



Eclipse Companion Product Authorization Keys

Release 9.0.5

EPICOR®

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.

Copyright © Epicor Software Corporation. 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: October 22, 2018

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
Companion Products Overview	8
Carton Packing Authorization Keys	9
Credit Card Authorization Keys	10
Dataware Authorization Keys	12
Document Imaging Authorization Keys	13
Electronic Data Interchange (EDI) Authorization Keys	14
E-mail Authorization Keys	15
Fax System Authorization Keys	16
Eclipse SQL Data Replication	18
Job Management Authorization Keys.....	19
Johnstone Suite	20
National Sales Tax Database Authorization Keys	20
Product Data Warehouse (PDW) Authorization Keys.....	21
Rentals Authorization Keys	23
RF Authorization Keys	24
Sales Force Automation (SFA) Authorization Keys.....	28
Showroom and Mobile.....	29
Strategic Pricing.....	31
Time Clock Authorization Keys	32
Web Commerce Authorization Keys	33
Index	35

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.

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 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 Imaging 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. Additional Menu Options

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.

See Also:

Authorization Keys Overview

Assigning Authorization Keys to Users

Tasks Not Available in Solar

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. Click [here](#) for a list.

- 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.

Companion Products Overview

Use the following topics to address authorization keys that need to be applied to users for companies that have the following companion products installed:

- B2B Commerce
- Credit Card
- Dataware
- Document Imaging
- EDI
- E-mail
- Fax System
- Job Management
- National Sales Tax Database
- Product Data Warehouse (PDW)
- Rentals
- RF
- Sales Force Automation (SFA)
- Time Clock
- Web Commerce

[Click here for a printable version of the Authorization for Companion Products documentation](#)

Carton Packing Authorization Keys

The following authorization keys control a user's ability to pack orders and load cartons. The carton packing functionality is part of the Carton Packing companion product. For more information, contact your inside salesperson.

CARTON.EDIT

Allows you to view and edit (Level 1) or override carton options (Level 2) for cartons and totes through Carton Packing Maintenance.

CONVERT.TOTE.TO.CARTON

For totes that contain a single order only, allows access to pack all contents on a tote directly to a carton without scanning each item.

When you convert totes to cartons, the system updates all quantities on the tote as packed in Carton Packing Maintenance.

PACK.BACK.ORDER.KEY

Allows access to decrease the to-pack quantity for products in Carton Packing. The system then generates a backorder for the product by the decreased amount.

PACK.BO.SHIP.COMPLETE

Allows users to add backorders to carton packing orders. If the order has a status of **Call When Complete**, **Ship When Complete**, or **Ship Line Complete** you must have this authorization key to backorder the items.

PACK.ORDER.CANCEL

Allows access to cancel packed orders from Order Entry.

Note: This authorization key is activated only if Order Packing is enabled for the ship via and branch.

PACK.PARTIAL.PICKED.ORDER

Allow access to pack staged items before the order is completely picked in Carton Packing Maintenance.

Credit Card Authorization Keys

The following authorization keys apply to the Credit Card Authorization companion product.

CC.TYPE.CHANGE.ALLOW

Allows access to change a credit card type on the Credit Card Default Billing Information window accessed from the Totals window in order entry or the Default Credit Card Information window in Customer Maintenance to a type that was not defined for the credit card.

CREDIT.CARD.ACCT

Allows access to standard (non Element Payment Services) credit card solutions by levels. More

This key is not valid if you have moved to using Element.

Job Roles	Sales personnel who take payment by credit card.
Levels 1 - 4	User sees only the last 4 digits.
Levels 5 - 10	User sees the number of digits equal to the level starting from left to right. For example, if the level is 5, you see the first digit, if it is 6, you see the second digit. You always see the last 4 digits.
11 - 97	User sees the first 6 digits and the last 4 digits.
98	User sees all digits. Assign this level to the select individuals in your company that are authorized to see a full credit card number. These individuals might not be your superusers.
99	Reserve this authorization for select superusers on your site that you want to have full credit card access, but that you do not want to enable to see credit card numbers in their entirety. Superusers are assigned level 99 of this authorization key by default.
Dependencies	None.
Additional Information	If you have not moved to the Credit Card Processing with Element Payment Services solution, and are still using the Credit Card Authorization companion product, use this key to assign users access to view credit card numbers. The level number determines the number of digits that display in historical data, such as logs.
Required For:	Maintenance Log Viewing for Credit Cards Running the Cash Box Journal

CREDIT.CARD.MANUALS

Allows access to manually authorize credit card payments, by entering an authorization code in the **Auth Code** field on an order's Credit Card Authorization screen. More

This key is not valid if you have moved to using Element.

Job Roles	Sales personnel who take payment by credit card.
Levels	None.
Dependencies	None.

Additional Information	<p>Manual payments are necessary if:</p> <ul style="list-style-type: none"> • You received a credit card payment using a system other than Eclipse. • The system cannot communicate with the credit card processor due to network or computer problems, which forces you to call merchant support for a manual authorization code.
-------------------------------	--

CREDIT.CARD.REQD.OVR

Allows access to override a customer requirement that requires credit card information in order entry.

CREDIT.CARD.RESETTLE

Allows access to the Credit Card Settlement Queue. [More](#)

This key is not valid if you have moved to using Element.

Job Roles	Sales personnel who take payment by credit card.
Levels	<ul style="list-style-type: none"> • Level 1 - Allows access in view-only mode. • Level 2 - Allows access to resettle, negate, and force settle a settlement using the Resettle and Negate options. • Level 3 - Allows access to remove and insert transactions on the detail window and use the Cancel option.
Dependencies	None.
Additional Information	None.
Required For:	Viewing the Credit Card Settlement Queue

CREDIT.CARD.SETUP

Allows access to edit and define credit card setup information to define credit cards for customers in Customer Maintenance. [More](#)

Required For:

Configuring the Element Credit Card Processor at Each Branch

Entering URL Addresses for Element Credit Card Processing

Dataware Authorization Keys

The following authorization key applies to the Dataware interface.

DW.MAINT

Allows access to maintain the Dataware interface. Complete this record if your company sends and retrieves ftp files from Dataware.

Document Imaging Authorization Keys

The following authorization key applies to the Document Imaging companion product and signature capture software.

IMG.EDIT.ALLOWED

Allows access to the Delete/Edit Indexes program. [More](#)

Job Roles	System Administrator.
Levels	None.
Dependencies	None.
Additional Information	Use this program to edit image information or index pointers for images attached using the document imaging or signature capture software. Also allows access to the Document Recall by Keyword feature, which you use to recall an image using a keyword search.
Required For:	<ul style="list-style-type: none">• Creating Custom Indexing Profile• Retrieving Images by Keyword

Electronic Data Interchange (EDI) Authorization Keys

The following authorization keys apply to the Electronic Data Interchange companion product.

EDI.ACTIVITY.VIEW

Allows access to view the EDI Activity Log. [More](#)

Job Roles	EDI Administrator.
Levels	<p>The level number, 1-99, determines which entries a user can view.</p> <p>A user can view log entries with a security level equal to or less than the level assigned to this authorization key.</p> <p>For example, a user with an EDI.ACTIVITY.VIEW level of 50 can view entries assigned a security level of 50 or lower, but cannot view entries with a security level of 51 or higher.</p>
Dependencies	None.
Additional Information	None.

EDI.DOCUMENT.EDITOR

Allows access to edit EDI documentation. No levels. No dependencies.

EDI.IN.REVIEW

Allows access to the EDI 810 Invoice Review Queue, 845 Contract Upload Queue, 855 P/O Acknowledgments Review Queue, and 856 Advance Ship Notice Review Queue. [More](#)

Job Roles	EDI Administrator.
Levels	<ul style="list-style-type: none"> • Level 1 - Allows access to view the user's own entries. • Level 2 - Allows access to view the entries of other users.
Dependencies	None.
Required For:	<ul style="list-style-type: none"> • Entering Additional EDI Documentation Information • Reviewing EDI Inbound 810 Invoices • Receiving EDI Transactions • Reviewing EDI 840 Quote Requests • Reprocessing 845 Pricing Contracts • Reviewing 855 P/O Acknowledgments • Managing 856 Advance Ship Notices

E-mail Authorization Keys

The following authorization keys apply to the Outbound E-mail Commerce companion product.

EMAIL.LOG.BCC

Allows access to edit the Outbound E-mail Logging BCC control maintenance record. Required for Outbound E-mail companion product.

EMAIL.SEND

Allows access to the Send E-mail program. For users not assigned this authorization key, **E-Mail** options are not active and e-mail is not available as a print status.

Fax System Authorization Keys

The following authorization keys apply to the Fax System companion product.

FAX.ALLOWED

Allows access to the fax system. More

Job Role	System Administrator
Levels	Level 1 - Allows access to fax memos.
	Level 2 - Allows access to fax documents such as sales orders, purchase orders, transfer orders, bids, and acknowledgments.
	Level 3 - Allows access to send a fax from the print spooler, accessed from System > Printers > Your/All Hold Entries .
Dependencies	None
Required For:	Fax options on any reports or data collection to send a fax electronically.

FAX.APPEND.DOC

Allows access to append documents to a fax memo. More

Job Role	System Administrator
Levels	The level number, 1-99, determines which documents the user can append. The user can append a document assigned a level equal to or lower than the user's level.
	Level 99 allows access to the Fax Append Documents program, where users can assign append document titles, file paths, and the authorization level required to use the document.
Dependencies	None
Required For:	Appending Documents to Faxes

FAX.PRIORITY

Allows access to assign priority levels to faxes on the Fax Memo window or edit priorities in the Outgoing Fax Status Queue. More

Job Role	System Administrator
Levels	Level 1 - Allows access to change the fax priority to Low.
	Level 2 - Allows access to change the fax priority to Low or Medium.
	Level 3 - Allows access to change the fax priority to Low, Medium, or High.
	Level 4 - Allows access to change the fax priority to Low, Medium, High, or Urgent.
Dependencies	None

Job Role	System Administrator
Required For:	<ul style="list-style-type: none"> Assigning a priority to a fax using the Priority field on the Fax Memo window. Changing a priority on a fax using the Priority column on the Outgoing Fax Status Queue.

FAX.RESET

Allows access to use the **Reset** option on the Outgoing Fax Status Queue to halt and reschedule active faxes. [More](#)

Job Role	System Administrator
Levels	None.
Dependencies	The system administrator needs to attach the RUN.FIXFAX program to a menu for the users authorized to run this program.
Additional Information	Allows access to use the RUN.FIXFAX program, which performs the 'fixfax' reset of the fax subsystem. The program displays the progress of the attempted reset of the fax subsystem.
Required For:	Using the Reset option on the Outgoing Fax Status Queue.

FAX.STATUS

Allows access to the Outgoing Fax Status Queue program. [More](#)

Job Role	System Administrator
Levels	<ul style="list-style-type: none"> Level 1 - Allows access to edit this user's own faxes. Level 2 - Allows access to the status of faxes assigned to other users.
Dependencies	None.
Required For:	<ul style="list-style-type: none"> Incoming Fax Status Queue Outgoing Fax Status Queue

Eclipse SQL Data Replication

The following authorization keys apply to the Eclipse SQL Data Replication companion product.

SQL.SERVER

New in Release 8.7.7

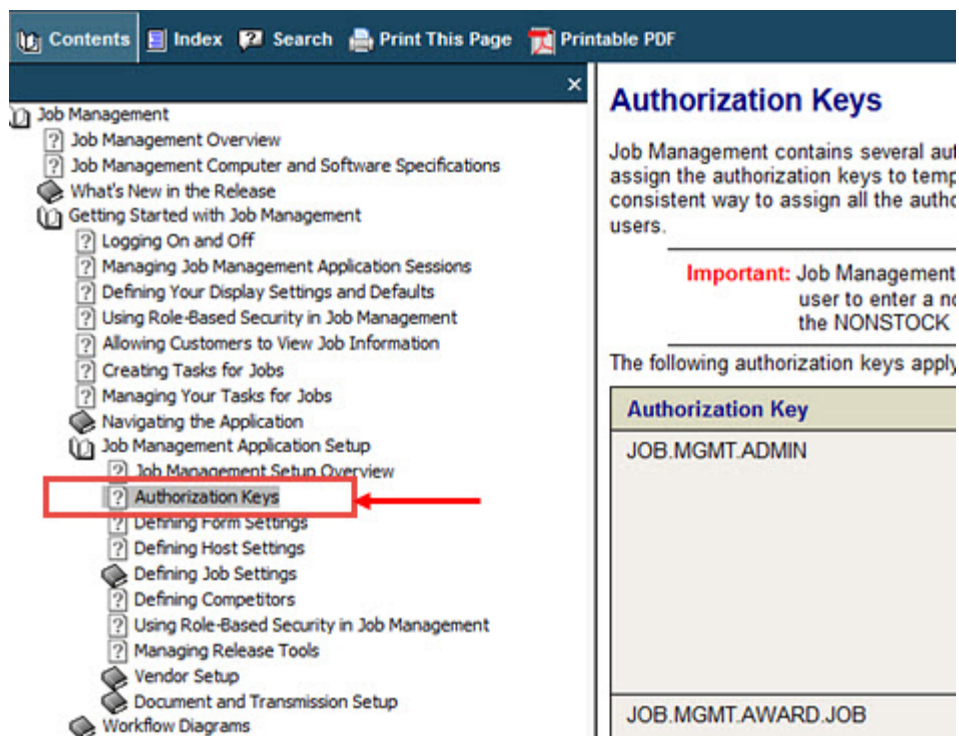
Allows access to view and create user-defined tables for SQL replication.

Job Management Authorization Keys

The Job Management authorization keys control a user's ability to access and use functionality within the Eclipse Job Management companion product. For more information about using Job Management and its authorization keys, use the online help attached to the Job Management application:

To access the Job Management authorization key information:

1. Log in to Job Management.
2. In the main menu bar, click **Help**.
3. From the **Contents** tab, click **Getting Started with Job Management**.
4. Click **Job Management Application Setup** and then **Authorization Keys**:



The screenshot shows the Eclipse Job Management online help interface. The left sidebar contains a tree view of the help contents. The 'Contents' tab is selected, and the tree is expanded to 'Job Management Application Setup', where 'Authorization Keys' is highlighted with a red box and a red arrow. The main content area displays the 'Authorization Keys' page. It includes an 'Important' note stating that a user must enter a non-stock user to assign authorization keys. Below this, a table lists the authorization keys that apply.

Authorization Key
JOB.MGMT.ADMIN
JOB.MGMT.AWARD.JOB

Johnstone Suite

The following authorization keys control a user's ability to access and use functionality within the Johnstone Suite companion product.

JS.PROD.INFO.EDIT

Allows users to add or edit information for Johnstone products.

JS.PROD.INFO.VIEW

Allows users to see Johnstone product information in view-only mode.

JS.WARR.OVERRIDE

Allows access to the Johnstone Warranty Entry from the Returned Goods Verification program.

National Sales Tax Database Authorization Keys

The following authorization key applies to the National Sales Tax Database companion product.

NATL.TAX.MAINT

Allows access to edit the sales tax rates using the National Sales Tax Database Maintenance program.

Product Data Warehouse (PDW) Authorization Keys

The following authorization keys apply to the Product Data Warehouse (PDW) companion product.

PDW.CATALOG.EDIT

Allows access to edit, delete, and unsync records in the PDW. More

Job Roles	System Administrators or Product Managers.
Levels	None.
Dependencies	None.
Additional Information	Users with this authorization can use the Del , Edit , and UnSync hot keys on the PDW Data Viewer screen.
Required For	Editing and unsyncing product information stored in the PDW Catalog using the PDW Data Viewer.

PDW.IMPORT.EXPORT.MAP

New in Release 9.0.4

Allows users to view or edit PDW import and export maps. More:

Job Roles	System Administrator.
Levels	<ul style="list-style-type: none">• Level 1 - Allows access to PDW import and export maps in view-only mode.• Level 2 - Allows access to edit the PDW import or export maps.
Dependencies	None.
Additional Information	None.

PDW.NONSTOCK.ENTRY

Allows access to import a record from the PDW to the system product file as a nonstock. More

Job Roles	System Administrator.
Levels	<ul style="list-style-type: none">• Level 1 - Allows access to import a record in view-only mode.• Level 2 - Allows access to change the imported data, but not the price.• Level 3 - Allows access to change the imported data and price.
Dependencies	None.
Additional Information	None.

PDW.PM.UPLOAD

Allows access to create a PDW record from Product Maintenance.

PDW.REINDEX.ALLOWED

Allows access to run the Rebuild PDW Index program. Required for Defining PDW Meta Data Items.

Rentals Authorization Keys

The following authorization keys apply to the Rental Maintenance companion product.

RENTAL.ALLOWED

Allows access to create rental agreements in Rental Agreement Entry.

RENTAL.MAINT

Allows access to view and edit rental information. More:

Job Roles	Sales personnel required to handle rental equipment.
Levels	Level 1 - Allows access in view-only mode.
	Level 2 - Allows access to do the following: <ul style="list-style-type: none">• Edit fields in Rental Equipment Maintenance for serialized products. All fields are read-only for non-serialized products.• Set up rental fees in the Valid Additional Rental Fees control maintenance record.• Edit the maintenance schedule in Rental Product Maintenance.• Set up meter usage tables in Rental Meter Usage Maintenance.• Retire rental equipment.• Set depreciation schedules.• Set maintenance schedules. Note: To allow users to access the Rental Rate Sheet Maintenance screen, also assign the OE.PRICE.VIEW.LEVEL authorization key.
	Level 3 - Allows access to do the following: <ul style="list-style-type: none">• Create and edit rental product records in Rental Product Maintenance.• Add and edit rental billing time codes in Rental Code Maintenance.
	Level 4 - Not active.

RENTAL.OVERCOMMIT.ITEM

Allows access to over-commit rental items that are not available.

RF Authorization Keys

The following authorization keys apply to the RF Warehouse Management companion product.

RF.AUDIT.OVRD

Allows access to use the **Audit Override** hot key on the Tote Auditing screen to bypass the audit when you do not have time to audit the tote before it needs to be delivered.

RF.BO.SHIP.COMPLETE

Allows access to back-order items for an order with a Ship When Complete status in RF picking, if the RF Enable Check For B/O Of Ship Complete control maintenance record is set to level 2.

RF.CHANGE.FINAL.LOC

Allows access to change the final staging location on the Order Staging screen. Define default staging locations in Customer Maintenance, Branch Maintenance, and Fleet Maintenance.

RF.CHANGE.STAGE.LOC

Allows access to change the staging location on the Tote Inquiry screen. Define default staging locations in Customer Maintenance, Branch Maintenance, and Fleet Maintenance.

RF.COUNT.ABORT

Allows access to handle variances that occur during a product ranking cycle count. More

Job Roles	RF users required to manage cycle count variances.
Levels	Level 0 - Complete related counts to find the variance.
	Level 1 - Complete related counts to find the variance. Queue the variance for an immediate cycle count, which the same user or another user can count at a later time.
	Level 2 - Complete related counts to find the variance. Queue the variance for an immediate cycle count, which the same user or another user can count at a later time. Adjust current location and ignore related locations. Make manual product quantity adjustments in RF Location Maintenance. To allow users to perform this function, also assign the PRD.LOCATION.MAINT authorization key at level 3.
Required For:	Performing RF User-Directed Cycle Counting
Additional Information	This authorization key, if assigned, overrides the Allow Abort From Related Counts control maintenance record for a product ranking cycle count. If you do not assign this authorization key, the control maintenance record determines whether the user must complete all related counts. The value No is equivalent to assigning level 0 to this record and Yes is equivalent to assigning level 2. We recommend using the authorization key to control cycle counting.

RF.COUNT.ABORT.IM

Allows access to handle variances that occur during an immediate cycle count. More

Job Roles	RF users required to manage cycle count variances.
Levels	Level 0 - Complete related counts to find the variance.

	Level 1 - Complete related counts to find the variance. Queue the variance for an immediate cycle count, which the same user or another user can count at a later time.
	Level 2 - Complete related counts to find the variance. Queue the variance for an immediate cycle count, which the same user or another user can count at a later time. Adjust current location and ignore related locations. Make manual product quantity adjustments in RF Location Maintenance. To allow users to perform this function, also assign the PRD.LOCATION.MAINT authorization key at level 3.
Required For:	Performing RF User-Directed Cycle Counting
Additional Information	This authorization key, if assigned, overrides the Allow Abort From Related Counts control maintenance record for a product ranking cycle count. If the authorization key not assigned, the control maintenance record determines whether the user must complete all related counts. The value No is equivalent to assigning level 0 to this record and Yes is equivalent to assigning level 2. The authorization key is a better way to control cycle counting.

RF.LOAD.OVRD

Allows access to load a tote that has not yet reached the status required for loading totes, as defined in the RF Tote Status Before Loading Trucks control maintenance record. Required for Using System-Directed Loading with RF Non-Manifest Picking.

RF.LOCATION.TYPE

Allows access to change the location type in the **T** (Type) field on the Receiving Verify screen and the Direct Put Away screen in the RF system. More

Job Roles	RF users required to change location types.
Levels	Level 1 - Allows access to change the location type from S (Stock) to F (Defective), O (Over Shipment), R (Review), or L (Display). Users at this level cannot change the location type back to S (Stock).
	Level 2 - Allows access to change any location type to any other location type.
Required For:	<ul style="list-style-type: none"> Receiving Product Using RF Using RF System-Directed Put Away
Additional Information	This authorization key, if assigned, overrides the Allow Abort From Related Counts control maintenance record for a product ranking cycle count. If the authorization key not assigned, the control maintenance record determines whether the user must complete all related counts. The value No is equivalent to assigning level 0 to this record and Yes is equivalent to assigning level 2. The authorization key is a better way to control cycle counting.

RF.PICK.QTY.INCREASE

Allows access to increase the picking quantity. More

Job Roles	RF users required to change picking quantities.
Levels	Level 1 - Allows access to increase the picking quantity only when the products and customer allow increases.
	Level 2 - Allows access to increase the picking quantity for products that allow increases, even when the customer does not.

	Level 3 - Allows access to increase the picking quantity for a customer that allows increases, even when the products do not.
	Level 4 - Allows access to increase the picking quantity, even when the products and customer do not allow increases.
Required For:	Increasing Pick Quantities to Package Amounts During RF Picking

RF.PNP.OVERRIDE

New in Release 8.7.9

Allows users to override the RF Pick Select display during the pick-and-pass warehouse process. We advise caution in assigning this authorization key. Picks completed out of sequence by a user adding a tote to pick items for an order prior to the tote being passed can result in unpicked pick-and-pass enabled line items and the previous tote may be directed to packing bypassing some intermediate zones.

RF.PR.D.PU.EDIT

Allows access to the Price Updating ID Maintenance window for cross-referencing barcodes to products. More

Job Roles	RF users required to cross reference barcodes to products.
Levels	Level 1 - Allows access in view-only mode. The Set as Primary option on this window is disabled.
	Level 2 - Allows access in edit mode.
Required For:	Increasing Pick Quantities to Package Amounts During RF Picking

RF.PUTAWAY.OVRD.LOC

Allows access to override and accept a scanned putaway location that is the primary location for another product. More

Job Roles	RF users required to override and accept a scanned putaway location that is the primary location for another product.
Levels	None.
Additional Information	When a scanned location is a primary location for another product, users not assigned this authorization key must scan another location.
	The system checks this authorization key when the RF Putaway Primary Location Override Warning control maintenance record is enabled.

RF.RECV.PUTAWAY.BO.QTY

Allows access to select the backorder option when using the **Qty** hot key on the RF Putaway screen. More

Job Roles	RF users required to adjust quantities during putaway.
Levels	None.
Additional Information	This option authorizes the user to backorder quantities at the time of RF Putaway.
Required for:	Handling Shortages During RF Put Away

RF.RECV.SHIPMENT.EDIT

Allows access to the Adjust Variance window in RF Recv Verify to resolve receiving discrepancies. More

Job Roles	RF users required to adjust variances during putaway.
Levels	None.
Additional Information	None.
Required for:	Splitting Put Away Quantities Between Locations Using RF

RF.RECV.VERF.BO.QTY

Allows access to select the backorder option when using the **Qty** hot key on the RF Verify screen. This authorizes the user to backorder quantities at the time of RF Receive/Verify.

Sales Force Automation (SFA) Authorization Keys

The following authorization keys apply to the Sales Force Automation (SFA) companion product.

SFA.ALLOWED

Allows access to use Sales Force Automation (SFA).

SFA.MAINT

Allows access to update any customer account, regardless of the accessible branches defined for the customer or the user. When users create customer accounts in SFA, they cannot assign accessible branches.

We recommend that you assign this key to the user designated in the SFA Administrator control maintenance record.

Showroom and Mobile

The following authorization keys apply to the Showroom and/or the Eclipse Mobile companion product.

BEACON.MAINT

Allows users to add beacon device information to the Showroom application.

MOBILE.ALLOW

Allows user access to Eclipse Mobile.

MOBILE.BUSINESS.SUM

Allows user access to the business summaries in Eclipse Mobile.

PROSPECT.MAINT

Allows access to the customer records marked as prospects through Customer Maintenance.

Job Roles	Sales personnel required to manage prospect information.
Levels	<ul style="list-style-type: none"> • Level 1 - Allows view-only access to prospect records. • Level 2 - Allows users to view and create prospect records. • Level 3 - Allows users to view, create, and edit a prospect record. Users must be and inside or outside salesperson for the record. • Level 4 - Allows users to view, create, edit or delete any prospect records regardless if they are a salesperson for the record.
Dependencies	Users without either the PROSPECT.MAINT or CUSTOMER.MAINT authorization keys assigned cannot display Customer Maintenance.
Additional Information	If users do not have CUST.MAINT authorization key, they can only display customer records that are marked as prospects and for which they are the inside or outside salesperson for that customer.
	The New Prospect option in Mobile is <i>unavailable</i> to users without the PROSPECT.MAINT or CUST.MAINT authorization keys. For dependencies, see <i>Additional Dependencies for PROSPECT.MAINT</i> below.

Additional Dependencies for PROSPECT.MAINT

The following are true for accessing Customer Maintenance and Prospect* information.

*Prospect refers to those customer records with the Prospect check box selected.

CUSTOMER.MAINT Level	PROSPECT.MAINT Level	Access Customer Maintenance Window	Prospect Access
Level 1	Level 1	View only.	View Only.
Level 1	Level 2	View only.	Create new Prospects in Customer Maintenance. Cannot edit any Prospects.
Level 1	Level 3	View only, unless Prospect is selected.	Create new Prospects. Edit Prospects to which the user is assigned as inside or outside salesperson.

CUSTOMER.MAINT Level	PROSPECT.MAINT Level	Access Customer Maintenance Window	Prospect Access
Level 1	Level 4	View only, unless Prospect is selected.	Full access to create, edit and delete Prospects.
Level 2	Any Level Assigned	Full access to standard customer and Prospect information and to create, edit and delete Prospect records.	
Any Level Assigned	Not Assigned	Standard access to Customer Maintenance from Sales Order Entry, but Prospects do not display.	
Not Assigned	Any Level Assigned	Access to Customer Maintenance from the Maintenance menu only. Customer Maintenance retrieves only Prospect records. Standard customer records are not displayed.	
Not Assigned	Not Assigned	No access to Customer Maintenance.	

Strategic Pricing

The following authorization keys apply to the Strategic Pricing companion product.

SPRC.CORE.STATUS.EDIT

Allows access to update the product Core Status at the customer and product level for Strategic Pricing. Users without this authorization key are allowed to view the core status in the Strategic Pricing Maintenance window. [More](#)

Job Roles	Purchasing agents, sales managers, anyone who deals with product pricing.
Additional Information	For more information about Strategic Pricing and product core statuses, see the following topics: <ul style="list-style-type: none"> • Eclipse Strategic Pricing Overview • Product Core Statuses Overview

SPRC.PRICE.EDIT

New in Release 9.0.2

Restricts pricing edits on Strategic Pricing orders. [More](#):

This authorization key provides a tool to restrict users from editing prices on strategic pricing orders. Use the following levels for your users' access:

- **Level 1** - Allows editing of prices without any restrictions if parameters are left undefined for orders you have created.
- **Level 1** - Allows editing of prices to only the categories, sizes, core status, or sell groups defined in the new Strategic Pricing Authorization Parameters window.

- **Level 2** - Allows editing of prices without any restrictions regardless of the settings in Strategic Pricing Authorization Parameters window or who created the order.

SPRC.VIEW.AUDIT

New in Release 9.0.2

Allows access to the Strategic Pricing Audit window through Sales Order Entry.

Time Clock Authorization Keys

The following authorization keys apply to the Time Clock companion product.

TIME.CLOCK.ADJUST

Allows access to view and edit time clock entries in the Time Clock Detail, Time Clock Accrual, and Equipment Time Clock Entry programs, and to view and edit an employee's time spent using equipment in the Equipment Time Clock Entry program. [More](#)

Job Roles	Payroll, Department Managers
Levels	<ul style="list-style-type: none"> • Level 1 - Allows access to view, but not edit, time clock entries for all users. • Level 2 - Allows access to view and edit time clock entries for all other users, but not edit your own. • Level 3 - Allows access to view and edit time clock entries for all users, including yourself. <p>All users have access to view their own time clock entries, with out granting additional authorization.</p>
Dependencies	If setting for access to adjust equipment time, also assign EQUIPMENT.MAINT.
Additional Information	<p>If you want to allow an employee access to view their time clock entries and make changes to the notes for an entry but not the clock in or clock out times, assign Level 1 of this authorization key and also assign TIME.CLOCK.NOTE.EDIT.</p> <p>For information about clocking time for equipment usage, Equipment Maintenance Overview.</p>

TIME.CLOCK.NOTE.EDIT

Allows a user to edit existing time clock notes in Time Clock Detail Maintenance, even if the user's setting for the TIME.CLOCK.ADJUST key does not allow editing. [More](#)

Job Roles	Payroll
Levels	None
Dependencies	None
Additional Information	<p>Assign this authorization key to your payroll personnel to allow access to edit employees time card notes, as necessary. Also assign this key to any employee you want to grant access to changing their time card notes. You might also assign this key to department managers to have note editing access for their employees time cards.</p> <p>For information about editing time clock entries, see Adding Notes to Time Clock Entries.</p>

Web Commerce Authorization Keys

The following authorization keys apply to the Web Commerce companion product.

PRODUCT.CAT.MAINT

Allows access to view (Level 1) and edit (Level 2) product categories for web order entry. Required for Creating Product Categories.

WOE.MAINT

Allows access to view (Level 1) and edit (Level 2) web order entry passwords and parameters assigned to customers and contacts on the B2B/WOE Remote Order Entry Parameters window in Customer Maintenance and the Contact WOE Parameters window. More

Job Roles	Users required to use B2B or WOE order entry.
Levels	None.
Dependencies	If the parent window (Remote Order Entry Parameters or Contact Maintenance) displays in view-only mode, then the WOE window (B2B/WOE Remote Order Entry Parameters or Contact WOE Parameters) displays in view-only mode, even if level 2 is assigned to the user.
Additional Information	None.
Required For:	<ul style="list-style-type: none">• Entering B2B/WOE Remote Order Entry Parameters• Setting Remote Order Entry Parameters

Index

A

authorization keys

- about 1

- credit card 10

- Dataware 12

- document imaging 13

- EDI 14

- e-mail 15

- fax 16

- imaging 13

- order entry

 - Web Commerce 33

- pricing

 - strategic 31

- products

 - PDW 21

- rentals 23

- SFA 28

- Strategic Pricing 31

- tax 20

- time clock 32

- user-defined 5

 - ELC Courses 5

- warehouse

 - RF 24

- what's new 4

- authorization keys/carton packing 9

- authorization, superuser 2

E

ELC Courses

- authorization keys

 - user-defined 5

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