Infor LX 8.4.1 or later Security Management Guide

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

Publication Information

Release: Infor LX 8.4.1 or later Release level

Publication date: January 29, 2024

Contents

About this guide

Intended audience

System Administrators responsible for configuring user access to menus, programs, warehouses, facilities, companies, and transaction effects.

Related documents

You can find the documents on Documentation Central, 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 at Documentation Central https://docs.infor.com. We recommend that you check this portal periodically for updated documentation.

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

Chapter 1 LX User Security Overview

This guide will assist you in configuring LX user profiles and setting up user security. It also includes configuration settings for SiM and IDF.

The Access Control features of Infor LX provide you with flexibility that allows many users to access the information, while also limiting user access to Infor LX programs and associated data. Infor LX has multiple 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 products for business roles or individual users.
- Program Access Control - This level is optional. Use this level to limit access to applications in the products for business roles or individual users.
- Warehouse Access Control - This level is optional. Use this level to limit access to warehouses in the applications for business units or individual users
- Facility Access Control - This level is optional. Use this level to limit access to facilities in the applications for business units or individual users
- Company Number Access Control - This level is optional. Use this level to limit access to companies in the applications for business units or individual users
- Order Type Access Control – 8.4.2 and above. This level is optional. Use this level to limit access to order types in the applications for business roles or individual users
- Order Class Access Control – 8.4.2 and above. This level is optional. Use this level to limit access to order classes in the applications for business roles or individual users
- Transaction Effect Access Control - This level is optional. Use this level to limit access to transaction effects in the applications for business roles or 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 applications for a group of users.

Verifying Installation of Products

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

To verify which 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 Formatline.
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 products are installed.

Chapter 2 User Profiles Configuration

User profiles used to access LX require some specific configurations. There are several types of access that different users will need. Grouping the users into groups using group profiles allows for easier authorization configurations. You may have several levels of user configurations, for example:

Standard User Access to LX, no access to LX database outside of LX.

Power User Access to LX, read access to LX database outside LX for reporting.

Admin User Access to LX, read/write access to LX database outside LX for applying MRs, fixes, PTFs, patches, etc., plus user profile management.

The user profiles for these user types may differ somewhat, but some basic settings will still be needed.

Admin users should be part of group SSA. Only admin users should be part of this group. User profile SSA is created during the product install and owns most of the objects in the LX libraries. Admin user profiles should have settings GRPPRF(SSA) OWNER(*GRPPRF). This allows for any objects that these users create to be owned by SSA, which would match existing delivered configurations.

Power users should be part of another group such as LXPWUSER and their user profiles should have settings GRPPRF(LXPWUSER) OWNER(*GRPPRF). The LXPWUSER profile would not have access to objects owned by SSA and would have use access to the LX database library and read access to some or all the files.

Standard users should be part of a different group such as LXUSER and their user profiles should have settings GRPPRF(LXUSER) OWNER(*GRPPRF). The LXUSER profile would not have access to objects owned by SSA and would have no access to the LX database library or files.

Example of a group profile for standard users would be:

```
CRTUSRPRF USRPRF(LXUSER) PASSWORD() STATUS(*ENABLED) USRCLS(*USER)
INLPGM(*NONE) INLMNU(*SIGNOFF) TEXT('LX User Group Profile') SPCAUT(*NONE)
GRPPRF(*NONE) OWNER(*USRPRF) GRPAUT(*NONE) SUPGRPPRF(*NONE)
```

Example of a standard user profile:

```
CRTUSRPRF USRPRF(LXUSR001) PASSWORD() STATUS(*ENABLED) USRCLS(*USER)
INLPGM(*NONE) INLMNU(*SIGNOFF) TEXT('first and last name') SPCAUT(*NONE)
GRPPRF(LXUSER) OWNER(*GRPPRF) GRPAUT(*NONE) SUPGRPPRF(AULUSER)
```

Note that for standard users additional settings may be required for users using a language that is not the system default. LANGID() CNTRYID() CCSID() may need to be set differently. Also, the password can be set to *NONE in a Single Sign-On environment.

System i Workspace users

If LX is being deployed in a web-based configuration and Infor System I Workspace with System I Manager is being used, then the following configuration will be required. Reviewing the security setup in the *Infor SI System Manager Installation Guide* is recommended to fully understand the user setup for proper security setup.

All LX users should have group profile AULUSER added to their supplemental groups and Admin users should also have AULSECOFR added.

IDF considerations

When setting up users IDF requires that any user profile that will be using a language (CCSID) other than the system default will need to have a CCSID assigned to the user profile that matches their language setting assigned in LX.

Chapter 3 LX User security setup

Setting up security for LX users is primarily defined to three key areas, (1) Access to programs and objects, (2) Limitations on functionality (function keys and action codes), and (3) Access to Data such as Warehouses, Facilities, Companies, Order Type, Order Class, and Transaction Effect codes. There are a few other areas of user setup, but these three areas cover the primary setup.

Setting up security for these areas is best done by defining groups, roles, and units before starting user setup. Once these groups, roles, and units are defined, setting up users is basically assigning the users to these areas.

Defining Roles

Business Roles are defined in Security Master Maintenance (SYS600) the same way users are. The user type is “R”. Roles can only be authorized to Products, Programs, Order Types, Order Classes, and Transaction Effects. Setting up roles defines what processing a user can access. Users can be assigned to more than one role. Set these up based on the type of functionality a role will perform in LX.

Defining Groups

Groups are defined in Group Security Maintenance (SYS603). They define the actions a user can take when they are in a LX programs or object. The authority assigned in SYS603 groups controls the function keys and action codes (FKAC) a user can use when in a program or object. Granting a group/user access to any of these setting is ignored if the user is not authorized to execute the program or object from SYS600 from either an assigned role or direct authorization. A user can be assigned to just one group.

Defining Units

Business Units are also defined in Security Master Maintenance (SYS600). The user type is “T”. Units can only be authorized to warehouses, facilities, and companies. Setting up units allows for grouping users into units that share common access to data. Users can be assigned to more than one unit. Set these up based on the data a unit will have access to in LX.

Defining Users

Use Security Type in Security Master Maintenance (SYS600) to indicate the access control for user.

Available Security Types:

- **S** - Security Officer
- **M** – Security Manager
- **U** - User
- **D** - Database Administrator (same as U)
- **P** - Programmer (same as U)
- **O** - Operator (same as U)
- **R** – Business Role (not used for individuals)
- **T** – Business Unit (not used for individuals)

Also, SYS603 should be used to configure the groups that users will be assigned to. Groups control what action codes and function keys users can use while in programs.

IDF security

LX security maps directly to IDF security.

- LX security for warehouses, facilities, and companies maps directly to IDF Auto-content security. To view these IDF settings for a single user, launch the User Profiles object, select a user, and view their details. Select the Values tab to see which warehouses, facilities, and companies the user is authorized to use. Additional settings are included in Values tab for financial authorities for CEA and/or EGLI for Ledgers, Books, and Years. Note the Finance tab shows the EGLI group the user is assigned to.
- In LX program, security is handled by SYS600 with Products and Programs security settings. In IDF, this would be security to access business objects and their functionality. This would be handled by CAS security. See Chapter 4 LX IDF Security Overview for details.

Sending LX security changes to IDF

LX retains security settings from previous versions for LX programs that are now business objects in IDF. For example, access to INV100 would now be access to Enterprise Items. LX maps settings from LX programs to IDF objects wherever possible. See the Security Mappings object on the Environment tab for details of the pre-configured mappings. Note these mappings also map function key and action code settings for some programs to the same functionality in the objects. Synchronize Security with IDF (SYS607D-01) allows for the population of IDF security settings for LX related object, plus auto-content security, financial groups in EGLI, and basic user access to environments. Run SYS607 as part of initial user setup after creating the IDF environment. It can be run once for all users. Choose the settings you want to use for sending LX security settings to IDF in Security Settings Maintenance (SYS802) accessed from System Parameter Generation (SYS800). Subsequent changes in Security Master Maintenance (SYS600) are automatically sent to IDF based on Security Setting Maintenance (SYS802) configurations. Changes to Roles or Units update IDF security for all users assigned to those Roles or Units. Changes to groups in SYS603 update IDF security.

There are components of IDF that are outside the scope of LX security so that security setup needs to be done directly in IDF. See Chapter 4 LX IDF Security Overview for details.

System i Manager security

LX sends menu and user information to System i Manager (SiM) to allow System i Workspace (SiW) to display menus for users. Whenever menus, users, or user access to menu options change, this information should be updated.

Initial environment setup should include running SiW Configuration Export Selection (SYS075) for all menus and users. When menus change, SYS075 should be rerun to update the menu information. In addition, the IDF menus need to be exported to SiM. This is done from the User Profiles object, *File* menu, *Host Jobs…* option, and selecting Export public metadata to Workspace.

Whenever a new user is added to LX, that user also needs to be added to SiM. Run SYS075 for each added user, or when a user's authority to products or programs is changed to update the user and their menus in SiM.

Infor Ming.le User Provisioning

BMR 78589 for LX 8.4.1 and LX Extension 3.0 adds support for Infor Ming.le User Provisioning. This enhancement allows for users created in Infor Ming.le IFS to be automatically added and configured for LX as well. Some of this functionality can also be used in LX environments using SiW without Infor Ming.le.

SYS802D now allows you to configure how you synchronize LX users with SiM. Once turned-on changes to user product and program security in SYS600 will propagate to SiM and SiW and update the user’s menus.

Table ERPUSR is the primary connecting point between LX and IFS users. It stores information that is shared by LX and IFS and connects IFS users to IBM user profiles.

See the Infor LX 8.4.x Configuration Guide for Infor Operating Service 12.x document for details on configuring this feature.

Chapter 4 LX IDF Security Overview

There are several areas of security to be setup for IDF. This chapter explains how to configure your security for allowing some users to manage IDF environments and settings, allowing some users to modify business objects, and managing which users can access what data in the Infor LX database.

Please note that this document only serves as a quick reference guide. Additional information about security is available in Power-Link and Net-Link in the Online Help and in the 5250 security menu accessed via STRIDF.

Security settings in IDF are updated several ways. (1) As noted above settings for LX related objects and tasks can be automatically updated when running SYS600 or SYS607, these updates will overwrite any settings for these objects and users that are done manually in IDF Security Maintenance. (2) The Security Maintenance menu in STRIDF allows you to configure many areas of IDF security including the settings for objects not part of core LX. Access to EGLI and CRMI objects for example will be managed here. (3) In Power-Link, Auto-Content values and EGLI Financial Groups are maintained.

Accessing IDF Security Maintenance

To access security maintenance:

1 Start a 5250 session

2 From a command line enter ADDLIBLE AMCESLIB

3 Enter STRIDF

4 Select an environment and press Enter twice

5 Specify **10**, **Security Maintenance**

6 Specify **1**, Area and task authorizations.

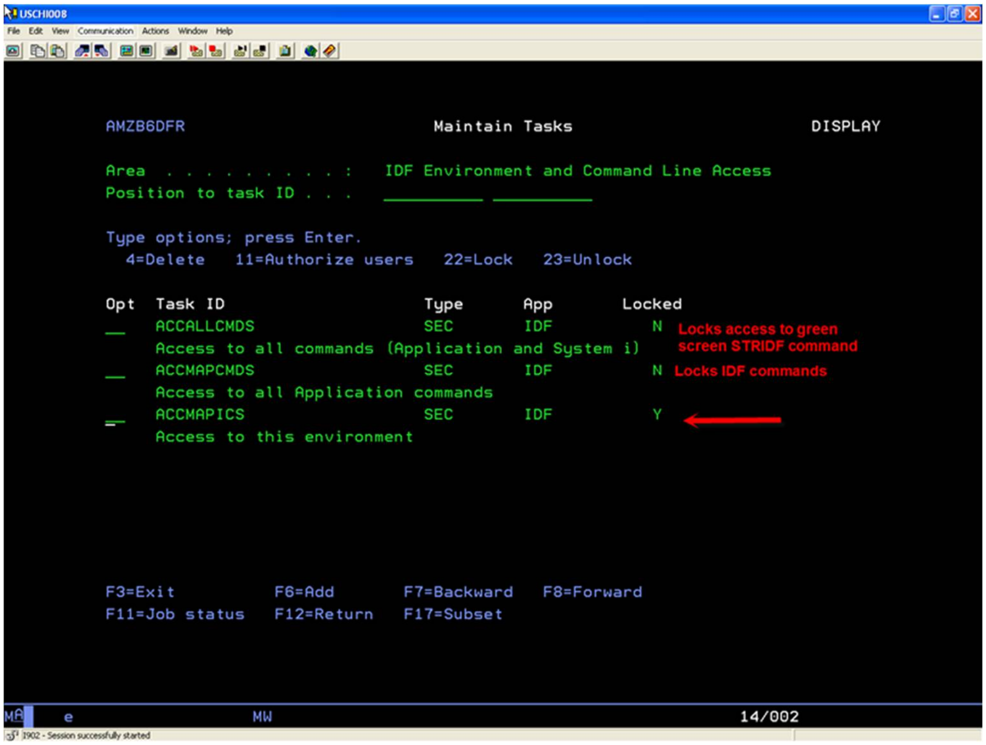
7 Specify **3**, **Keep this task unlocked**.

8 Select IDF Server

IDF Environment User Access Control

To restrict user access to the IDF environment:

1 Select option 2 to change IDF Environment and Command Line Access.



```
AMZB6DFR                         Maintain Tasks                        DISPLAY

Area  . . . . . . . . . . :   IDF Environment and Command Line Access
Position to task ID . . .     __________ __________

Type options; press Enter.
  4=Delete    11=Authorize users    22=Lock    23=Unlock

Opt  Task ID                    Type      App       Locked
___  ACCALLCMDS                 SEC       IDF          N
     Access to all commands (Application and System i)
___  ACCMAPCMDS                 SEC       IDF          N
     Access to all Application commands
___  ACCMAPICS                  SEC       IDF          Y
     Access to this environment




F3=Exit          F6=Add       F7=Backward   F8=Forward
F11=Job status   F12=Return   F17=Subset


MA    e                    MW                                    14/002
```

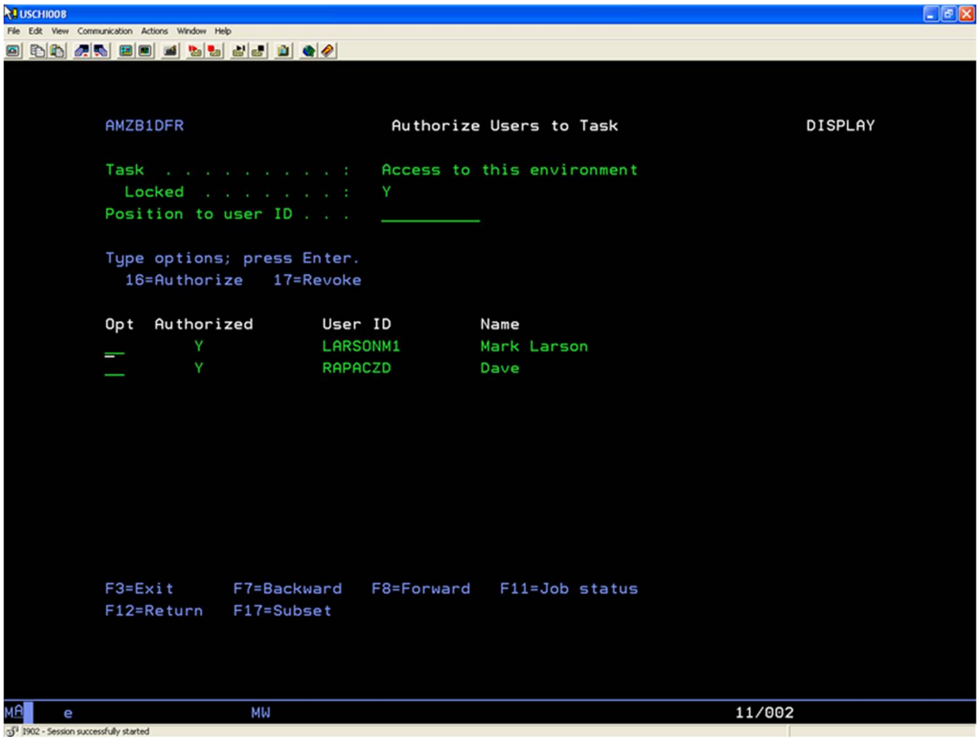
Locks access to green screen STRIDF command

Locks IDF commands

1902 - Session successfully started

2 The **Access to this environment** option controls the user’s ability to log in to the selected environment.

- **a** To lock the option for this environment, specify **22**.
- **b** To unlock it, specify **23**.
- **c** To select users that are authorized to be in the environment, specify **11**.
- **d** Note that in SYS800/SYS802 Security Settings Maintenance there is setting “Authorize LX users to IDF environment”. If that setting is set on, then adding users to LX will automatically authorize the user to the IDF environment and no action is required in CAS Security.



```
AMZB1DFR                    Authorize Users to Task                    DISPLAY

Task  . . . . . . . . . :   Access to this environment
  Locked  . . . . . . . :   Y
Position to user ID . . .   __________

Type options; press Enter.
  16=Authorize   17=Revoke

Opt  Authorized       User ID        Name
__        Y           LARSONM1       Mark Larson
__        Y           RAPACZD        Dave




F3=Exit      F7=Backward   F8=Forward   F11=Job status
F12=Return   F17=Subset
```

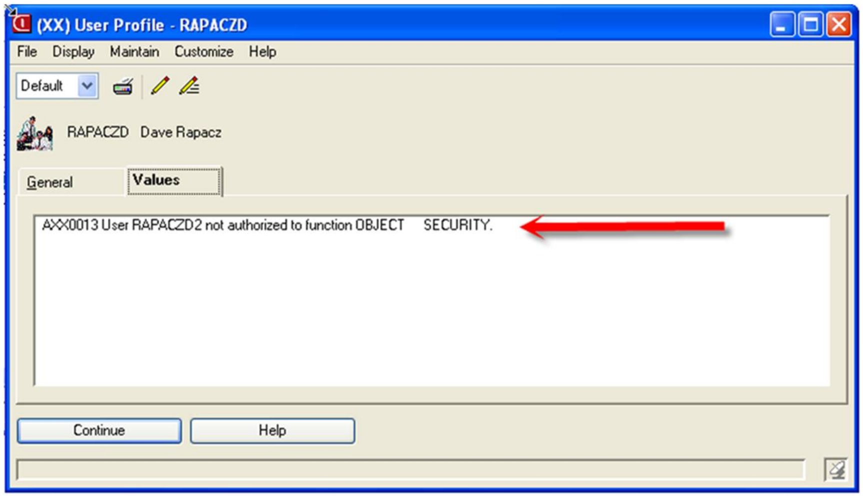
```
MA     e              MW                               11/002
1902 - Session successfully started
```

3 To control access levels, specify **16** or **17**.

IDF Content Security Access

To configure who can modify user profiles in IDF, you need to setup security for assigning security for business objects in Client Administration.

Note: This screen demonstrates that RAPACZD2 is not authorized to change user RAPACZD.


(XX) User Profile - RAPACZD
File Display Maintain Customize Help
Default
General
Values
Continue
Help

RAPACZD Dave Rapacz

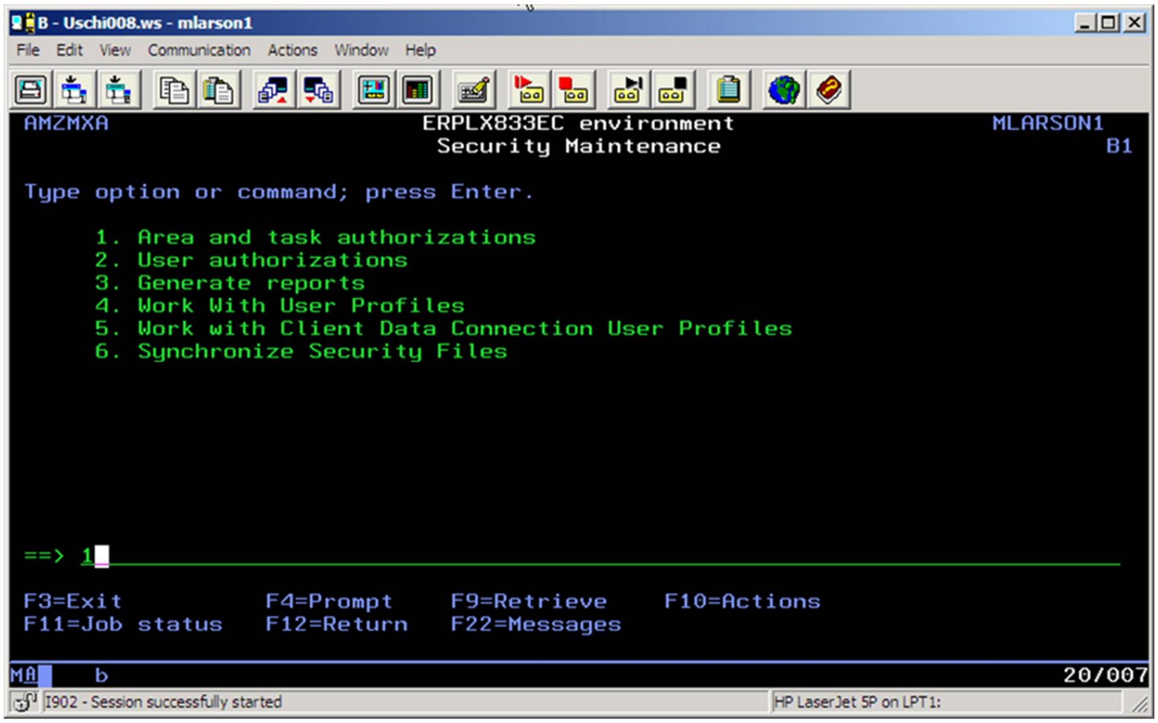
AXX0013 User RAPACZD2 not authorized to function OBJECT SECURITY.

To allow access:

1 Start IDF (STRIDF) and select the environment you want to secure.

2 Specify **10**, **Security Maintenance**.

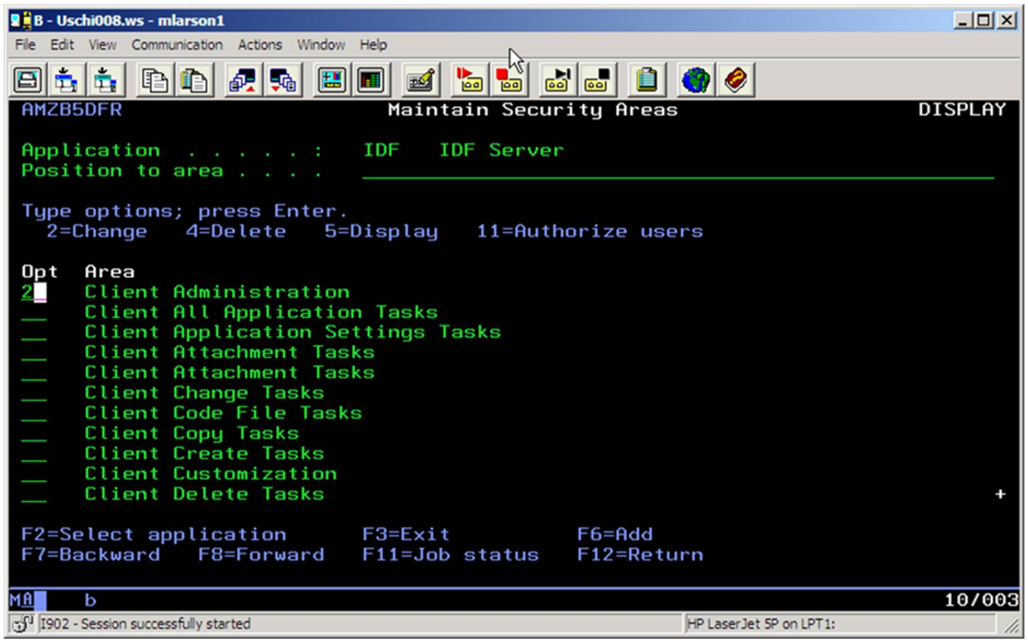
3 Specify **1** for Area and task authorizations.



B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

```
AMZMXA                  ERPLX833EC environment                  MLARSON1
                          Security Maintenance                        B1

Type option or command; press Enter.

     1. Area and task authorizations
     2. User authorizations
     3. Generate reports
     4. Work With User Profiles
     5. Work with Client Data Connection User Profiles
     6. Synchronize Security Files





==> 1

F3=Exit          F4=Prompt    F9=Retrieve    F10=Actions
F11=Job status   F12=Return   F22=Messages
MA     b                                                        20/007
I902 - Session successfully started          HP LaserJet 5P on LPT1:
```

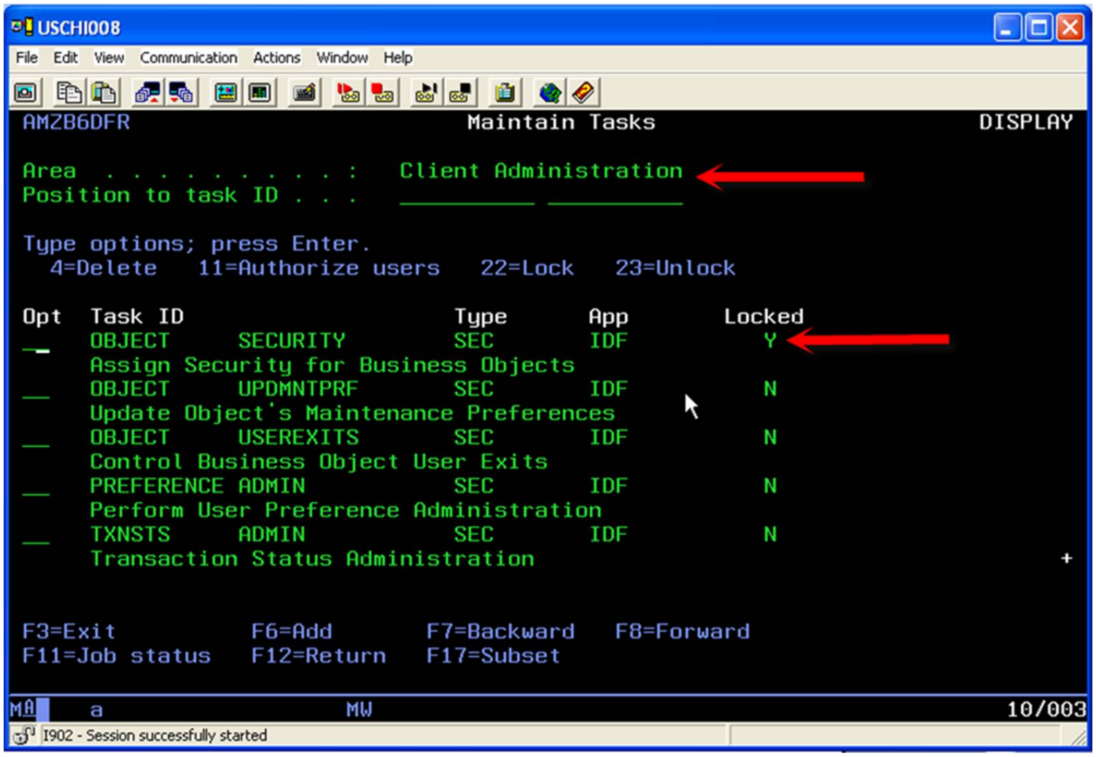
4 Specify **2** for **Client Administration**.



B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

```
AMZB5DFR                 Maintain Security Areas                DISPLAY

Application  . . . . . :   IDF   IDF Server
Position to area . . . .   

Type options; press Enter.
  2=Change   4=Delete   5=Display   11=Authorize users

Opt  Area
2    Client Administration
__   Client All Application Tasks
__   Client Application Settings Tasks
__   Client Attachment Tasks
__   Client Attachment Tasks
__   Client Change Tasks
__   Client Code File Tasks
__   Client Copy Tasks
__   Client Create Tasks
__   Client Customization
__   Client Delete Tasks                                          +

F2=Select application       F3=Exit          F6=Add
F7=Backward   F8=Forward    F11=Job status   F12=Return
MA     b                                                       10/003
I902 - Session successfully started       HP LaserJet 5P on LPT1:
```

5 Specify **22** for the **OBJECT SECURITY** task to activate security.

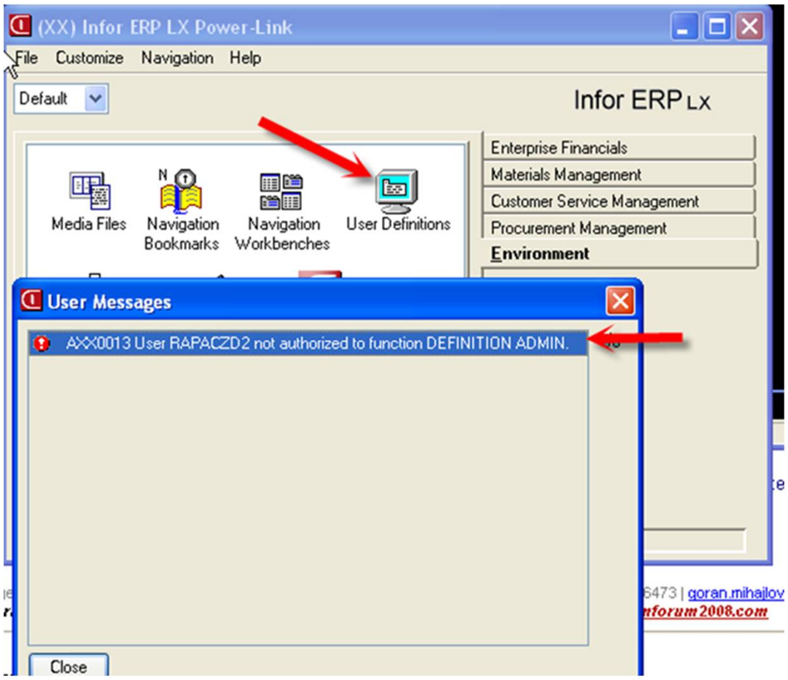


```
AMZB6DFR                         Maintain Tasks                         DISPLAY

Area . . . . . . . . . . :   Client Administration
Position to task ID . . .    __________ __________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

Opt  Task ID                      Type      App        Locked
 _   OBJECT     SECURITY          SEC       IDF          Y
     Assign Security for Business Objects
 __  OBJECT     UPDMNTPRF         SEC       IDF          N
     Update Object's Maintenance Preferences
 __  OBJECT     USEREXITS         SEC       IDF          N
     Control Business Object User Exits
 __  PREFERENCE ADMIN             SEC       IDF          N
     Perform User Preference Administration
 __  TXNSTS     ADMIN             SEC       IDF          N
     Transaction Status Administration                                    +

F3=Exit          F6=Add       F7=Backward    F8=Forward
F11=Job status   F12=Return   F17=Subset

MA    a                  MW                                          10/003
I902 - Session successfully started
```

6 Specify **11** to select users that will be authorized.

IDF User Definitions

To configure the users that can update User Definitions, use the Perform User Definition Maintenance option under Client Administration in IDF.

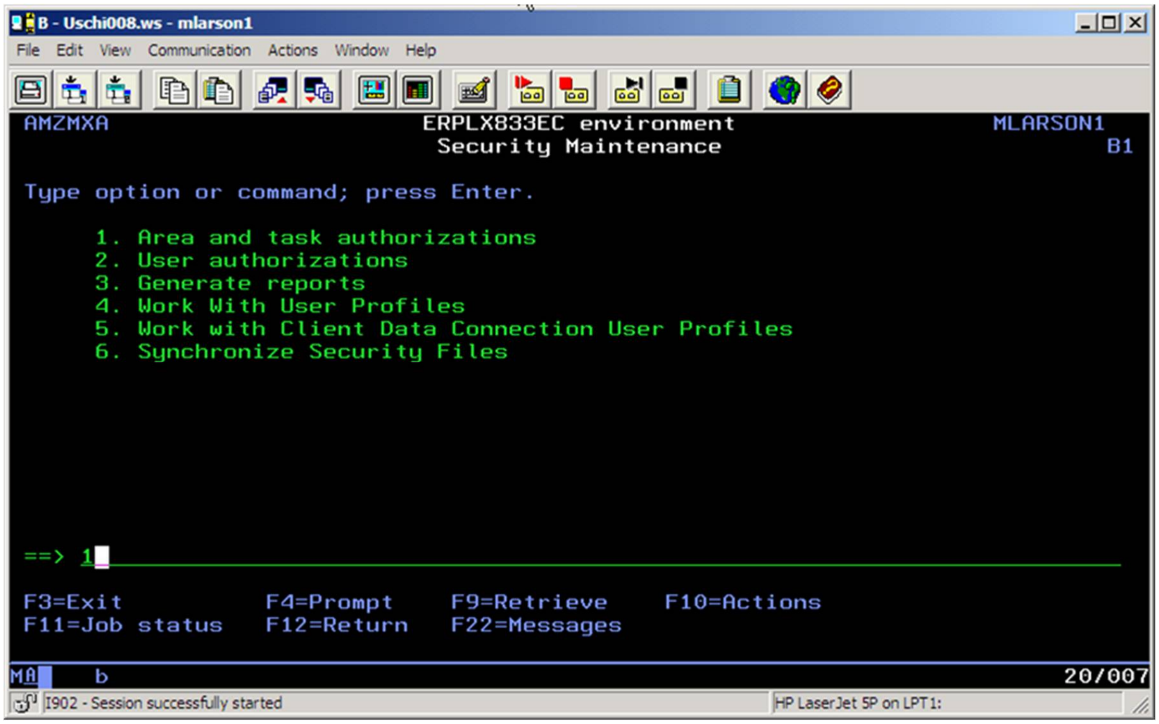


AXX0013 User RAPACZD2 not authorized to function DEFINITION ADMIN.

1 Start IDF and select the environment you want to secure.

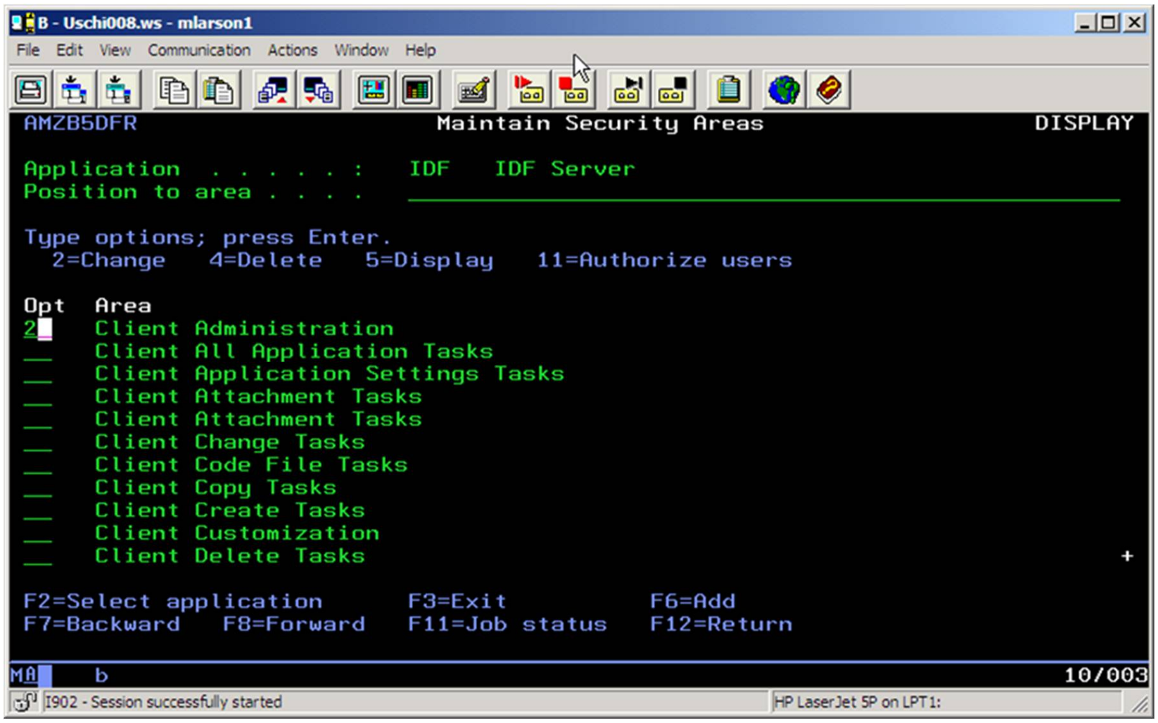
2 Specify **10**, **Security Maintenance**.

3 Specify **1** for Area and task authorizations.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

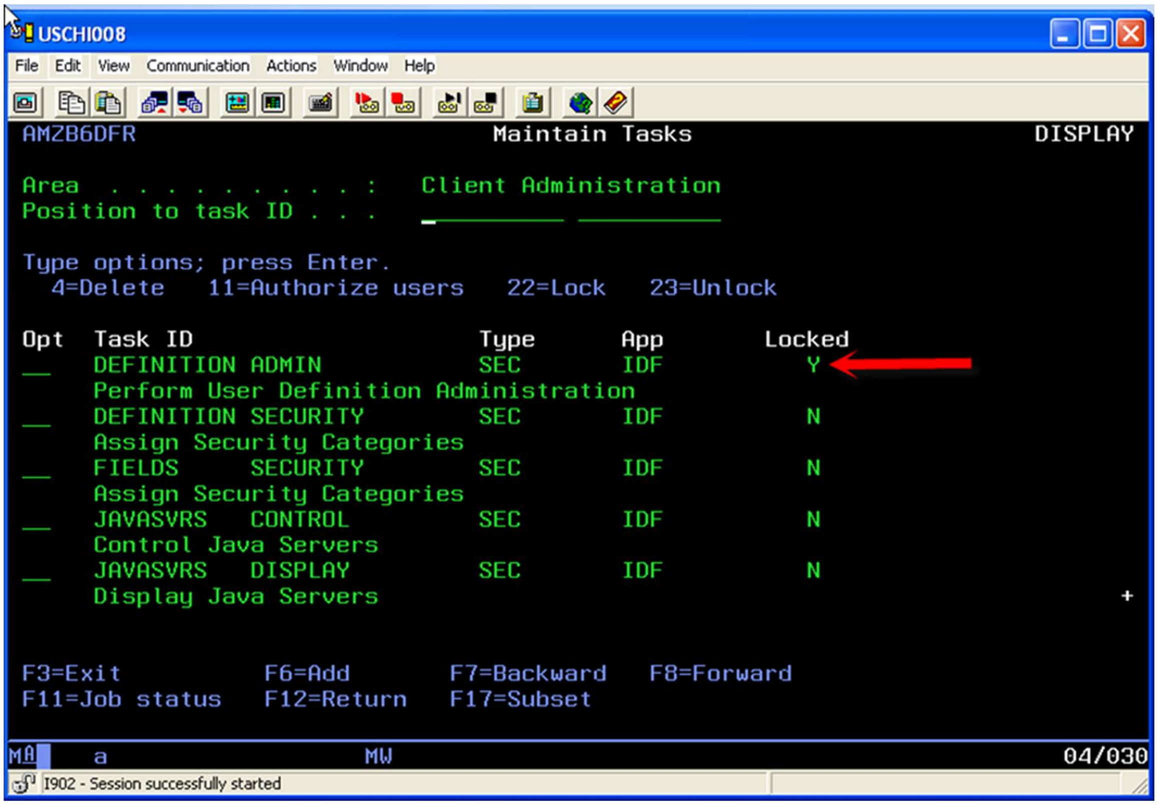
```
AMZMXA                    ERPLX833EC environment                 MLARSON1
                           Security Maintenance                        B1

Type option or command; press Enter.

     1. Area and task authorizations
     2. User authorizations
     3. Generate reports
     4. Work With User Profiles
     5. Work with Client Data Connection User Profiles
     6. Synchronize Security Files




==> 1

F3=Exit          F4=Prompt    F9=Retrieve     F10=Actions
F11=Job status   F12=Return   F22=Messages

MA     b                                                              20/007
I902 - Session successfully started                 HP LaserJet 5P on LPT1:
```

4 Specify **2** for **Client Administration**.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

```
AMZB5DFR                        Maintain Security Areas                  DISPLAY

Application . . . . . . :   IDF    IDF Server
Position to area . . . .    ______________________________________________

Type options; press Enter.
  2=Change    4=Delete    5=Display    11=Authorize users

Opt  Area
2    Client Administration
__   Client All Application Tasks
__   Client Application Settings Tasks
__   Client Attachment Tasks
__   Client Attachment Tasks
__   Client Change Tasks
__   Client Code File Tasks
__   Client Copy Tasks
__   Client Create Tasks
__   Client Customization
__   Client Delete Tasks                                                      +

F2=Select application        F3=Exit           F6=Add
F7=Backward    F8=Forward    F11=Job status    F12=Return
MA      b                                                                10/003
I902 - Session successfully started        HP LaserJet 5P on LPT1:
```

5 Specify **22** for **DEFINITION ADMIN** to activate security.



```
AMZB6DFR                         Maintain Tasks                          DISPLAY

Area . . . . . . . . . :   Client Administration
Position to task ID . . .  __________  __________

Type options; press Enter.
  4=Delete    11=Authorize users    22=Lock    23=Unlock

Opt  Task ID                    Type      App       Locked
__   DEFINITION ADMIN           SEC       IDF          Y
     Perform User Definition Administration
__   DEFINITION SECURITY        SEC       IDF          N
     Assign Security Categories
__   FIELDS     SECURITY        SEC       IDF          N
     Assign Security Categories
__   JAVASVRS   CONTROL         SEC       IDF          N
     Control Java Servers
__   JAVASVRS   DISPLAY         SEC       IDF          N
     Display Java Servers                                                     +


F3=Exit          F6=Add        F7=Backward    F8=Forward
F11=Job status   F12=Return    F17=Subset
MA      a              MW                                                04/030
I902 - Session successfully started
```

6 Specify **11** to select users that are authorized.

Security to change data on all IDF Business Objects

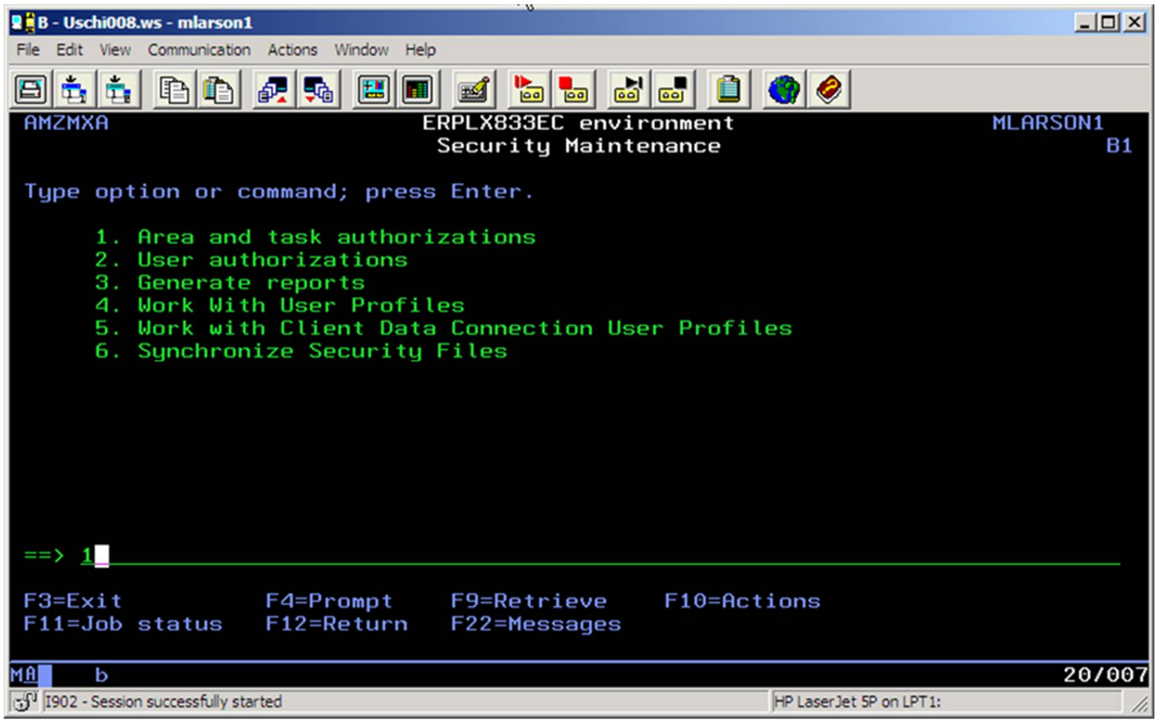
If you want to verify a user can only use Business Objects for inquiry, use the Maintain Business Objects option under Client Administration.

Note: This is Global for all Business Objects.

1 Start IDF and select the environment you want to secure.

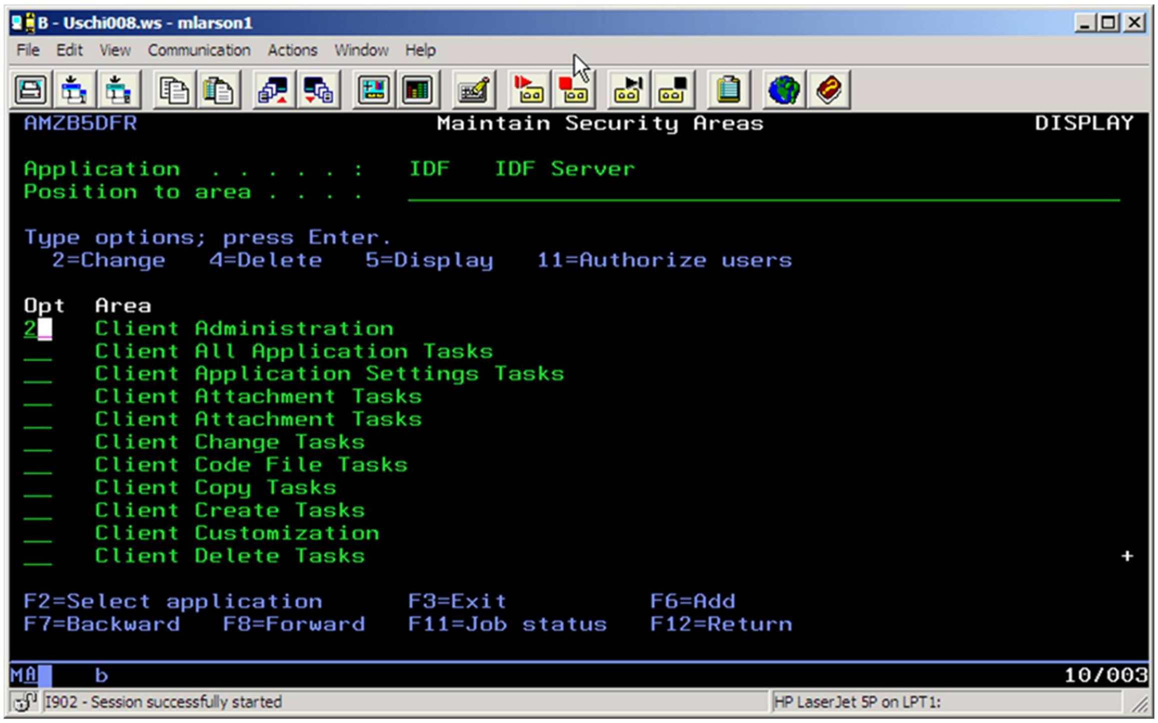
2 Specify **10**, **Security Maintenance**.

3 Specify **1** for Area and task authorizations.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

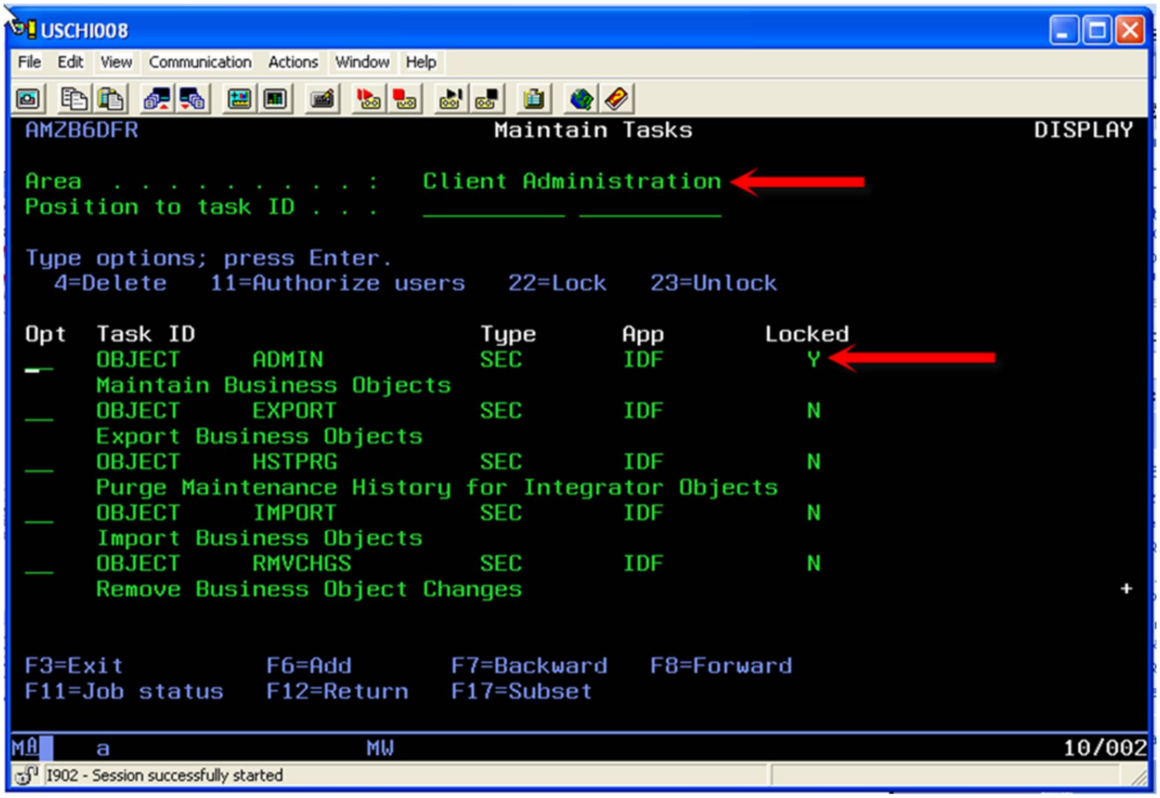
```
AMZMXA                    ERPLX833EC environment                  MLARSON1
                           Security Maintenance                         B1

Type option or command; press Enter.

     1. Area and task authorizations
     2. User authorizations
     3. Generate reports
     4. Work With User Profiles
     5. Work with Client Data Connection User Profiles
     6. Synchronize Security Files

==> 1

F3=Exit          F4=Prompt    F9=Retrieve    F10=Actions
F11=Job status   F12=Return   F22=Messages
MA    b                                                              20/007
```

4 Specify **2** for **Client Administration**.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

```
AMZB5DFR                  Maintain Security Areas                 DISPLAY

Application . . . . . . :   IDF    IDF Server
Position to area . . . .    ____________________________________________

Type options; press Enter.
  2=Change   4=Delete   5=Display   11=Authorize users

Opt   Area
2     Client Administration
__    Client All Application Tasks
__    Client Application Settings Tasks
__    Client Attachment Tasks
__    Client Attachment Tasks
__    Client Change Tasks
__    Client Code File Tasks
__    Client Copy Tasks
__    Client Create Tasks
__    Client Customization
__    Client Delete Tasks                                                +

F2=Select application        F3=Exit          F6=Add
F7=Backward    F8=Forward    F11=Job status   F12=Return

MA    b                                                           10/003
I902 - Session successfully started          HP LaserJet 5P on LPT1:
```

5 Specify **22** for the **OBJECT ADMIN** to activate security.



```
AMZB6DFR                     Maintain Tasks                        DISPLAY

Area . . . . . . . . . . :   Client Administration
Position to task ID . . .    __________ __________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

Opt  Task ID                    Type      App        Locked
__   OBJECT     ADMIN           SEC       IDF           Y
     Maintain Business Objects
__   OBJECT     EXPORT          SEC       IDF           N
     Export Business Objects
__   OBJECT     HSTPRG          SEC       IDF           N
     Purge Maintenance History for Integrator Objects
__   OBJECT     IMPORT          SEC       IDF           N
     Import Business Objects
__   OBJECT     RMVCHGS         SEC       IDF           N
     Remove Business Object Changes                                     +

F3=Exit          F6=Add        F7=Backward    F8=Forward
F11=Job status   F12=Return    F17=Subset

MA    a                  MW                                       10/002
I902 - Session successfully started
```

6 Specify **11** to select users that are authorized.

Preventing IDF end users from changing public cards

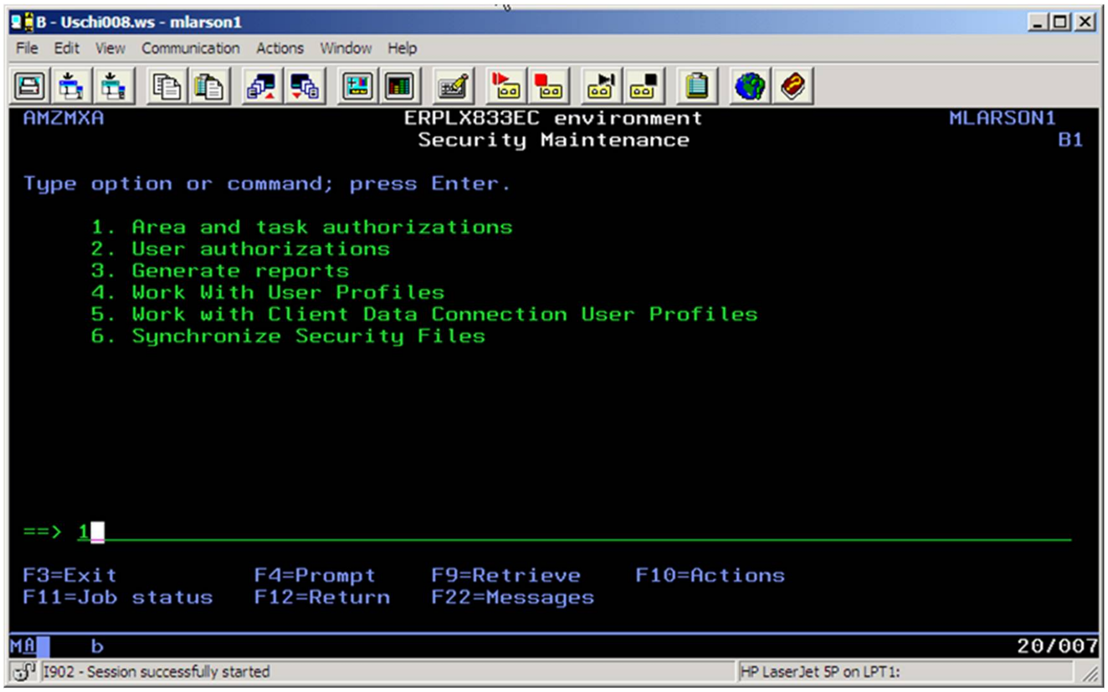
To prevent users from changing public cards, use the Maintain Public Cards option under Client Customization.

Note: This is Global for all Business Objects.

1 Start IDF and select the environment you want to secure.

2 Specify **10**, **Security Maintenance**.

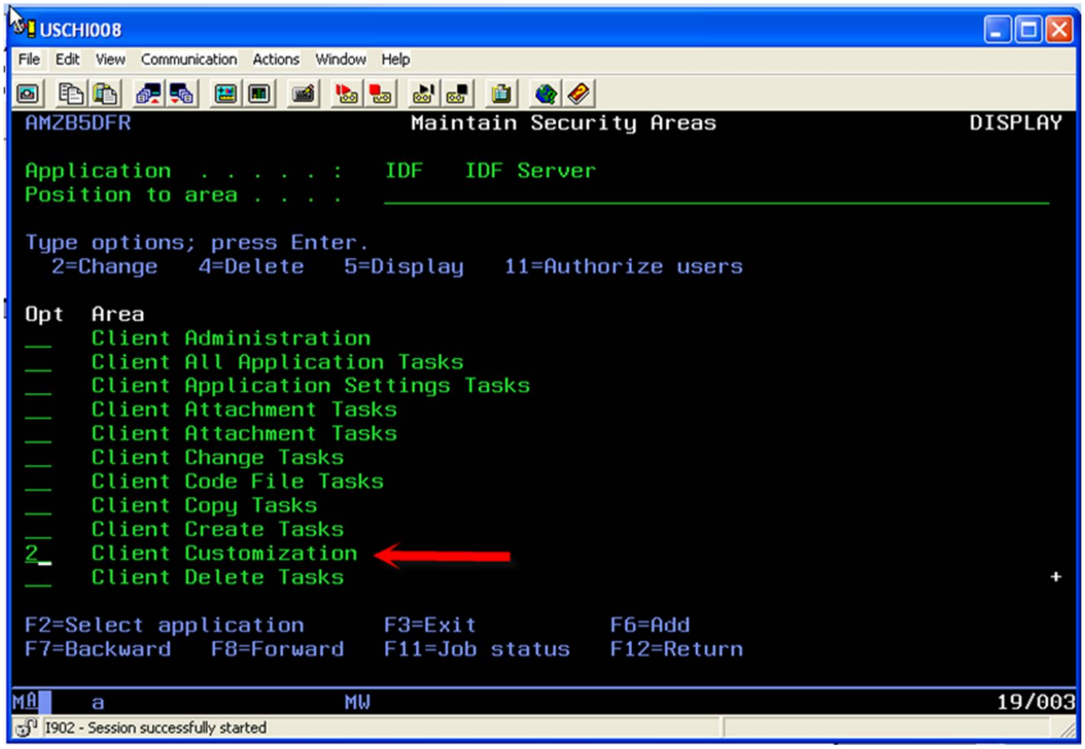
3 Specify **1** for Area and task authorizations.



B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

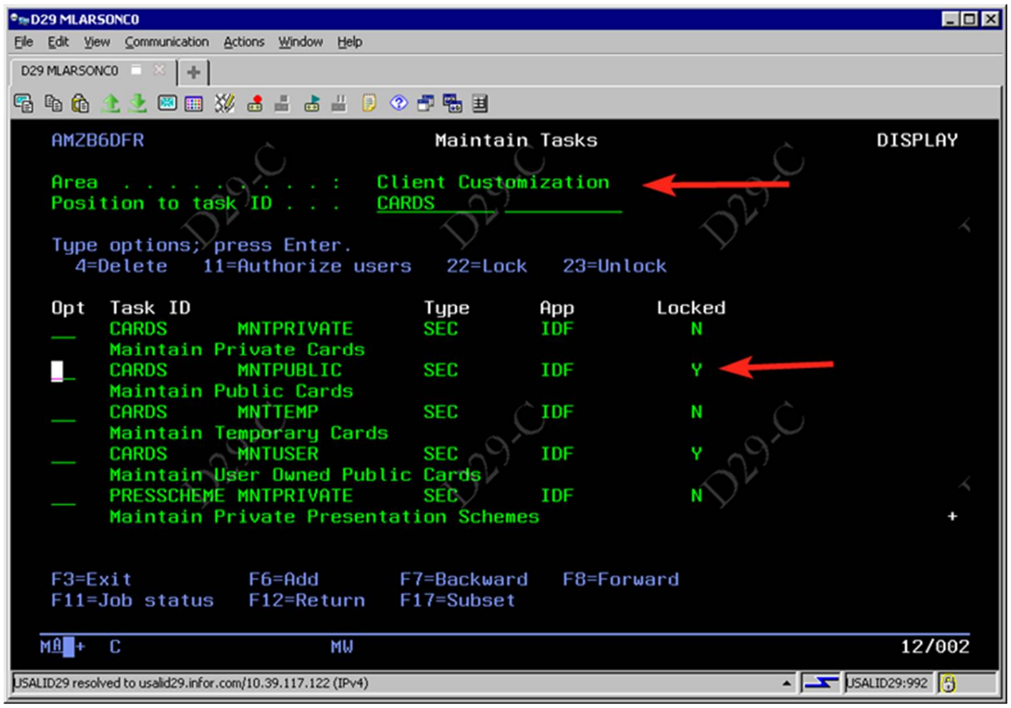
```
AMZMXA                    ERPLX833EC environment                    MLARSON1
                           Security Maintenance                           B1

Type option or command; press Enter.

     1. Area and task authorizations
     2. User authorizations
     3. Generate reports
     4. Work With User Profiles
     5. Work with Client Data Connection User Profiles
     6. Synchronize Security Files




==> 1

F3=Exit          F4=Prompt    F9=Retrieve    F10=Actions
F11=Job status   F12=Return   F22=Messages
MA     b                                                            20/007
```

4 Specify **2** for C**lient Customizations**.


USCHI008
File Edit View Communication Actions Window Help
I902 - Session successfully started

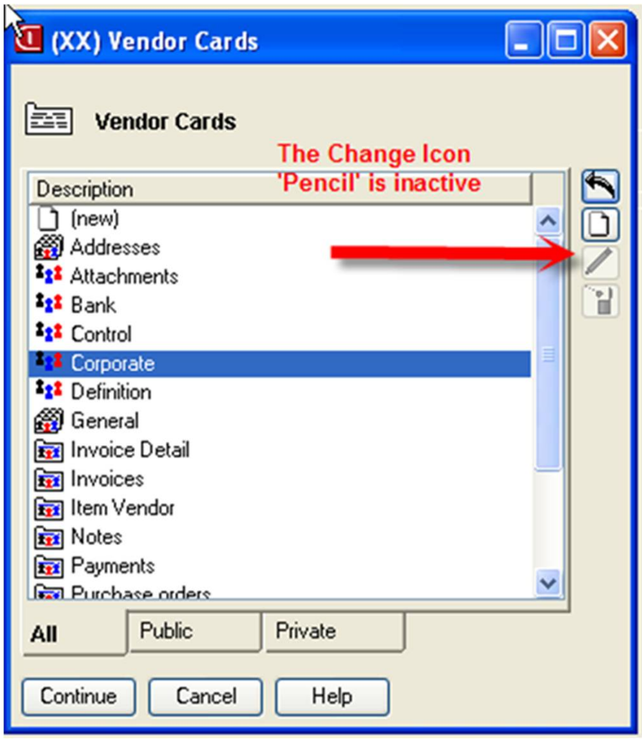
```
AMZB5DFR                          Maintain Security Areas                  DISPLAY

Application  . . . . . . :   IDF    IDF Server
Position to area . . . .     ____________________________________________________

Type options; press Enter.
  2=Change    4=Delete    5=Display    11=Authorize users

Opt  Area
__   Client Administration
__   Client All Application Tasks
__   Client Application Settings Tasks
__   Client Attachment Tasks
__   Client Attachment Tasks
__   Client Change Tasks
__   Client Code File Tasks
__   Client Copy Tasks
__   Client Create Tasks
2_   Client Customization
__   Client Delete Tasks                                                      +

F2=Select application       F3=Exit          F6=Add
F7=Backward     F8=Forward  F11=Job status   F12=Return

MA     a                    MW                                            19/003
```

5 Specify **22** for **CARDS MNTPUBLIC** to activate the security. Then, specify **11** to select the individual users that should have access to this function.

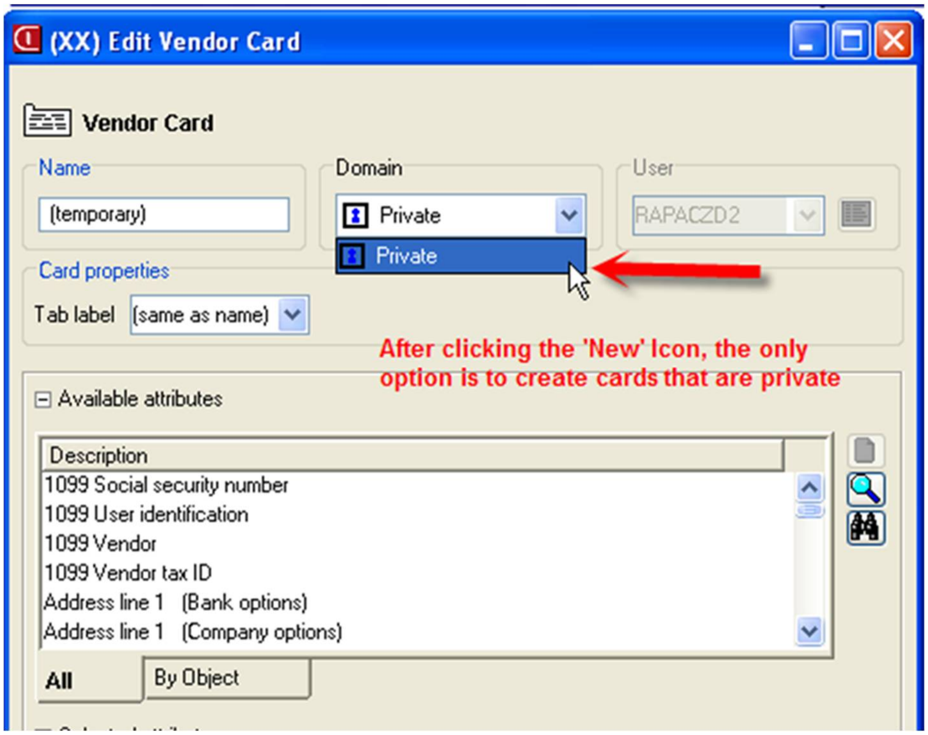

D29 MLARSONC0
File Edit View Communication Actions Window Help
D29 MLARSONC0
USALID29 resolved to usalid29.infor.com/10.39.117.122 (IPv4)
USALID29:992

```
AMZB6DFR                        Maintain Tasks                        DISPLAY

Area . . . . . . . . . . :   Client Customization
Position to task ID . . .    CARDS  __________

Type options; press Enter.
  4=Delete   11=Authorize users    22=Lock    23=Unlock

Opt  Task ID                    Type      App        Locked
__   CARDS      MNTPRIVATE      SEC       IDF        N
     Maintain Private Cards
__   CARDS      MNTPUBLIC       SEC       IDF        Y
     Maintain Public Cards
__   CARDS      MNTTEMP         SEC       IDF        N
     Maintain Temporary Cards
__   CARDS      MNTUSER         SEC       IDF        Y
     Maintain User Owned Public Cards
__   PRESSCHEME MNTPRIVATE      SEC       IDF        N
     Maintain Private Presentation Schemes                                +


F3=Exit         F6=Add        F7=Backward    F8=Forward
F11=Job status  F12=Return    F17=Subset

MA + C                      MW                                          12/002
```

6 To see the security in action, specify any card to change and note that the pencil option is inactive.



The Change Icon 'Pencil' is inactive



After clicking the 'New' Icon, the only option is to create cards that are private

Similar to securing public cards are the settings that allow users to create temporary cards (CARDS MNTTEMP) and User owned public cards (CARDS MNTUSER). The configuration for these security tasks is quite similar to CARDS MNTPUBLIC.

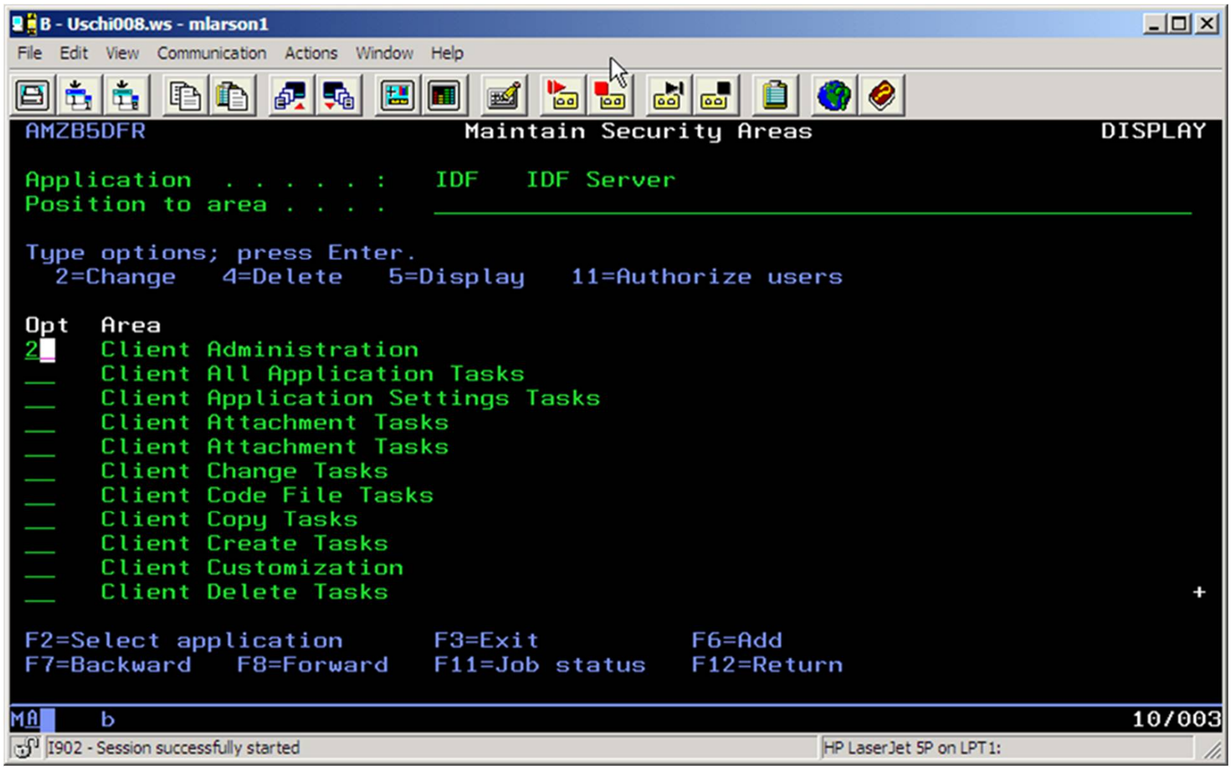
Preventing users from using IDF Link Manager

To prevent users from using Link Manager to start and stop IDF environments:

1 Start IDF and select the environment you want to secure.

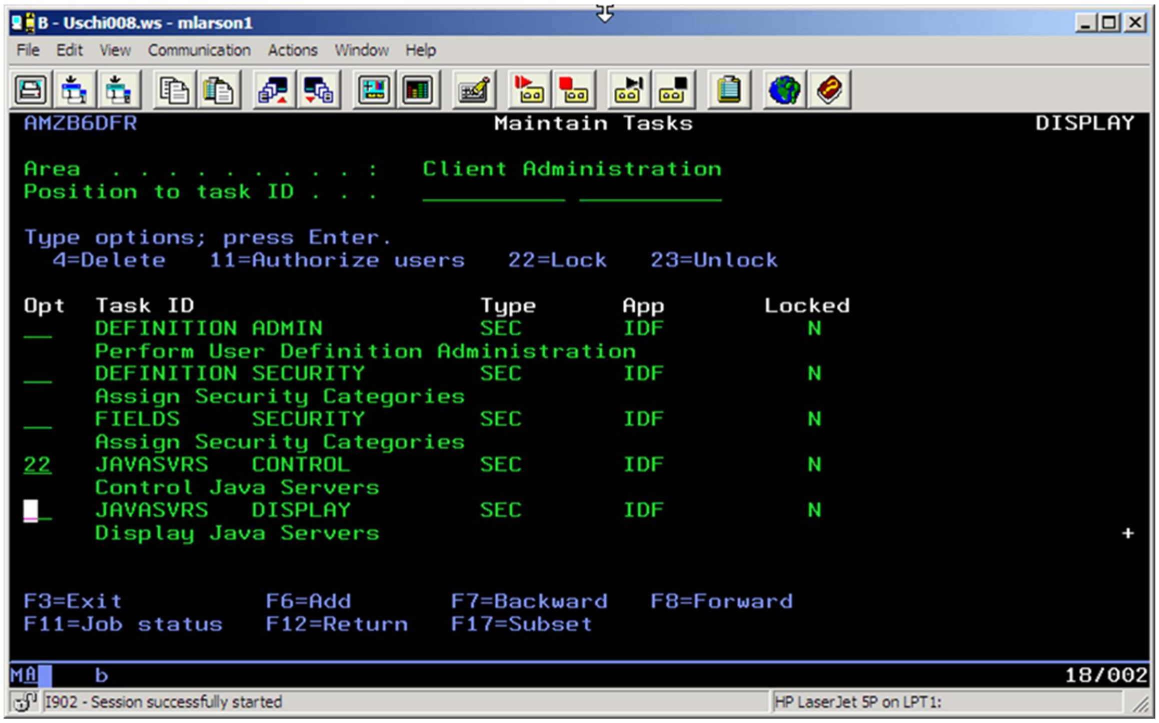
2 Specify **1** for Area and task authorizations.

3 Specify **2** for **Client Administration**.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

```
AMZB5DFR                      Maintain Security Areas                    DISPLAY

Application . . . . . . :   IDF   IDF Server
Position to area . . . .    __________________________________________

Type options; press Enter.
  2=Change    4=Delete    5=Display    11=Authorize users

Opt   Area
2     Client Administration
__    Client All Application Tasks
__    Client Application Settings Tasks
__    Client Attachment Tasks
__    Client Attachment Tasks
__    Client Change Tasks
__    Client Code File Tasks
__    Client Copy Tasks
__    Client Create Tasks
__    Client Customization
__    Client Delete Tasks                                                      +

F2=Select application         F3=Exit           F6=Add
F7=Backward    F8=Forward     F11=Job status    F12=Return

MA    b                                                                   10/003
I902 - Session successfully started                HP LaserJet 5P on LPT1:
```

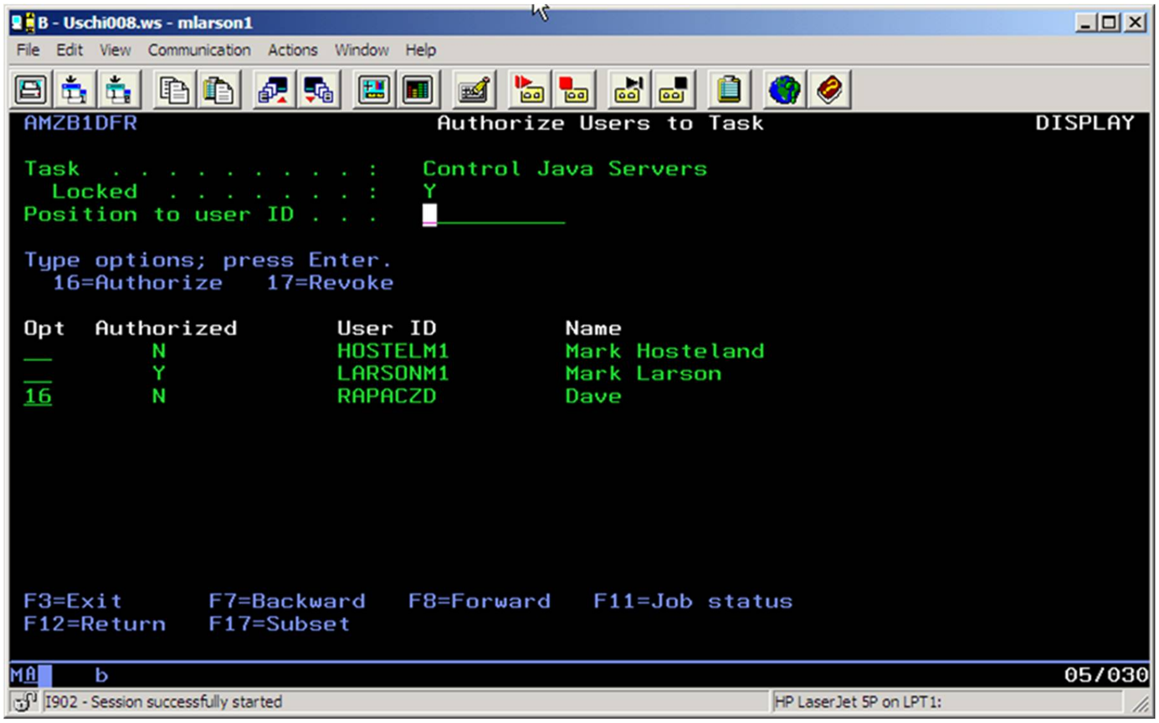
4 Specify **22** on **JAVASVRS CONTROL** to lock the task.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help
I902 - Session successfully started
HP LaserJet 5P on LPT1:

```
AMZB6DFR                        Maintain Tasks                       DISPLAY

Area . . . . . . . . . . :  Client Administration
Position to task ID . . .   __________ __________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

Opt  Task ID                    Type      App       Locked
__   DEFINITION ADMIN           SEC       IDF         N
     Perform User Definition Administration
__   DEFINITION SECURITY        SEC       IDF         N
     Assign Security Categories
__   FIELDS     SECURITY        SEC       IDF         N
     Assign Security Categories
22   JAVASVRS   CONTROL         SEC       IDF         N
     Control Java Servers
_    JAVASVRS   DISPLAY         SEC       IDF         N
     Display Java Servers
                                                                          +

F3=Exit          F6=Add        F7=Backward    F8=Forward
F11=Job status   F12=Return    F17=Subset

MA     b                                                            18/002
```

5 To select user that are allowed access, specify **11**.

6 Then, specify **16** for each user that should be granted access or choose **17** to revoke a user's access.


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help
I902 - Session successfully started
HP LaserJet 5P on LPT1:

```
AMZB1DFR                    Authorize Users to Task                  DISPLAY

Task . . . . . . . . . . :  Control Java Servers
  Locked . . . . . . . . :  Y
Position to user ID . . .   __________

Type options; press Enter.
  16=Authorize   17=Revoke

Opt  Authorized        User ID          Name
__       N             HOSTELM1         Mark Hosteland
__       Y             LARSONM1         Mark Larson
16       N             RAPACZD          Dave




F3=Exit      F7=Backward    F8=Forward    F11=Job status
F12=Return   F17=Subset

MA     b                                                            05/030
```

Secure IDF object's tasks

All LX 8.4 IDF objects have CAS security added. To review and maintain object's security:

1 Start IDF and select the environment you want to secure.

2 Select 10, Security Maintenance.

3 Select 1, Area and task authorizations.

4 The list of LX 8.4 product applications in IDF is:

- ACR LX Accounts Receivable
- COM LX Common Application Support
- LCS LX Customer Service Management
- LEF LX Enterprise Financials
- LPD LX Enterprise Product Data Mgt
- LMM LX Materials Management
- LOP LX Order-Based Production Mgt
- LPM LX Procurement Management
- LRB LX Rate-Based Production Mgt

If STTi is installed this product application may also be secured:

- STT Serial Number Tracking and Tracing

For CRMi use the following product applications to secure objects:

- CRM Customer Relationship Management
- CSM Customer Service Management

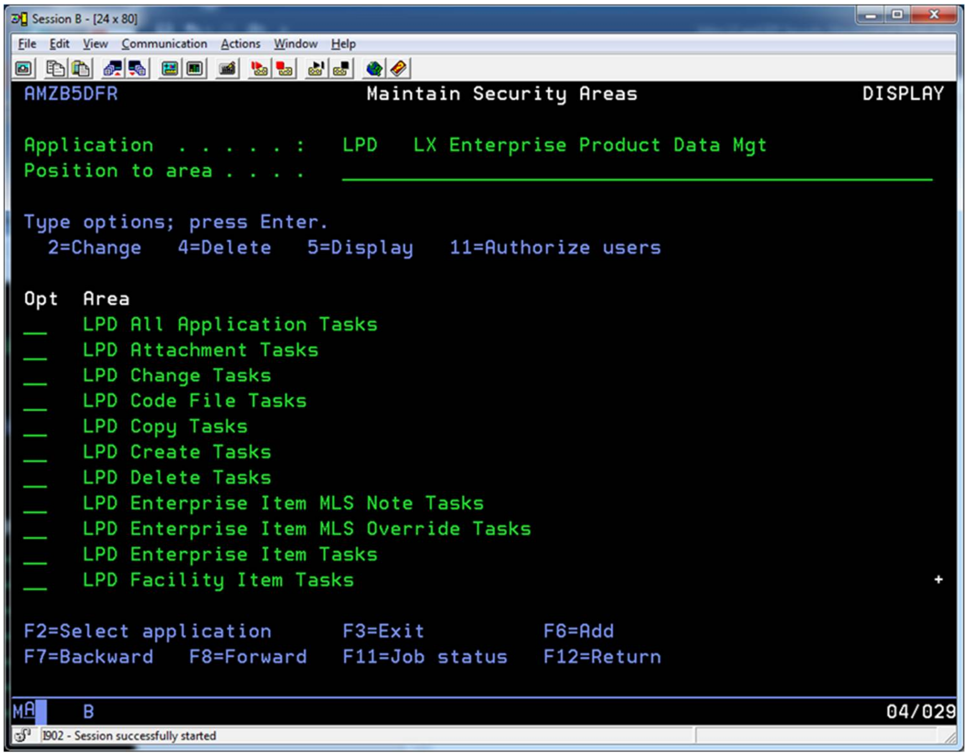
For EGLi use the following product applications to secure objects:

- EGL Enterprise General Ledger

For Brazil Pack use the following product applications to secure objects:

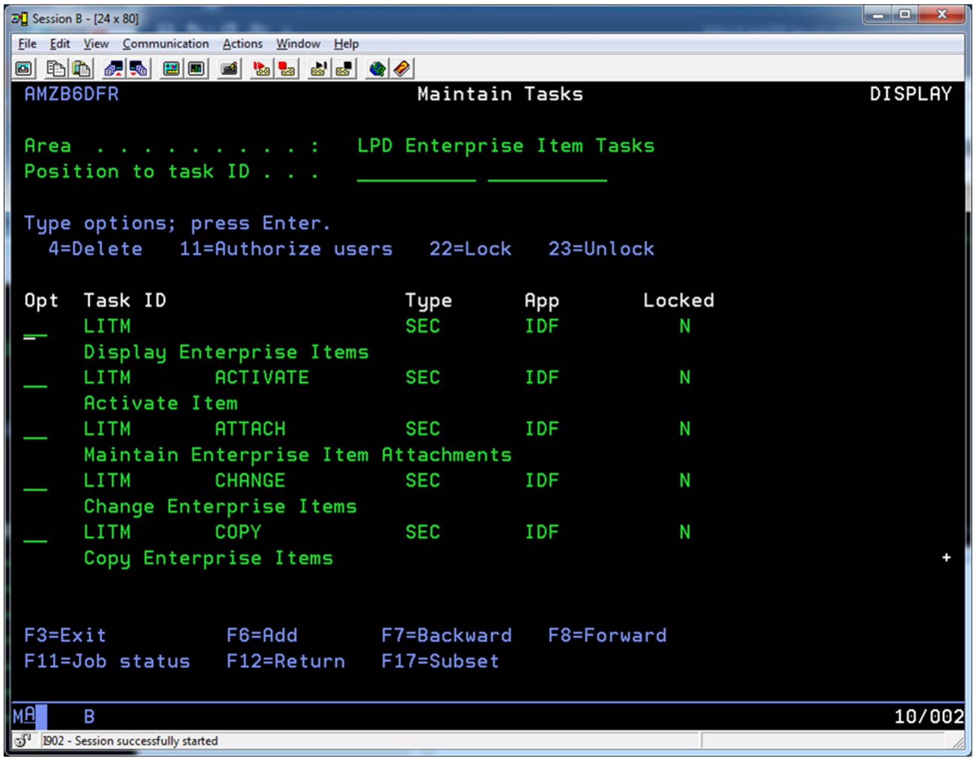
- LBP LX Brazil Production Mgt

5 Select an application. The **Maintain Security Areas** screen lists all available application tasks.



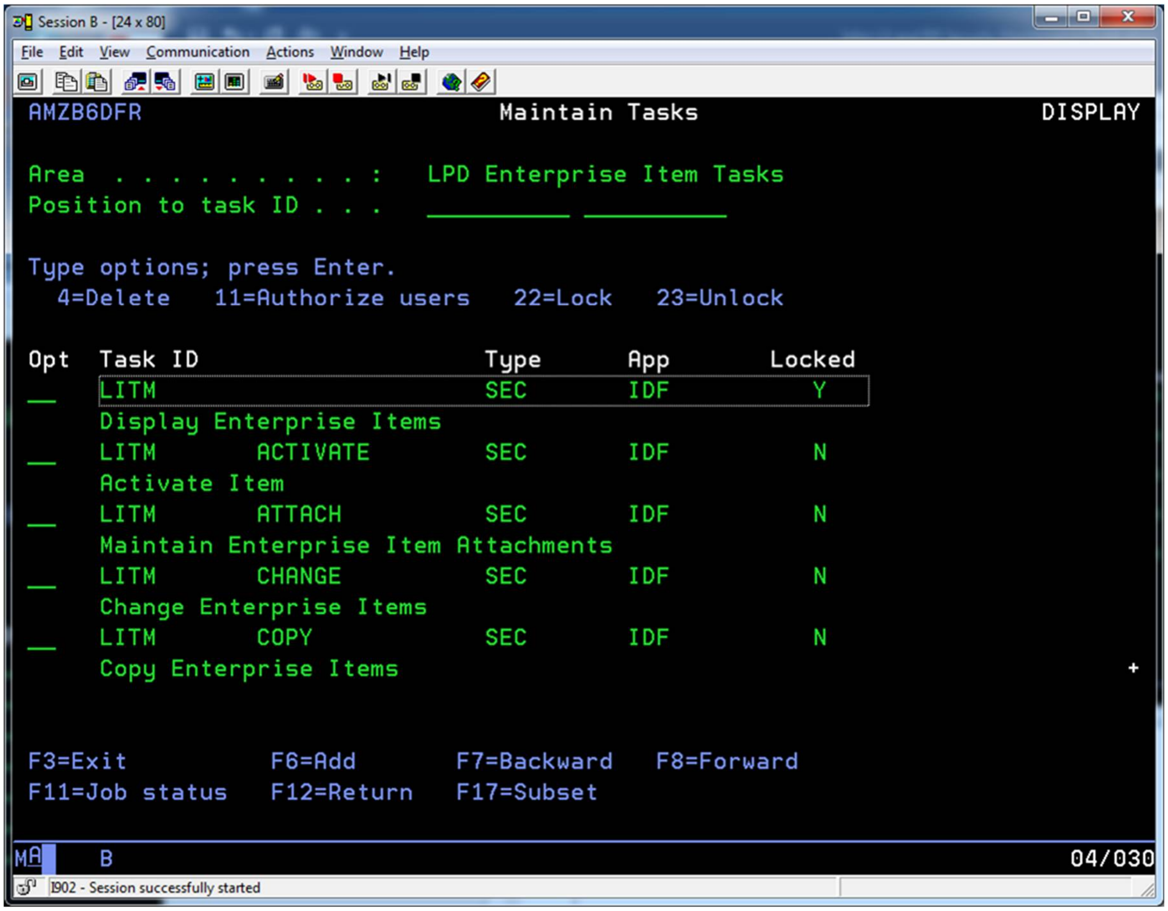
```
AMZB5DFR                     Maintain Security Areas                    DISPLAY

Application  . . . . . :   LPD   LX Enterprise Product Data Mgt
Position to area . . . .   __________________________________________________

Type options; press Enter.
  2=Change   4=Delete   5=Display   11=Authorize users

Opt  Area
__   LPD All Application Tasks
__   LPD Attachment Tasks
__   LPD Change Tasks
__   LPD Code File Tasks
__   LPD Copy Tasks
__   LPD Create Tasks
__   LPD Delete Tasks
__   LPD Enterprise Item MLS Note Tasks
__   LPD Enterprise Item MLS Override Tasks
__   LPD Enterprise Item Tasks
__   LPD Facility Item Tasks                                                  +

F2=Select application      F3=Exit          F6=Add
F7=Backward   F8=Forward   F11=Job status   F12=Return

MA     B                                                                 04/029
I902 - Session successfully started
```

6 Use option **2=Change** for selected task.



```
AMZB6DFR                        Maintain Tasks                          DISPLAY

Area  . . . . . . . . . :   LPD Enterprise Item Tasks
Position to task ID . . .   __________ __________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

Opt  Task ID                    Type      App       Locked
__   LITM                       SEC       IDF          N
     Display Enterprise Items
__   LITM       ACTIVATE        SEC       IDF          N
     Activate Item
__   LITM       ATTACH          SEC       IDF          N
     Maintain Enterprise Item Attachments
__   LITM       CHANGE          SEC       IDF          N
     Change Enterprise Items
__   LITM       COPY            SEC       IDF          N
     Copy Enterprise Items                                                    +


F3=Exit          F6=Add       F7=Backward   F8=Forward
F11=Job status   F12=Return   F17=Subset

MA     B                                                                 10/002
I902 - Session successfully started
```

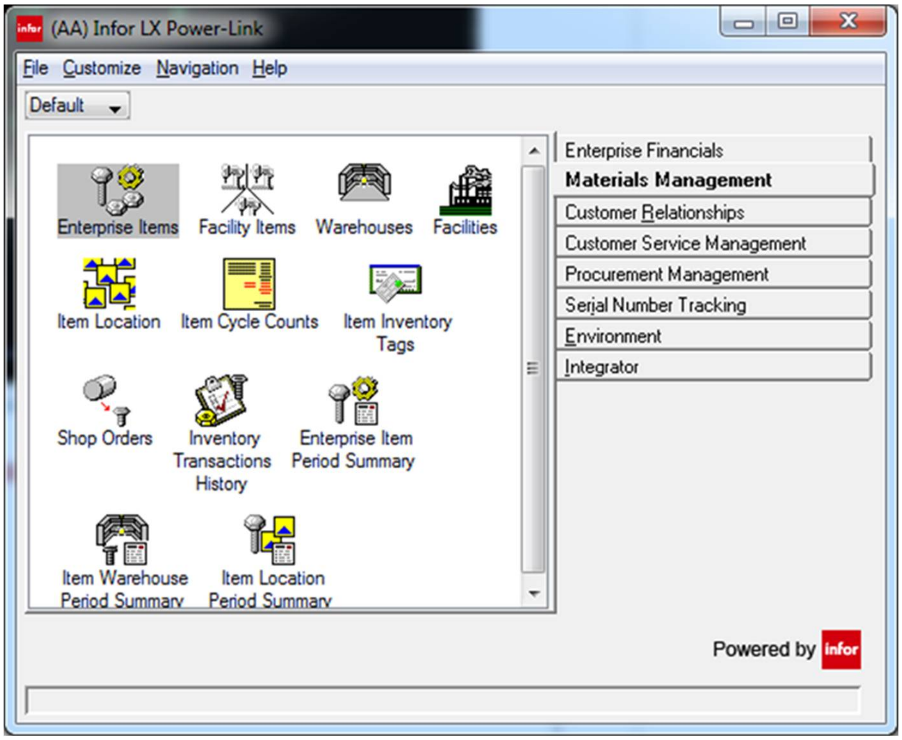
7 Use option **22=Lock** to activate task's security. The Locked flag is set to **Y**.



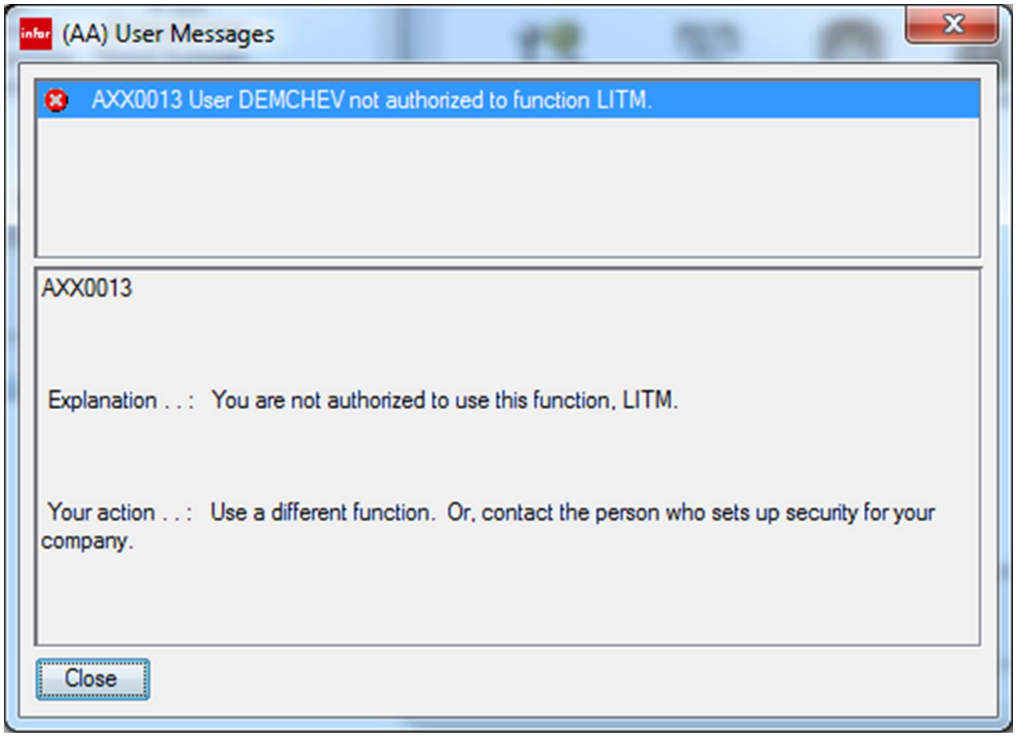
```
AMZB6DFR                  Maintain Tasks                          DISPLAY

Area . . . . . . . . . :   LPD Enterprise Item Tasks
Position to task ID . . .   __________ __________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

Opt  Task ID                    Type      App       Locked
__   LITM                       SEC       IDF          Y
     Display Enterprise Items
__   LITM       ACTIVATE        SEC       IDF          N
     Activate Item
__   LITM       ATTACH          SEC       IDF          N
     Maintain Enterprise Item Attachments
__   LITM       CHANGE          SEC       IDF          N
     Change Enterprise Items
__   LITM       COPY            SEC       IDF          N
     Copy Enterprise Items                                         +

F3=Exit          F6=Add        F7=Backward    F8=Forward
F11=Job status   F12=Return    F17=Subset

MA     B                                                       04/030
I902 - Session successfully started
```

As a result, the User will not be able to execute this task. In this example, user will not be able to open Enterprise Item object.

8 Start IDF and try to open Enterprise Item object:



The error message is displayed.



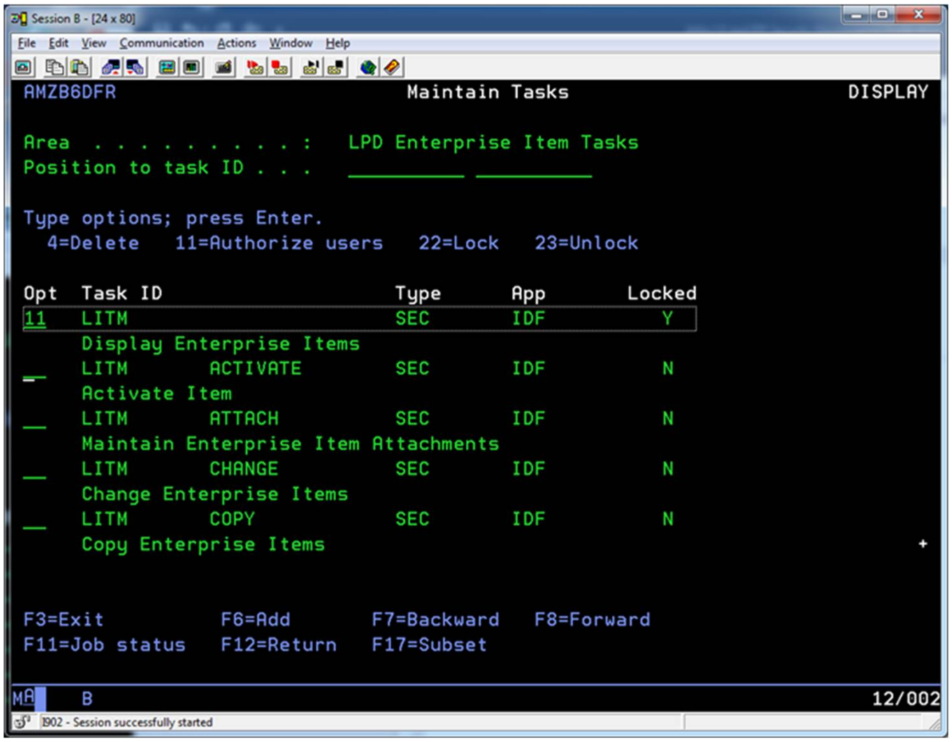
AXX0013 User DEMCHEV not authorized to function LITM.

AXX0013

Explanation . . : You are not authorized to use this function, LITM.

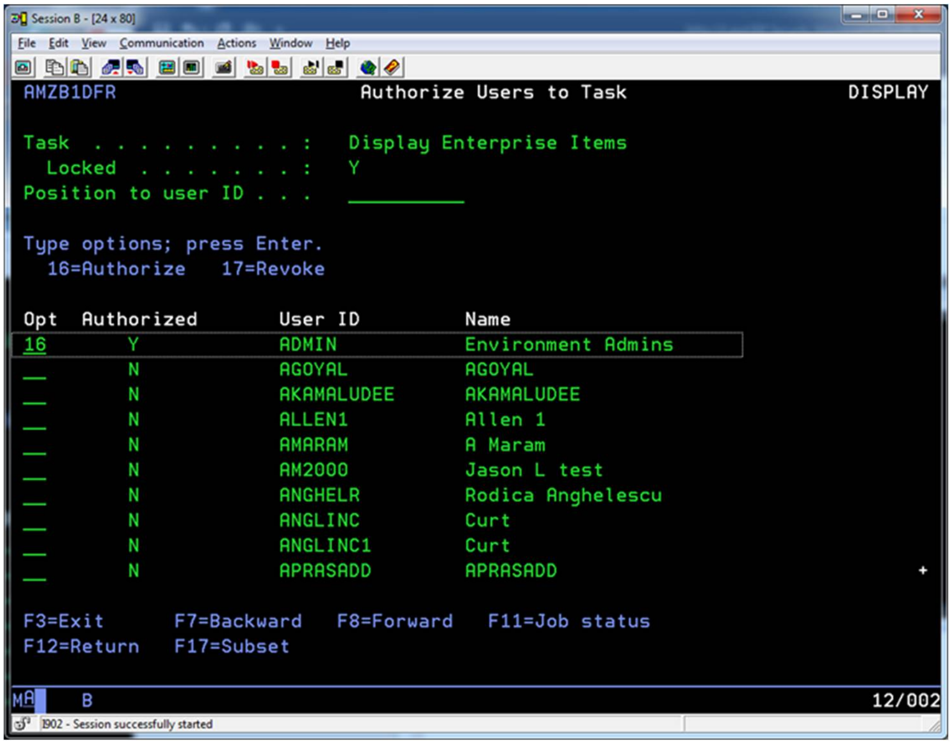
Your action . . : Use a different function. Or, contact the person who sets up security for your company.

9 To authorize user to the task, use option **11=Authorize users**.



```
AMZB6DFR                         Maintain Tasks                          DISPLAY

Area . . . . . . . . . . :   LPD Enterprise Item Tasks
Position to task ID . . .    __________ __________

Type options; press Enter.
  4=Delete    11=Authorize users    22=Lock    23=Unlock

Opt  Task ID                     Type      App       Locked
11   LITM                        SEC       IDF            Y
     Display Enterprise Items
_    LITM       ACTIVATE         SEC       IDF            N
     Activate Item
_    LITM       ATTACH           SEC       IDF            N
     Maintain Enterprise Item Attachments
_    LITM       CHANGE           SEC       IDF            N
     Change Enterprise Items
_    LITM       COPY             SEC       IDF            N
     Copy Enterprise Items                                                    +

F3=Exit          F6=Add       F7=Backward    F8=Forward
F11=Job status   F12=Return   F17=Subset

MA    B                                                                  12/002
1902 - Session successfully started
```

10 Use code **16=Authorize** to authorize user to the task.



```
AMZB1DFR                     Authorize Users to Task                     DISPLAY

Task . . . . . . . . . . :   Display Enterprise Items
  Locked . . . . . . . . :   Y
Position to user ID . . .    __________

Type options; press Enter.
  16=Authorize    17=Revoke

Opt  Authorized         User ID         Name
16        Y             ADMIN           Environment Admins
_         N             AGOYAL          AGOYAL
_         N             AKAMALUDEE      AKAMALUDEE
_         N             ALLEN1          Allen 1
_         N             AMARAM          A Maram
_         N             AM2000          Jason L test
_         N             ANGHELR         Rodica Anghelescu
_         N             ANGLINC         Curt
_         N             ANGLINC1        Curt
_         N             APRASADD        APRASADD                              +

F3=Exit      F7=Backward   F8=Forward   F11=Job status
F12=Return   F17=Subset

MA    B                                                                  12/002
1902 - Session successfully started
```

Locate LPD Field Level Security. It has two tasks that secures two sets of attributes:

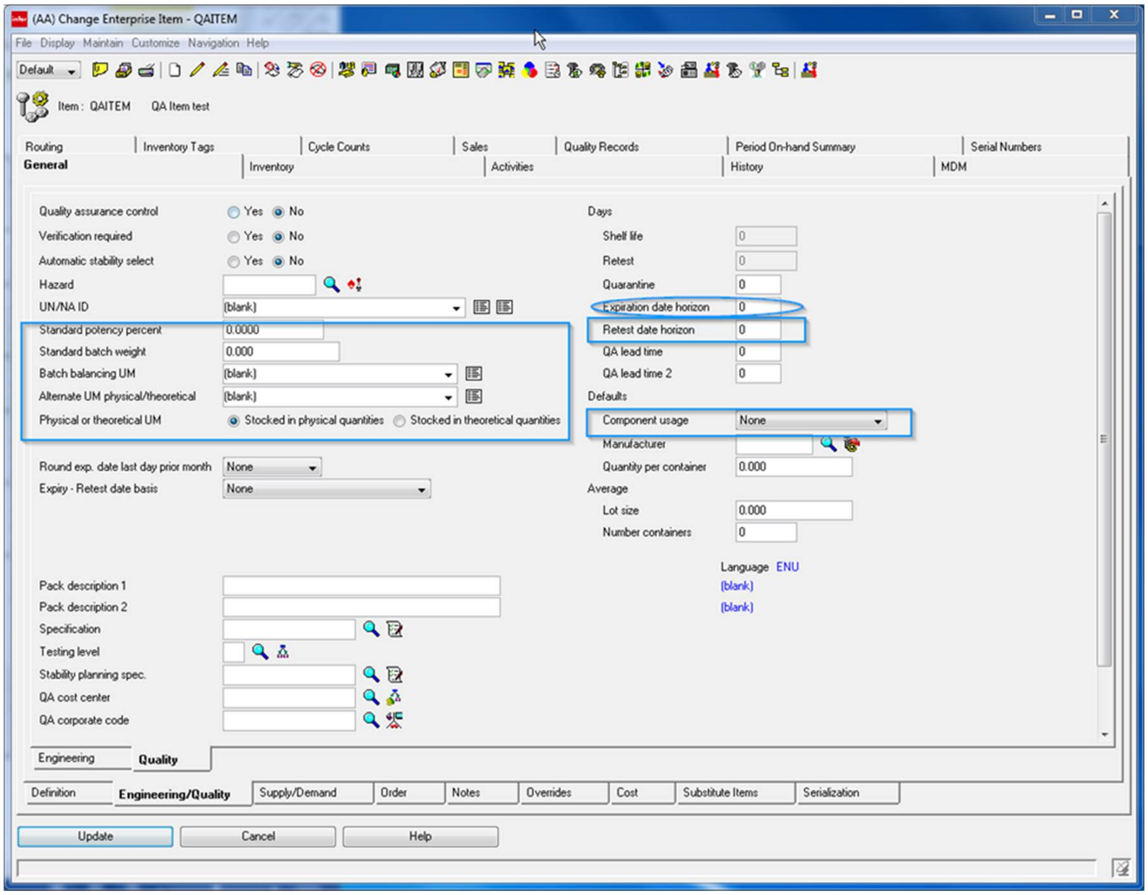
- Maintain LX QMS fields

- Maintain LX API fields

If you locked the task, only authorized users can maintain the group of the attributes.

When a user is authorized to the task:

Open Item. The attributes are input allowed and you can change them.



Item : QAITEM QA Item test

Quality assurance control ○ Yes ● No

Verification required ○ Yes ● No

Automatic stability select ○ Yes ● No

Hazard

UN/NA ID (blank)

Standard potency percent 0.0000

Standard batch weight 0.000

Batch balancing UM (blank)

Alternate UM physical/theoretical (blank)

Physical or theoretical UM ● Stocked in physical quantities ○ Stocked in theoretical quantities

Round exp. date last day prior month None

Expiry - Retest date basis None

Pack description 1

Pack description 2

Specification

Testing level

Stability planning spec.

QA cost center

QA corporate code

Days

Shelf life 0

Retest 0

Quarantine 0

Expiration date horizon 0

Retest date horizon 0

QA lead time 0

QA lead time 2 0

Defaults

Component usage None

Manufacturer

Quantity per container 0.000

Average

Lot size 0.000

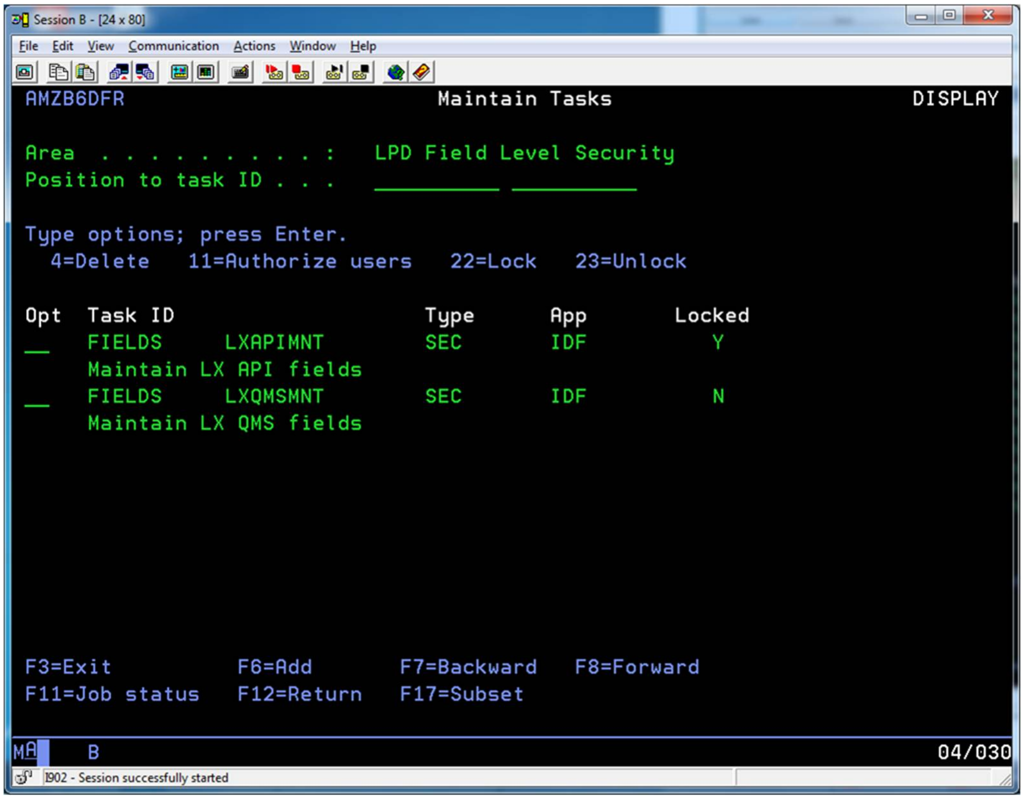
Number containers 0

Language ENU

(blank)

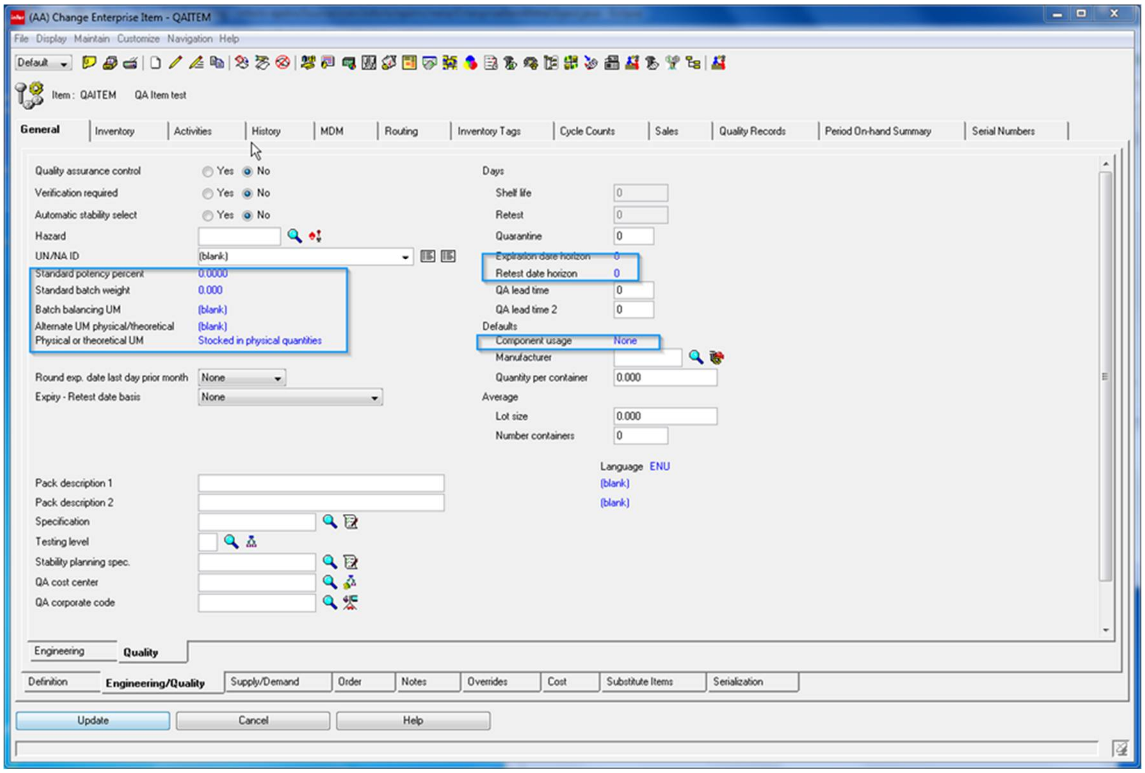
(blank)

Lock LPD Field Level Security/Maintain LX API fields.


Session B - [24 x 80]
File Edit View Communication Actions Window Help
MA B 04/030
I902 - Session successfully started

```
AMZB6DFR                     Maintain Tasks                        DISPLAY

Area . . . . . . . . . :  LPD Field Level Security
Position to task ID . . .  __________ __________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

Opt  Task ID                     Type     App       Locked
__   FIELDS     LXAPIMNT          SEC      IDF           Y
     Maintain LX API fields
__   FIELDS     LXQMSMNT          SEC      IDF           N
     Maintain LX QMS fields








F3=Exit          F6=Add       F7=Backward   F8=Forward
F11=Job status   F12=Return   F17=Subset
```

The attributes become protected.



Item : QAITEM QA Item test

Quality assurance control ○ Yes ● No

Verification required ○ Yes ● No

Automatic stability select ○ Yes ● No

Hazard

UN/NA ID (blank)

Standard potency percent 0.0000

Standard batch weight 0.000

Batch balancing UM (blank)

Alternate UM physical/theoretical (blank)

Physical or theoretical UM Stocked in physical quantities

Round exp. date last day prior month None

Expiry - Retest date basis None

Pack description 1

Pack description 2

Specification

Testing level

Stability planning spec.

QA cost center

QA corporate code

Days

Shelf life 0

Retest 0

Quarantine 0

Expiration date horizon 0

Retest date horizon 0

QA lead time 0

QA lead time 2 0

Defaults

Component usage None

Manufacturer

Quantity per container 0.000

Average

Lot size 0.000

Number containers 0

Language ENU

(blank)

(blank)

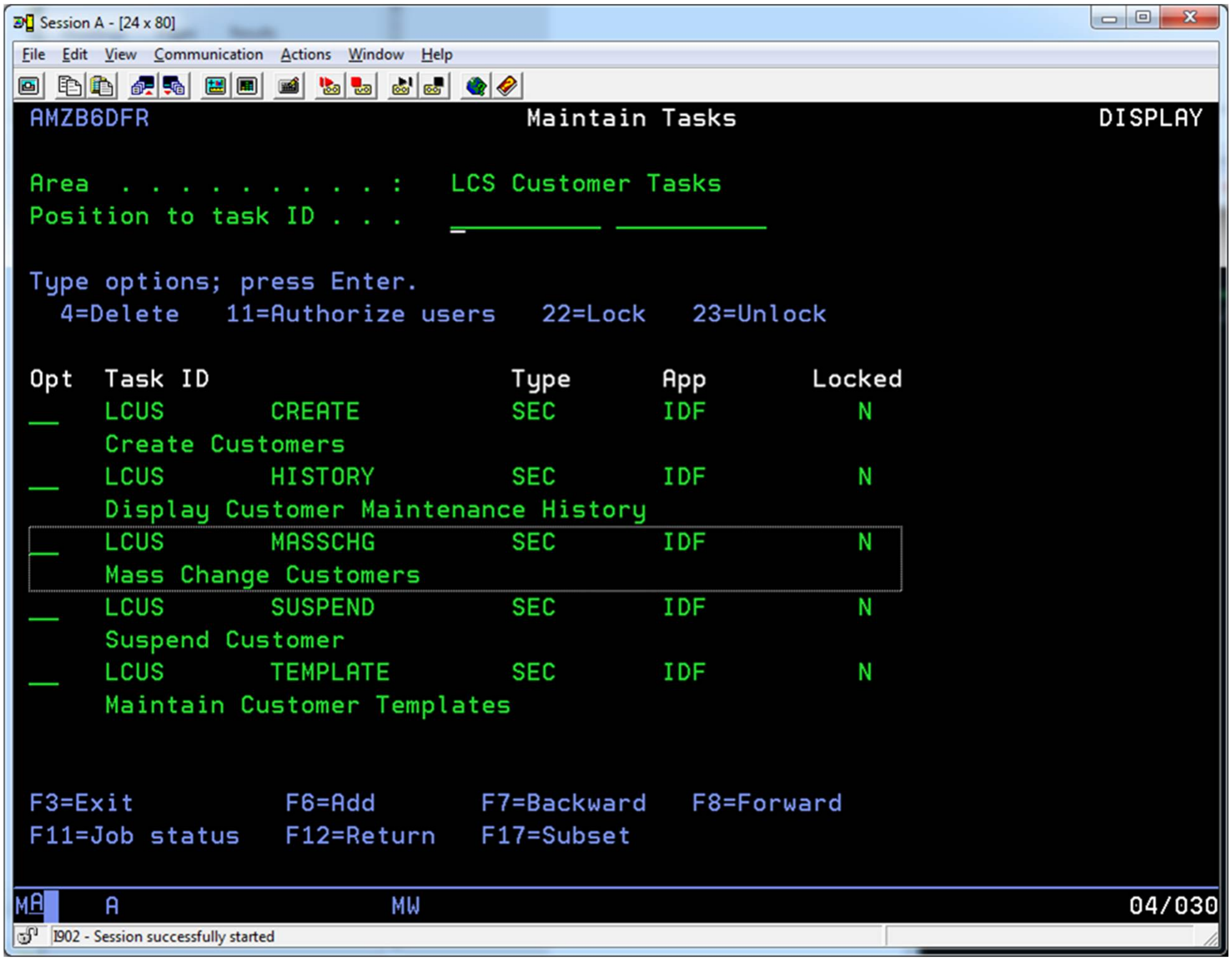
Securing IDF Mass Change and Mass Delete actions

This is strongly recommended to secure the tasks that allows mass update or delete actions.

The following tasks are:

- Mass Change Customers
- Mass Change Item Costs
- Mass Change Vendors
- Mass Change Enterprise Items
- Mass Delete Item Costs
- Mass UPC Update for Enterprise Item

In order to secure them, you have to lock these tasks using the action 22=Lock (see the previous topic for details). You may authorize none or limited number of experienced users to these tasks.



```
 AMZB6DFR                         Maintain Tasks                        DISPLAY

 Area . . . . . . . . . :   LCS Customer Tasks
 Position to task ID . . .  __________ __________

 Type options; press Enter.
   4=Delete   11=Authorize users   22=Lock   23=Unlock

 Opt  Task ID                   Type      App       Locked
 __   LCUS       CREATE         SEC       IDF          N
      Create Customers
 __   LCUS       HISTORY        SEC       IDF          N
      Display Customer Maintenance History
 __   LCUS       MASSCHG        SEC       IDF          N
      Mass Change Customers
 __   LCUS       SUSPEND        SEC       IDF          N
      Suspend Customer
 __   LCUS       TEMPLATE       SEC       IDF          N
      Maintain Customer Templates


 F3=Exit          F6=Add        F7=Backward   F8=Forward
 F11=Job status   F12=Return    F17=Subset

MA     A                  MW                                              04/030
```

1902 - Session successfully started

Chapter 5 Updating IDF security from LX

The Copy Security to IDF (CPYSECIDF) command was a tool used with LX 8.3.5 and 8.4.0 to help with the setup of user security in IDF for LX. In LX 8.4.1, CPYSECIDF has been replaced by several programs and objects. CPYSECIDF should no longer used.

These LX security areas can be mapped to IDF security:

LX Security	IDF CAS Security
Data Security: Company	Auto-Content Security: Company (LX)
Data Security: Facility	Auto-Content Security: Facility (LX)
Data Security: Warehouse	Auto-Content Security: Warehouse (LX)
Data Security: CEA Ledger, Book, Year	Auto-Content Security: Ledger Ledger; Book Ledger; Book; Year
Data Security: CEA Ledger, Book, Year	Auto-Content Security: EGLI Ledger EGLI Ledger; Book EGLI Ledger; Book; Year
Access Security: Product	Business Object
Access Security: Program	Business Object
Access Security: Function Keys and Action Codes	Business Object Actions

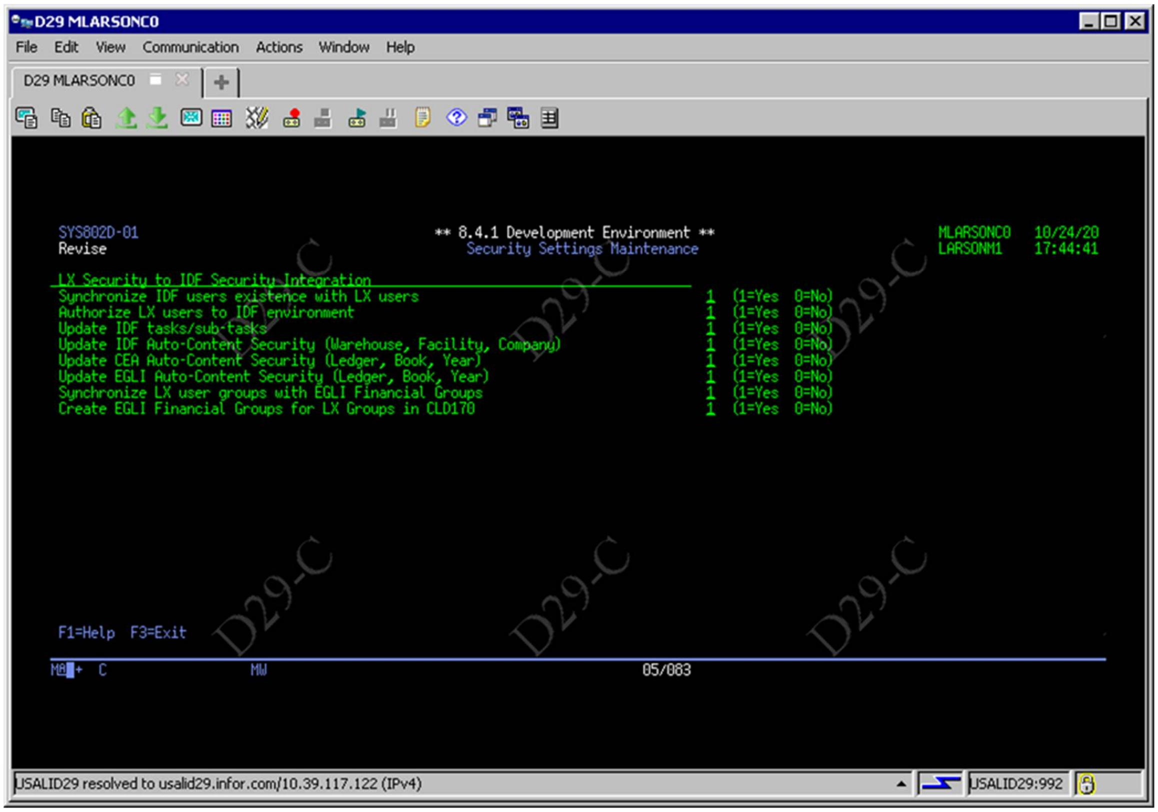
Data security for Company, Facility, and Warehouse in LX is setup in SYS600 for each user, either directly for a user or through assigned Business Units. Data security for CEA Ledger, Book, and Year in LX is set up in CLD177 for each user via their group in SYS600. These same values are migrated to IDF and can be viewed and modified in the User Profiles business object.

Access security for products and programs is controlled by SYS600 for users, either directly for a user or through assigned Business Roles. Function Keys and Action Codes security is controlled by SYS603 for groups assigned to users in SYS600. These settings map to Business Object actions such as create, change, copy, activate, suspend.

The steps to configure, initialize, and maintain user security integration with IDF are as follows.

Set IDF integration defaults

For initial setup use SYS800/SYS802 Security Settings Maintenance to choose the default settings you wish to use to update IDF security settings from LX. These settings will be the default settings when SYS607 is run, but can be changed when running SYS607, plus those settings will be used by other programs like SYS600 or SYS603 to update IDF security.



```
SYS802D-01                    ** 8.4.1 Development Environment **        MLARSONC0   10/24/20
Revise                            Security Settings Maintenance          LARSONM1    17:44:41

LX Security to IDF Security Integration
Synchronize IDF users existence with LX users                       1  (1=Yes  0=No)
Authorize LX users to IDF environment                               1  (1=Yes  0=No)
Update IDF tasks/sub-tasks                                          1  (1=Yes  0=No)
Update IDF Auto-Content Security (Warehouse, Facility, Company)     1  (1=Yes  0=No)
Update CEA Auto-Content Security (Ledger, Book, Year)               1  (1=Yes  0=No)
Update EGLI Auto-Content Security (Ledger, Book, Year)              1  (1=Yes  0=No)
Synchronize LX user groups with EGLI Financial Groups               1  (1=Yes  0=No)
Create EGLI Financial Groups for LX Groups in CLD170                1  (1=Yes  0=No)




F1=Help  F3=Exit

MA + C            MW                                   05/083

USALID29 resolved to usalid29.infor.com/10.39.117.122 (IPv4)             USALID29:992
```

Synchronize IDF users existence with LX users

When a user is created or deleted in SYS600 then user will be created or deleted in IDF security.

Authorize LX users to IDF environment

When a user is created in SYS600, the user is authorized to access the IDF environment.

Update IDF tasks/sub-tasks

Either when a user’s products or programs authorities change directly or when they are assigned to or removed from Roles, or when an assigned Role’s products or programs authorities are changed, the user’s access to business objects may change also.

Update IDF Auto-Content Security (Warehouse, Facility, Company)

When a user’s authorities to warehouses, facilities, or companies change either directly or when they are assigned to or removed from Units, or when an assigned Unit’s authorities to warehouses, facilities, or companies are changed, the user’s access to business objects may change also.

Update CEA Auto-Content Security (Ledger, Book, Year)

When CEA Ledger/book/year security changes for a group, all users in that group will have their Auto-content security for CEA updated in IDF also.

Update EGLI Auto-Content Security (Ledger, Book, Year)

When CEA Ledger/book/year security changes for a group, all users in that group will have their Auto-content security for EGLI updated in IDF also.

Synchronize LX user groups with EGLI Financial Groups

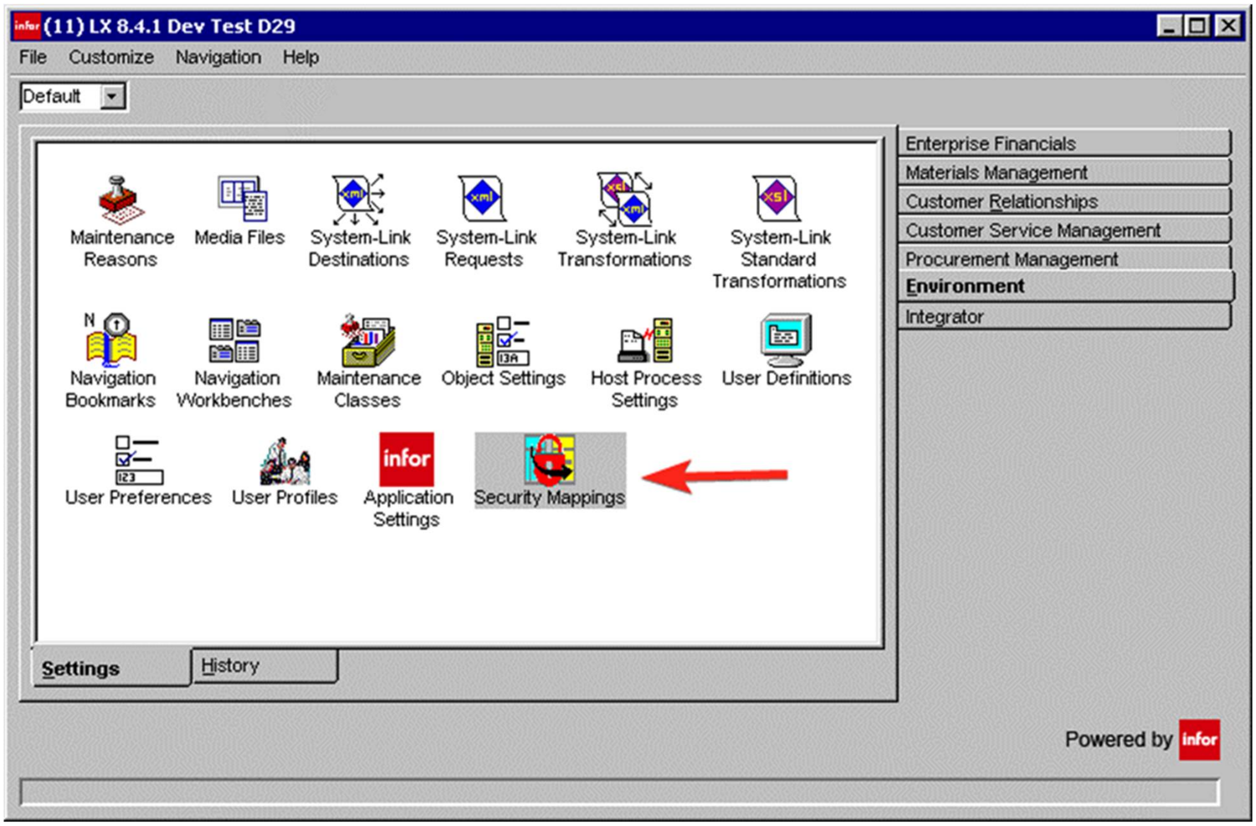
When a user’s group is changed in SYS600 the EGLI Financial group assigned to the user will also be updated. Use the User Profiles object to view a user’s EGLI Financial Group.

Create EGLI Financial Groups for LX Groups in CLD170

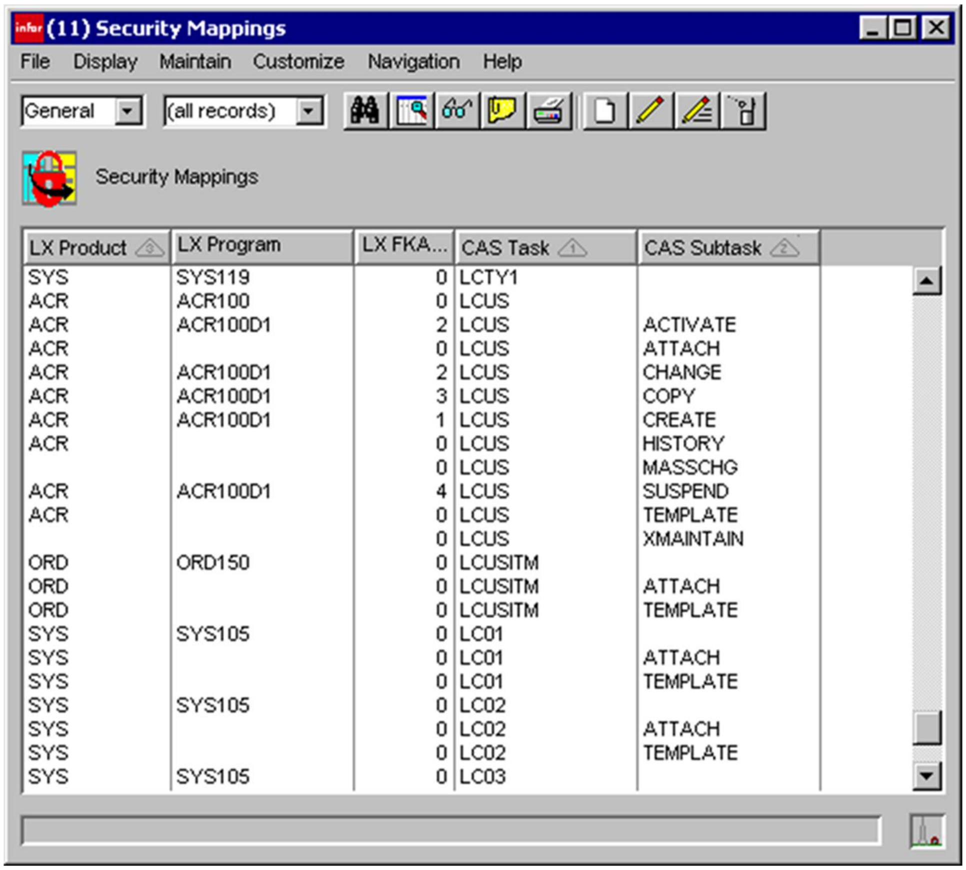
When a new group is created in CLD170, also create an EGLI Financial Group.

Configuring Security Mappings

To change the default mapping of LX product/program/FKAC to IDF business object security settings launch the Security Mappings object from the **Environment** tab.



This object shows for each CAS security task/sub-task, the security in LX that will provide access to it. For example, the LCUS task is for the Customers object. Anyone that is authorized to ACR or ACR100 in LX security will be able to launch the Customers object and view the data. LCUS also has sub-tasks for ACTIVATE, CHANGE, COPY, CREATE, and SUSPEND. These are mapped to ACR100D1 numbered items 1,2,3,4. Those are SYS603 settings and any user assigned to a group in LX that has authority to these tasks will also have that same authority in Customers. For example, any user assigned to a group that has authority to ACR100D1 action “1” will have authority to LCUS CREATE and will be able to create customers in the Customers object.



LX Product	LX Program	LX FKA...	CAS Task	CAS Subtask
SYS	SYS119	0	LCTY1	
ACR	ACR100	0	LCUS	
ACR	ACR100D1	2	LCUS	ACTIVATE
ACR		0	LCUS	ATTACH
ACR	ACR100D1	2	LCUS	CHANGE
ACR	ACR100D1	3	LCUS	COPY
ACR	ACR100D1	1	LCUS	CREATE
ACR		0	LCUS	HISTORY
		0	LCUS	MASSCHG
ACR	ACR100D1	4	LCUS	SUSPEND
ACR		0	LCUS	TEMPLATE
		0	LCUS	XMAINTAIN
ORD	ORD150	0	LCUSITM	
ORD		0	LCUSITM	ATTACH
ORD		0	LCUSITM	TEMPLATE
SYS	SYS105	0	LC01	
SYS		0	LC01	ATTACH
SYS		0	LC01	TEMPLATE
SYS	SYS105	0	LC02	
SYS		0	LC02	ATTACH
SYS		0	LC02	TEMPLATE
SYS	SYS105	0	LC03	

LX security settings are mapped to IDF CAS Security by the ZXYP file. There are two types of records in ZXYP, SYS600 based entries for product and program authorities and Function Key Action Code (FKAC) settings from SYS603.

SYS600 based settings

Records with LX FKAC Sequence = 0 map SYS600 product or program authorities to IDF CAS Security Tasks and Subtasks. Note that LX Program only uses the first 6 chars when mapping SYS600 programs.

Function Key Action Code (FKAC) settings

Records with LX FKAC Sequence <> 0 map Function Key Action Code settings from Program Option Authorities File (ZAUP) to IDF CAS Security Tasks and Subtasks. For these settings, the full program name is used for LX Program.

All CAS Security Tasks related to LX business objects have been added to ZXYP although many do not have a direct correlation to LX security settings, so the LX Product and LX Program fields are left blank and no LX to IDF security is mapped. If you wish to map LX security to these tasks, update the LX Product and/or LX Program fields for those tasks you wish to map. Additionally, if you create custom IDF objects that have CAS Security task created you can add records to Security Mappings to map SYS600 products and/or programs or FKAC options to those tasks.

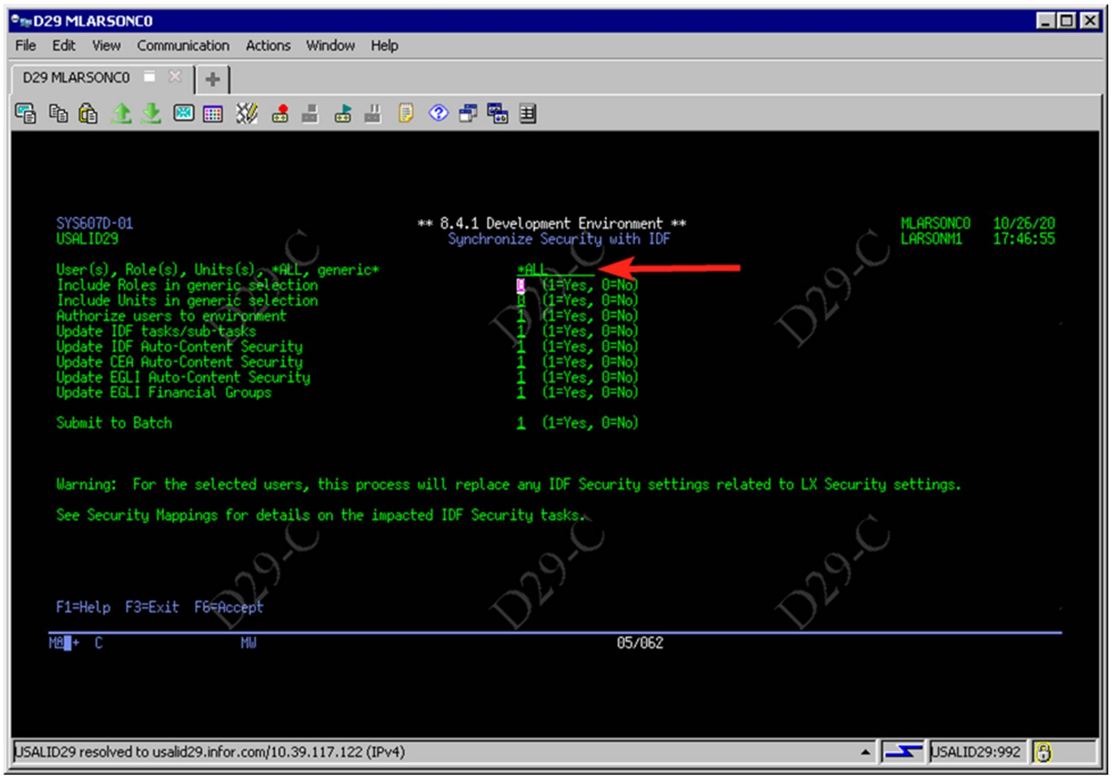
Any CAS security settings in IDF that do not have records in Security Mappings with LX Product or LX Program values are not impacted by LX processing and will need to be managed through IDF Security Maintenance. Examples would be authority to CRMi or EGLI objects. Although, you could add new mappings, for example, if someone is authorized to ACR100, you may grant them access to the CRMi Accounts or Contacts objects, or maybe if someone is authorized to certain CEA programs you may grant them access to EGLI objects. Use the IDF security menu option Area and task authorizations to locate the tasks to assign. See Chapter 4 LX IDF Security Overview for details.

One special CAS task is the ACCMAPICS task that allows users access to the environment, which is controlled for LX users via SYS802 Authorize LX users to IDF environment setting. With this setting turned on when users are added in SYS600, they are also granted access to the IDF environment.

Once all security mappings are configured, the initial synchronization can be done.

Run SYS607 for initial synchronization

Use SYS607 to update all users IDF security from LX security. It can also be used for a subset of users or users assigned to Roles or Units.



```
SYS607D-01                ** 8.4.1 Development Environment **            MLARSONC0   10/26/20
USALID29                      Synchronize Security with IDF               LARSONM1    17:46:55

User(s), Role(s), Units(s), *ALL, generic*            *ALL
Include Roles in generic selection                    0  (1=Yes, 0=No)
Include Units in generic selection                    0  (1=Yes, 0=No)
Authorize users to environment                        1  (1=Yes, 0=No)
Update IDF tasks/sub-tasks                            1  (1=Yes, 0=No)
Update IDF Auto-Content Security                      1  (1=Yes, 0=No)
Update CEA Auto-Content Security                      1  (1=Yes, 0=No)
Update EGLI Auto-Content Security                     1  (1=Yes, 0=No)
Update EGLI Financial Groups                          1  (1=Yes, 0=No)

Submit to Batch                                       1  (1=Yes, 0=No)


Warning:  For the selected users, this process will replace any IDF Security settings related to LX Security settings.

See Security Mappings for details on the impacted IDF Security tasks.



F1=Help  F3=Exit  F6=Accept

M0 +  C             MW                                  05/062
```

USALID29 resolved to usalid29.infor.com/10.39.117.122 (IPv4)   USALID29:992

Once all users have been synchronized with IDF security, ongoing security changes will be automatically updated based on the settings in SYS802 when SYS600 or SYS603 are used to update LX roles’, units’, or users’ security.