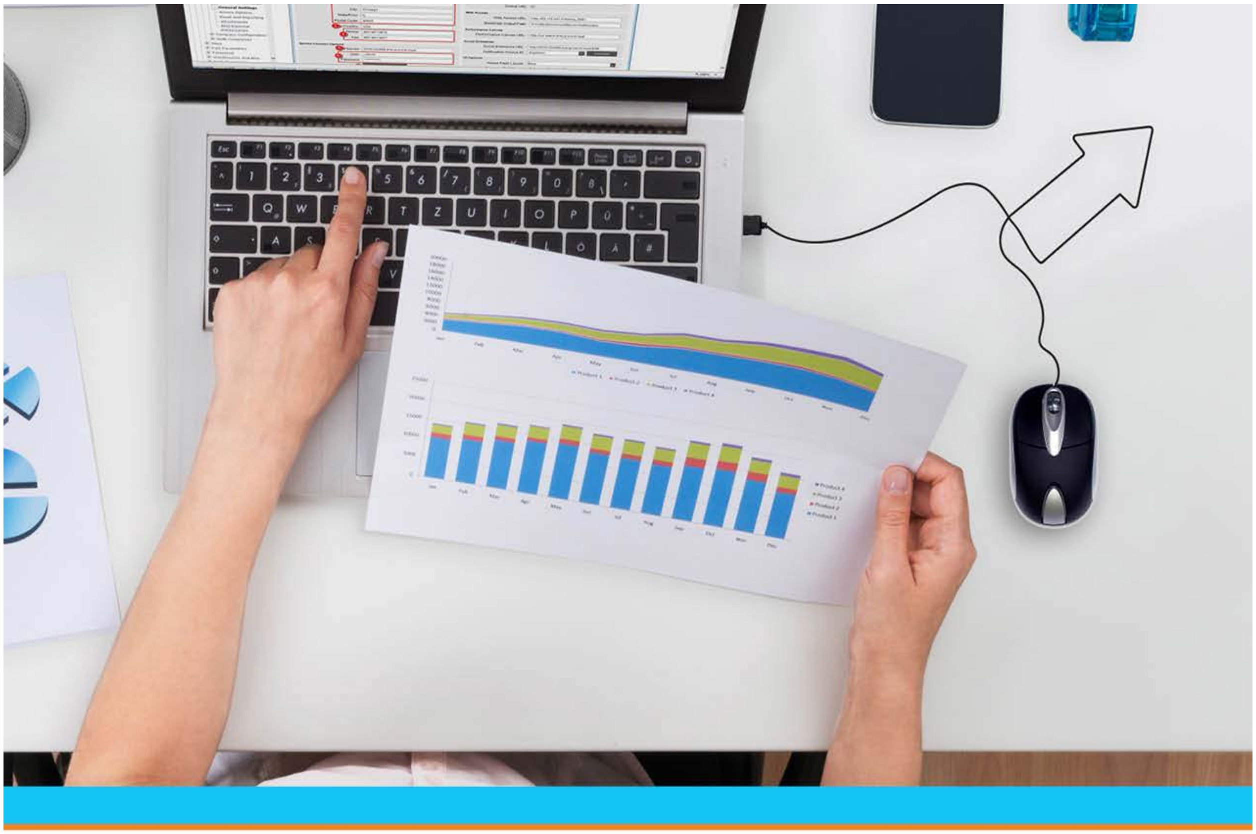

Solar Eclipse Phantoms, Reports, and System Maintenance Authorization Keys

Release 9.0.5

Disclaimer

This document is for informational purposes only and is subject to change without notice. This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication. However, Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims any applicable implied warranties, such as fitness for a particular purpose, merchantability, satisfactory quality or reasonable skill and care. As each user of Epicor software is likely to be unique in their requirements in the use of such software and their business processes, users of this document are always advised to discuss the content of this document with their Epicor account manager. All information contained herein is subject to change without notice and changes to this document since printing and other important information about the software product are made or published in release notes, and you are urged to obtain the current release notes for the software product. We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice. The usage of any Epicor software shall be pursuant to an Epicor end user license agreement and the performance of any consulting services by Epicor personnel shall be pursuant to Epicor's standard services terms and conditions. Usage of the solution(s) described in this document with other Epicor software or third party products may require the purchase of licenses for such other products. Where any software is expressed to be compliant with local laws or requirements in this document, such compliance is not a warranty and is based solely on Epicor's current understanding of such laws and requirements. All laws and requirements are subject to varying interpretations as well as to change and accordingly Epicor cannot guarantee that the software will be compliant and up to date with such changes. All statements of platform and product compatibility in this document shall be considered individually in relation to the products referred to in the relevant statement, i.e., where any Epicor software is stated to be compatible with one product and also stated to be compatible with another product, it should not be interpreted that such Epicor software is compatible with both of the products running at the same time on the same platform or environment. Additionally platform or product compatibility may require the application of Epicor or third-party updates, patches and/or service packs and Epicor has no responsibility for compatibility issues which may be caused by updates, patches and/or service packs released by third parties after the date of publication of this document. Epicor® is a registered trademark and/or trademark of Epicor Software Corporation in the United States, certain other countries and/or the EU. All other trademarks mentioned are the property of their respective owners.

Publication Date: October 22, 2018

Table of Contents

Authorization Keys Overview

Authorization keys define users' permissions. To grant permissions, you need to assign authorization keys to users in their user records. Some keys have multiple levels of authority associated with them. For example, AP.ALLOWED authorizes a user to access A/P Entry in view-only mode if set to level 1 and in edit mode if set to level 2. In most cases, each higher level inherits the previous level's functions.

You can assign authorization keys to templates that correspond with job descriptions. Assigning a template to a user is a quick and consistent way to assign all the authorization keys required for a particular job. For example, templates for purchasing, sales, and counter personnel contain all the authorization keys needed to perform those functions.

- Any authorization key assigned in addition to a template containing the same key overrides the setting of the key in the template.
- The setting in the **Template Authorization Key Level Hierarchy** control maintenance record determines which level the system applies when the same authorization key with different levels appears in multiple templates assigned to the same user.

The SUPERUSER authorization key located at the bottom of the list of available keys assigns the highest level of all authorizations to a user. A superuser can perform all system functions. Only the system administrator should have this authorization.

The authorization key descriptions in this help project are grouped by functional areas, such as accounting, inventory, and order entry. To locate the description of a designated authorization key, search the help project using the key name.

Superuser Authorization

Assign the SUPERUSER authorization key to users who require access to every function with maximum privilege. System managers, their superiors, company owners, and Eclipse personnel can use this authorization key.

SUPERUSER

Allows the access granted by all the authorization keys at the highest level of authorization. More.

Job Roles	Administrators and Managers.
Levels	None. Check **Important** note below.
Dependencies	None. Check **Important** note below.
Additional Information	Any authorization key assigned in addition to the SUPERUSER key overrides the SUPERUSER level of authorization for that key.
	Users assigned a lower-level authorization key authority are restricted to that authorization key. This allows users full access to the system, but be restricted to certain areas, if needed, such as overriding replacement product descriptions with OE.PRODUCT.DESC.OVRD.
	To test a system function with a lower level of authority, superusers can override their default level of authorization for a designated authorization key. To do this, assign the designated key (in addition to the SUPERUSER key) with the override level or the related detail information that restricts the user's actions.

Important

Superuser authorization *does not include* several authorization keys. These authorization keys limit a user's access and require that you enter additional detail information when you assign them, therefore they are not included in SUPERUSER access.

Authorization Key	When this key is not assigned...
GL.ACCOUNTS	the user can access all G/L accounts.
INVALID.PRODUCT.LINES	no product lines are invalid.
INVALID.VEN.TYPES	no vendor types are invalid. The user can access all vendor types.
MESSAGE.GROUP.TYPES	the user can access all message group types.
POE.SCHEDULE	the system does not set the **Auto Scheduling** option on the POE Body window to a default value.
SOE.CREDIT.REL.RANK	the user can release orders for any customer, based on the user's level assignment in the SOE.CREDIT.RELEASE authorization key.
SOE.SCHEDULE	the system does not set the **Auto Scheduling** option on the SOE Body window to a default value.
TOE.SCHEDULE	the system does not set the **Auto Scheduling** option on the TOE Body window to a default value.
VALID.BLINES	all buy lines are valid. The user can edit product records in all buy lines.
VALID.PLINES	all price lines are valid. The user can edit product records in all price lines.
VALID.PRODUCT.LINES	all product lines are valid.
VALID.VEN.TYPES	all vendor types are valid. The user can access all vendor types.
WIN.DIRECT.CREATE.DIR	the user cannot export a report from the system using the Windows Direct Options program.

New and Revised Authorization Keys for this Release

For each Eclipse release, the documentation provides a table listing all authorization keys that have been revised or added to the system since the last release.

For a list of the new and revised authorization keys, see the Feature Summary documentation.

Creating User-Defined Authorization Keys

For some Eclipse applications, you can create user-defined authorization keys. After creating the key, you need to assign it to the designated application and to users to control their access to that application.

For example, in Product Data Warehouse, you can create a user-defined authorization key that controls a user's ability to view the sales price but not the buying price of a product. After creating the authorization key, assign it to a metadata item in Metadata Maintenance and then to your users in User Maintenance.

In Document Imaging, you can create a user-defined authorization key that controls a user's ability to edit an image. After creating the authorization key, add it to the **Valid Imagine Auth Keys** control maintenance record, assign it to an image profile Document Profile Maintenance, and then to your users in User Maintenance.

In Sell Matrix Maintenance and Product Lifecycle Maintenance, you can use user-defined authorization keys to control a user's ability to override a price restriction on a sell matrix or a product lifecycle.

In Eclipse Reports, you can use user-defined authorizations to limit what a user views, such as limiting categories, report sources, and data elements in the report sources. For more about Eclipse Reports, launch the online help from the Eclipse Reports application.

For applying user-defined rules to fields, you can create authorization keys that limit the user's ability to edit fields or view data.

Important: We recommend creating and using a standard naming convention when creating your authorization keys, such as beginning all key names with UD. In addition, to make searching for your authorization keys easier, do not use spaces or special characters in the names.

User-defined authorization keys always display at the bottom of a standard authorization key list. For example, if you are entering a key and you press **F10** for a list to scroll through, the user-defined keys always display at the bottom.

To create user-defined authorization keys:

1. From the **Tools** menu, select **User Defined Authorization Keys** to display User Defined Authorization Keys Maintenance.

   You can also access the window from the following menu paths:

   - **Tools > PDW > User Defined Authorization Keys**
   - Tools > System Files > Document Imaging > User Defined Authorization Keys
   - System > System Files > User Defined Authorization Keys
   - System > Custom > Add On Products > Document Imaging > User Defined Authorization Keys

2. In the **Key** field, enter a name for the authorization key you want to create.
3. In the **Levels** field, enter the authorization levels to assign to the authorization key. For example, to assign three different levels to the authorization key, enter 1 in the first field and 3 in the second.

   Note: Levels are *required* for user-defined authorization keys, but can create an authorization key with only one level.

4. In the **Default Level** field, enter the default authorization level for the authorization key, if you are assigning levels to the authorization key.
5. Save the authorization key and exit the window.

Assigning Detail Authorizations

Authorization keys provide access to different parts of the system based on user IDs. For several authorization keys, you can also limit the use based on other criteria in combination with the assigned authorization keys. Use the **Detail** window for each key to enter additional parameters.

To assign detail authorization:

1. From the **System > System Files** menu, select **User Maintenance** and display the user for which you want to assign detail authorization for an authorization key.
2. From the **Maintenance** menu, select **Authorization Keys** to display the Authorization Key/Template Maintenance window.
3. Select one of the authorization keys to assign detail.

   Not all authorization keys have detail limitations. Select from the following:

   - AR.ADJUSTMENT.ALLOWED
   - CR.CREDIT.ALLOWED
   - GL.ACCOUNTS
   - INVALID.PRODUCT.LINES
   - INVALID.VEN.TYPES
   - MESSAGE.GROUP.TYPES
   - SOE.CLOSED.ORDER.EDIT.VIA
   - SOE.CLOSED.PRC.EDIT - Limit users to edit a price based on the ship via.
   - SOE.CLOSED.QTY.EDIT - Limit users to edit a quantity based on the ship via.
   - SOE.CREDIT.REL.RANK
   - VALID.BLINES
   - VALID.PLINES
   - VALID.PRODUCT.LINES
   - VALID.VEN.TYPES

   Note: While the **Detail** option is accessible on other authorization keys, if you add detail information to an authorization key not on this list, the system may not respect the parameters.

4. Click **Assign** to move the authorization key to the right-hand column.
5. From the **Edit** menu, select **Detail** to display the detail parameters.
6. Enter the parameters to limit the authorization key and click **OK**.

   The associated detail parameters are validated fields based on the authorization key with which you are working. For example, if you select the VALID.PLINES authorization key, the system validates your entries to active price lines in the system.

7. Save your changes and exit the window.

Daily Planner Authorization Keys

The following authorization key applies to using the Daily Planner.

DAILY.PLANNER

Allows access to the Daily Planner program. More:

Job Roles	All users
Levels	**Level 1** - Allows access to view and edit the user's own daily schedule.
	Level 2 - Same as level 1.
	Level 3 - Allows access to view, but not edit, another user's daily schedule.
	Level 4 - Allows access to view and edit any user's entries.
Dependencies	None.
Required For:	All Daily Planner activities.

Mass Load Authorization Keys

The following authorization key applies to using the Mass Load program.

MASSLOAD.ALLOWED

Allows access to the Mass Load Full Screen File Update program.

Phantom Status Authorization Keys

The following authorization keys apply to using the Phantom Status window.

KILL.PHANTOM

Allows access to use the **Kill** option on the Phantom Status window to stop any phantom process displayed on the window that is running or sleeping.

KILL.PROCESS

Allows access to use the **Kill Process** option on the Phantom Status window to stop any phantom process (not limited to those displayed on the window) that is running or sleeping. More:

Job Roles	System Administrator and Managers who need to monitor and reports.
Levels	None.
Dependencies	None.
Additional Information	Users with this authorization can also use selection criteria to display groups of similar processes for selective or mass deletion.

PHANTOM.EDIT

Allows access to edit entries on the Phantom Status and Remote Reporting Status Queue windows. More:

Job Roles	System Administrator and Managers who need to monitor and reports.
Levels	**Level 1** - Allows access to view the user's own jobs.
	Level 2 - Allows access to edit or delete the user's own jobs. Allows access to change the user ID of the user's own jobs to another user. If a user assigned at this level changes the user ID, the system displays the following message: Once this is changed, you will not be able to change back to your User. Continue (Y/N)? If the process scheduled is a Report Writer, the **Edit** hot key displays the Report Driver screen, where the user can change the **Sample** field and then access the **Print**, **Hold**, **Opts**, **Notes**, **Column Data**, and **Selection Data** hot keys. If the process scheduled is a G/L Report Generator the **Edit** hot key displays the GL Report Generator driver screen, where the user can change the branch, as of date, company name, and account template fields and use the **Print**, **Hold**, and **Opts** hot keys.
	Level 3 - Allows access to view the jobs of any user.
	Level 4 - Allows access to edit or delete any user's jobs. Allows access to change the user ID of any user's job to another user.
Dependencies	None.
Additional Information	None.

PHANTOM.MANAGER.CONTROL

Allows access to control the number of phantom processes running at the user level on the User Phantom Maintenance screen and the system level on the Phantom Status screen. More:

Job Roles	System Administrator and Managers who need to monitor and reports.
Levels	**Level 1** - Allows access to view your user-level parameters.
	Level 2 - Allows access to view your user-level and the system-level parameters.
	Level 3 - Allows access to edit your user-level parameters.
	Level 4 - Allows access to edit your user-level and the system-level parameters.
Dependencies	None.
Additional Information	Required to add or edit **User Phantom Options** area from the Additional User Data window in User Maintenance..

PHANTOM.MANAGER.PRIORITY

Allows access to view and edit the priorities assigned to phantom processes in the Phantom Manager screen. More:

Job Roles	System Administrator and Managers who need to monitor and reports.
Levels	**Level 1** - Allows access to view the Phantom Manager screen.
	Level 2 - Allows access to change the priority assigned to the user's own phantom processes.
	Level 3 - Allows access to change the priority assigned to any user's phantom processes, kill a process, or force a queued process to run.
Dependencies	None.
Additional Information	None.

PHANTOM.THREAD.COUNT

Allows access to spawn phantom threads for running the A/P Aging Report. Enter the maximum thread count (1-99) the user can spawn. If you leave this record blank, the user can only run the report in a single thread.

Reports Authorization Keys

The following authorization key applies to running reports.

ER.IGN.HEIR.OK

Allows access to the branch hierarchy options. If users have this authorization key assigned, then they are prompted whether they want to ignore the branch hierarchy when running the report.

REPORTER.ADMIN

Assign to users so they are authorized to stop reports and grant authorization to data, but do not have super user status within Eclipse Reports.

This authorization key relates solely to running Eclipse Reports. For more information about setting up Eclipse reports, launch the application and view the online help.

REPORTER.EDIT

Assign to users so they can view, create, and edit reports using Eclipse Reports. In addition, this gives permission to use export options within Eclipse Reports.

This authorization key relates solely to running Eclipse Reports. For more information about setting up Eclipse reports, launch the application and view the online help.

REPORTER.VIEW

Assign to users so they can view reports using Eclipse Reports.

This authorization key relates solely to running Eclipse Reports. For more information about setting up Eclipse Reports, launch the application and view the online help.

WIN.DIRECT.CREATE.DIR

Allows access from report windows to the Windows Direct Options window, which you can use to download reports to a shared UNIX directory. More:

Job Roles	Users required to download reports to a shared directory on the system.
Levels	**Level 1** - Allows access to send reports to a folder specified on the Detailed Selection window.
	Level 2 - Allows access to create subfolders for folders in the following places: • In the **Windows Folder** field on the Windows Direct Options window. • On the Detailed Selection window for the authorization key, if the user has access to User Maintenance.
	Level 3 - Allows access to create folders or subfolders in the following places: • In the **Windows Folder** field on the Windows Direct Options window. • On the Detail Selection window for the authorization key, if the user has access to User Maintenance.

Additional Information	After assigning the authorization key, use the **Detail** option to display the Detail Selection window, where you can enter the names of folders and subfolders to which the user can export reports. If you do not enter any folder names, users cannot export a report from the system using the Windows Direct Options program unless you assign them WIN.DIRECT.CREATE.DIR at level 3. **Note:** Superuser authorization does not include this authorization key. To set this key for a superuser, assign it in addition to the SUPERUSER authorization key.
Required for:	Using the Windows Direct Option on Reports

Scheduler Authorization Keys

The following authorization key applies to the Scheduler.

SCHEDULER

Allows access to edit events in the Daily Schedule and Detail Schedule Maintenance programs and use the Purge Schedule Detail program. More:

Job Roles	Managers or other users required to edit daily schedules.
Levels	**Not assigned** - Users have full control over the events they create, except for purging. For all events that a user does not create, the user can only alter their own personal information on the event. Personal information includes the user's alarm status, public notes, private notes, attendance, and inclusion in the event.
	Level 1 - Allows access to edit but not delete events the user does not create. Allows access to purge events the user created from the user's own schedule.
	Level 2 - Allows access to edit and delete events the user did not create. Allows access to purge events the user created from other users' schedules.
Required For:	• Scheduling Events • Entering Detailed Information for an Event

Solar Eclipse Authorization Keys

The following authorization keys apply to using Solar Eclipse.

SOLAR.ADD.IMAGES

Allows access to add any .jpg image to the archive for use in toolbar customization. More:

Job Roles	Users required to add images for toolbars.
Levels	None.
Additional Information	For users not assigned this key, the **Import Image** button is not active in the Toolbar Customization window in Solar Eclipse.

SOLAR.CHANGE.COMPANY.LOGO

New in Release 9.0

Allows users to change the default Epicor logo to your company logo for the new 9.0 user interface. Users must be assigned this authorization key to change the logo. Users with SUPERUSER assignation will also be required to have this authorization key assigned.

> **Note:** Logos must be less than 500KB in size and in either .PNG or .JPG format. The system alerts you if the image file is too large.

SOLAR.EDIT.TOOLBAR

Allows access to the Toolbar Customization window to create and edit user-defined toolbars in Solar Eclipse. More:

Job Roles	Users required to add images for toolbars.
Levels	**Level 1** - Allows access to view the user's toolbar template.
	Level 2 - Allows access to edit toolbars and assign them to users.
	Level 3 - Allows access to add, edit, and restrict menu items.

SOLAR.OE.SORT.ITEMS

Allows access to sort line items in Sales Order Entry in Solar Eclipse.

SOLAR.OVRD.SYSTEM.THEME

New in Release 9.0.1

Allows users to override the current Solar Theme assigned even if the theme is globally assigned using the **Solar Theme Options** control maintenance record.

> **Note:** Users *must* be assigned this authorization for the override to be available. Being assigned as a SUPERUSER is not sufficient.

Spooler Authorization Keys

The following authorization keys apply to the Spooler.

DOWN.LOAD

Allows access to download data to the user's PC hard drive or floppy drive from the Spooler program using the Your/All Hold Entries programs. More:

Job Roles	Users required to download data to your computer.
Levels	None.
Additional Information	You can send reports to the Hold file and then copy them to a PC word processing, spreadsheet, or database program.
Required For:	• Report Options and Printing • Working with Spooled Reports

SPOOLER.FORWARD.EDIT

This authorization key works with the reports in Spooler Control. More:

Job Roles	Users required to download data to your computer.
Levels	**Level 1** - Allows access to view and add names to the forward list of any report. The user cannot make any other changes to the forward list.
	Level 2 - Allows access to edit the forward list of any report.
Additional Information	Users who are not assigned this authorization key and are not the report creator, cannot view the forward list for the report, add names to the forward list, or forward the report to other users.
	The report creator can edit the forward list for the report regardless of the level assigned with this authorization key.
Required For:	• Report Options and Printing • Working with Spooled Reports

SPOOLER.MANAGEMENT

Allows access to use designated programs on the Spooler Management menu. More:

Job Roles	Users required to download data to your computer.
Levels	**Level 1** -Reserved for future use. Functionality, if assigned, is the same as not assigning the authorization key.
	Level 2 - Allows access to the Kill a Print Job program.
	Level 3 - Allows access to the Kill a Print Job, Stop Spooler, and Start Spooler programs.
Additional Information	All other functions on the **Spooler Management** menu are available to any user who has access to that menu.
Required For:	• Report Options and Printing • Working with Spooled Reports

SPOOLER.UPLOAD.AUTH

Allows access to use the **Upload** function on the Spooler Control window to transfer a document from your PC to the Spooler.

If you upload a document through Your Hold Entries, the document also displays in Spooler Control, which you access from System > Printers > All Hold Entries.

System Maintenance Authorization Keys

The following authorization key applies to System Maintenance.

COMM.PROFILE.MAINT

New in Release 9.0.4

Allows users to create and edit FTP profiles both standard and secure. For more information about creating and using communication profiles, see About Communication Profiles in the System Maintenance documentation.

SYSTEM.PROGRAMMING

Allows access to use the following label format maintenance programs:

- User-Defined Shipping Documents
- User-Defined Receiving Documents
- User-Defined Transfer Documents
- User-Defined Product Documents
- User-Defined Customer Documents
- User-Defined PN Xref Documents

SQL.SERVER

New in Release 8.7.7

Allows access to view and create user-defined tables for SQL replication.

Telemarketing Authorization Keys

The following authorization key applies to the Telemarketing Queue.

TELEMARKETING

Allows access to the Telemarketing Queue. More

Job Roles	Sales marketing personnel.
Levels	• **Level 1** - Allows access to view the logged on user's telemarketing queue. Users designated as telemarketing managers can also view the queues of the salespeople assigned to them. Allows access to change the entry in the **Salesperson** field only for the logged on user and salespeople for whom the user is the telemarketing manager. • **Level 2** - Allows access to view any user's telemarketing queue. Allows access to change the entry in the **Salesperson** field.
Dependencies	None.
Additional Information	The queue displays telemarketing data for customers for whom the user is assigned as the inside or outside salesperson.

TradePower Authorization Keys

The following authorization key applies to the Eclipse interface to the TradePower PowerLink software.

TRADEPOWERS.FTP

Allows access to the **TradePower** menu and programs.

User-Defined Windows and Help Authorization Keys

The following authorization keys apply to user-defined windows and help information.

HELP.EDIT

Allows access to create user-defined F9 help.

HELP.F11.EDIT

Allows access to vie (Level 1) and create (Level 2) user-defined F11 help.

USER.DEFINED.ASSIGN

Allows access to assign a user-defined window to another window. Does not allow access to assign a user-defined window to a menu.

USER.DEFINED.DEFINE

Allows access to create or edit a user-defined window.

User-Defined View Authorization Keys

The following authorization keys apply to setting user-defined views in windows where you can change your view to see different information.

> **Note:** These authorization keys apply to Solar Eclipse only.

SOLAR.UD.VIEW.CREATE

Allows users access to User-Defined View Maintenance to create and save their own user-defined views.

User-Defined Maintenance is available in any window where you can change your view to see different information. For more information about user-defined views, see User-Defined Views Overview in the Application Maintenance documentation.

SOLAR.UD.VIEW.ASSIGN

Allows users access to the Template menu in User-Defined View Maintenance to create save view templates.

Users with this authorization key can then assign views to templates and assign templates to users. Users with this authorization key can also edit user-defined views they have been assigned through a template. For more information about user-defined views, see User-Defined Views Overview in the Application Maintenance documentation.

Index