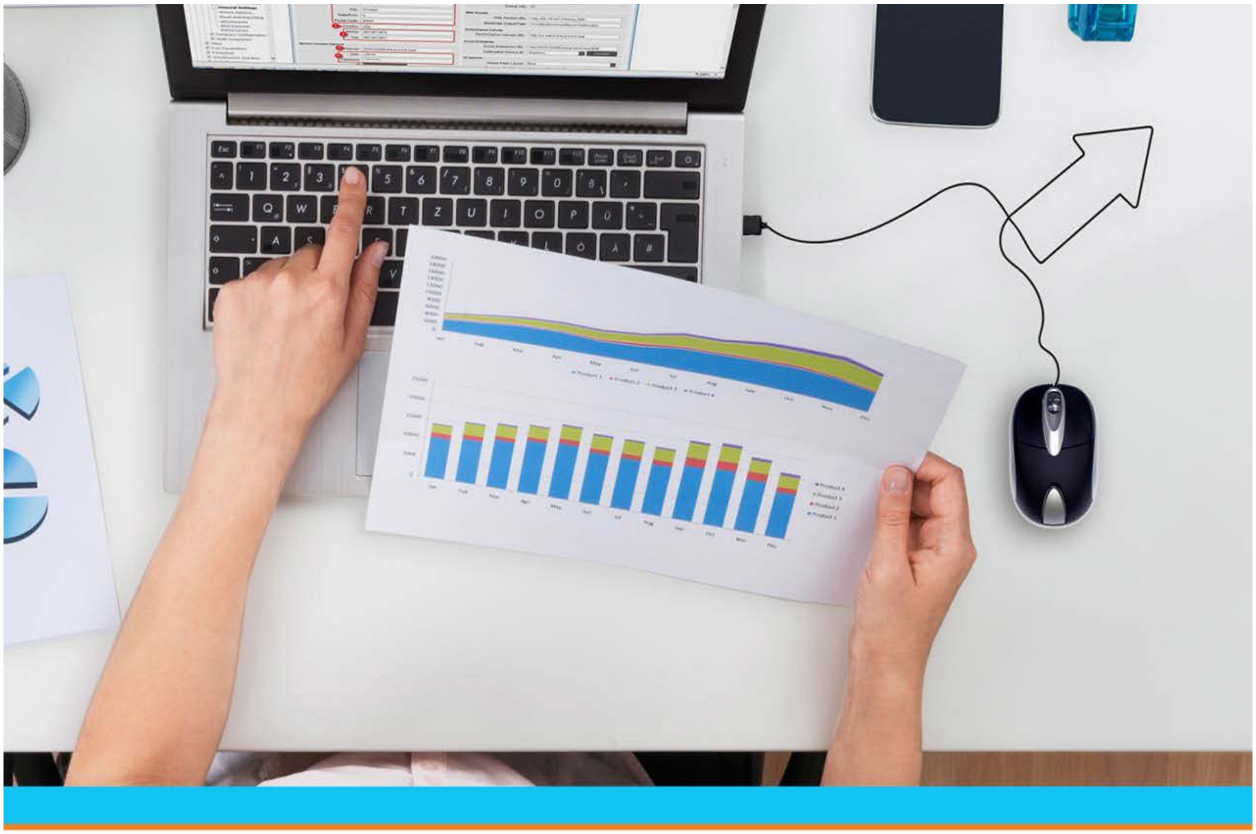

Eclipse File Maintenance Authorization Keys

Release 9.0.5

Disclaimer

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

Publication Date: October 22, 2018

Table of Contents

Authorization Keys Overview

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

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

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

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

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

Superuser Authorization

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

SUPERUSER

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

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

<table>
<tr><td><b>Job Roles</b></td><td>Administrators and Managers.</td></tr>
<tr><td><b><i>Important</i></b></td><td>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.
<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 <b>Auto Scheduling</b> 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 <b>Auto Scheduling</b> option on the SOE Body window to a default value.</td></tr>
<tr><td>TOE.SCHEDULE</td><td>the system does not set the <b>Auto Scheduling</b> 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>
</td></tr>
</table>

New and Revised Authorization Keys for this Release

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

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

Creating User-Defined Authorization Keys

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

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

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

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

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

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

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

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

To create user-defined authorization keys:

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

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

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

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

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

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

Assigning Detail Authorizations

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

To assign detail authorization:

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

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

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

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

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

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

7. Save your changes and exit the window.

Activity Logs Authorization Keys

The following authorization keys apply to viewing and editing information in the activity logs.

Viewing Activity Log Entries

The following authorization keys allow access to Activity Log Viewing.

- **CUST.ACTIVITY.VIEW**

  Use for viewing the Customer Activity Log. More:

Job Roles	System Administrator.
Levels	The level number, 1-99, determines which entries the user can view. Users can view log entries with a security level equal to or less than the level assigned to the corresponding authorization key. For example, a user with an 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.
Dependencies	Additional keys also determine the level of security assigned to activity log entries the user makes, if the **Use User's Sec Level As Default For Queue Entries** control maintenance record is set to **Yes**.
Additional Information	All users assigned the SYSTEM.ACTIVITY.VIEW authorization key, regardless of the level, can see system-generated log entries.

- **ORD.ACTIVITY.VIEW**

  Use for viewing the Order Activity Log. More:

Job Roles	System Administrator.
Levels	The level number, 1-99, determines which entries the user can view. Users can view log entries with a security level equal to or less than the level assigned to the corresponding authorization key. For example, a user with an 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.
Dependencies	Additional keys also determine the level of security assigned to activity log entries the user makes, if the **Use User's Sec Level As Default For Queue Entries** control maintenance record is set to **Yes**.
Additional Information	All users assigned the SYSTEM.ACTIVITY.VIEW authorization key, regardless of the level, can see system-generated log entries.

- **PRD.ACTIVITY.VIEW**

  Use for viewing the Product Activity Log. More:

Job Roles	System Administrator.
Levels	The level number, 1-99, determines which entries the user can view. Users can view log entries with a security level equal to or less than the level assigned to the corresponding authorization key. For example, a user with an 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.

	The system assigns security level 1 to all entries in the Product Activity Log. All users, regardless of their assigned view level, can view entries in this log. If the **Remote Customer** field in the user's record contains an entry, the user cannot access the log from Inventory Inquiry. A remote customer may not view the Product Activity Log.
Dependencies	Additional keys also determine the level of security assigned to activity log entries the user makes, if the **Use User's Sec Level As Default For Queue Entries** control maintenance record is set to **Yes**.
Additional Information	All users assigned the SYSTEM.ACTIVITY.VIEW authorization key, regardless of the level, can see system-generated log entries.

- **SYSTEM.ACTIVITY.VIEW**

Use for viewing the System Activity Log. More:

Job Roles	System Administrator.
Levels	The level number, 1-99, determines which entries the user can view. Users can view log entries with a security level equal to or less than the level assigned to the corresponding authorization key. For example, a user with an 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.
Dependencies	Additional keys also determine the level of security assigned to activity log entries the user makes, if the **Use User's Sec Level As Default For Queue Entries** control maintenance record is set to **Yes**.
Additional Information	All users assigned the SYSTEM.ACTIVITY.VIEW authorization key, regardless of the level, can see system-generated log entries.

- **USER.ACTIVITY.VIEW**

Use for viewing the User Activity Log. More:

Job Roles	System Administrator.
Levels	The level number, 1-99, determines which entries the user can view. Users can view log entries with a security level equal to or less than the level assigned to the corresponding authorization key. For example, a user with an 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.
Dependencies	Additional keys also determine the level of security assigned to activity log entries the user makes, if the **Use User's Sec Level As Default For Queue Entries** control maintenance record is set to **Yes**.
Additional Information	All users assigned the SYSTEM.ACTIVITY.VIEW authorization key, regardless of the level, can see system-generated log entries.

- **VENDOR.ACTIVITY.VIEW**

Use for viewing the Vendor Activity Log. More:

Job Roles	System Administrator.
Levels	The level number, 1-99, determines which entries the user can view. Users can view log entries with a security level equal to or less than the level assigned to the corresponding authorization key. For example, a user with an 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.
Dependencies	Additional keys also determine the level of security assigned to activity log entries the user makes, if the **Use User's Sec Level As Default For Queue Entries** control maintenance record is set to **Yes**.
Additional Information	All users assigned the SYSTEM.ACTIVITY.VIEW authorization key, regardless of the level, can see system-generated log entries.

Creating Activity Log Entries and Appending Messages

The following authorization keys allow access to create activity log entries (trackers) or append messages to existing log entries.

- **CUST.ACTIVITY.EDIT**

Use to create and append to Customer Activity Log entries. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Create an activity log entry and view own entries. • **Level 2** - Also append comments to own entries. • **Level 3** - Also view the entries of other users. • **Level 4** - Also append comments to the entries of other users. • **Level 5** - Reserved for future use.
Additional Information	Users on the follow-up list of a tracker can append comments to the entry regardless of their level of authorization.

- **ORD.ACTIVITY.EDIT**

Use to create and append to Order Activity Log entries. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Create an activity log entry and view own entries. • **Level 2** - Also append comments to own entries. • **Level 3** - Also view the entries of other users. • **Level 4** - Also append comments to the entries of other users. • **Level 5** - Reserved for future use.
Additional Information	Users on the follow-up list of a tracker can append comments to the entry regardless of their level of authorization.

- **PRD.ACTIVITY.EDIT**

Use to create and append to Product Activity Log entries. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Create an activity log entry and view own entries. • **Level 2** - Also append comments to own entries. • **Level 3** - Also view the entries of other users. • **Level 4** - Also append comments to the entries of other users. • **Level 5** - Reserved for future use.
Dependencies	For the PRD.ACTIVITY.EDIT function to work, also assign the PRD.ACTIVITY.VIEW authorization key.
Additional Information	Users on the follow-up list of a tracker can append comments to the entry regardless of their level of authorization.

- **SYSTEM.ACTIVITY.EDIT**

Use to create and append to System Activity Log entries. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Create an activity log entry and view own entries. • **Level 2** - Also append comments to own entries. • **Level 3** - Also view the entries of other users. • **Level 4** - Also append comments to the entries of other users. • **Level 5** - Reserved for future use.
Dependencies	None.
Additional Information	Users on the follow-up list of a tracker can append comments to the entry regardless of their level of authorization.

- **USER.ACTIVITY.EDIT**

Use to create and append to User Activity Log entries. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Create an activity log entry and view own entries. • **Level 2** - Also append comments to own entries. • **Level 3** - Also view the entries of other users. • **Level 4** - Also append comments to the entries of other users. • **Level 5** - Reserved for future use.
Dependencies	None.
Additional Information	Users on the follow-up list of a tracker or part of a message group on the follow-up list can append comments to the entry regardless of their level of authorization.
	For the USER.ACTIVITY.EDIT function to work, also assign the user the USER.ACTIVITY.VIEW authorization key. If users have an entry in the **Remote Customer** field in their User Maintenance settings, the **Log** option does not display on the Inventory Inquiry screen/window.

- **VENDOR.ACTIVITY.EDIT**

Use to create and append to Vendor Activity Log entries. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Create an activity log entry and view own entries. • **Level 2** - Also append comments to own entries. • **Level 3** - Also view the entries of other users. • **Level 4** - Also append comments to the entries of other users. • **Level 5** - Reserved for future use.
Dependencies	None.
Additional Information	Users on the follow-up list of a tracker can append comments to the entry regardless of their level of authorization.

Editing Activity Log Comments

The following authorization keys allow access to original and appended comments made by the user in the corresponding activity log entries.

- **CUST.ACTIVITY.CMT.EDIT**

Use to access original and appended comments made by the user in the Customer Activity Log. More:

Job Roles	System Administrator.
Levels	None.
Dependencies	For this key to work, also assign the CUST.ACTIVITY.VIEW authorization key.
Additional Information	None.

- **ORD.ACTIVITY.CMT.EDIT**

Use to access original and appended comments made by the user in the Order Activity Log. More:

Job Roles	System Administrator.
Levels	• **Level 2** or **3** - To edit the user's own entries. • **Level 4** - To edit the entries of other users.
Dependencies	For this key to work, also assign the ORD.ACTIVITY.VIEW authorization key.
Additional Information	None.

- **PRD.ACTIVITY.CMT.EDIT**

Use to access original and appended comments made by the user in the Product Activity Log. More:

Job Roles	System Administrator.
Levels	None.

Dependencies	For this key to work, also assign the PRD.ACTIVITY.VIEW authorization key.
Additional Information	None.

- **SYSTEM.ACTIVITY.CMT.EDIT**

Use to access original and appended comments made by the user in the System Activity Log. More:

Job Roles	System Administrator.
Levels	None.
Dependencies	For this key to work, also assign the SYSTEM.ACTIVITY.VIEW authorization key.
Additional Information	None.

- **USER.ACTIVITY.CMT.EDIT**

Use to access original and appended comments made by the user in the User Activity Log. More:

Job Roles	System Administrator.
Levels	None.
Dependencies	For this key to work, also assign the USER.ACTIVITY.VIEW authorization key.
Additional Information	None.

- **VENDOR.ACTIVITY.CMT.EDIT**

Use to access original and appended comments made by the user in the Vendor Activity Log. More:

Job Roles	System Administrator.
Levels	None
Dependencies	For this key to work, also assign the VENDOR.ACTIVITY.VIEW authorization key.
Additional Information	None.

Authorization Keys for Authorization Keys

The following authorization key applies to maintaining user-defined authorization keys.

UD.AUTH.KEY.EDIT

Allows access to create and edit user-defined authorization keys for some applications. More:

Job Roles	System Administrator
Levels	None
Dependencies	None
Examples	For example, in Product Data Warehouse, you can create an 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 users in User Maintenance.
Additional Information	Use the User Defined Authorization Keys screen to create user-defined authorization keys.
Required For:	User Defined Authorization Keys

Branch and Territory Authorization Keys

The following authorization keys control a user's ability to view and edit branch and territory records.

BRANCH.MAINT

Allows access to Branch Maintenance and windows accessed from it to view and edit branch records. More:

Job Roles	System Administrators, Branch Managers
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	None
Additional Information	The system uses branch designations for control maintenance records; customer, vendors, and user home branches for pricing, accounting, reporting, and tracking purposes, accounting and general ledger postings, pricing, and tax jurisdictions. For more information about branches, see Branch and Territory Maintenance Overview in the Entity Maintenance documentation.
Required For:	• Adding Branches to Territories • Activating Branches For Customer Purchases • Assigning Branch Access to Vendors • Defining Vendor Branch Override Capabilities • Branch Maintenance • Assigning Ship Via Branch Overrides • Inventory Inquiry Branches from Branch Maintenance • Setup Requirements for Check Authorization • Verifying Check Processors For Branches • Customer Maintenance • Strategic Pricing Branch Maintenance • User Maintenance • Vendor Maintenance

TERRITORY.MAINT

Allows access to Territory Maintenance and windows accessed from it to view and edit territory records. More:

Job Roles	System Administrators, Branch or Regional Managers
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	None
Additional Information	A territory is a group of branches. Territory priorities creates the branch hierarchy, which allows you to define branch-specific settings at the territory level. For more information about branches, see Branch and Territory Maintenance in the Entity Maintenance documentation.
Required For:	Territory Maintenance Overview

Buy and Sell Matrix Functions Authorization Keys

The following authorization keys apply to the buy and sell matrix functions.

SMATRIX.COGS.EDIT

Allows users to cost-of-goods-sold (COGS) costs on Sell Matrix Maintenance and Quick Sell Matrix Maintenance. More:

Job Roles	Purchasing agents.
Levels	None.
Dependencies	Users must also have the SMATRIX.MAINT set to level 4.
Required For:	Editing cost-of-goods-sold on Sell Matrix Maintenance and Quick Sell Matrix Maintenance.

SMATRIX.COST.EDIT

Allows users to edit costs on Sell Matrix Maintenance and Quick Sell Matrix Maintenance. More:

Job Roles	Purchasing agents.
Levels	None.
Dependencies	Users must also have the SMATRIX.MAINT set to level 4.
Required For:	Editing costs on Sell Matrix Maintenance and Quick Sell Matrix Maintenance.

BMATRIX.MAINT

Allows access to the Buy Matrix Maintenance and Quick Buy Matrix Maintenance programs. More:

Job Roles	Purchasing Agents
Levels	**Level 1** - Allows access in view-only mode.
	Level 2 - Allows access to create a new buy matrix cell. Also allows access to edit or delete buy matrix cells.
	Level 3 - Functions the same as level 2, and allows view-only access to all cost and purchasing information. Allows update access to the purchasing information listed in level 1 *for branches to which the user has access*. The user can view cost overrides, but not edit them, using the **Cost Ovrd** option on the Buy Matrix Maintenance window and the **Cost Override** hot key on the Quick Buy Matrix Maintenance window.
	Level 4 - Functions the same as level 2, and allows access to view and update all purchasing and cost information. Allows access to create and edit cost overrides using the **Cost Ovrd** option on the Buy Matrix Maintenance screen and the **Cost Override** option on the Quick Buy Matrix Maintenance window.
Dependencies	None.
Additional Information	When users access Buy Matrix Maintenance through purchase order entry, the information displays as view-only regardless of the level assigned with this authorization key.

Required For:	• Buy Matrix Maintenance • Quick Buy Matrix Copying

SMATRIX.MAINT

Allows access to the Sell Matrix Maintenance and Quick Sell Matrix Maintenance programs. More:

<table>
<tr><td><b>Job Roles</b></td><td>Purchasing Agents</td></tr>
<tr><td rowspan="4"><b>Levels</b></td><td><b>Level 1</b> - Allows view-only access to sell information in Sell Matrix Maintenance and the following views in Quick Sell Matrix Maintenance:
• Prices
• Rebates
• Direct Rebates
• Price/Qty
The user cannot see cost information. The user has no update access.</td></tr>
<tr><td><b>Level 2</b> - Allows view-only access to sell and cost information in Sell Matrix Maintenance and the following views in Quick Sell Matrix Maintenance:
<table>
<tr><td>Prices</td><td>Gross Profit</td></tr>
<tr><td>Costs</td><td>Price/Qty</td></tr>
<tr><td>Direct Costs</td><td>Sell Price Override</td></tr>
<tr><td>Rebates</td><td>Cost Override Date</td></tr>
<tr><td>Direct Rebates</td><td>Direct Cost Override</td></tr>
<tr><td>Prices/Cost</td><td></td></tr>
</table>
The user has no update access.</td></tr>
<tr><td><b>Level 3</b> - Allows view-only access to all cost and sell information.
Allows update access to the sell information listed in level 1 <i>for branches to which the user has access</i>. The user can view cost overrides, but not edit them, using the <b>Maintenance > Cost Override</b> in Sell Matrix Maintenance and the <b>Maintenance > Cost Override</b> option in the Quick Sell Matrix Maintenance.</td></tr>
<tr><td><b>Level 4</b> - Allows access to view and update all sell and cost information.
Allows access to create and edit cost overrides using the <b>Maintenance > Cost Override</b> option in Sell Matrix Maintenance screen and the <b>Maintenance > Cost Override</b> option on the Quick Sell Matrix Maintenance screen.
• To edit COGS, you must also have the SMATRIX.COGS.EDITT authorization key assigned.
• To edit COST, you must also have the SMATRIX.COST.EDIT authorization key assigned.</td></tr>
<tr><td><b>Dependencies</b></td><td>In addition to assigning this authorization key, you must also assign the SMATRIX.MAINT.CUS.CLASS authorization key.</td></tr>
<tr><td><b>Additional Information</b></td><td>When users access Sell Matrix Maintenance through sales order entry, the information displays as view-only regardless of the level assigned with this authorization key.</td></tr>
<tr><td><b>Required For:</b></td><td>• Buy Matrix Maintenance
• Quick Buy Matrix Copying
• Overriding Pricing from Order Entry</td></tr>
</table>

SMATRIX.MAINT.CUS.CLASS

Used in conjunction with SMATRIX.MAINT, this authorization key further restricts the ability to view, create, and edit matrix cells. More:

Job Roles	Purchasing Agents
Levels	• **Not Assigned** - Allows access to matrix cells in view-only mode, as determined by the SMATRIX.MAINT authorization key. • **Level 1** - Allows access to create or edit Customer matrix cells. Class and Type/Quote matrix cells are view-only, as determined by the SMATRIX.MAINT authorization key. • **Level 2** - Allows access to create or edit Customer and Class matrix cells. Type/Quote matrix cells are view-only, as determined by the SMATRIX.MAINT authorization key. • **Level 3** - Allows access to create and edit Customer, Class and Type/Quote matrix cells**.**
Dependencies	Assign this authorization key in addition to the SMATRIX.MAINT authorization key. Access to Class matrix cells is also determined by the OE.PRICE.CLASS.LEVEL authorization key.
Additional Information	A user assigned SMATRIX.MAINT at level 3 cannot create or edit a cost override for a matrix cell. If the user is also assigned SMATRIX.MAINT.CUS.CLASS at level 1, they can create, edit, or delete a customer specific matrix cell, but still do not have access to the cost override functionality at the matrix cell level.
Required For:	• Buy Matrix Maintenance • Overriding Pricing from Order Entry • Viewing Customer Vendor Specific Part Number Details

UD.MATRIX.UPLOAD

Allows access to upload data for creating a buy or sell matrix to your Hold file and define a layout for creating matrix cells from the uploaded data. With this authorization key, users can select the **Matrix Upload User Defined** option using the **Process** option on the Spooler Control window.

Note: Matrix Upload User Defined is a user-defined option, which you set up on the User Defined Upload Processing window to call the MATRIX.USER.DEFINED subroutine.

Company Comments Authorization Keys

The following authorization key controls a user's ability to create and edit company-wide standard comments.

COMPANY.COMMENT.EDIT

Allows access to create and edit company-wide standard comments that are available to all users to add to or use in place of free-form tracker append comments, tracker closing comments, and fax comments.

Contact Authorization Keys

The following authorization key controls a user's ability to view and edit contact records.

CONTACT.MAINT

Allows access to Contact Maintenance depending on the need. More:

Job Roles	Accounts Payable
Levels	• **Level 1** - Allows access to only view contact records. • **Level 2** - Allows access to create contact records. • **Level 3** - Allows access to edit a contact record, only if the user is the inside or outside salesperson for that contact's primary entity. • **Level 4** - Allows access to edit or delete all contact records.
Dependencies	None.
Additional Information	The WOE.MAINT authorization key, defined for Customer Maintenance, also applies to Contact Maintenance.
	If you have Level 3 or Level 4 assigned, when you are managing an order and want to change contact information, the system prompts you to replace the main contact, add as additional parameter, or use it for that order only. In this scenario, if you have Level 3 you must also be assigned as the inside or outside salesperson on the contact record.
Required For:	• Handling EDI Custom Data on Orders • Setting up WIT Vendors • Entering User Defined Data for Entities • Invoice Batch File Layout for Third-Party Billing • Statement Batch File Layout for Third-Party Billing • Entering User-Defined Data for Products • Managing Contacts Through Contact Maintenance • Managing Fax Information • Managing Call Tracking Entries

CONTACT.PH.EMAIL.OE.UPD

New in Release 9.0.5

Allows users to update the contact's phone number or email address directly from the Sales order Entry Header tab. More:

Job Roles	Order entry personnel.
Levels	None.
Dependencies	None.
Additional Information	If unassigned, users must access Contact Maintenance directly to update the phone number or email address. Standard authorization applies.
	The CONTACT.MAINT authorization key is not required for this feature.

Control Maintenance Authorization Keys

The following authorization keys control a user's ability to view and edit restricted control maintenance records. Assign the following authorization keys only if Support has enabled this functionality for your system.

CONTROL.MAINT.EDIT

Allows access to edit restricted control maintenance records. More:

Job Roles	System Administrator or Manager
Levels	The level number, 0-999, determines which records the user can edit.
Dependencies	None.
Additional Information	Users assigned a level with this authorization key can edit restricted control maintenance records assigned a level equal to or less than their level. Users with the CONTROL.PARAMETERS.AUTH authorization key can set the authorization levels for each control maintenance record.
Required For:	Control Maintenance

CONTROL.MAINT.VIEW

Allows access to view restricted control maintenance records. More:

Job Roles	System Administrator or Manager
Levels	The level number, 0-999, determines which records the user can edit.
Dependencies	None.
Additional Information	Users assigned a level with this authorization key can view restricted control maintenance records assigned a level equal to or less than their level.
Required For:	Control Maintenance

CONTROL.PARAMETER.AUTH

Allows access to restrict users from viewing and editing designated control maintenance records. More:

Job Roles	System Administrator or Manager
Levels	Users with this authorization can assign view levels or other authorization key levels to control maintenance records to restrict who can view and edit the records.
Dependencies	To allow users to view restricted control maintenance records, assign one of the following: • The CONTROL.MAINT.VIEW authorization key with a level equal to or higher than the level assigned to the record. • Another designated authorization key and level required for viewing. To allow users to edit restricted control maintenance records, assign one of the following: • The CONTROL.MAINT.EDIT authorization key with a level equal to or higher than the level assigned to the record. • Another designated authorization key and level required for editing.

Additional Information	Assign control record levels in the Control Record Authorization screen, available through the system's Program Editor. If you leave the Control Record Authorization Maintenance screen blank for a control maintenance record, any user who has access to Control Maintenance can view and edit the settings for that control maintenance record. The Program Editor is located on the **System > System Programming** menu. Enter program **CONTROL.PARAMETER.MAINT**.
Required For:	Control Maintenance

Customer Maintenance Authorization Keys

The following authorization keys control a user's ability to use, view, and edit customer records.

CUST.BRANCH.EDIT

New in Release 9.0.2

Restricts users to edit customer information according to their home branch. More:

Job Roles	Sales personnel
Levels	• **Level 1** - Allows users to edit only customer whose home branch equals the user's home branch. • **Level 2** - Allows users to edit only customers whose home branch is included in the User's Branch Access List. • **Level 3** - Allows users to edit all customers regardless of their home branch assignment.
Dependencies	Users must also have CUSTOMER.MAINT, Level 2.
Required For:	Editing Sales Order Entry Header Information

CUST.BR.AUTH.ONETIME

Allows access to activate a customer for a one-time-only transaction in Sales Order Entry or Cash Receipts Entry, if the customer is *not* set up being active or inactive for the sales branch. More:

Job Roles	Sales personnel
Levels	Enter an authorization level, 0-99.
Dependencies	You can assign this authorization key only when you enable the **Display Customers/Vendors Who Are Inactive At A Branch** control maintenance record.
Additional Information	To set up a customer for a branch, list the branch on the customer's Accessible Branches window. A customer is inactive when the **Active** field for a branch on the Accessible Branches window in Customer Maintenance is set to **N** and active when the **Active** field is set to **Y**. When a user enters a transaction from a branch not listed on the customer's Accessible Branches window, the system displays the following prompts: Don't Activate, Activate for Branch, and Activate for Onetime Use. Users assigned an authorization level greater than or equal to the level entered in the **One-Time Activation Level** field on the customer's Accessible Branches window can activate the customer for a one-time-only transaction. When a user activates a customer for a one-time-only transaction, the system does not add the branch to the Accessible Branches window.
Required for:	• Entering Cash Receipts • Defining Customer Branch Override Capabilities • Viewing and Searching for Orders Using Quick SOE

CUST.BR.AUTH.OVRD

Allows access to permanently activate a vendor for transactions in Sales Order Entry or Cash Receipts Entry, if the customer is *not* set up as being active or inactive for the sales branch. More:

Job Roles	Sales personnel
Levels	Enter an authorization level, 0-99.
Dependencies	You can assign this authorization key only when you enable the **Display Customers/Vendors Who Are Inactive At A Branch** control maintenance record.
Additional Information	To set up a customer for a branch, list the branch on the customer's Accessible Branches window. A customer is inactive when the **Active** field on the Accessible Branches window is set to **N** and active when the **Active** field is set to **Y**. When a user enters a transaction from a branch not listed on the customer's Accessible Branches window, the system displays the following prompts: Don't Activate, Activate for Branch, and Activate for Onetime Use. Users assigned an authorization level greater than or equal to the level entered in the **Branch Activation Level** field on the customer's Accessible Branches window can activate the customer. When a user activates a customer, the system adds the branch to the customer's Accessible Branches window and sets the **Active** field to **Y**.
Required For:	Identifying Customers Who Can Buy Regulated Products

CUST.CERTIFY.EDIT

Allows access to edit the Product Certification Maintenance window. Required for Identifying Customers Who Can Buy Regulated Products.

CUST.CREDIT.EDIT

Allows access to view and edit the system default and customer record Credit Control Parameters. More:

CUSTOMER.MAINT	CUST.CREDIT.EDIT	Default Credit Control Parameters	Customer Credit Control Parameters
Not assigned	Not assigned	View	Cannot view
Not assigned	Assigned	Edit	Cannot view
Level 1	Assigned	Edit	View
Level 2	Assigned	Edit	Edit

Required For: Managing Credit Control Parameters

CUST.DEMAND.BR.OVRD

Allows access to edit the **Branch Demand Override** field on the Additional Customer Information window.

Required for: Entering Additional Customer Information

CUST.PH.EMAIL.OE.UPD

New in Release 9.0.5

Allows users to update the customer's phone number or email address directly from the Sales order Entry Header tab. More:

Job Roles	Order entry personnel.
Levels	None.
Dependencies	None.
Additional Information	If unassigned, users must access Customer Maintenance directly to update the phone number or email address. Standard authorization applies.
	Neither the CUSTOMER.MAINT or CUSTOMER.MAINT.LEVEL authorization key are required for this feature.

CUST.POINTS

Allows access to Points Maintenance to view and edit customer points information. More:

Job Roles	Sales personnel
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access to edit numbers in the **Redeemed** column. • **Level 3** - Allows access to edit numbers in the **Adjustments** column.
Additional Information	Use the **Edit Points** option on the Customer Point Maintenance window to access Points Maintenance.
Required For:	• Running the Customer Points By Price Line Report • Setting Up Products for the Customer Points Program

CUST.PRICING.EDIT

Allows a user with CUSTOMER.MAINT level 2 authorization to edit the data on the Customer Pricing/Printing window. More:

Required For:

- Assigning Primary Currencies to Foreign Customers
- Defining Customer Records for Faxed Statements
- Faxing Multiple Statements Posting
- Posting Service Charges to Past Due Accounts
- Printing Statements
- Defining Customer Invoice Printing Options
- Handling Currency for the Aged Receivables by Salesperson Report
- Changing Sales Order Currency

CUST.SALES.HIST.ALLOWED

Allows access to view data in the Customer Sales History file.

CUST.TAX.VIEW

Allows view-only access to the **Sales Tax** and **Tax Groups** menu options in Customer Maintenance. More:

Job Roles	Sales personnel
Levels	None.
Dependencies	None.
Additional Information	If a user is assigned this authorization key *or* the SOE.TAX.EDIT authorization, they have access to the **Sales Tax** and **Tax Groups** menu options in Customer Maintenance.
	In addition, consider the setting level in the CUSTOMER.MAINT.LEVEL authorization key and the **Customer Maintenance Authorization Levels** control maintenance record for the **Pricing** menu within Customer Maintenance.
Required For:	Managing Customer Tax through Customer Maintenance

CUSTOMER.MAINT

Allows access to Customer Maintenance to view and edit customer records. More:

Job Roles	Sales personnel
Levels	• **Level 1** - Allows access in view-only mode. However, a user assigned Level 1 of this authorization key can create new customers in sales order entry. • **Level 2** - Allows access in edit mode. If a user has Level 2 of this key, you also need to assign the correct levels in CUSTOMER.MAINT.LEVEL.
Dependencies	None.
Required For:	• A/R Collection Queue • A/R Inquiry • Bank Deposit Summary Report • Branch Maintenance • Customer Maintenance Authorization Levels • Contact Maintenance • Managing the Additional Customer Information Settings • Managing Customer Credit Control Parameters • Customer Maintenance • Fleet Maintenance Schedules • Product Location Maintenance • Sales Order Inquiries

CUSTOMER.MAINT.LEVEL

Restricts access to edit information in Customer Maintenance. More:

Job Roles	Sales personnel
Levels	To control a user's ability to edit customer information using a field, menu, or tab on the Customer Maintenance window, assign this key and an authorization level 0-99. The default level is 20.
Dependencies	This authorization key works with the **Customer Maintenance Authorization Levels** control maintenance record.
Additional Information	To use a field, menu option, or tab for editing purposes, the user's assigned level must be equal to or greater than the security level assigned to the designated field or menu option in the **Customer Maintenance Authorization Levels** control maintenance record. If a user is not authorized to edit information at the assigned level, menu options or tabs display information in view-only mode.
Required For:	• Managing the Additional Customer Information Settings • Managing Customer Credit Control Parameters • Customer Maintenance

SLSMN.CUSTOMER.MAINT

Allows the sales person to view and/or edit customer records and enter sales orders. More:

Job Roles	Sales personnel
Dependencies	Directly related to the CUSTOMER.MAINT authorization key. See Levels description below.

Levels:

If CUSTOMER.MAINT is...	and SLSMN.CUSTOMER.MAINT is...	The salesperson can...
Level 1	not assigned	• view customer records. • enter sales orders for customers.
	Level 1	• view customer records. • enter sales orders only for customers to whom the salesperson is assigned in Customer Maintenance.
	Level 2	• view customer records. • enter sales orders for customers. • edit the **InSlsp** and **OutSlsp** fields on the New Customer Entry window, only if the current value is this user's ID.
	Level 3	• view customer records. • enter sales orders for customers. • edit **InSlsp** and **OutSlsp** fields on the New Customer Entry window.

If CUSTOMER. MAINT is...	**and SLSMN. CUSTOMER. MAINT is...**	**The salesperson can...**
Level 2	not assigned	• edit customer records. • enter sales orders for customers.
	Level 1	• edit records only for customers to whom the salesperson is assigned as an Out Salesperson or In Salesperson in Customer Maintenance. • view records for customers to whom the salesperson is not assigned.
	Level 2	• enter sales orders for all customers. • edit customer records. • enter sales orders only for customers to whom the salesperson is assigned in Customer Maintenance.
	Level 3	• edit all customer records. • enter sales orders for all customers.

Dictionary Maintenance Authorization Keys

The following authorization key applies to accessing dictionary files.

DICT.MAINT

Allows access to the dictionary files, including access through the Report Writer/Mass Load programs.
More:

Job Roles	System Administrator.
Levels	This key is usually reserved for system administration personnel. • **Level 1** - Allows access to only view dictionary items. • **Level 2** - Allows access to view dictionary items and add new dictionary items. • **Level 3** - Allows access to edit dictionary items and add new dictionary items.
Dependencies	None.
Required For:	• Creating Order Entry View Elements • Entering User Defined Data for Entities • Creating Customer-Specific Prompts • Creating Dictionary Items • Validating Dictionary Items • Import Map Maintenance • Defining PDW Import Layouts • Mapping PDW Data Elements to Eclipse Dictionary Items • Mapping PDW Import Data • Report Writer/Mass Load

IMPORT.DICTIONARIES

Allows users to access and use Dictionary Import options.

Entity Authorization Keys

The following authorization keys control a user's ability to view and edit customer and vendor records.

ACT.TRIG.SUBR.OVRD

Allows access to edit information on the Subroutine Override window. More:

Job Roles	System Administrator.
Levels	None.
Dependencies	Users not assigned this authorization key can access these windows in view-only mode..
Additional Information	Accessed from Activity Trigger Maintenance, and the Activity Trigger Override Maintenance window in the Activity Trigger Subroutine Overrides control maintenance record.

ENTITY.PN.EDIT

Allows access to the Customer/Vendor Specific Part Numbers window. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Allows access to view items. • **Level 2** - Allows access to view and edit items. • **Level 3** - Allows access to also delete items.
Dependencies	None.
Additional Information	Users assigned this authorization key at any level who access the system through Remote Order Entry only have access in view-only mode.
Required for:	• Creating and Deleting Customer/Vendor Specific Part Numbers • Displaying the Customer/Vendor Specific Part Numbers • Viewing Customer/Specific Part Number Details

ENTITY.TRIGGER

Allows access to Activity Trigger Maintenance.

For users not assigned this key, the **Activity Trigger** option in Customer or Vendor Maintenance is not active.

Equipment Authorization Keys

The following authorization key applies to tracking equipment costs.

EQUIPMENT.MAINT

Allows access to Equipment Maintenance. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Allows access to view equipment maintenance information. • **Level 2** - Allows access to edit equipment maintenance information.
Dependencies	None.
Required For:	• Tracking Equipment Costs and Usage • Verifying Equipment A/P and Journal Entry Posting • Creating and Deleting Equipment Maintenance Records

Hot Swap Authorization Keys

The following authorization keys apply to the Hot Swap Server application.

SYNC.ACCOUNT.MAINT

Allows access to Sync Account Maintenance in the Hot Swap Server application. More:

Job Roles	System Administrator.
Levels	**Level 1** - Allows access to enter the Socket Communication Account Maintenance screen to create and edit individual sync accounts. Allows access to view the HotStandBy Status Inquiry screen.
	Level 2 - Allows access to manage system-level sync parameters, which affect more than one sync account, using the System Sync Parameters screen, the Sync Dataset Maintenance screen, and the Sync Configuration Maintenance screen. Allows access to use the **Reset Totals**, **Change Status**, and **Change Reporting Server** hot keys on the HotStandBy Status Inquiry screen.
Dependencies	None.
Additional Information	None.

SYNC.UPDATE.DATA

Allows access to verify and update sync account data. More:

Job Roles	System Administrator.
Levels	**Level 1** - Allows access to verify sync accounts from the Remote File Verification / Update screen and the Release Control Account Sync screen.
	Level 2 - Allows access to update sync account data on the Remote File Verification / Update screen, the Release Control Account Sync screen, and the Data Copying Utility.
Dependencies	None.
Additional Information	None.

Job Bid Authorization Keys

The following authorization key controls a user's ability to maintain job bids.

JOB.BID.MAINT

Allows access to Job Bid Maintenance to view and edit job bid information. More:

Job Roles	System Administrator.
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	None.
Additional Information	None.

Message Group Authorization Keys

The following authorization keys apply to accessing message groups.

MESSAGE.GROUP

Allows access to send messages to message groups. More:

Job Roles	Managers.
Levels	The level number, 1-99, determines the groups to which the user can send messages.
	Users can only send messages to groups with a security level equal to or less than their MESSAGE.GROUP level. For example, a user with a MESSAGE.GROUP level of 50 can send messages to groups assigned a security level of 50 or lower, but cannot send messages to groups with a security level of 51 or higher.
Dependencies	None.
Additional Information	Use the right-click **Detail** option to specify to message groups the users are allowed to make changes to. For more information, see Assigning Authorization Keys to Users.
	There is no connection between the MESSAGE.GROUP authorization key level assigned to a user and the ability of that user to view or edit the names of users in a message group. To prohibit a user from viewing or editing message groups, do not assign that user the Message Group Maintenance menu program.

MESSAGE.GROUP.TYPES

Limits access to view or edit only specified message group types in Message Group Maintenance. More:

Job Roles	Managers.
Levels	None.
	Superuser authorization does not include this authorization key. To set this key for a superuser, assign it in addition to the SUPERUSER authorization key.
Dependencies	If you assign this authorization key without specifying any detail, the user cannot view or edit any message group types. This authorization key is applicable only if the **Valid Message Group Types** control maintenance record defines message groups.
Additional Information	If you do not assign this authorization key, a user can view or edit all message group types.
	After assigning the authorization key, use the **Detail** option to display the Detail for MESSAGE.GROUP.TYPES Selection window, where you create the list of message group types the user can access.

Pricing Authorization Keys

The following authorization keys apply to Price Line Maintenance, Price Sheet Entry, Commission Plan Maintenance, and Pricing Management.

BR.AUTH.VIEW.PRIC

New in Release 9.0.2

Allows users to view product pricing information for their authorized branches. Authorized branches are based on the **Authorized** field in User Accessible Branches settings in User Maintenance.

BR.COST.ACTIVITY.VIEW

Allows access to view branch cost entries in the Product Activity Log and allows access to view the Branch Costs Inquiry window. More:

Job Roles	Purchasing Agents
Levels	None
Dependencies	• PRD.ACTIVITY.VIEW to view the Product Activity Log. • PRODUCT.MAINT to view the Branch Costs Inquiry window.
Additional Information	Assign this authorization key to anyone who needs to compare average cost, last, cost, landed average cost, or landed costs for products in a branch. The system maintains costs at the branch level because your buying patterns might differ across multiple branches. For information about the product activity log, see Viewing Product Activity Logs in the Manual Warehouse documentation. For information about viewing and comparing costs at each branch, see Viewing and Editing Branch Costs in the Pricing documentation.

BUY.SELL.GROUP.MAINT

Allows access to Buy/Sell Group Maintenance to view (Level 1) and edit (Level 2) records.

COMM.PLAN.MAINT

Allows access to Commission Plan Maintenance to view (Level 1) and edit (Level 2) commission plans.

PRICE.CHANGE.OVRD

Allows access to override pricing on a product that has a restricted matrix.

Required for: Creating Individual Matrix Cells

PRICE.LINE.MAINT

Allows access to Price Line Maintenance to view and edit records. More:

Job Roles	Purchasing agents.
Levels	**Level 1** - Allows access in view-only mode.
	Level 2 - Allows access to edit price lines listed in the VALID.PLINES authorization key.
	Level 3 - Allows access to edit all price lines.

Required For:	Price Line Maintenance Buy/Sell Group Maintenance Product Maintenance Combination Group Maintenance

PRICE.SHEET.ENTRY

Allows access to Price Sheet Entry to view and edit price sheets. More:

Job Roles	Purchasing Agents
Levels	**Level 1** - Allows access in view-only mode.
	Level 2 - Allows access to edit price lines listed in the VALID.PLINES authorization key.
	Level 3 - Allows access to edit all price lines.
Required For:	Price Sheet Entry

PRICE.SHEET.MAINT

Allows access to Product Price Sheet Maintenance to view or edit prices and costs. More:

Job Roles	Purchasing agents, pricing managers.
Levels	**Level 1** - Allows access in view-only mode.
	Level 2 - Allows access to edit prices and costs if the basis is 0.00, or the number of days since the basis was assigned a non-null value, or an effective date exceeds the days specified in the **Number Of Days After Which The Users Can Edit Old Prices** control maintenance record.
	Level 3* - Edit any local price sheet basis that is *not* marked to inherit values from the default price sheet.
	Level 4* - Allows access to edit all prices and costs on any price sheet except the tilde (~) price sheets. These are also called null price sheets.
	Level 5* - Allows access to edit all prices and costs on price sheets without restrictions.
Additional Information:	*** New or changed in Release 8.7.8.** During upgrade any users with previous Level 3 access are automatically switched to Level 5 access to ensure backward compatibility for users.
Required For:	Price Sheet Entry Assigning Pricing Values to Product Price Sheets Maintaining Price Sheets for Different Branches

PRICE.SHEET.UPDATE

Allows access to use the **Update Prices** option on the Price Sheet Entry window to display the Price Sheet Entry/Update window.

Required for: Manually Updating Prices and Printing Worksheets for Manual Updates

SELL.GROUP.REBATE.MAINT

Allows access to manage sell groups using Sell Group Rebate Maintenance. Users not assigned this authorization key cannot access this window. More:

Job Roles	Purchasing agents, pricing managers.
Levels	**Level 1** - Allows access in view-only mode.
	Level 2 - Allows access to edit prices sell groups.
Additional Information	Users not assigned this authorization key cannot access this window.
Required For:	• Creating Buy and Sell Groups • Creating Price Lines • Overriding Prices on Orders • Subtotaling and Repricing Job Bids • Subtotaling and Repricing Orders

SOE.MIN.SELL.PRICE

Allows the user to set a minimum sell price basis in the Buy/Sell Group Maintenance and, if repricing, allow the user to enter a price below the minimum sell price set. More:

The system checks the product's sell group first for a valid minimum price. If a basis field is not selected, the system defaults to the price line level.

In Sales Order Entry, if a user tries to manually override a selling price using the **Unit Price** field, the **GP%** field, the **Subtotals** option, or Job Bid Subtotal Maintenance the system compares the price entered to the price specified in the **Minimum Sell Price basis** field in Buy/Sell Group Maintenance. The user cannot change the price to less than the minimum price indicated.

Printer Authorization Keys

The following authorization key controls a user's ability to maintain printer location information.

PRINTER.LOCATION.MAINT

Allows access to Printer Location Maintenance to view and edit printer location information. More:

Job Roles	All users.
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Required For	Printer Location Maintenance

Product Maintenance Authorization Keys

The following authorization keys apply to Product Maintenance and Dynamic Kit Maintenance.

DYNAMIC.KIT.EDIT

Allows access to edit and create dynamic kits in Product Kit Maintenance. More:

Job Roles	Purchasing agents.
Levels	• **Level 1** - Allows access to edit a dynamic kit. • **Level 2** - Allows access to create a dynamic kit.
Required For	Creating Product Kits
Additional Info	Users not assigned this authorization key can only view data in Product Kit Maintenance.

MSDS.MAINT

Allows access to view and edit Hazard Classification information associated with a product on the MSDS Sheet Maintenance window. More:

Job Roles	Purchasing agents.
Levels	**Level 1** - Allows access to view Hazard Classification and MSDS information. The user cannot edit the information or attach MSDS sheets to products.
	Level 2 - Allows access to edit Hazard Classification and MSDS information and attach MSDS sheets to products.
Additional Info	Allows access to view and attach Material Safety Data Sheets (MSDS) to products on the Product MSDS Information window. Users cannot edit the information in the MSDS files. They can only attach the sheets to or delete the sheets from products. **Note:** Users with this authorization cannot attach MSDS sheets from the MSDS Review Queue. The MSDS Sheet Maintenance window in this instance is view-only.
Required For	• Product Maintenance • MSDS Sheet Maintenance

MTR.EDIT

New in Release 9.0.1

Allows users to enter and edit Mill Test Reports (MTR) heat numbers on the Enter Heat Numbers windows from Product Maintenance, Warehouse Confirmation Queue, and Sales Order Entry. More:

Job Roles	Sales order entry counter personnel.
Levels **New in Release 9.0.2**	• **Level 1** - Allows users to add required and new heat numbers, but cannot edit existing heat numbers. • **Level 2** - Allows users to create and edit heat numbers and MTR images. • **Level 3** - Allows users access for both Level 1 and Level 2, but users can also delete heat numbers and images.
Required For	Adding heat numbers and MTR images on orders.
Additional Info	While you can assign this authorization key through the Eterm application, the Mill Test Reports heat number features are only available through the Solar application.

NONSTOCK

Allows access to create and edit nonstock records. More:

Job Roles	Sales personnel required to enter nonstock products.
Levels	**Level 1** - Allows users assigned the SOE.ALLOWED, POE.ALLOWED, or TOE.ALLOWED authorization key access to create a record for a nonstock product and enter a price and cost. Once the user saves a new nonstock record, the information is view-only.
	Level 2 - Allows access to change the **Buy Line**, **Default List** price, **Price Base**, **Formula** and **G/L Type** fields, and use the **Pricing** option to display the Product Price Sheet Maintenance window.
	Level 3 - Allows access to change the **Default Cost** field.
	Level 4 - Allows access to change the description of a product defined as a nonstock in Eclipse, and activates the **Product Maintenance** option on the NonStock Entry window.
Required For	• Managing Global Buy/Sell Basis Names in Price Lines • Copying Transfers to Bids • NonStock Entry • Procurement Confirmation • Product Price Sheet Maintenance • Picking Products with the RF In Process Screen • Receiving Products with the RF Recv Verify Screen • Posting Dead Stock Products to Trading Partner Connect • Work Order Entry Material Detail
Additional Information	To allow a user to change the product unit of measure on the NonStock Entry window, also assign the OE.NSTK.UOM.EDIT authorization key.

PRD.SUBS.MAINT

Allows access to use the **Substitute** option in Product Maintenance to assign substitute products to a product record. More:

Job Roles	Purchasing agents.
Levels	None.
Additional Info	Allows access to use the **Substitute** option, in purchase order entry, sales order entry, and transfer order entry to make substitutions on an order.
Required For	• Purchase Order Inquiries • Marking Products as Substitutes • Using Inventory Inquiry for Substitute Products • Sales Order Inquires

PRODUCT.FAMILY.MAINT

Allows access to Product Family Maintenance to view and edit product families. More:

Job Roles	Users on sites with WOE activated.
Levels	• **Level 1** - Allows access to view product families. • **Level 2** - Allows access to edit product families.
Required For	Product Family Maintenance

PRODUCT.MAINT

Allows access to Product Maintenance. More:

Job Roles	Sites with WOE activated.
Levels	**Level 1** - Allows access to only view product records. All options except for **Delete**, **Copy**, and **Sequence** on the Product Maintenance window are available in view-only mode.
	Level 2 - Allows access to create and edit product records in the buy lines and price lines for which the user is authorized. Access to the Branch Costs window is view-only. **Note:** To activate the **Product Location Maintenance** option on the Product Maintenance window for users, also assign the PRD.LOCATION.MAINT authorization key.
	Level 3 - Allows additional access to edit data on the Branch Costs window.

Required For	• Suggested Work Order Queue • Branch Costs Inquiry • Viewing and Editing Branch Costs • Catalog Maintenance • Eclipse B2B Commerce • Editing and Verifying PDW Product Updates • Exporting PDW Data to the Eclipse Product File • PDW Mass Product Import • Verifying PDW Products Assigned to a Price Sheet • Verifying Price Sheets For PDW Price Updates • PDW / Eclipse Product File Sync Utility • PDW Catalog Search • PDW Data Viewer • Inventory Inquiry • Defining Tracker Task Codes in Task Code Maintenance • Customer Specific Part Number • NonStock Product Entry • Entering Inventory Counts • Purchase Order Inquiries • Verifying Price Sheets for PDW Price Updates • Adding New Products While Updating Prices • Auto Updating Product Pricing Information • User Defined Auto Price Updating • Resequence Buy Line • Product Family Maintenance • Resequence Price Line • Creating Product Kits • Creating Product Records • Defining Accessible Branches for Products • Defining Original Tire Tread Depth for Products • Defining Vendor Catalog Locations for Products • Displaying Product Records • Enabling Stock/Nonstock Determination for Products • Entering Miscellaneous Product Information • Maintaining MSDS Records

	• Setting Minimum Gross Profit Percentages for Products • Setting Product Buy Package Quantities • Setting Up Products for the Customer Points Program • Using Product Family Selection • Viewing Product Demand and Procurement • Setting Units of Measure for Product Records • Defining Pricing in Foreign Currencies • Assigning Pricing Criteria to Products • Assigning Pricing Values to Product Price Sheets • Creating Price Lines • Defining Data Sources and Columns for Price Sheets • Sales Order Inquiries • Strategic Pricing Product Maintenance • Transfer Order Inquiries • Trading Partner Connect • Work Order Inquiries

PRODUCT.MAINT.LEVEL

Restricts access to edit information in Product Maintenance. More:

Job Roles	Users required to use product maintenance.
Levels	None.
Additional Information	This authorization key works with the **Product Maintenance Authorization Levels** control maintenance record.
	To control a user's ability to edit product information using a field or menu option on the Product Maintenance window, assign this key and an authorization level 0-99. The default level is 20. To use a field or menu option for editing purposes, the user's assigned level must be equal to or greater than the security level assigned to the designated field or menu option in the **Product Maintenance Authorization Levels** control maintenance record. If a user is not authorized to edit information at the assigned level, menu options display information in view-only mode.
	To give a user unrestricted access to editing information in Product Maintenance, assign PRODUCT.MAINT level 2, but do not assign this key.
Required For	• Product Maintenance

Ship Via Authorization Keys

The following authorization key applies to Ship Via Maintenance.

SHIP.VIA.MAINT

Allows access to Ship Via Maintenance:

- **Level 1 -** Allows access in view-only mode.
- **Level 2 -** Allows access in edit mode.

Terminal Authorization Keys

The following authorization key controls a user's ability to maintain terminal information.

TERMINAL.SETUP

Allows access to Terminal Setup to view (Level 1) and edit (Level 2) terminal information.

Terms Authorization Keys

The following authorization key applies to Terms Maintenance.

TERMS.MAINT

Allows access to Terms Maintenance to view (Level 1) and edit (Level 2) records.

User Maintenance Authorization Keys

The following authorization keys apply to maintaining user records and accessing the User Job Queue.

AUTH.PWD.MAINT

Allows access to create authorization passwords to allow users access to authorization-protected tasks. More

Job Roles	System Administrators, Managers
Levels	The level number, 1-999, determines the type of authorization passwords the user can create.
	Level 0 - The user can create a password set for one-time use. The system deleted the password from the list after one use.
	Levels 1 to 998 - The user can create a password for multiple use for the number of days equal to the level number. If the user changes the expiration date, it cannot be later than the system-generated date or earlier than the current date. The system deletes the password from the list following the expiration date.
	Level 999 - The user can create a password set for multiple use with no expiration date. The password is available for use until the user removes it from the list.
Dependencies	None
Examples	For example, only authorized users can approve pricing adjustments that exceed defined limits. Typically, these users are in management positions. When a non-authorized user enters a pricing adjustment in order entry that exceeds the designated limits, the system displays the following prompt: Enter Authorized Password. • Authorized users can enter their Eclipse password at the prompt. For example, an authorized manager walks over to the order taker's terminal and enters the manager's Eclipse password. • Authorized users can create authorization passwords, which they can tell another user to enter on their behalf. The user requesting the override enters the authorization password at the prompt. This eliminates the need for a manager to walk over to the other user's terminal to respond to the prompt.
Additional Information	Every time a user enters an authorization password at a password prompt, the system sends a message to the user who created the password that describes the password, who used it, and the reason for using it. For one-time password, the message also indicates that the password is now expired.

BB.MAINT.EDIT.ALL

New in Release 9.0

Allows users to edit all messages in the Bulletin Board Maintenance window regardless of who created them.

USER.BRANCH.MAINT

Allows access from User Maintenance to view and edit the branches and territories a user can access. More

Job Roles	System Administrators, Managers
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	USER.MAINT.ALLOWED
Additional Information	In addition to assigning branches to a user, this authorization key allows you to set limits to only inventory inquiries or only sales order functions in a branch, as needed. For more information about users' branch assignments, see Assigning Branches to Users in the Application Maintenance documentation.

USER.JOB.QUEUE

Allows access to view user job queues. More

Job Roles	System Administrators, Department supervisors or managers
Levels	• **Level 1** - Allows access to view the user's own queue. • **Level 2** - Allows access to view any user's queue. • **Level 3** - The same as level 2.
Dependencies	None
Additional Information	Typically, assign Level 2 to department supervisors or managers who would need access to a user's queue in that user's absence. Users not assigned this key have the equivalent of Level 1 authorization.

USER.KEY.MAINT

Allows access from User Maintenance to view or edit authorization keys. More

Job Roles	System Administrators, Department supervisors or managers
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	USER.MAINT.ALLOWED
Additional Information	The system does not save authorization key edits made by users assigned USER.MAINT.ALLOWED level 1.

USER.MAINT.ALLOWED

Allows access to the User Maintenance window. More

Job Roles	System Administrators, Department supervisors or managers
Levels	• **Level 1** - Allows access to view user records. • **Level 2** - Allows access to view and create user records. • **Level 3** - Allows access to view, create, and edit user records.

Dependencies	None
Additional Information	To access more advanced settings when creating user records, such as setting passwords and defining branch access, you need to assign the other authorization keys described in this topic for individual set up areas.
Required For:	• Assigning Custom Menus • Creating User Records • Using Prototyping to Create User Records

USER.PASSWORD.EDIT

Allows access to edit the password of any user and modify the password parameters. More

Job Roles	System Administrators
Levels	None
Dependencies	USER.MAINT.ALLOWED
Additional Information	Only system administrators should be assigned this key.

USER.TERR.MAINT

Allows access from User Maintenance to view and edit the types of territories (reporting, viewable, and editable) for which a user is authorized. More

Job Roles	System Administrators, Department supervisors or managers
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	USER.MAINT.ALLOWED
Additional Information	Companies generally use territories for inquiry and reporting purposes. Users can have different levels of access to territories. You can authorize some users to use territories only for reporting purposes, Level 1, and others to view and edit the branches assigned to the territories, Level 2.
Required for:	Defining Authorized Territories for Users

USER.VIEW.SELECT

Allows access from User Maintenance to view or edit the sales, purchase, and transfer order entry views and templates assigned to a user. More

Job Roles	System Administrators, Department supervisors or managers
Levels	• **Level 1** - Allows access in view-only mode. • **Level 2** - Allows access in edit mode.
Dependencies	USER.MAINT.ALLOWED
Additional Information	Because not all views are appropriate for all users, assign each user the order entry views related to their job function.
Required for:	• Assigning Order Entry Views and Templates to Users • Editing Order Entry View Templates

Vendor Maintenance Authorization Keys

The following authorization keys control a user's ability to use, view, and edit vendor records.

VEN.BR.AUTH.ONETIME

Allows access to activate a vendor for a one-time-only transaction in Purchase Order Entry or A/P Entry, if the vendor is *not* set up as being active or inactive for the purchasing branch. More:

Job Roles	Managers who want to grant access to users for one-time-only transactions for a specific vendor.
Levels	Enter an authorization level, 0-99.
	Users assigned an authorization level (0-99) greater than or equal to the level (0-99) entered in the **One-Time Activation Level** field on the vendor's Accessible Branches window can activate the vendor for a one-time-only transaction.
	When a user enters a transaction from a branch not listed on the vendor's Accessible Branches window, the system displays the following prompts: Don't Activate, Activate for Branch, and Activate for Onetime Use.
Dependencies	To set up a vendor for a branch, list the branch on the vendor's Accessible Branches window. Activate the vendor by setting the **Active** field to **Y**.
Additional Information	When a user activates a vendor for a one-time-only transaction, the system does not add the branch to the Accessible Branches window. You can assign this authorization key only when you set the **Display Customers/Vendors Who Are Inactive At A Branch** control maintenance record to **Yes**.
Required For	Defining Vendor Branch Override Capabilities

VEN.BR.AUTH.OVRD

Allows access to permanently activate a vendor for transactions in Purchase Order Entry and A/P Entry, if the vendor is *not* set up as being active or inactive for the purchasing branch. More:

Job Roles	Managers who want to grant access to users for one-time-only transactions for a specific vendor.
Levels	Enter an authorization level, 0-99.
	Users assigned an authorization level greater than or equal to the level entered in the **Branch Activation Level** field on the vendor's Accessible Branches window can activate the vendor.
Dependencies	To set up a vendor for a branch, list the branch on the vendor's Accessible Branches window. Activate the vendor by setting the **Active** field to **Y**.
Additional Information	When a user enters a transaction from a branch not listed on the vendor that is not designated as active or inactive for a branch, the system displays the following prompts: Don't Activate, Activate for Branch, and Activate for Onetime Use.
	When a user activates a vendor, the **Active** field on the Accessible Branches window in Vendor Maintenance changes from **N** to **Y**. You can assign this authorization key only when you enable the **Display Customers/Vendors Who Are Inactive At A Branch** control maintenance record.
Required For	Defining Vendor Branch Override Capabilities

VEND.REBATE.EDIT

New in Release 9.0

Allows users to view and edit Vendor Volume Rebate program information, run the Vendor Volume Rebate Build, and purge program information. Users must also be assigned VENDOR.MAINT Level 1 or higher.

VEND.REBATE.VIEW

New in Release 9.0

Allows users to view in view-only mode the Vendor Volume Rebate program information, the Vendor Volume Rebate Build, and purge program information. Users must also be assigned VENDOR.MAINT Level 1 or higher.

VENDOR.MAINT

Allows access to Vendor Maintenance to view and edit vendor records. More:

Job Roles	Users required to view or edit vendor records.
Levels	**Level 1** - Allows access in view-only mode.
	Level 2 - Allows access in edit mode.
	Further definition of user-level access described in VENDOR.MAINT.LEVEL.
Dependencies	If a user has Level 2 of this key, you also need assign the correct levels in VENDOR.MAINT.LEVEL.
Additional Information	None.
Required For	• A/P Inquiry • Assigning Vendors to Buy Lines • Specifying the Vendor Target for Buy Lines • Adding Vendors to Contact Maintenance Using a Wizard • Creating Vendor Records • Entering Additional Customer Information • Inquiring About Purchase Orders

VENDOR.MAINT.LEVEL

Allows access to edit vendor information by level to each field in Vendor Maintenance. More:

Job Roles	Users required to edit vendor records.
Levels	To control a user's ability to edit vendor information using a field or menu option on the Vendor Maintenance window, assign this key and an authorization level 0-99. The default level is 20.
	To use a field or menu option for editing purposes, the user's assigned level must be equal to or greater than the security level assigned to the designated field or menu option in the **Vendor Maintenance Authorization Levels** control maintenance record. If a user is not authorized to edit information at the assigned level, menu options display information in view-only mode.
Dependencies	This authorization key works with the **Vendor Maintenance Authorization Levels** control maintenance record.

Additional Information	None.
Required For	Creating Vendor Records

Zip Code Authorization Keys

The following authorization keys apply to creating and deleting zip codes.

ZIP.CODE.ENTRY

Allows access to Zip Code Maintenance. More:

Job Roles	Users required to manage zip codes for customers.
Levels	**Level 1 -** Allows access in view-only mode. The windows displayed from Zip Code Maintenance using the **Branch Tax Jurisdiction Override** and **Ship Vias by Branch** options are also view-only.
	Level 2 - Allows access in edit mode. Also allows access to create a new zip code when creating a new customer in sales order entry.
Dependencies	None.
Required For	Maintaining Zip Codes

ZIP.CODE.DELETE

Allows access to delete a zip code.

Index