



Sales Analysis

Release 8.7.5

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.

Epicor Eclipse Release 8.7.5 Online Help Documentation

Copyright © Epicor Software Corporation 2012. All rights reserved. No part of this publication may be reproduced in any form without the prior written consent of Epicor Software Corporation.

Publication Date: January 11, 2013

Table Of Contents

| | |
|---|----|
| Authorization Keys Overview | 1 |
| Superuser Authorization | 2 |
| New and Revised Authorization Keys for this Release | 4 |
| Creating User-Defined Authorization Keys..... | 5 |
| Assigning Detail Authorizations | 7 |
| Activity Based Costing (ABC) Authorization Keys | 8 |
| Unquality Event Tracking (UET) Authorization Keys | 10 |
| Index | 11 |

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. |
| | 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. |

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

6. Save your changes and exit the window.

Activity Based Costing (ABC) Authorization Keys

The following authorization keys apply to activity based costing.

 **What do you think?** Please provide feedback to eclipse.documentation@epicor.com about the new authorization key format and descriptions below.

ABC.AUTO.CODES

Allows access to edit the auto group code in the **Auto Group** column in the ABC Code Maintenance window. More:

| | |
|-------------------------------|--|
| Levels | None. |
| Dependencies | None. |
| Additional Information | Activity Based Costing may not be enabled for your organization. Check with the system administrator if this authorization key is not activated. |

ABC.DOWNLOAD

Allows access to download information from the ABC Log Viewing window to another file or program, such as an Excel spreadsheet. More:

| | |
|-------------------------------|--|
| Levels | None. |
| Dependencies | None. |
| Additional Information | Activity Based Costing may not be enabled for your organization. Check with the system administrator if this authorization key is not activated. |

ABC.EDIT

Allows access to edit ABC log entries. More:

| | |
|-------------------------------|---|
| Job Roles | System Administrator |
| Levels | <ul style="list-style-type: none"> • Level 1 - Allows access to edit the user's own log entries. Entries from other users and entries the user has downloaded display in view-only mode. • Level 2 - Allows access to edit log entries from other users. Downloaded log entries display in view-only mode. • Level 3 - Allows access to edit downloaded log entries. Level 3 authorization is required to delete a log entry. |
| Dependencies | None. |
| Additional Information | Activity Based Costing may not be enabled for your organization. Check with the system administrator if this authorization key is not activated. |

ABC.MAINT

Allows access to maintain ABC system related functions. More:

| | |
|-------------------------------|---|
| Levels | None. |
| Dependencies | None. |
| Additional Information | These functions include the programs listed on the Events > Activity Based Costing > Maintenance menu. |
| Effectuated Areas | ABC Codes Maintenance ABC Parameter Maintenance |

ABC.MANUAL

Allows access to manually log ABC codes using ABC Log Entry. More:

| | |
|-------------------------------|--|
| Levels | None. |
| Dependencies | None. |
| Additional Information | Activity Based Costing may not be enabled for your organization. Check with the system administrator if this authorization key is not activated. |

Unquality Event Tracking (UET) Authorization Keys

The following authorization keys apply to unquality event tracking.

UET.DOWNLOAD

Allows access to download a record of selected unquality events from UET System Log Viewing to a file on a PC. More

| | |
|-------------------------------|---|
| Job Roles | System administrators. |
| Levels | None. |
| Dependencies | None. |
| Additional Information | Also allows access to download end-of-month customer and vendor data to a file on a PC, using the UET Monthly Download to PC program. |
| Required For: | Downloading Unequality Event Information. |

UET.EDIT

Allows access to view and edit unquality event codes. More:

| | |
|-------------------------------|--|
| Job Roles | System administrators. |
| Levels | Level 1 - Allows access to view all UET code entries, but edit only the user's own entries. |
| | Level 2 - Allows access to edit any UET code entry, except those that users have downloaded to a file on a PC. |
| | Level 3 - Allows access to edit any UET code entry, including those that users have downloaded to a file on a PC. |
| Dependencies | None. |
| Additional Information | None. |
| Required For | Maintaining UET Codes |

UET.MAINT

Allows access to maintain UET system related functions. These functions include UET Code Maintenance, UET Parameter Maintenance, UET/PC Customer Report Table, and UET/PC Vendor Report Table.

UET.MANUAL

Allows access to manually enter event data in the UET system through the UET Log Entry program. Access to view or edit unquality events is not allowed.

Index

A

authorization keys

ABC 8

about 1

UET 10

user-defined 5

what's new 4

authorization, superuser 2

R

release 8

authorization keys..... 4

S

superuser authorization

about 2

U

user-defined

authorization keys

creating..... 5

W

what's new in the release

authorization keys 4