



A/P, A/R, G/L, and Exchange Rates 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
Creating User-Defined Authorization Keys.....	4
Assigning Detail Authorizations	6
Accounts Payable (A/P) Authorization Keys.....	7
Accounts Receivable Authorization Keys	12
General Ledger (G/L) Authorization Keys	17
Exchange Rates Authorization Keys.....	20
Index	21

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.																												

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 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.

Accounts Payable (A/P) Authorization Keys

The following authorization keys apply to Accounts Payable functions.

AP.ALLOWED

Allows access to the A/P Entry program. More:

Job Roles	Accounts Payable
Levels	<p>Level 1 - Allows access to accounts payable records in view-only mode and use of the Notes and Advice options.</p> <p>Level 2 - Allows access to create and edit accounts payable records, except for amounts in the P/O Total column in the A/P Entry window.</p>
Dependencies	To allow users to edit the P/O Total column, assign the AP.PARTIAL.OK authorization key.
Additional Information	<p>When you display a payable in a closed period, the Manual Check option is still active to offset invoices against credit memos and to manually post the check. For information about posting manual checks, see Posting Manual Checks in the Accounts Payable documentation.</p> <p>Assign this key to allow users to drill into payables from the A/P Preview Queue, Purchase Order Entry, and Work Order Entry.</p>
Required For:	<p>A/P Entry</p> <p>A/P Recurring Entry</p> <p>POE Inquiry</p> <p>Work Order Inquiry</p>

AP.CHANGE.CHECK.POST.DATE

Allows access to change the post date of a check in the Single Check Printing and Print Checks programs. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	None
Additional Information	This authorization key does not affect the date for checks that you post manually.
Required for:	<p>Printing Single Checks</p> <p>Printing Multiple Checks</p>

AP.EDIT.CLOSED.PERIOD

New in Release 9.0.2

Allows users that have a the AP.ALLOWED authorization key, Level 2 to edit the following fields in A/P Entry after a closed period: **Invoice Date**, **Due Date**, **Pay Date**, **Batch ID**, **Payment Terms**, **Invoice Number**, and **Remittance Advice**.

AP.EDIT.REC.PO

Allows access to edit a purchase order that has been reconciled to a payable, approved or not approved, as long as it has not been paid. More:

Job Roles	Accounts Payable
Dependencies	None
Additional Information	If the user is assigned this key and AP.EDIT.REC.PO.UNAP, the AP.EDIT.REC.PO key takes precedence. If the payable has been paid, the purchase order displays as view only, regardless of the authorization setting.
Required For:	Entering and Editing Lot Item Material Details Itemizing Material Prices and Costs Order Entry Scheduling Changing Order Entry Statuses

AP.EDIT.REC.PO.UNAP

Allows access to edit a purchase order that has been reconciled to an unapproved payable. More:

Job Roles	Accounts Payable
Dependencies	None
Additional Information	If the payable is approved, then the purchase order displays as view-only. If the user has this key and AP.EDIT.REC.PO, the AP.EDIT.REC.PO setting takes precedence. If the payable has been paid, the purchase order displays as view only, regardless of the authorization setting.

AP.EDIT.VIEW.ONLY.NOTES

Allows access from A/P Entry to edit notes in the A/P Notes window, even if the payable is view-only. More:

Job Roles	Accounts Payable
Levels	None.
Dependencies	AP.ALLOWED must be set to Level 1 or higher.
Examples	Assign this authorization key to give a user who only has view access in A/P Entry the opportunity to make notes about the payable, even those they do not have access to edit the payable directly.
Additional Information	Notes entered in the detail note mode are included in the General Ledger Report. For information about notes in payables, see Entering Payables in the Accounts Payable documentation.
Required For:	A/P Entry

AP.GEN.VDR.INFO.EDIT

Allows access to update the payee and address information when entering payables for customer refunds or other one-time vendor payments. **More:**

Job Roles	Accounts Payable
Levels	None
Dependencies	AP.ALLOWED set to Level 2.
Examples	Users with this authorization key can use a single generic vendor for refunds and one-time payments and override the vendor's name and address in the Remit-to field in A/P Entry. Without this authorization key, users can add the generic vendor to the payable, view, and edit existing payables, but are unable to override the remit-to information.
Additional Information	Remit-to information on a payable is only editable for generic vendors, as defined in Vendor Maintenance. For more information about using generic vendors for refunds and other one-time payments, see Printing Customer Refund Checks or Making One-Time Payments in the Accounts Payable documentation.
Required For:	A/P Entry

AP.MANUAL.APPROVE

Allows access to override the **Approved** flag to **Yes** in A/P Entry and the A/P Preview Queue even if the invoice reconciliation difference is outside the allowable variance for the vendor. **More:**

Job Roles	Accounts Payable
Levels	None
Dependencies	AP.ALLOWED set to Level 2.
Examples	A vendor sends you an invoice that exceeds the allowable over or short percentages or dollar variance set at the system level or for the vendor. Therefore, the system does not approve the invoice. Assign your senior A/P personnel or your A/P manager this authorization key to authorize payments on a case-by-case basis where the invoice is outside the allowed variance for the vendor.
Additional Information	The A/P Over/Short Maximum Parameters control maintenance record determines the percentage or dollar amount a purchase order can be over or less than the invoice amount when reconciling the purchase order in A/P. The Over/Short Percentage and Over/Short Dollars fields in a vendor's record override the settings in the control maintenance record.
Required For:	A/P Entry A/P Recurring Entry

AP.PARTIAL.OK

Allows access to change the **P/O Total** amount in A/P Entry. **More:**

Job Roles	Accounts Payable
Levels	None

Dependencies	AP.ALLOWED set to Level 2.
Required For:	A/P Entry

AP.PREVIEW.PRINT.CHECK

Allows access to print checks from the A/P Preview Queue using the **Print Check** option. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	AP.ALLOWED
Additional Information	Setting this authorization key allows the user to print all the checks for all the approved payables for a vendor on one check, or to print single checks for payables. To include a signature on the printed checks, also assign AP.SIGNATURE.PRINT. To allow a user to change the posting date for a check, assign AP.CHANGE.CHECK.POST.DATE in addition to this key.
Required For:	A/P Preview Queue

AP.PREVIEW.QUEUE.EDIT

Allows access to change an invoice's due date and approval status using the **Pay On Date** and **Approved** columns in the A/P Preview Queue. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	None
Additional Information	Users who do not have this authorization key assigned can view the A/P Preview Queue, but cannot update the due date or approval status. To allow users to drill into payables from the A/P Preview Queue, also assign AP.ALLOWED.
Required For:	A/P Preview Queue

AP.SIGNATURE.PRINT

Allows access to print an imaged signature on A/P checks. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	None
Additional Information	During A/P check printing, the system checks to see if this authorization key is assigned to the user running the program. If the authorization key is not assigned, the system prompts the user for a password. If the user does not enter a password, the checks print without the signature. Superuser authorization does not include this authorization key. To allow a superuser to print an imaged signature on checks, assign this authorization key in addition to the SUPERUSER authorization key.

Required For:	Printing Single Checks Printing Multiple Checks
----------------------	--

CD.REUSE.CHECK.NO

Allows access to reuse check numbers in the Cash Disbursement, Check Printing, and Void Check programs. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	None
Examples	If you are printing checks and the printer destroys a number of checks in a row you might want to reprint the checks using the same check number.
Additional Information	If you reverse a check in a closed accounting period, you cannot reuse the check number when you cut a new check.
Required For:	Printing Single Checks Printing Multiple Checks

CD.VOID.EFT

Allows access to delete an electronic funds transfer disbursement (EFT check) that has already been released. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	None
Additional Information	Voiding an EFT check requires that you contact the bank to void the electronic transfer of funds to the vendor. The system only undoes the application of the EFT check to the associated payables in Eclipse. For information about voiding checks, see Voiding Checks in the Accounts Payable documentation.
Required For:	Voiding Checks

INVOICE.PROCESS.ENTRY

New in Release 9.0.4

Allows users to enter invoices manually through the Invoice Processing Entry window for EDI.

Note: You must have the Electronic Data Interchange (EDI) companion product to use this feature.

Accounts Receivable Authorization Keys

The following authorization keys apply to Accounts Receivable functions.

APPLY.CR.HKEY

Allows access to apply credits using the **Apply Credits** option in the Cash Receipts window. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	CR.ALLOWED
Additional Information	For information about applying payments to open invoices, see Entering Cash Receipts in the Accounts Receivable documentation.
Required For:	Entering Cash Receipts

AR.ADJUSTMENT.ALLOWED

Limits the dollar amount of invoices that the user can write off in the Automatic A/R Invoice Write Off utility. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	This entry works with the Write Off Amount field in the A/R Invoice Write Off utility.
Additional Information	Use the details to enter a maximum dollar the user is allowed to write off. If you leave it blank, the system allows any dollar amount.
Required For:	Automatically Writing Off A/R Invoices

AR.ADJUSTMENT.LIMIT

Limits the user that can apply adjustments and the maximum amount for which they can apply an adjustment.

AR.ALLOWED

Allows access to the A/R Inquiry program. More:

Job Roles	Accounts Receivable
Levels	None
Dependencies	None
Additional Information	Displays A/R Items as an option on the Fast Select list in order entry, even when the user is not assigned the SOE.CLOSED.ORDER.EDIT key. Assign this authorization key to Eclipse Mobile users that require access to accounts receivable information from their mobile device.

Required For:	A/R Inquiry Mobile A/R Inquiry Order Entry Selections Sales Order Inquiries
----------------------	--

AR.ALLOWED.HOMEBR, AR.ALLOWED.HOMETR

If a home branch or home territory is assigned at the user level, these authorization keys limit users to viewing information on customers in their home branch or territory for the A/R Inquiry and A/R Ledger. More:

Job Roles	Accounts Receivable
Levels	Level 1 - If the customer's branch is different from the user's home branch, then A/R Inquiry and A/R Ledger display an alert that the user is not authorized to view the customer data. Level 2 - If the customer's branch is different from the user's home branch, then A/R Inquiry and A/R Ledger display account information, but not sales orders.
Dependencies	These authorization keys are mutually exclusive with AR.ALLOWED. Users should not be assigned both, however if both are assigned, the system uses AR.ALLOWED and all branches or territories are viewable.
Additional Information	If users have the AR.ALLOWED authorization key, but NEITHER of these authorization keys assigned, they can access any sales orders in A/R Inquiry.
Required For:	A/R Inquiry A/R Ledger

AR.CUSTOMER.RANK

Allows users to add or edit customer rankings through A/R Inquiry.


AR.INQUIRY.SUM

Allows users to see summary amounts of the branches in A/R Inquiry. When this authorization key **Detail** field is populated, users have restricted access to see the summary amounts for the indicated branches. If the **Detail** field is left blank, users can view summary amounts for all branches. Superusers can see all branch information.

AR.INQ.STATUS.EDIT

Allows users to edit the **Invoice Status** column in the A/R Inquiry screen. More:

* New in Release 8.7.8

Job Roles	Accounts receivable personnel, credit manager, or branch manager.
Levels	None
Dependencies	None
Additional Information	Required for editing the Invoice Status and the Cash Receipt Note columns in A/R Inquiry. These fields display with the Invoice Status Code view using View Manager  .
Required For:	Changing information in A/R Inquiry for the invoice status. For more information, see <i>Viewing Customer Receivable Information</i> in the Accounts Receivable online help documentation.

AR.PAYMENT.BY.CC

Allows the user to either accept a negative amount as payment in the **Payment Amount** or **Total Payment Amount** field in the Account Payment window. Also gives the user the ability to change the processing fee percentage for an individual payment. More:

Job Roles	Accounts Receivable, Sales Counter Managers
Levels	None
Dependencies	None
Additional Information	The processing fee that this authorization key allows a user to override is defined in the Account Payment Setup control maintenance record. For more information about receiving payments for an account balance, see Receiving Payments for Accounts in the Accounts Receivable documentation.
Required For:	Receiving Payments by Credit Card Receiving Payments for Customer Account by Credit Card

AR.PROG.BILL.INQ

New in Release 9.0.5

Allows users to create billings from the Progress Billing Queue. More:

New in Release 9.0.5

Job Roles	Accounts receivable personnel, credit manager, or branch manager.
Levels	None
Dependencies	None
Additional Information	Allows users to creating billings from the Progress Billings Queue. Without this key, the billing portion of the queue is disabled.
Required For:	Using the Progress Billing Queue

AR.STATEMENT

Allows access to the Print Statements program. More:

Job Roles	Accounts Payable
Levels	Level 1 - Allows access to print or fax statements for one customer. Users with this level can only select the Individual Customer statement printing option in the Statement Options field in the Print Statements window. Level 2 - Allows access to select any of the statement printing options in the Print Statements program. The default option for users with this level is All Batch Stmt Customers , which prints statements for all customers who are flagged for batch statement printing in their customer record.
Dependencies	None
Additional Information	For more information about printing statements, see in the Accounts Receivable documentation.
Required For:	Printing Statements

CR.ALLOWED

Allows access to the Cash Receipts Entry program. More:

Job Roles	Accounts Payable
Levels	Level 1 - Allows access to view cash receipts records. Level 2 - Allows access to create and edit cash receipts records.
Dependencies	None
Additional Information	This authorization key also grants or restricts permissions to entering batch cash receipts. To allow users to apply credits, also assign APPLY.CR.HKEY. To allow users to apply anticipation credits, also assign CR.ANTICIPATION.CREDIT.
Required For:	Entering Cash Receipts Entering Batch Cash Receipts

CR.ADJUSTMENT.LIMIT

New in Release 9.0.4

Allow users to make adjustments up to a specific dollar amount per invoice and per cash receipt. More:

Job Roles	Accounts Payable
Levels	No Levels. Use the Edit>Detail option on the authorization key to indicate the maximum dollar adjustment allowed for the user.
Dependencies	None
Additional Information	If the user tries to make an adjustment over the authorized limit, an error message displays and provides two options: <ul style="list-style-type: none"> • Lower the Limit - User is returned to the adjustments window and can enter a lower adjustment amount. • Remove the Adjustment - No adjustment is made, the system does not store any value, and the adjustment window closes.

CR.CREDIT.ALLOWED

Allows access to apply and adjust credits, but not apply other cash, including corrections in G/L closed periods. More:

Job Roles	Accounts Payable
Levels	None.
Dependencies	Use the right-click Detail option to specify which banks for which the users are allowed to make these changes. For more information, see Assigning Authorization Keys to Users.
Additional Information	When assigned, the Amount field, Delete , and Write Off menu options are disabled. Users may need APPLY.CR.HKEY assigned, if the Apply Credits menu is needed for their job role.
Required For:	Entering Cash Receipts Entering Batch Cash Receipts

CR.ANTICIPATION.CREDIT

Allows access to generate an anticipation credit from the Cash Receipts window. More:

Job Roles	Accounts Payable
Levels	None
Dependencies	CR.ALLOWED
Additional Information	Anticipation credit is a reward that selected customers can receive if they pay their invoices prior to the due date. For more information about anticipation credits, Anticipation Credit Basis in the Accounts Receivable documentation.
Required For:	Entering Cash Receipts Entering Batch Cash Receipts

General Ledger (G/L) Authorization Keys

The following authorization keys apply to General Ledger functions.

GL.ACCOUNTS

Limits access to view designated general ledger accounts in G/L Inquiry. Users not assigned this key to limit the accounts they can see can view all accounts in G/L Inquiry. More:

Job Roles	Accounting Personnel
Levels	None
Dependencies	After assigning the authorization key, use the Detail option to display the Detail Selection window, where you build the list of accounts the user can view. For more information, see Assigning Authorization Keys to Users.
Additional Information	This authorization key applies only to G/L Inquiry. 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 General Ledger Using G/L Inquiry

GL.BRANCH.EDIT

Allows access to edit the **G/L Branch** field in the Additional Header Information window for a sales order generation. Changing the branch in this field changes the branch that records the general ledger posting for the order. More:

Job Roles	Accounting Personnel
Levels	None
Dependencies	None
Additional Information	The general ledger account for a sales order is determined by the Branch That Controls Branch That Receives Credit For the Sale and Branch That Receives Credit For The Sale control maintenance records.
Required For:	Changing the G/L Branch on the Additional Sales Order Header Information window.

GL.BRANCH.OVERRIDE

Allows access to post a journal entry to a G/L account that is not accessible to the branches defined as accessible for the account. More:

Job Roles	Accounting Personnel
Levels	None
Dependencies	None

Additional Information	<p>When a user attempts to post a journal entry to an account that is not accessible to the branch, the system checks this authorization key, displays a warning, and does one of the following:</p> <ul style="list-style-type: none"> • If this key is assigned, asks if the user wants to post to an inaccessible branch. • If this key is not assigned, prompts the user to enter a password to post to an inaccessible branch. • If the user continues, the system posts the journal entry to the designated account and then prompts the user to activate the G/L account for that branch. • If the user enters Yes, the system adds the branch to the account's list of accessible branches. • If the user enters No, the system does not add the branch to the account's list of accessible branches. <p>For information about setting accessible branches for a general ledger account, see Restricting Accessible Branches for G/L Accounts in the General Ledger documentation.</p>
-------------------------------	---

GL.CLOSE.DATE.EDIT

Allows access to edit general ledger closing dates in the edit dates in the Change G/L Closing Date window. More:

Job Roles	Senior Accounting Personnel, Financial Officers
Levels	<ul style="list-style-type: none"> • Level 1 - Allows access to change any date except the Audit Close Date. • Level 2 - Same as level 1. • Level 3 - Allows access to also change the Audit Close Date. Assign Level 3 authorization only to the individual who has the final responsibility for the company's financial integrity.
Dependencies	GL.MAINT
Additional Information	Closing dates are not necessarily period end dates, only the cut offs for modifications to entries up through that date. If a user has access to edit closing dates, they can change the dates for only themselves and the session they are currently running, for a specific user, or to all users.
Required For:	Changing the G/L Closing Date

GL.MAINT

Allows access to G/L maintenance and setup programs. More:

Job Roles	Accounting Personnel, System Administrators
Levels	<ul style="list-style-type: none"> • Level 1 - Allows access to the G/L Account Maintenance program for creating and maintaining general ledger accounts. • Level 2 - Allows access to the G/L Account Maintenance, the G/L Product Types, and G/L Sales Sources programs.
Dependencies	None

Additional Information	<p>Use G/L Account Maintenance to setup your accounts and templates.</p> <p>Use product types to define categories that describe the product types you sell, for example, plumbing, electrical, and commodities. Use sales sources to define profit areas within a branch, such as showroom, or counter. The system uses product types and sales sources to determine the revenue account to which it posts sales.</p>
Required For:	<ul style="list-style-type: none"> • Defining G/L Allocations • Defining G/L Product Types • Sales Sources Overview • G/L Account Maintenance • Creating G/L Report Templates

GL.REPORTING

Allows access to the G/L Report Generator to run reports such as balance sheets, income statements, and profit and loss statements. More:

Job Roles	Accounting Personnel, Finance Managers
Levels	None
Dependencies	None
Additional Information	<p>The G/L Report Generator allows you to run standard reports, such as operating statements, and also allows you to create custom reports on your general ledger. For more information about the G/L Report Generator, see G/L Reports Overview in the General Ledger documentation.</p>

Exchange Rates Authorization Keys

The following authorization key applies to the foreign exchange rate function.

EXCHANGE.RATE.EDIT

Allows access to edit exchange rates in Exchange Rate Maintenance. Users not assigned this key can only view exchange rates. More:

Job Role	Accounting
Levels	None
Dependencies	None
Additional Information	<p>Exchange rates require additional setup, including setting up the general accounts to record losses and gains due to the fluctuation in rates. Setting these accounts up requires the appropriate general ledger account authorization. However, you can authorize a user to edit exchange rates in the Exchange Rate Maintenance window without authorizing them for general ledger.</p> <p>For more information about editing exchange rate information, see Defining Exchange Rates in the Accounting Setup documentation. For information about foreign exchange rate support in the system, see Foreign Exchange Rates Overview in the Account Setup documentation.</p>
Required For:	<ul style="list-style-type: none"> • Defining Exchange Rates • Approving Payable Invoices • Viewing Payable Invoices • Defining Customer Pricing Options • Changing Sales Order Currency

Index

A

AP.ALLOWED 7

AP.EDIT.CLOSED.PERIOD 7

authorization keys

about 1

accounting

accounts payable 7

accounts receivable 12

general ledger 17

exchange rates 20

file maintenance

exchange rates 20

pricing

cost and exchange rates 20

user-defined 4

ELC Courses 4

authorization, superuser 2

E

ELC Courses

authorization keys

user-defined 4

P

pricing

cost and exchange rates 20

S

superuser authorization

about 2

U

user-defined

authorization keys

creating 4