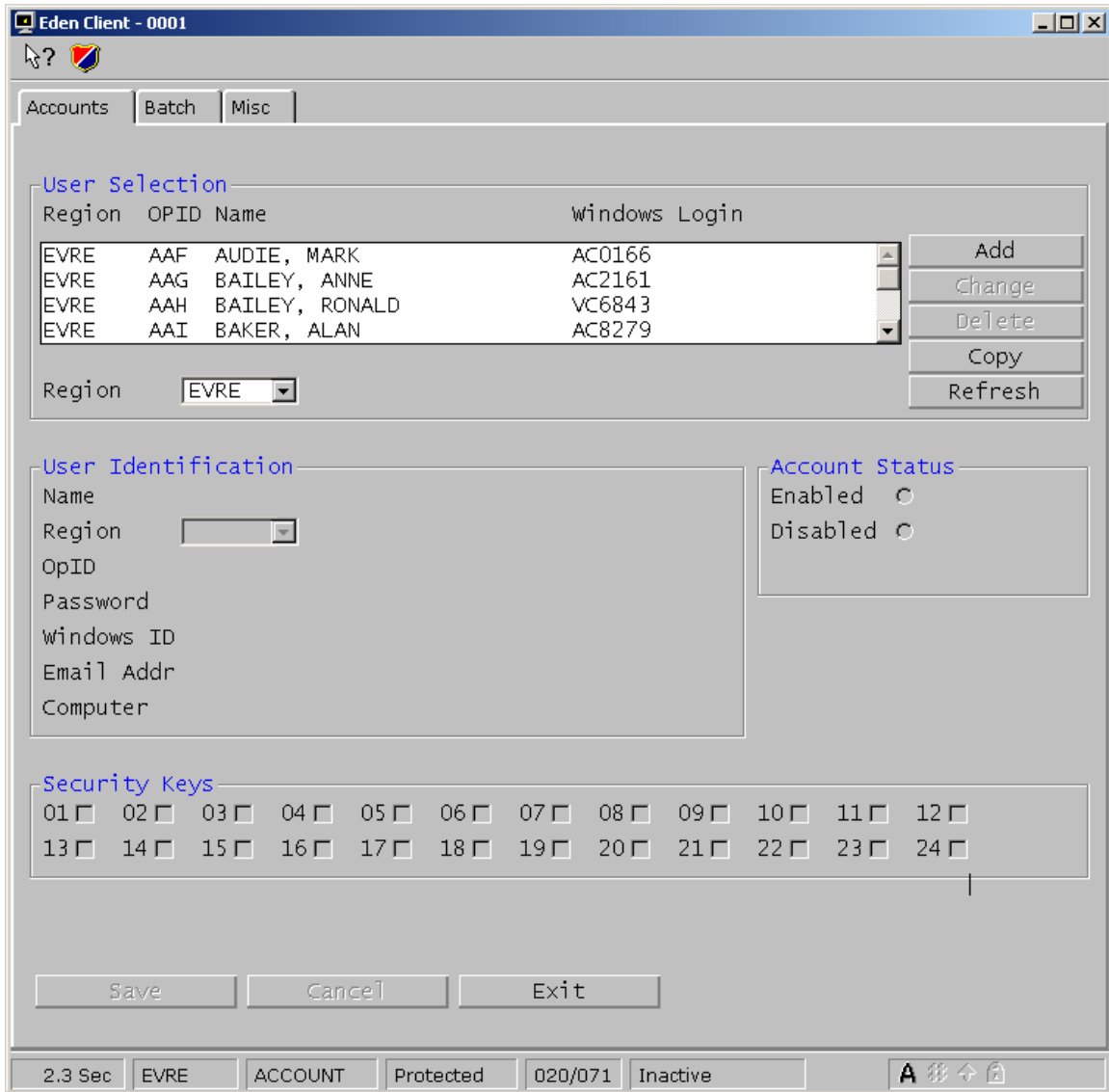


Figure 1 – Opening screen of User Security system

The display above is a typical User Security screen, showing the list of defined users in the User Selection area. Note that the list of users displayed will always start by including only those users that are defined in the region in which the User Security feature is being accessed. In this case, the system is attached to the EVRE region and therefore the displayed list includes only user accounts that are defined in the EVRE region.

Note that the 'Region' drop down list, in the User Selection area, will include all

regions for which the currently logged on Eden user has authority to access the User Security system. Also, in the event the User Security system is being run on the physical Eden Server machine, by a Windows Administrator this drop down list will include all known regions.

Administering User Accounts

New User Accounts may be added by using the 'Add' button, which is always enabled. To add a new account, click the Add button and the display will be enabled for data input.

Existing User Accounts may be changed by first selecting the account in the displayed list of users and then clicking the 'Change' button. Note that the Change button is only enabled and click-able when a user in the list is selected and no other change is already in progress.

Existing User Accounts may be deleted by first selecting the account in the displayed list of users and then clicking the 'Delete' button. Note that the Delete button is only enabled and click-able when a user in the list is selected and no other operation is already in progress.

Existing User Accounts may be copied from region to region by using the 'Copy' button. Accounts may be copied either en mass, i.e., all accounts for the region will be copied, or only a single selected account will be copied. To copy all accounts from one region to another simply click the Copy button. The displayed Copy dialog will allow all User Accounts to be copied. To copy only one User Account, first select the account from the displayed list and then click the Copy button.

To refresh the list of displayed User Accounts, either after an Add, Change, Delete or Copy has completed, or after selecting a new region from the Region drop down list, use the Refresh button.

User Account information and settings

The Accounts tab of the User Security system allows for the entry and changing of the following items. A sample change operation is shown below.

The screenshot shows a window titled "Eden Client - 0001" with a menu bar containing "Accounts", "Batch", "Miscellaneous", and "Access Times". The "Accounts" tab is active. The window is divided into several sections:

- User Selection:** A table with columns "OPID", "Region Name", and "Windows Login". The first row is selected and contains "EHS", "SHSA", "ETHAN SCHULTZ", and "ADMINISTRATOR". To the right of the table are buttons for "Add", "Change", "Delete", "Copy", and "Refresh". Below the table is a "Region" dropdown menu set to "SHSA".
- User Identification:** A form with fields for "Name" (ETHAN SCHULTZ), "Region" (SHSA), "OpID" (EHS), "Password" (masked with asterisks), "Windows ID" (ADMINISTRATOR), "Email Addr", and "Computer".
- Account Status:** Two radio buttons: "Enabled" (selected) and "Disabled".
- Security Keys:** A grid of 24 checkboxes, numbered 01 to 24, all of which are checked.
- Buttons:** "Save", "Cancel", and "Exit" buttons are located at the bottom of the main form area.
- Status Bar:** At the bottom of the window, there is a status bar with fields for "0.6 Sec", "SHSA", "ACCOUNT", "009/012", "Inactive", and a user icon labeled "a #".

Sample Change screen

The items that may be set during an Add or Change operation their uses and descriptions are as follows:

Name

The Name field may be used to record the users actual name. The contents entered here are for documentary purposes only and do not affect any system processing except that if the EManager Security tab 'CICS UserID' settings are set to 'Eden Name', the value entered here will be returned when this user is signed on and their application calls the EXEC CICS ASSIGN USERID api.

Region

The Region drop down list, when in Add mode, will contain all the region names the signed on user is able to access. When Adding a new user, select the appropriate region name from the list. When Changing an existing User Account, the Region Drop down will be protected and may not be changed. If it is desired to copy a User Account from one region to another, use the Copy button.

OPID

The OPID field, which is protected except while adding new users, contains the three character operator ID code used by the user to login to Eden.

Password

The password field will display all '*' characters during an update to hide the existing value of the field, however, the password field may be overtyped to change the users password if desired. Note, be sure to clear the password field completely before attempting to change the entered value. Passwords may not include the '*' character. The values for valid passwords are based upon the EManager defined minimum and maximum length as well as the minimum alphabetic and numeric content rules. Invalid passwords will be flagged as such and an appropriate error message displayed.

Note also that changes to passwords made here are not subject to the previous password history rules as defined in EManager. The passwords entered or changed here are automatically set as expired, thus requiring the user to change it immediately upon sign on.

Windows ID

The Windows ID field is used to record the user name this person logs into Windows with. The name entered is used as an alternate key to the security file and is used during single sign-on processing as described above. Note that if the 'CICS UserID' settings are set to 'Windows Name', the value entered here will be returned when this user is signed on and their application calls the EXEC CICS ASSIGN USERID api.

Computer

If a value is entered in the Computer field, Eden will restrict access to this user unless they are logging in from the specified computer.

Email

If the Lost Password feature is enabled for the region, the users email address must be entered in the Email field. This field has no other purpose than it's use in conjunction with the Lost Password feature.

Account Status

The Account Status radio buttons may be used to enable or disable a user account. Additionally, if a User Account is disabled, a brief message will be displayed directly below the radio buttons indicating whether the account was manually disabled, or if it was disabled due to excessive password violations.

Security Keys

The 24 switches available correspond to the security keys that may be entered along with program names in the System Configuration field as described above. The 24 values that may be turned on or off by selecting the check-box buttons, are also used to form the 24 bit value returned to application programs via use of the ASSIGN OPSECURITY CICS API call. The values selected for security keys are also used throughout the Eden JOBS system which controls access to the batch facilities of Eden Server. These same security keys may also be used to control access to individual CICS transactions as well.

Access to the Eden JOBS Administration system is controlled by , in addition to being controlled through the use of the Security keys the security key settings here. In order for a user to have access to the JOBS Administration system, their account information must have that security selected which match the security key defined as the JOBS Administration access key in EManager for the user's sign-on region.

Access to the Eden User Security system, unless signing in directly from the physical Eden Server machine is also controlled by the security key settings here. In order for a user to have access to the User Security system, their account

information must have that security selected which match the security key defined as the User Security access key in EManager for the user's sign-on region.

Batch System Access

Batch System access

Access to all user functions of the Eden Server Batch System available through the JOBS system is controlled by the settings on the Batch tab of the User Security system. A sample of these settings is shown below.

The screenshot shows a window titled "Edens Client - 0001" with a "Batch" tab selected. The window is divided into two main sections: "Job Queue Access" and "Print Queue Access".

Job Queue Access:

- Execution Classes: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Full Control Classes: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- View Only Classes: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Accessible Job Types:
 - Owned Jobs Only:
 - System Jobs:

Print Queue Access:

- Full Control Classes: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- View Only Classes: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Accessible Job Types:
 - Owned Jobs Only:
 - System Jobs:

At the bottom of the dialog are "Save", "Cancel", and "Exit" buttons. The status bar at the bottom shows: 0.4 Sec, SHSA, BATCH, Enhanced, 004/072, Inactive, and a user icon.

Job and Print Queue Access

Note the tab is divided into two main areas; Job Queue Access and Print Queue Access. The Job Queue Access areas are used to control the users ability to submit jobs, alter the settings of already submitted jobs and which jobs the user can access in only a view-only mode. access The items shown here control the following access privileges to the Eden Job Queue:

Execution Classes

The Execution Classes settings control which PID classes a user may submit jobs to. Entries should be made for each of the up to 26 classes (A through Z) for which the user is to be allowed to run jobs in.

Full Control Classes

The Control Classes settings control which Job Queue entries a user may change settings for. If a user has 'control' authority for a PID class then they will be able to change the settings for a job, such as changing the schedule and or other job settings.

View Only Classes

The View Classes settings control which Job Queue entries a user may view job logs for. Entries should be made for each of the up to 26 classes (A through Z) for which the user is to be allowed to view job logs for.

Owned Jobs only

The Owned Jobs only settings causes the users security settings to be such that they will only be able to access jobs in the Job Queue which they personally own. Note, this setting has no effect on which jobs a user may submit, only which jobs they may access that are already submitted.

System Jobs

The System Jobs access check box controls whether the user will be able to submit jobs to and access jobs that are in the 'SYSTEM' job queue area. Note the 'system' job queue area is not a special or separate job queue. Instead 'system' is simply a reserved Eden Server region name.

Print Queue Access

Access to the Eden Print Queue is controlled by the entries made in the Print Queue access area. No access to the Print Queue for any purpose is allowed without a user account having at least one entry in the Print Queue Access area.

View Only Classes

The View Classes settings control which Print Queue entries a user may view and print. Entries should be made for each of the up to 26 classes (A through Z) for which the user is to be allowed to view and print.

Ctrl Classes

Full Control Classes

The Full Control Classes settings control which Print Queue entries a user may change settings for, and or delete.

Owned Jobs only

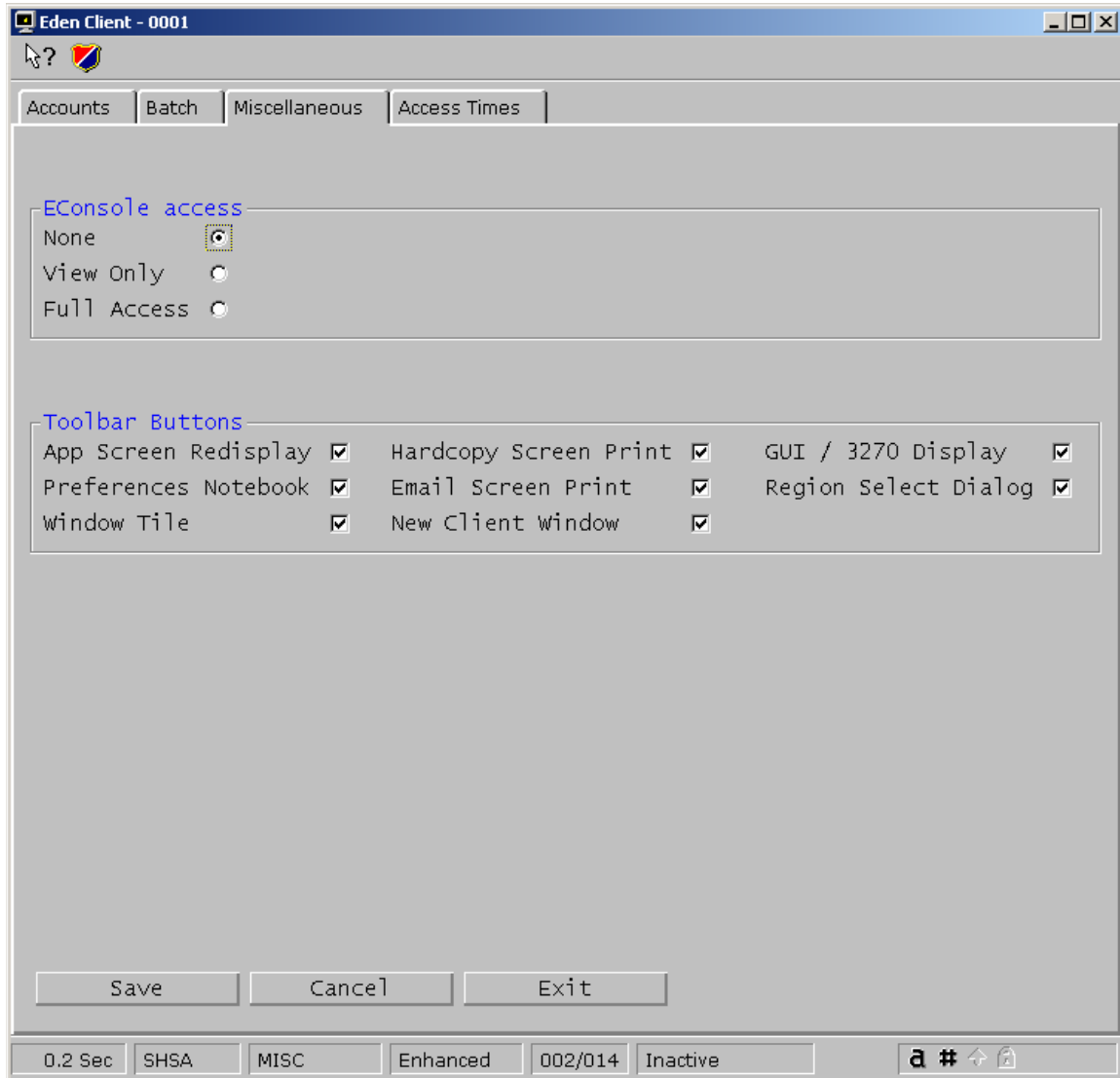
The Owned Jobs only settings causes the users security settings to be such that they will only be able to access print queue entries which they personally own.

System Job access

The System Job access check box controls whether the user will be access print queue entries that are in the 'SYSTEM' print queue area. Note the 'system' print queue area is not a special or separate print queue. Instead 'system' is simply a reserved Eden Server region name.

EConsole and Client Toolbar Access

Access to the Eden Remote Console feature, EConsole, as well as configuration of available buttons on this users Eden Client toolbar may be performed using the controls on the Miscellaneous tab, as shown below.



Users for whom EConsole access is desired should have either the View Only or Full Access radio buttons selected in the EConsole access area. The default setting for a user account is 'None'. Users whose setting is for 'View Only' will be able to view any item in the EConsole window, including system configuration notebooks and all standard monitor windows. Such View Only users will also be able to scroll and search the text in the System Log Window, however, View Only users may not submit System Log commands, nor can they save (Ok or Apply) settings on any of EConsole's system notebooks.



Users whose EConsole setting is 'Full Access' may perform all functions available to View Only users, and additionally they may submit console commands as well as update configuration settings in any EConsole notebook. It is important to note that Full Access users not only have full control over Eden Server, but should also be considered to have Full Access over the entire Windows Operating System of the Eden Server machine. This is because the Eden Server System Log window may be used as a system command prompt, which unless special security measures are taken over the Eden Server Windows Login account, will typically have Administrator Rights to the machine.


Note that in addition to specifying some level of EConsole Access for a user here, the Eden Server machine must also be configured to allow EConsole Access, as well as the specific IP addresses from which EConsole Access may be granted. See the Eden Server Administrators guide for complete information on setting up the Eden Server side access from EConsole.



Toolbar Settings


For those installations that do not wish to allow Eden Client users to have a full compliment of Client Toolbar buttons, these controls allow specific buttons to be enabled or disabled on a per user account basis. Note, however, that the EManager Security tab setting for 'Default Toolbar', if selected, will override a specific user account setting that is disabled. Therefore, to effectively manage which toolbar buttons a user may access, the EManager 'As Per Security' setting must be made in the Toolbar settings of the Security tab.


The settings available, and the toolbar buttons they control are as follows:


App Screen Redisplay, when selected, causes the client window redisplay buttons   to be included in the toolbar.


Hardcopy Screen Print, when selected, causes the Print Window button  to be included in the toolbar.


GUI / 3270 Display, when selected, causes the display mode change button  and  to be included in the toolbar.

Preferences Notebook, when selected, causes the User Preferences notebook button  to be included in the toolbar.

Email Screen Print, when selected, causes the Email button  to be included in the toolbar.

Region Select Dialog, when selected, causes the region selection button  to be included in the toolbar.

Window Tile, when selected, causes the client window tile button  to be included in the toolbar.

New Client Window, when selected, causes the Start-a-new-client button  to be included in the toolbar.

Limited Access dates and times

The controls on the Access Times tab allow a user account to be limited in the days of the week and times of day during which login to an Eden Server region is allowed. Access may be granted on a day-by-day basis in 30 minute intervals.

| | 12P | 3A | 6A | 9A | 12A | 3P | 6P | 9P | |
|-----------|-----|----|----|------------------|--------|----|----|----|---------------|
| Sunday | | | | | | | | | |
| Monday | | | | YYYYYYYYYYYYYYYY | | | | | 09:00A-05:00P |
| Tuesday | | | | YYYYYYYYYYYYYYYY | | | | | 09:00A-05:00P |
| Wednesday | | | | YYYYYYYYYYYYYYYY | | | | | 09:00A-05:00P |
| Thursday | | | | YYYYYYYYYYYYYYYY | | | | | 09:00A-05:00P |
| Friday | | | | YYYYYY | YYYYYY | | | | 09:00A-05:00P |
| Saturday | | | | | | | | | |

No Access Before No Access After

Save Cancel Exit

0.2 Sec SHSA TIMES Protected 021/076 Inactive A # ↕ 🔒

Daily Access Times

The daily access times area allows for each day of the week to be set for limited, full or no access. Leaving all fields in this area blank is the default setting, which grants access at any time. Making at least one entry will limit the accounts access time to the entry(s) made. For example, in the above sample display, the user account is limited to Monday through Friday from 9:00 am to 5:00 pm, with no access at all on Saturday or Sunday.

Making entries in the 'per-day' fields may be accomplished in one of two ways.

First, access times may be entered directly in the space provided to the right. Times may be entered as full times, i.e., 09:00a, or as simple times, i.e., 9a. Note that all times entered are rounded to the nearest 30 minute interval. For example entering 9:15 will be rounded up to 9:30.

Second, the time scale field may be set to contain 'Y' for each 30 minute period the account is allowed access. The time scale field is 48 characters long, with each character representing one 30 minute period of the day. The first position of the scale represents from midnight through 12:30 am, the next position represents from 12:30 am through 1:00 am, and so on. Note that when using the time scale field to enter allowed times, it is possible to define more than 1 access period. For example, the above display allows the user access on Friday from 9:00 am until noon, and then again from 1:00 pm through 5:00 pm.

Limited Access Period

In addition to allowing access on a day-of-the-week and time-of-day basis, the Limited Access Period controls can be used to define the beginning and ending dates that a user can access Eden. For example, if a consultant or temporary worker is to work only for a short duration – for example from January through May, enter a '01/01/2006' date in the 'No Access Before' field, and a '05/31/2006' date in the 'No Access After' field. In this case the user would only be able to access Eden during January through May of 2006.

Note that regardless of which type of access limits are imposed – time-of-day or not-before / not-after dates, Eden Server will perform access checking at login time, and if required, Eden Server will automatically remove the user from the system when their time expires. Note that a warning message is sent to the user 2 minutes prior to them being disconnected.