Infor LX CEA Access Control User Guide

8.4 or later

Copyright © 2020 Infor

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

Publication Information

Release: Infor LX 8.4 or later

Publication date: December 15, 2020

Contents

About this guide **5**
Intended audience 5
Related documents 5
Contacting Infor 5

Chapter 1 Introduction **7**
Verifying Installation of CEA Products 7

Chapter 2 Using CEA Access Online **9**
Using Product Access Control 9
Creating a User Profile 9
Setting Product Access Control for a UserProfile 10
Using Program Access Control 14
Setting Program Access Control for a User Profile 15
Using Function/Action Access Control 17
Understanding Function/Action AccessControl 17
Basic Functions and Actions 17
Create 18
Revise 18
Copy 19
Delete 19
Display 19
Application-Specific Functions andActions 20
Add Reject and Add Allow 21
Post, Approve, and Void 21
Transfer 22
Allocation 22
Consolidations and Translations 22
Execute 22
Period 22

Select....23
De-Select....23
Setting Function/Action Access Control....23
Setting Function/Action Access Control for User Groups....23
Associating User Profiles with User Groups....26

Chapter 3 Security Rules....29

Security Rules....29
Setting up User Groups....29
Results of Security Rules....30
Events Processing....30
Account Inquiry/Structure Inquiry....30
Creating Rules....30
Example 1....31
Segment Rule 1....31
Segment Rule 1 - Allow seq. 1....31
Segment Rule 1 - Allow seq. 2....31
Example 2....31
Account Rule 1....31
Account Rule 1 - seq. 1....32
Example 3....32
Segment Rule 1 (No Allow Rule)....32
Account Rule 1....32
Account Rule #1 - Allow seq. 1....32
Account Rule #1 - Allow seq. 2....32
Assigning a Security Code to a User Group....32
Setting Security Rules for a User Group....33
Activating Security Rules....36

About this guide

Intended audience

System Administrators and Financial Administrators responsible for configuring user access to CEA menus, programs, and CEA account access.

Related documents

You can find the documents in the product documentation section of the Infor Support portal, as described in "Contacting Infor" on page 5.

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1 Introduction

The Access Control features of Infor LX Configurable Enterprise Accounting (CEA) provide you with flexibility that allows many users to access financial information, while limiting user access to critical and confidential financial information. CEA has three levels of control that allow you to set up varying degrees of user information access.

- Product Access Control - This is the highest level of access control. Use this level to limit access to the CEA products for individual users.
- Program Access Control - This is the middle level of access control. This level is optional. Use this level to limit access to applications in the CEA products for individual users.
- Function/Action Access Control - This is the lowest level of access control. Use this level to limit access to the actions or functions in the CEA applications for a group of users.

Verifying Installation of CEA Products

You must install the CEA products on your system before you can set up any levels of access control. When you install the CEA products, they are disabled. You must set up access control to use these products.

To verify which CEA products are installed on your system, use the Installed Products Format (SYS821) program in the System Parameters application. Perform these steps:

1. Access the Infor LX applications.
2. On the SYS menu, select System Parameters Maintenance, SYS800D.
3. On the Infor LX System Parameter Generation screen, SYS800D-01, specify 5=Display next to Installed Products Format line.
4. Press **Enter**.
5. The system displays the Installed Products Format screen. This screen lists the products that are installed on your system. Verify that the CEA products are installed.

Chapter 2 Using CEA Access Online

Using Product Access Control

Set up product access control in the Security Maintenance (SYS600) program in the System Parameters application.

Product Access Control limits user access to the five CEA applications:

- Configurable Ledger (CLD)
- Advanced Budgeting and Analysis (CBA)
- Enterprise Structures and Consolidations (ENT)
- Configurable Currency Translation (CCT)
- Advanced Transaction Processing (ATP)

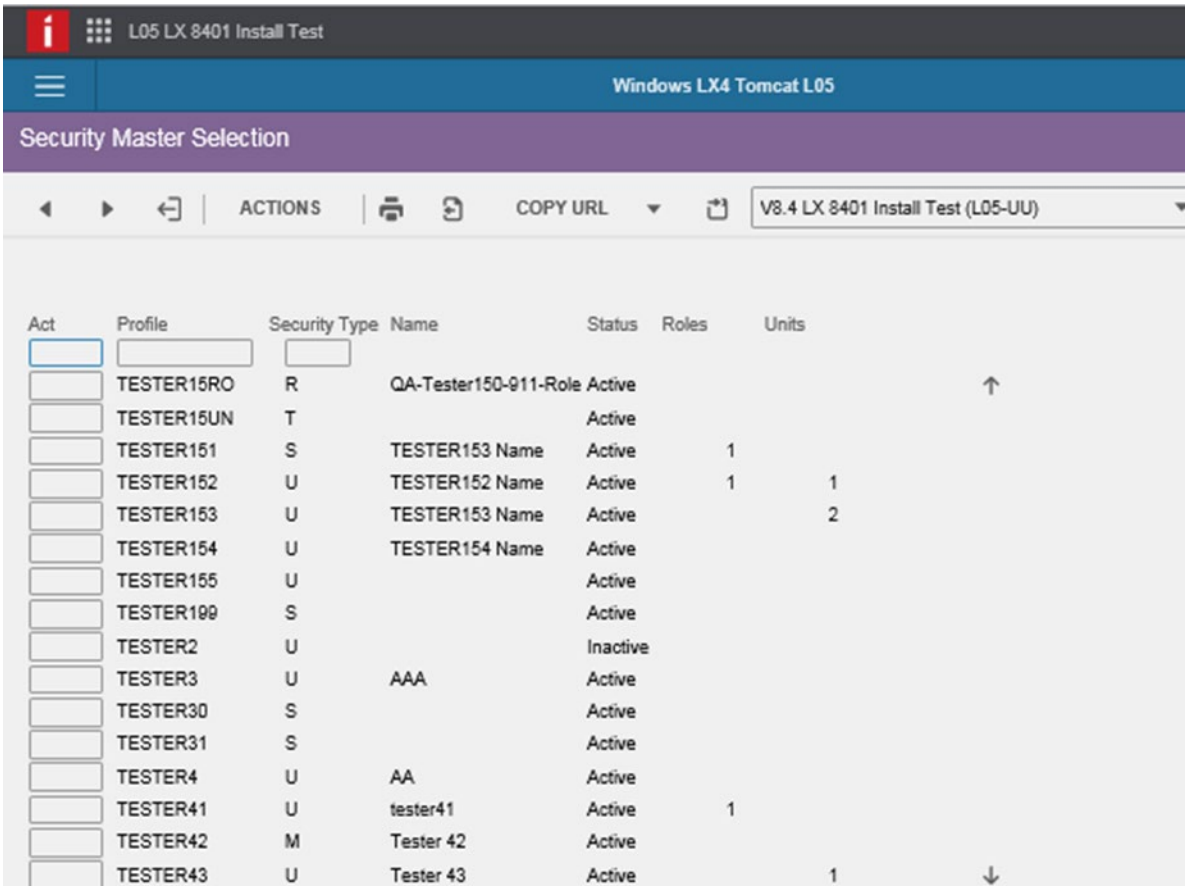
Manage product access control through user profiles. To use the CEA applications, each user must have a unique user profile. The user profile is then associated with a list of products that the user can and cannot access. In addition, you can associate the user profile with a user group, with additional access control levels. The Infor LX Access Control Officer adds, changes, and deletes user profiles in Security Maintenance (SYS600) in the System Parameters application.

Creating a User Profile

To add a user profile, perform the following steps:

1 Access the Infor LXsoftware.

2 On the SYS menu, select User Authorization Maintenance, SYS600D1. The system displays the Security Master Selection (SYS600D1-01) screen. This screen displays a list of user profiles and their associated security type and status.



3 On the first line, specify **1=Create** and enter a user profile and a security type. To copy an existing user profile, specify **3=Copy** next to the user profile then press enter and enter a new user profile and security type.

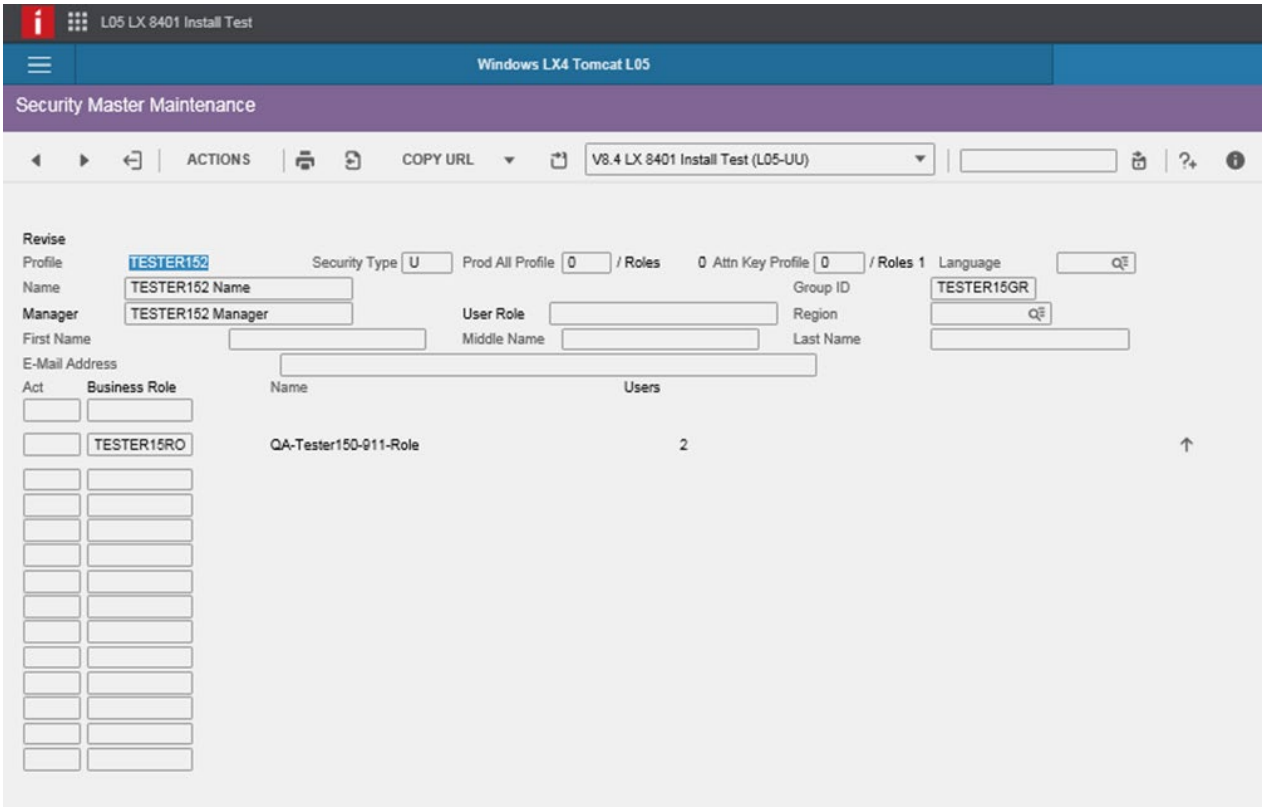
4 Press **Enter**. The system displays the Security Master Maintenance screen.

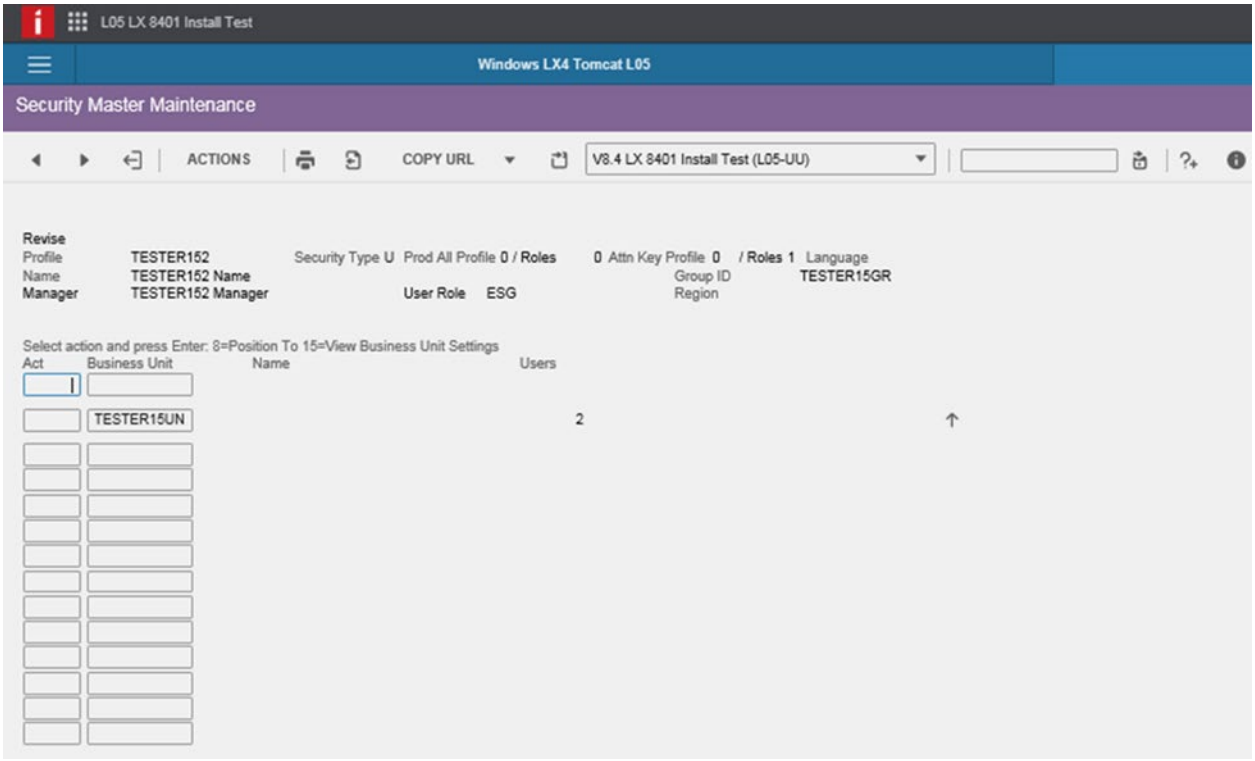
5 Use this screen to assign product access to a user profile. If you are copying an existing user profile, specify the User ID for the new user.

Setting Product Access Control for a User Profile

After you create a user profile, complete the options on the Security Master Maintenance screen. To set product access control, perform the following steps:

1 Create or select a user profile on the Security Master Selection screen. The system displays the Security Master Maintenance screen.


L05 LX 8401 Install Test
Windows LX4 Tomcat L05
Security Master Maintenance
ACTIONS
COPY URL
V8.4 LX 8401 Install Test (L05-UU)
Revise
Profile TESTER152
Security Type U
Prod All Profile 0 / Roles 0
Attn Key Profile 0 / Roles 1
Language
Name TESTER152 Name
Group ID TESTER15GR
Manager TESTER152 Manager
User Role
Region
First Name
Middle Name
Last Name
E-Mail Address
Act
Business Role
Name
Users
TESTER15RO
QA-Tester150-911-Role
2


L05 LX 8401 Install Test
Windows LX4 Tomcat L05
Security Master Maintenance
ACTIONS
COPY URL
V8.4 LX 8401 Install Test (L05-UU)
Revise
Profile TESTER152
Security Type U
Prod All Profile 0 / Roles 0
Attn Key Profile 0 / Roles 1
Language
Name TESTER152 Name
Group ID TESTER15GR
Manager TESTER152 Manager
User Role ESG
Region
Select action and press Enter: 8=Position To 15=View Business Unit Settings
Act
Business Unit
Name
Users
TESTER15UN
2

2 Complete the options on this screen. These options determine the type of access control for this user.

Security Type

Indicate the type of access control for this user. Select one of the following types:

- **S** - Security Officer
- **O** - Operator
- **P** - Programmer
- **D** - Database Administrator
- **U** - User
- **M** – Security Manager
- **T** – Business Unit
- **R** – Role (Business Role)

Prod All

Specify **1** to authorize the user to a list of all Infor LX applications. Otherwise, specify 0=No or Blanks = Determined by Role(s) assigned to user.

Attn Key

Specify **1** to authorize the user to the Attention Key. Otherwise, specify 0=No.

Language

Specify the language of the user. The default is blank and it is used for English.

Group ID

Indicate the group to which this user is assigned for group options, commands, and applications. This Group ID is used for the Function/Action level of CEA Access Control. For additional information, see the Function/Action section.

Region

Specify the region code to associate with this User ID.

Name

Specify the profile’s name

Manager

Enter the manager’s name

Role

Specify the profile’s role

First Name

Enter the first name of the User ID

Middle Name

Enter the middle name for the User ID

Last Name

Enter the last name for the User ID

E-mail address

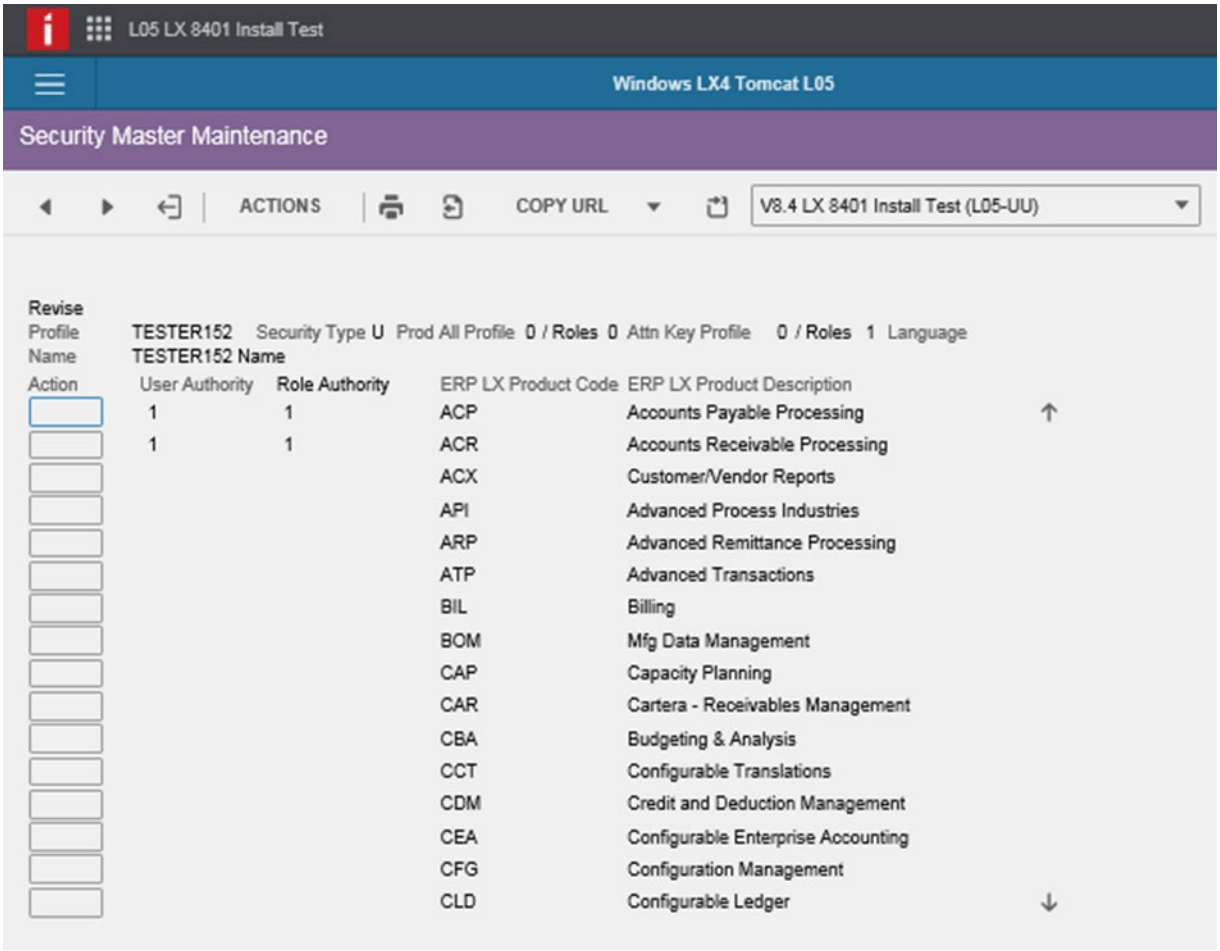
Enter the e-mail address for the User ID

Business Role

Specify the role or business role to assign to the user profile.

Business Unit

Specify the business unit to assign to the user profile.



3 Complete the options on this screen. These options determine the type of access control for this user.

Authority

Determine whether the user is authorized to access each listed application. Valid options are:

1 = Authorized to the product

0 = Not authorized to the product

Blanks = Determined by Role(s) assigned to user

LX Product Code

Lists the three-letter codes that identify the applications.

LX Product Description

Displays the descriptive names for the product codes.

4 Press **Enter**. The system saves the product access control information and displays the Security Master Maintenance - Programs screen, where you can set up Program Access Control. For information on setting up Program Access Control, see the following section.

Using Program Access Control

Program Access Control limits user access to certain applications in the CEA products. This level of access control is optional. You can set up Program Access Control in two ways:

- A user has access to an application, but is denied access to a specific program in that application
- A user is denied access to an application, but is allowed access to a specific program in the application

The following table lists all the CEA programs and the products they belong to.

Program Code	Program Description	Product
CEA107D1	Macro Definition	ATP
CEA110D1	Subsystem Event Determination	ATP
CEA111D1	Allocation Definition	CBA
CEA104D1	Alias Definition	CLD
CLD109D1	Exchange Rate Definition	CLD
CEA101D1	Chart of Accounts Definition	CLD
CLD107D1	Currency Definition	CLD
CEA106D1	Account Cross Reference	CLD
CEA105D1	Ledger Definition	CLD
CEA500D1	Events Processing	CLD
CEA108D1	Model Definition	CLD
CEA300D1	Account Inquiry Definition	CLD
CEA100D1	Segment Definition	CLD

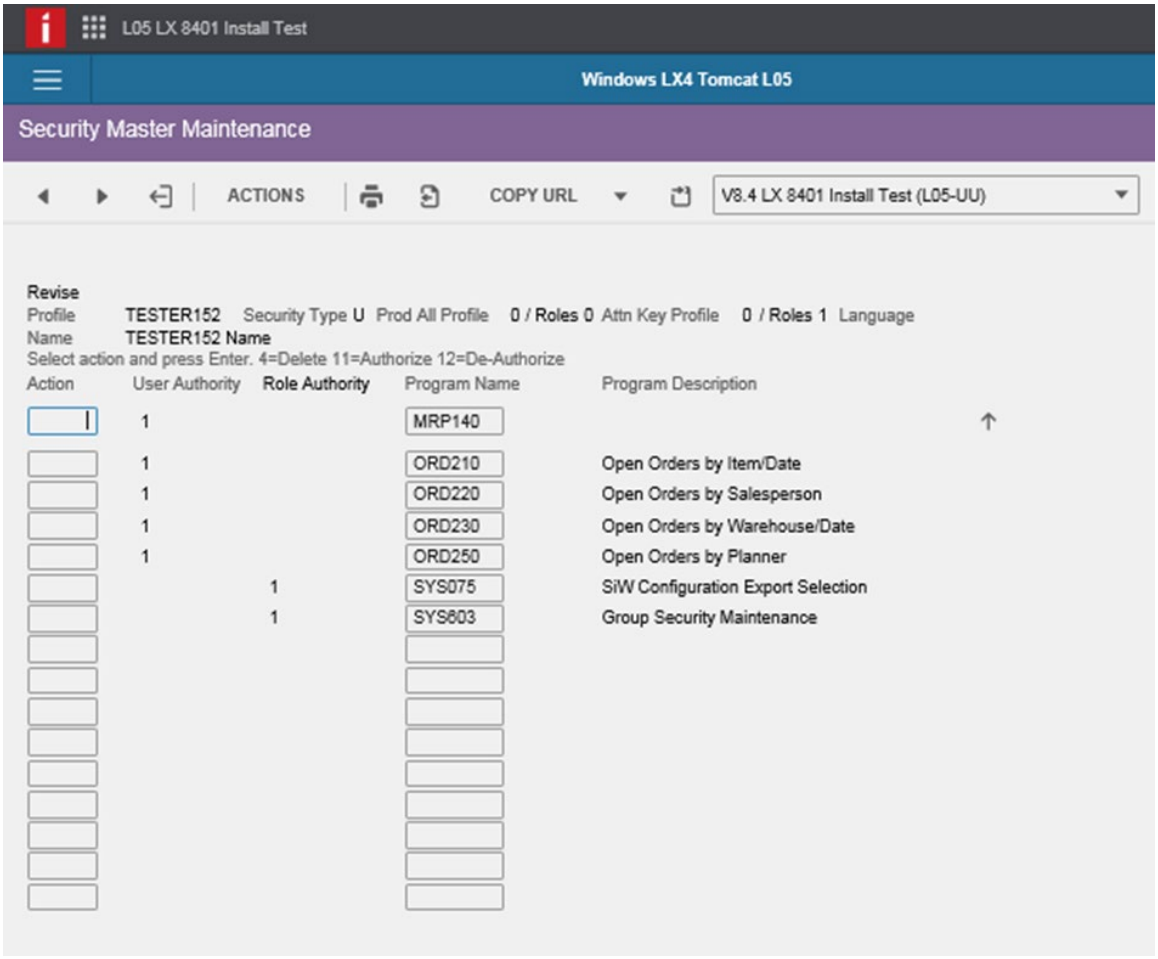
Program Code	Program Description	Product
CEA102D1	Period Table Definition	CLD
CEA109D1	Event Definition	CLD
CEA103D1	Account Rules Definition	CLD
CLD185D1	Rate Type Definition	CLD
CEA116D1	Process Monitor	CLD
CEA312D1	Structure Inquiry	ENT
CEA113D1	Consolidation Mapping Definition	ENT
CEA114D1	Process Definition	CLD
CEA115D1	Process Sequence Definition	CLD
CEA112D1	Structures Definition	ENT
CEA310D1	Journal Inquiry Processing	CLD
CEA510D	Journal Entry Review	CLD
CLD540D2	Post Deferred	CLD

Setting Program Access Control for a User Profile

You can also manage program access control through user profiles. To maintain program access control, the security officer must first create a user profile. See Creating a User Profile for more information.

To set program access control for a user, perform the following steps:

1. Access the Infor LX software.
2. On the SYS menu, select User Authorization Maintenance, SYS600D1. The system displays the Security Master Selection (SYS600D1-01) screen. This screen displays a list of user profiles and their associated security type and status.
3. Select a user profile and specify **Revise**. The Security Master Maintenance screen displays the user profile you selected for maintenance.
4. Press **Enter**. The system displays the Security Master Maintenance - Programs screen.



If you set the Security Type to **User** and authorize the user to all Infor LX products, you cannot use this screen to set Program Access Control.

5 Complete the fields on this screen.

Authority

Determines whether the user is authorized to this program. The valid values are:

0 = **Not authorized to the user**. The user cannot use this program.

1 = **Authorized to the user**. The user can use this program.

Blanks = Determined by Role(s) assigned to user.

You can grant authorization for an entire application but specify exceptions, or revoke authority for an entire application but allow inclusion on the Security Master Maintenance – Program screen.

Program Name

Specify the first six-characters of the object code assigned to a menu option. For example, the object code for Period Table is CEA102D1. Specify CEA102.

6 Press **Enter**.

7 The system saves the Program Level Access Control information and displays the next screen, which is not related to CEA Access Control. Click **Cancel** to exit this screen.

Using Function/Action Access Control

Function/Action Access Control limits the types of functions or actions that a user can perform in a particular program. This access control differs from Product and Program Access Control in the following ways:

- It is assigned to a user group instead of a user profile. These user groups are then associated with individual user profiles.
- It is assigned by program.

You set up Function/Action access control levels in the Group Security Maintenance (SYS603) program.

Understanding Function/Action Access Control

For users to have Function/Action access control in a program, they must first have access to the program. You can set up this access three ways:

- The user has access to the entire application
- The user has access to the application but is denied access to certain programs in the application
- The user does not have access to the application but does have access to certain programs in the application

When the user has access to the program, the following describes how Function/Action access control works:

1 When the user accesses the program, the system checks the Group Security Maintenance program for the group associated with this user.

2 If this group is denied access to certain functions or actions in that program, the system disables the menu options and buttons for the denied functions and actions.

In addition, access control that applies to parent records also applies to any associated child records.

Basic Functions and Actions

This section lists and explains the basic functions and actions that apply to most of the CEA programs.

Most of the CEA programs include the following four basic functions and actions:

- Create
- Revise
- Copy
- Delete
- Display

Create

When you have Create authority:

- You can add records to a file
- When you have Create authority for a parent record, you automatically receive Create authority for all child records, unless a program-specific access control parameter prevents this

When you are denied Create authority:

- You cannot add records to a file
- The system disables all related line actions and screen actions (**Accept**,
- **Create**, and **New Event**)

The **Create** function is not available in the Journal Inquiry (CEA310D1) and Post Deferred (CLD540D2) programs.

Revise

When you have Revise authority:

- You can change the field values of records in a file.
- You should also have Display authority to view records using the appropriate line actions.
- You can activate parent and child records that have a status of inactive.
- When you have Revise authority for a parent record, you also automatically have Revise authority for all child records.

When you are denied Revise authority:

- You cannot change the field values of records.
- The system disables all related line actions and screen actions (**Update** and **Activate**).

You may have Revise authority for a parent record, but you cannot add or delete any child records unless you also have Create and Delete authority.

The **Revise** function is not available in the Post Deferred (CLD540D2) program.

Copy

When you have Copy authority you can copy a record with all its details to create a new record.

When you are denied Copy authority, you cannot copy a record.

Delete

When you have Delete authority

- You can deactivate or erase records from a file
- You should also have Display authority to view records using the appropriate line actions
- When you have Delete authority for parent records, you also have Delete authority for all child records unless a program-specific access control parameter prevents this

When you are denied Delete authority:

- You cannot deactivate or erase records from a file
- The system disables all related line actions and screen actions (**Delete** and **Delete** key)

Authority can be provided to a group in Group Maintenance, SYS603, to make the Delete option available in Journal Inquiry Processing (CEA310D1) for non-posted journals. A user must be a member of the group to have the Delete option available to them.

The Delete option is not available in the Account Cross Reference (CEA106D1) program.

Display

When you have Display authority:

- You can view the records in a file.
- When you have Display authority for a parent record, you also automatically have Display authority for all child records, unless a program-specific access control parameter prevents this.

When you are denied Display authority:

- You cannot view records in a file.
- The system disables all related line actions and screen actions (**Display**).

With Display authority, you may have the authority to view data but not have the authority to change it.

Application-Specific Functions and Actions

This section lists and explains some of the functions and actions that are unique to individual programs. These functions and actions allow you to set up additional access control for critical functions or access to sensitive information.

These functions and actions and the programs they affect are listed in the table below.

Function or Action	Programs Affected
Translate	Segment Definition
Add Allow	Account Rules
Add Reject	Account Rules
View Full String	Account Rules
Notes	Model Definition
Add	Allocation Maintenance
Execute Allocation	Event Definition
Components	Structures
Links	Structures
Transfer	Ledger Definition
Accept	Process Definition
Consolidate	Process Definition
Translate	Process Definition
Execute	Process Definition
Build Rounding Account	Process Definition
Accept	Process Sequence
Execute	Process Sequence
Accept	Account Inquiry
Accept and Run	Account Inquiry
Period Detail	Account Inquiry Results
Periods	Account Inquiry Results
Account/String Description	Account Inquiry Results
Scroll Account String	Account Inquiry Results
View Column Definition	Account Inquiry Results
Previous	Account Inquiry Results

Function or Action	Programs Affected
Next	Account Inquiry Results
Accept	Structure Inquiry
Tree	Structure Inquiry
Accept and Run	Structure Inquiry
Periods	Structure Inquiry Results
Multiple Posting - All	Events Processing
Multiple Posting – Selected	Events Processing
Segments	Events Processing
Analysis	Events Processing
Notes	Events Processing
View Summarized Lines	Events Processing
Accept	Events Processing
Post	Events Processing
Approve	Events Processing
Void	Events Processing
Accept	CEA Archive/Purge Selection
Select	Post Deferred
De-Select	Post Deferred

Add Reject and Add Allow

Add Reject and Add Allow authority are specific to the Account Rules program. Instead of the Add authority used in all other programs, Account Rules has two levels of Add authority:

- Add Reject allows you to add reject rules.
- Add Allow allows you to add only allow rules that apply to existing reject rules.

Post, Approve, and Void

Post authority affects both Events Processing and Post Deferred. Approve and Void authorities are specific to the Events Processing program. You can be denied authority to any or all of these actions. When you have authority to any of these actions, you can open a record and perform the action to it by selecting the appropriate option on the initial Events Processing screen.

Transfer

Transfer authority is specific to the Ledger, Book and Journal Source, CEA105D1. This authority allows you to transfer opening balances. To transfer opening balances, use F10=Transfer in the Book Definition screen, CEA105D3-01. The system displays the Transfer window and allows you to execute this process. You must specify a retained earnings event in the Ledger Definition screen, CEA105D2-01, to use the transfer functionality.

Allocation

Allocation authority is specific to the Process Definition program. This authority allows you to execute an allocation for an allocation event record. To execute an allocation, use the Execute screen action on the program's Processes Maintenance Panel. The system displays the Allocation Execution Window and allows you to execute this process.

Consolidations and Translations

Consolidations and Translations authority are specific to the Process Definition program.

- Consolidations authority allows you to display and maintain consolidation records on the Process Definition Selectionscreen
- Translations authority allows you to display and maintain translation records on the Process Definitionscreen.

Use F13=Filters to display the consolidation and translation records.

Execute

Execute authority affects different programs in different ways.

- In the Process Definition and Process Sequence programs, when you use **Execute**, the system executes the process record that is currently open.
- In the Account Inquiry and Structure Inquiry programs, when you use **Execute**, the system displays the information resulting from thecriteria specified in the first screen.

When you are denied Execute authority in any of these programs, the system disables the **Execute** function key.

Period

Period authority is specific to the Account Inquiry and Structure Inquiry programs. In the Account Inquiry Definition and Structure Inquiry Results screens, the F9=Periods function key allows you to access period-specific information for the inquiry. If this detail information is sensitive or confidential,

you can deny users Period authority. This allows them to view the account balance information but not the supporting detail information. If you do not have Period authority, the system does not display the Periods function key.

Select

Select authority is specific to Post Deferred/Batch Post Restart, CLD540D1. When access to this action is granted, the **Select** option of the File menu is enabled. The user is allowed to select a transaction for posting.

De-Select

De-Select authority is specific to the Post Deferred application. When access to this action is granted, the **De-Select** option of the File menu is enabled.

The user is allowed to de-select a transaction to exclude it from posting.

Setting Function/Action Access Control

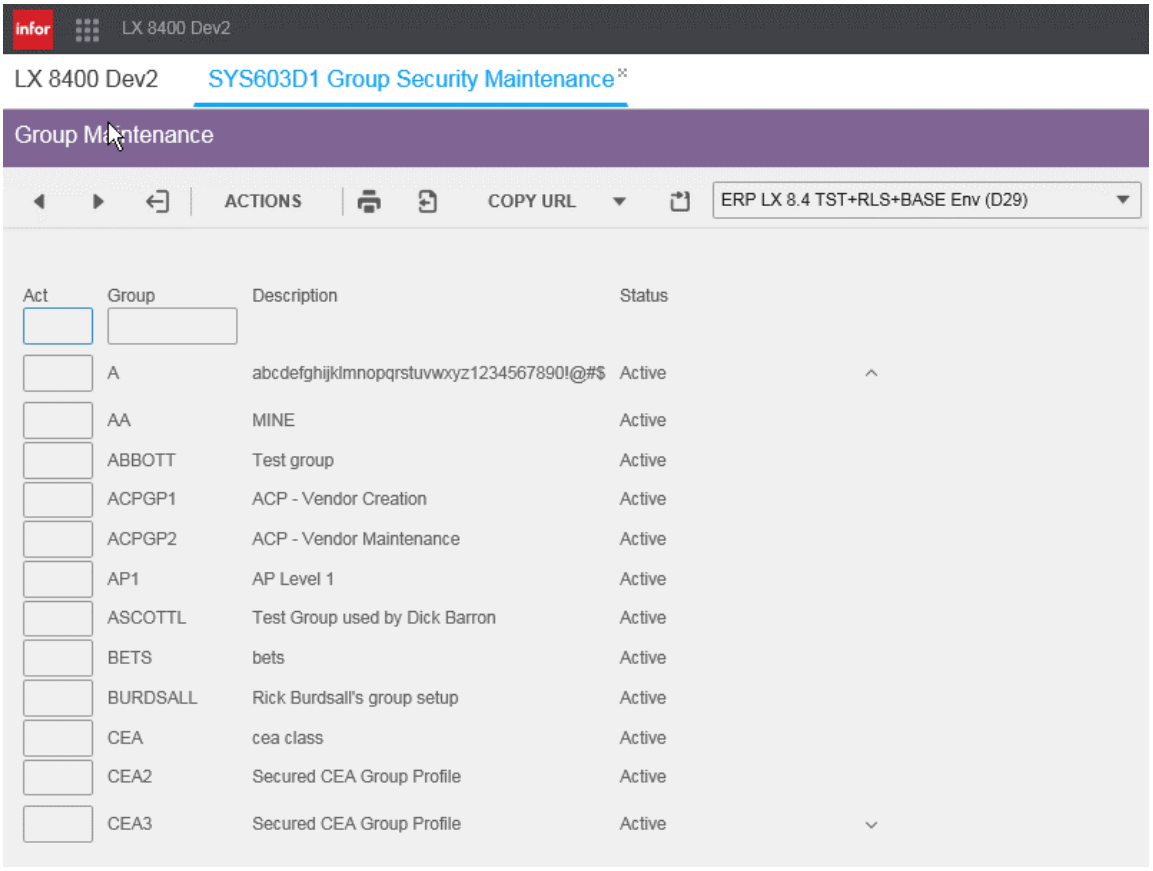
To set Function/Action access control, you must perform two procedures:

1. Set Function/Action access control levels for user groups in the Group Security Maintenance (SYS603) program.
2. Associate individual user profiles with user groups in the User Authorization Maintenance (SYS600) program.

Setting Function/Action Access Control for User Groups

To set Function/Action access control levels for a user group, perform the following steps:

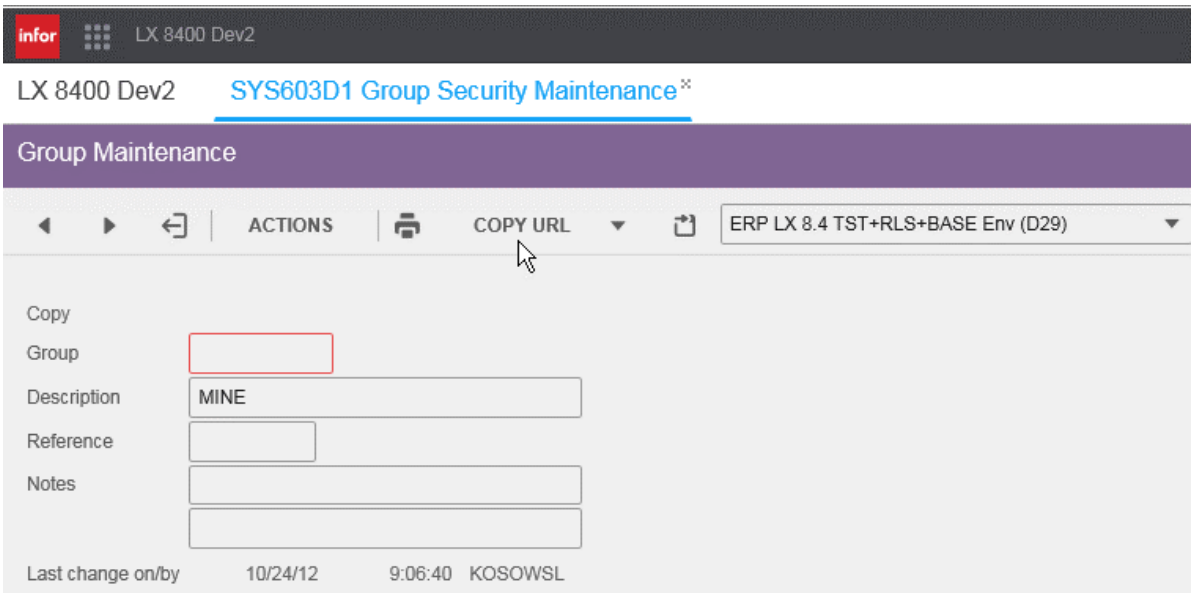
1. Access the Infor LXsoftware.
2. On the SYS menu, select Group Security Maintenance, SYS603D1. The system displays the Group Maintenance list screen (SYS603D1-01), displaying a list of existing user groups with their descriptions and status.



3 Enter the user group name in the Group field.

4 To create a user group you can also copy and rename an existing user group.

5 Press **Enter**. The system displays the Group Maintenance Data screen.



6 Complete the following fields on this screen:

Group

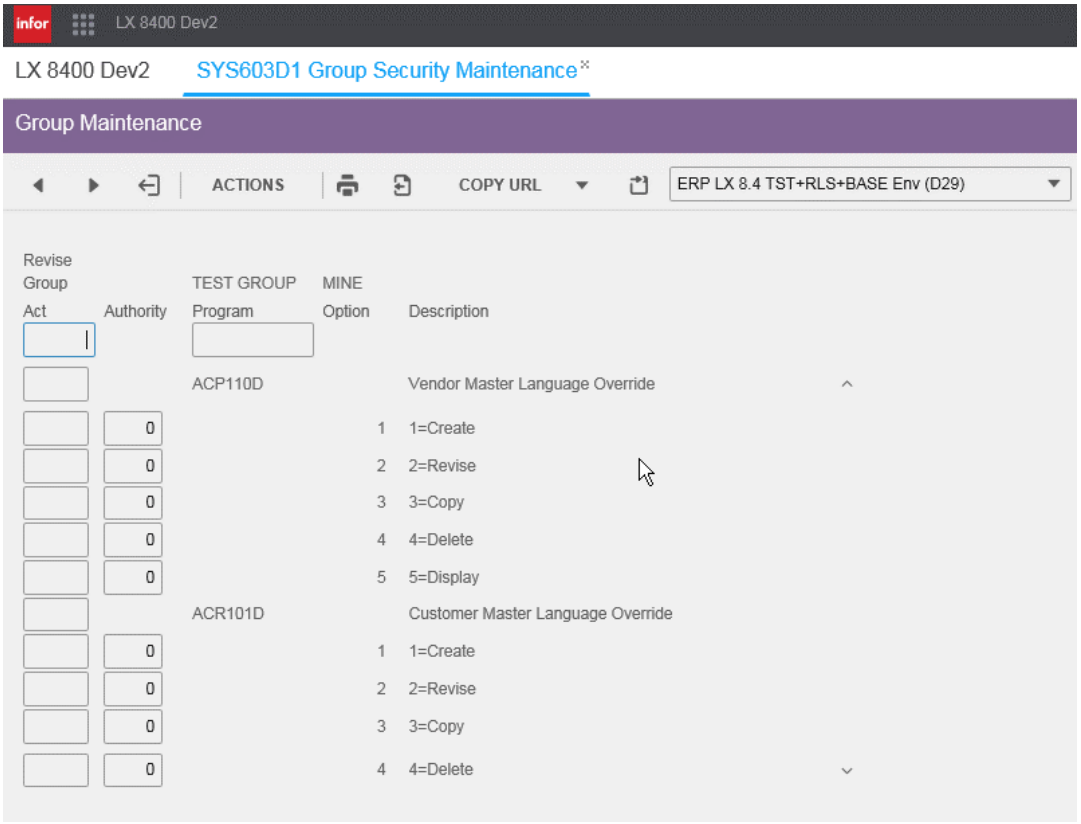
Displays the group ID you created.

Description

Type the description of this group.

7 Press **Enter** to create the group.

8 To maintain access control options for this group, specify **Options** next to the group record. The system displays the Group Maintenance authority list screen with the group you selected for maintenance.



This window contains the following options:

Authority

Specify **1** to grant this group authority to the function. Specify **0** to deny this group authority to the function.

Program

Displays the program you can secure or authorize for this group.

Option

Displays the option number assigned to a function or action in a program.

Description

Displays the full description of the function or action corresponding to this option number.

Step 11 is required if you create a user group. When you initially create a user group, you must authorize the group to all functions and actions before selecting or deselecting individual access control options. When you are maintaining an existing user group, this step is not necessary.

9 Required for new groups only. When you initially create a user group, use the **Authorize All** screen action to authorize the group to all functions and actions.

10 Perform one of the following actions:

- To authorize access to a particular function for a user group, specify **1** for the appropriate option.
- To deny access to a particular function for a user group, specify **0** for the appropriate option.
- To authorize this user group to all functions and actions, select **Authorize All** from the Actions menu. This option is helpful when you want to allow the group access to most functions, but deny them access to few functions.

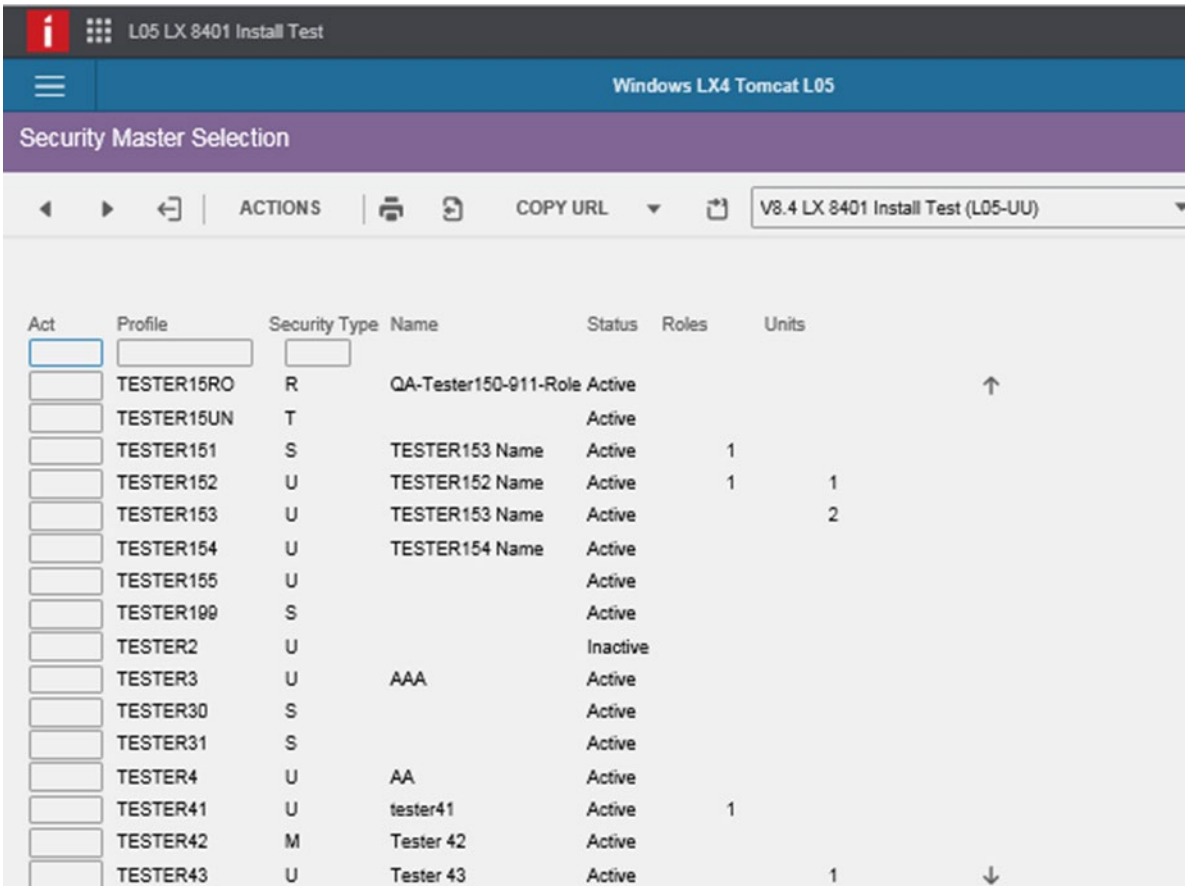
11 Press **Enter** to save your changes and exit the screen.

Associating User Profiles with User Groups

In order to apply the Function/Action access control levels to individual users, you must associate each individual user profile with a group code. To do this, perform the following steps:

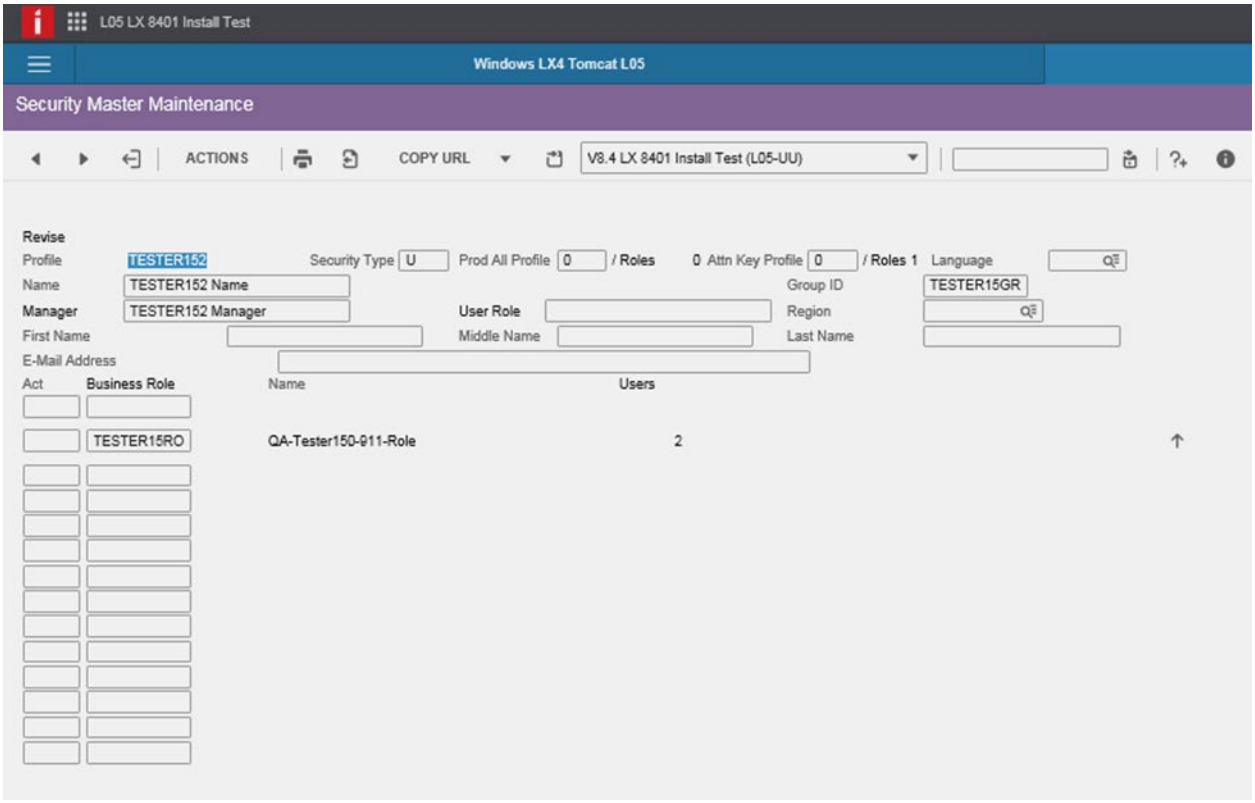
1 Access the Infor LX software.

2 On the SYS menu, select User Authorization Maintenance, SYS600D1. The system displays the Security Master Selection (SYS600D1-01) screen. This screen displays a list of user profiles and their associated security type and status.



3 Select a user profile, specify **Revise**, and press **Enter.** Select a user profile, specify **Revise**, and press **Enter.**

4 The system displays the Security Master Maintenance screen (SYS600D2-7) with the user profile you selected.



5 Enter a valid group code in the Group ID field to assign this user to the group.

6 Press **Enter**.

Chapter 3 Security Rules

Security Rules

The Security Rules control monitors and limits user access to inquiry and posting privileges. This control allows a system administrator to determine access to the posting of events in Events Processing (CEA500D1) and the inquiry of posted events in Account Inquiry (CEA300D1) and Structure Inquiry (CEA312D1) for user groups at the chart, ledger, segment value, and/or account string level. Users are then restricted to only post to accounts containing certain segment values/account strings and to only view results of posted accounts that contain specific segment values/account strings.

A system administrator first needs to assign users to user groups. The system administrator gives these groups varying levels of security access, depending on the access levels needed by the users of that group. Users in each group have access to accounts containing the same segment values/account strings giving them privileges to post (access to post only), view (access to view only), post and view (all access) or post and limited view (journal line details are restricted in Account Inquiry, Events Processing, and CLD reports). A user group can be restricted from access to certain segment values/account strings (no access). For example, managers can have authorization to view the results of and post to accounts containing all segment values/account strings, so managers would be given all access (all access) privileges. On the other hand, an employee in the Accounts Payable or Accounts Receivable department may only be authorized to post to accounts containing specific segment values/account strings and may not be given privileges to view the results of those accounts (access to post only). If no security access level is assigned, the group may view and post to accounts containing all segment values/account strings (no rules apply). This is the system default.

Security Reject and Allow rules, set up by a system administrator in the Security Rules Maintenance (CLD175) application, define the security privileges for user groups. The use of security rules is easily activated with one step in the CEA Control Parameters (CEA 820) application.

Setting up User Groups

To utilize the Security Rules Optimization feature, a system administrator can assign security codes to 100 pre-defined user groups. User groups are created in the Group Security Maintenance (SYS603) program. All users assigned to this group possess the same level of security.

A system administrator can assign security codes for up to 100 of the user groups. All user groups in excess of 100 are still administered by all security reject/allow rules assigned to them but are not able to utilize the optimized process.

Each of the security codes and access levels are assigned to user groups and are mapped to the account strings and stored in the Account Cross Reference (CEA106D1) file.

Once security codes have been assigned, the system administrator must:

- Determine which level each group is allowed access.
- Determine which segment values/account strings are assigned to which user groups.
- Create security rules for specific segment values/account strings and assign these groups to the created rules.
- Select the rules to be processed. Processing can be done in either batch mode or interactively.
- The Security Rules flag must be on in the CEA Control Parameters program before any rules are effective.

Results of Security Rules

Anytime an event is processed using new account strings, the security optimization code is created at the same time the Account Cross Reference record is created. The result of this process is the creation of a 100-character field that is stored in the Account Cross Reference (CEA106D1) program and used as a reference for future security validation.

Events Processing

During the posting process in the Events Processing (CEA500D1) program the account number is examined and an error message is displayed for each journal or journal line that the user is not authorized to post in Events Processing (CEA500D1).

Account Inquiry/Structure Inquiry

During the inquiry process in the Account Inquiry (CEA300D1) and Structure Inquiry (CEA312D1) programs, only the accounts that the user's group is authorized to is shown. A message will not display to tell the user which accounts they are not authorized to view.

Creating Rules

An accounts security status can be determined by two different types of rules. The first type is a Segment Security Rule, which assigns access status based on a single segment of the account

string. The second type is an Account Security Rule, which assigns access status based on the combination of all the segments of the account string. With each type of rule there are Reject rules and Allow rules. All reject rules automatically assign an access status of No Access. Allow Rules, which have to be a subset of a Reject Rule, change an account's security status from No Access to Inquiry Only, Post Only, Post and Inquiry or Post and Limited Inquiry. Similar to Account Rules, a Reject rule must be created that restricts all the needed accounts and then creates Allow rules that change the needed accounts to their desired status.

Both types of rules allow the use of the wildcard characters * and ?. Use of the wildcard charters is advised to minimize the number of rules that are created. Through the use of wildcards a number of accounts may receive different security levels from different rules. In these cases, the security level that is recorded is the one with the lowest Access Type, based on the Access Type's numeric reference from any allow rule.

Example 1

With the following rules, all accounts that have an ACCT segment value between 4000 and 4999 the user group would be able to Post Only. For all accounts that have an ACCT segment value between 5000 and 5999 the user group would be able to Post to and Inquire about.

Segment Rule 1

Reject all accounts where ACCT=*

Segment Rule 1 - Allow seq. 1

Post Only status for all accounts where ACCT=4*

Segment Rule 1 - Allow seq. 2

Post and Inquire status for all accounts where ACCT=5*

Example 2

With the following Account Security Rule, the user group would be able to Post and Inquire on any event posted to Company 01.

Account Rule 1

Reject all accounts that = *-*-*-*. (All accounts would be rejected.)

Account Rule 1 - seq. 1

Post and Inquire status for any account that = 01-*-*-*. (All account for company 01).

Example 3

If the Account String = 01-101-4100-10000 (CO-DPT-ACCT-PROJ). With the following rules, this account would receive an Inquiry Only status. Therefore, the user group would not be able to post to this account but could inquire about any event posted to this account.

Segment Rule 1 (No Allow Rule)

Reject all accounts where segment value = 4100.

Account Rule 1

Reject all accounts that = *-*-41??-*. (Give all accounts in all COs, all DPTs, between 4100 and 4199 and all PROJ a security status of No Access).

Account Rule #1 - Allow seq. 1

Post only status to all accounts that = *-*-41??-*. (Change the Security status for all accounts in all COs, all DPTs, between 4100 and 4199 and all PROJs to Post Only).

Account Rule #1 - Allow seq. 2

Inquiry only status to all accounts that = *-*-410?-*. (Change the Security status for all accounts in all COs, all DPTs, between 4100 and 4109 and all PROJs to Inquiry Only).

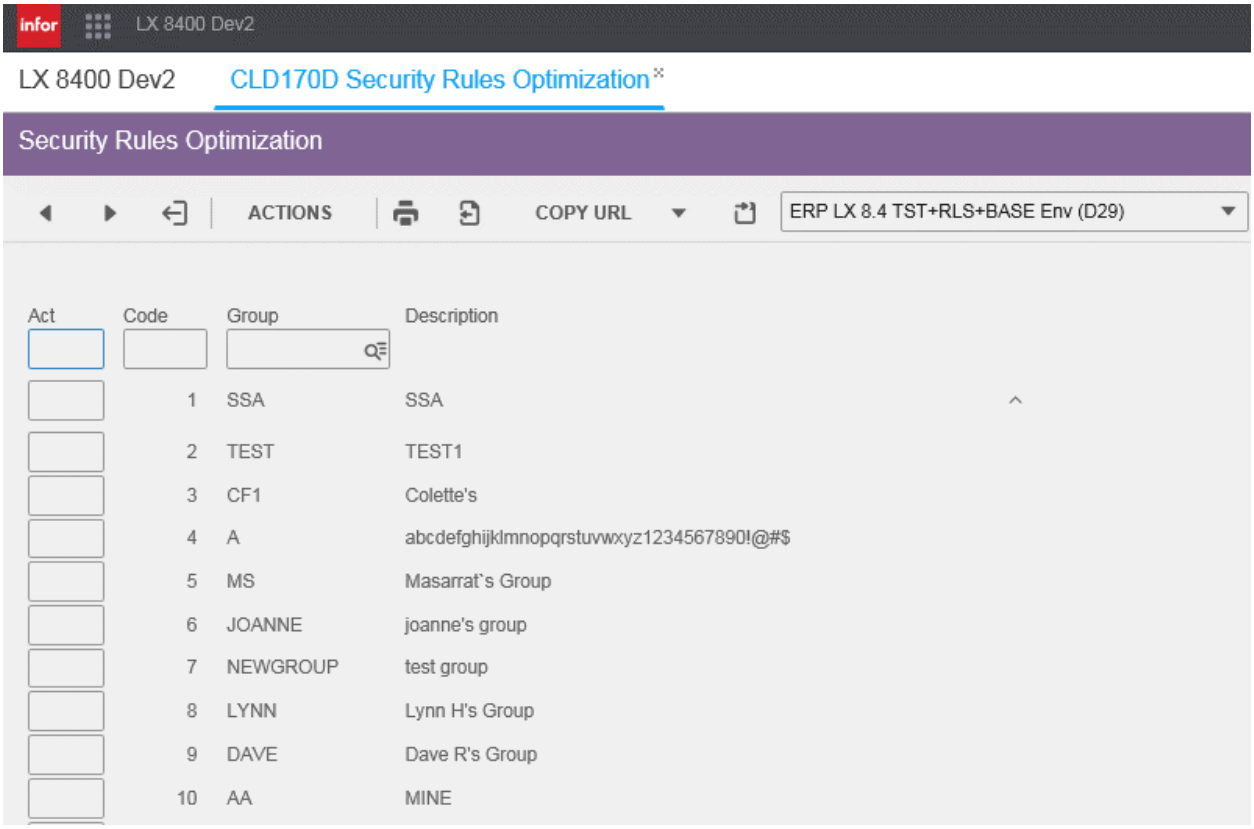
Assigning a Security Code to a User Group

To set Security Rules for a user group, perform the following steps:

1 Log on to Infor LX.

2 Access Security Rules Optimization.

The system displays the Security Rules Optimization screen. Use this screen to assign predefined user groups to security access codes.



3 Specify Create, and then enter an unused Security Code number (1 to 100) and the valid user group name.

4 Press **Enter**.

The Security Rules program also has a reporting feature that lists the last additions or changes that were made to security rules. This feature allows a system administrator to analyze any updates made to user groups or any security codes.

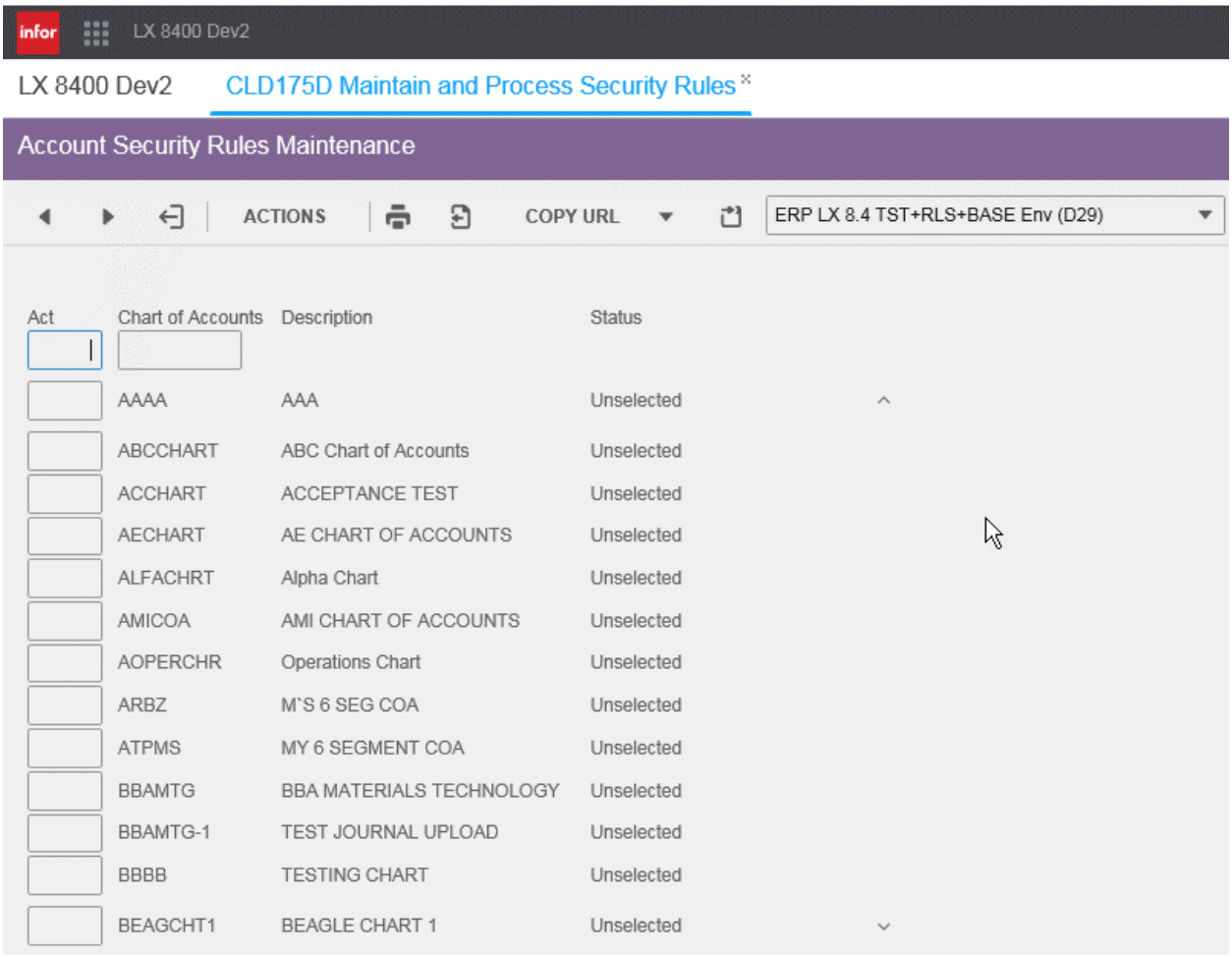
Setting Security Rules for a User Group

When determining which segment values/account strings the user groups are or are not privileged to, a system administrator must determine the Chart of Accounts to use. The following screen displays valid Charts of Accounts. To establish security rules for a chart of accounts, perform the following steps:

1 Log on to Infor LX.

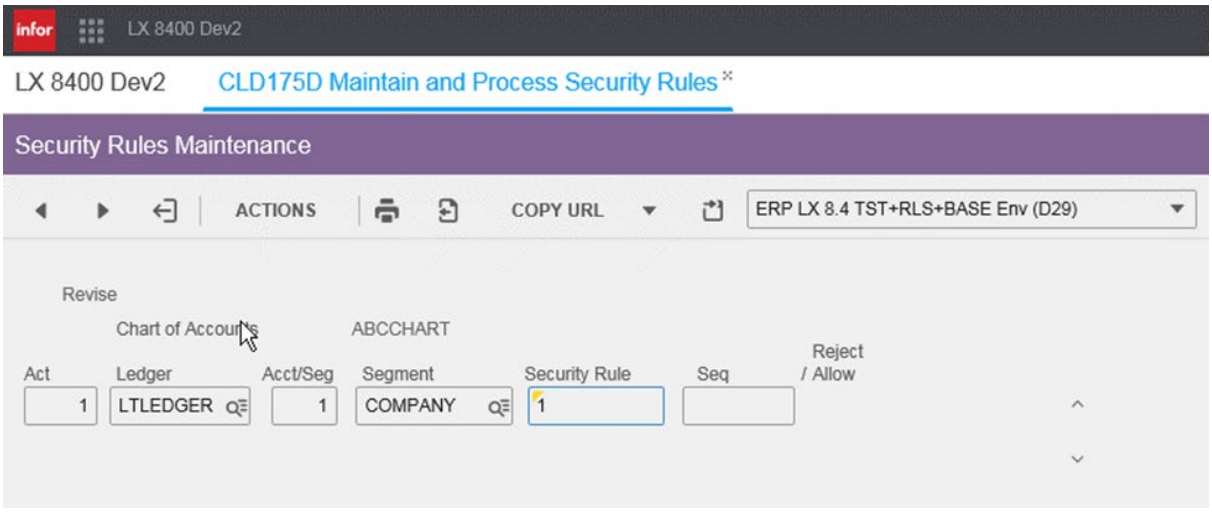
2 Access Maintain and Process Security Rules.

3 On the Filter screen, select **Accounts Security Rules** and then press Enter**.** The system displays the Account Security Rules Maintenance screen.



4 Select a Chart of Accounts and position to it.

5 Specify **Revise**. The screen below displays the security rules for the selected Chart of Accounts. Rules are created copied, revised or deleted from this window.

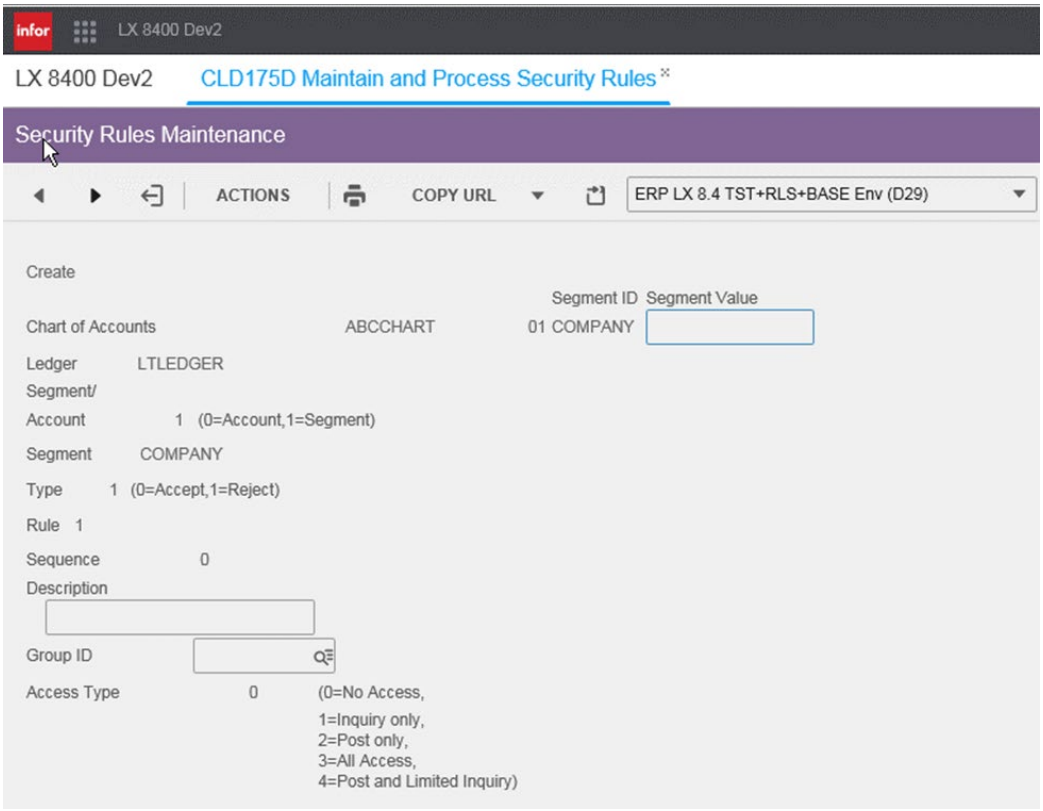


To create a rule for the selected Chart of Accounts, perform the following steps:

1 In the Act field, select **Create**.

2 Enter a Ledger, Account/Segment Type (to determine if rules are at the account string or segment value level), Segment (if defined at the Segment Value level), Rule Name and Sequence Number (if the rule is an allow rule).

3 Press **Enter**.



4 Enter the value for the segment selected, a description of the rule, and the user group affected by this rule. Enter * in the Group ID field to include all user groups. You can enter an Individual group for either an allow or reject rule.

5 Specify an Access Type. Valid values are **1**=**Inquiry only**, **2**=**Post only, 3**=**All Access** and **4**=**Post and Limited Inquiry.** This field is enabled for Allow Rules only. The value **0** = **Reject** allows none of the above four options.

6 Press **Enter**.

After you have created all the security rules in Security Rules Maintenance, return to the Security Rules Maintenance screen. Select the chart of accounts for processing. From this screen, you can select multiple records to be processed and then process these rules in either a batch or interactive mode.

7 Select a Chart of Accounts and position to it.

8 Use F17=Post Batch or F18=Post Interactive. This updates the security optimization string used when the Events Processing and Account Inquiry or Structure Inquiry applications are processed.

The CEA509B program applies the security rules to the appropriate accounts when the process is run interactively or in batch mode. You can monitor this process in the Work with Spool Files (SYS909D1) and Work with Batch Job (SYS908D1) applications. After the rules have been processed, the user is returned to the Configurable Ledger screen.

After all rules have been created, the appropriate security has been determined and assigned, and the rules have been processed in batch or interactive mode from the Security Rules Maintenance Window, you must turn on the Security Rules flag needs to be turned on in the CEA Control Parameters screen. Until this flag is turned on, all users have access to post and inquire on all segment values/account strings. For the rules just created, the same result as if no rules applied.

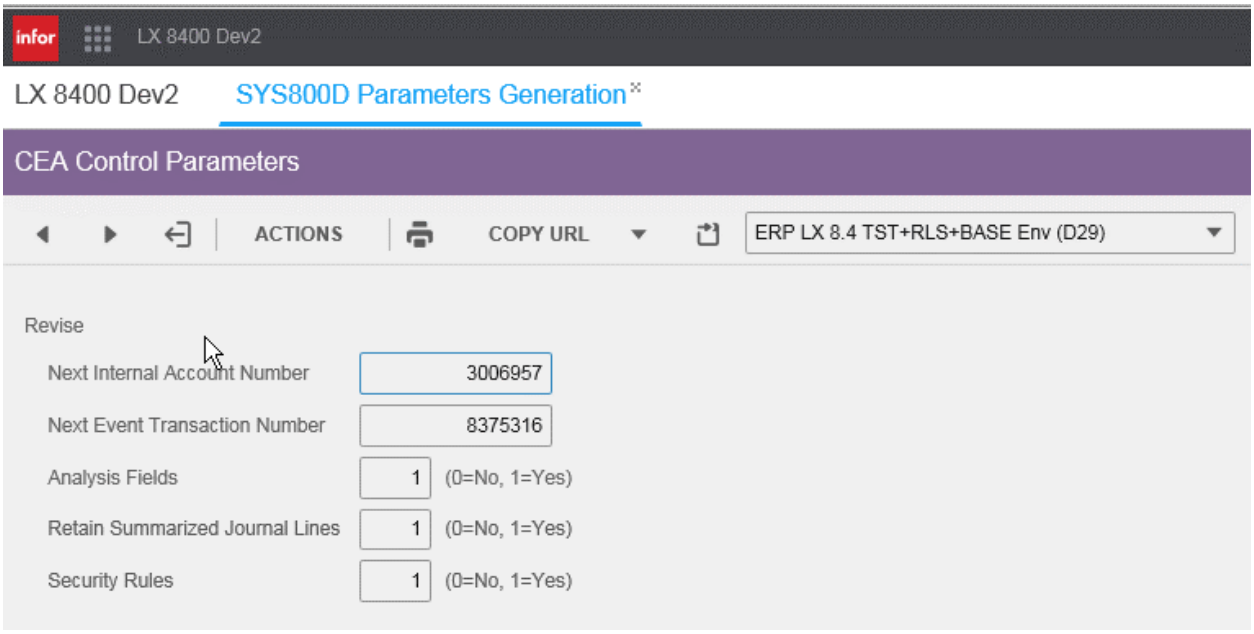
Activating Security Rules

Perform the following steps to activate Security Rules for user groups:

1 Log on to Infor LX.

2 Access Parameters Generation, SYS800D.

3 Scroll down to CEA Control Parameters and select **Revise**.



4 On the CEA Control Parameters screen, specify **1** next to Security Rules and press **Enter**.

Users in all groups are authorized to view the results of transactions posted before the Security Rules flag is turned on in the CEA Control Parameters (CEA820) program.

To de-activate Security Rules in CEA Control Parameters, you must delete all security rules established in Security Rule Maintenance to fully remove rules for all Charts/Ledgers combinations from the database. To do this, select a reject rule and specify **Delete** on the Security Rule Maintenance screen. When you delete a Reject rule, you also delete all Allow rules corresponding to that Reject rule.