Infor IDF for Infor LX Security Maintenance Guide for 8.4.0

Publication Information

Release: Infor IDF for Infor LX 8.4.0

Publication date: May 5, 2023

Contents

About this guide

This guide provides information for configuring security in an IDF environment linked to an LX environment.

Intended audience

This guide is intended for the system administrator or consultant who configures IDF for use with LX.

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 docs.infor.com or 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 LX IDF Security Overview

There are several areas of security to be setup for IDF. This guide 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.

Chapter 2 Starting Security Maintenance

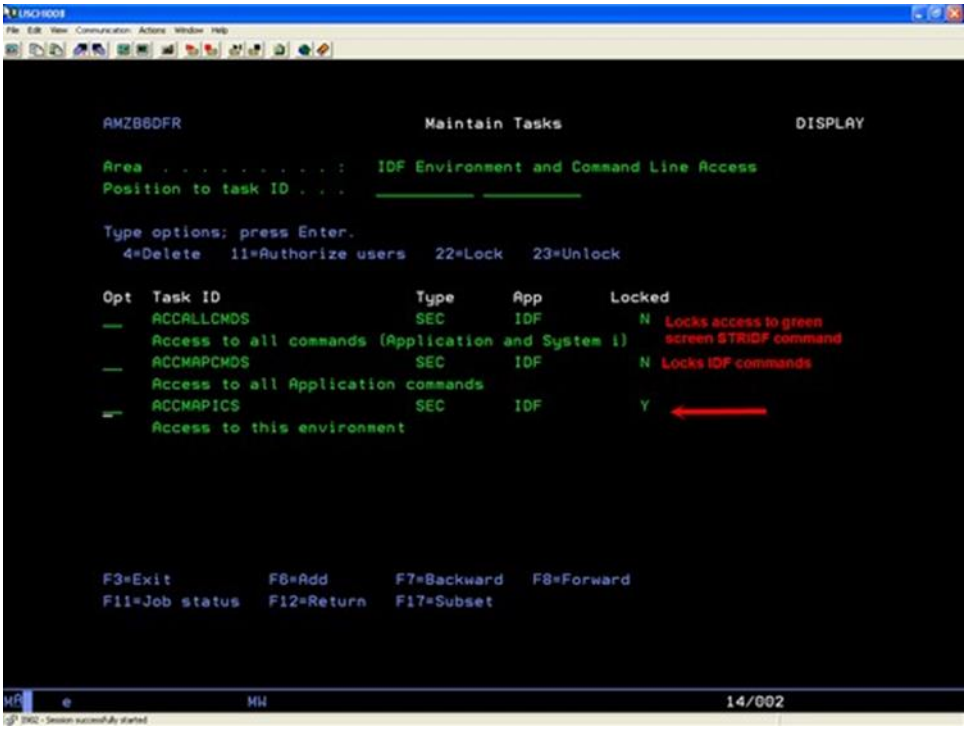
To start security maintenance:

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.

Chapter 3 Environment User Access Control

To restrict user access to the IDF environment:

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

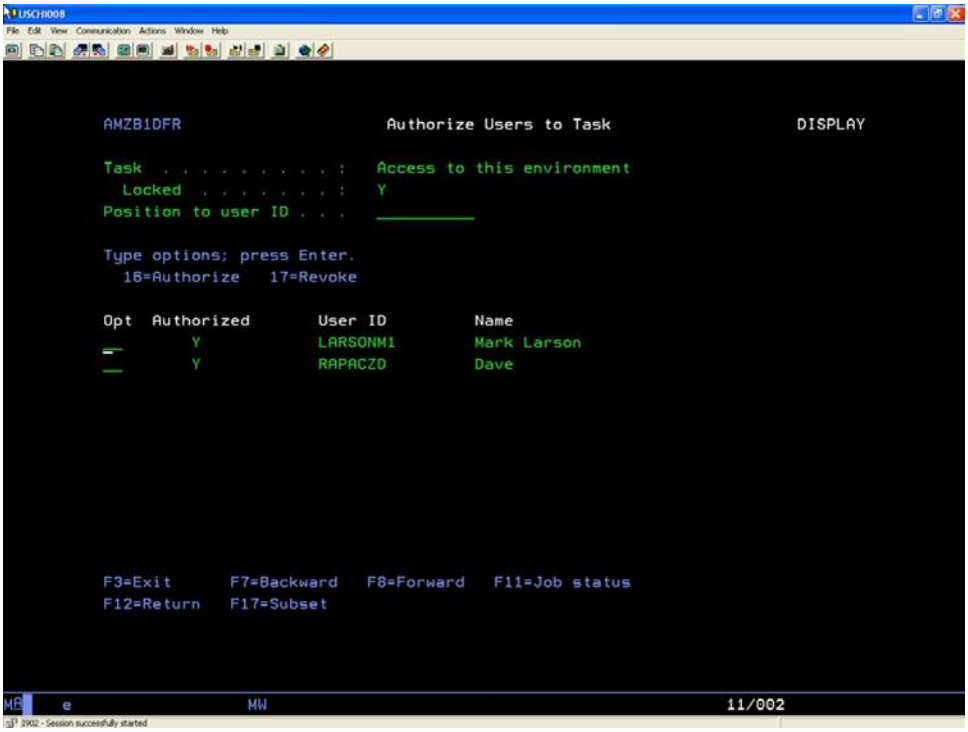


2 The **Access to this environment** option controls the user's ability to log in to the selected environment.

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**.

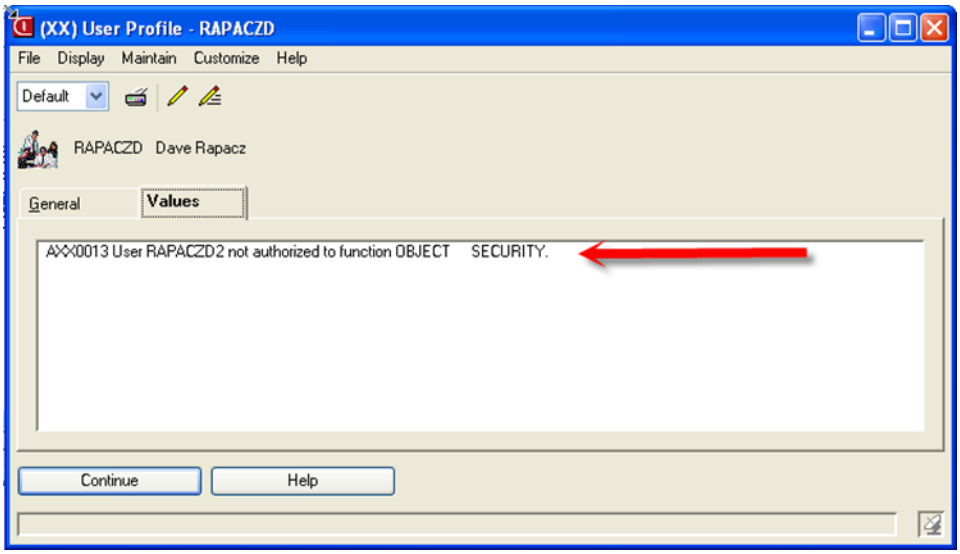


3 To control access levels, specify **16** or **17**.

Chapter 4 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.

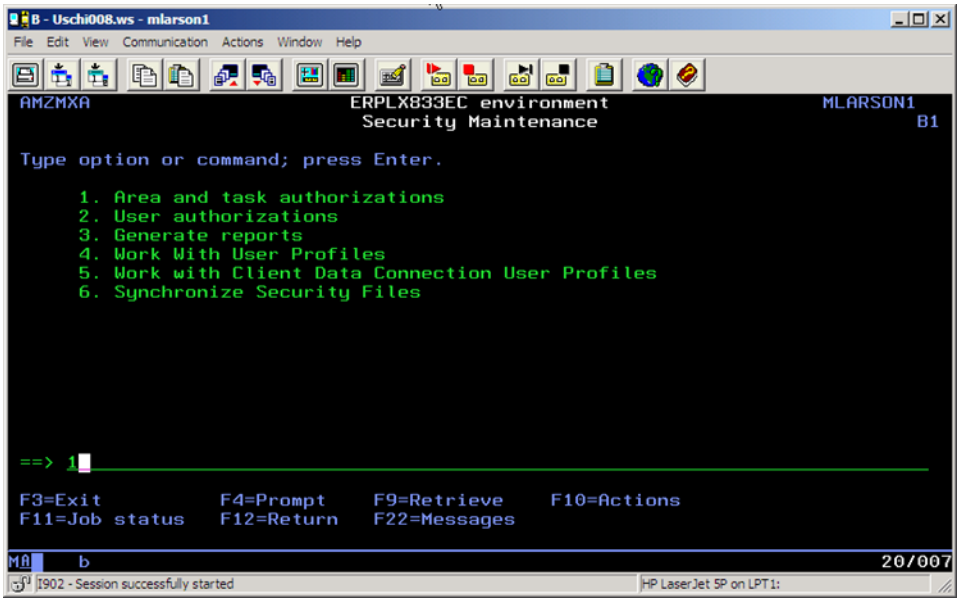


To allow access:

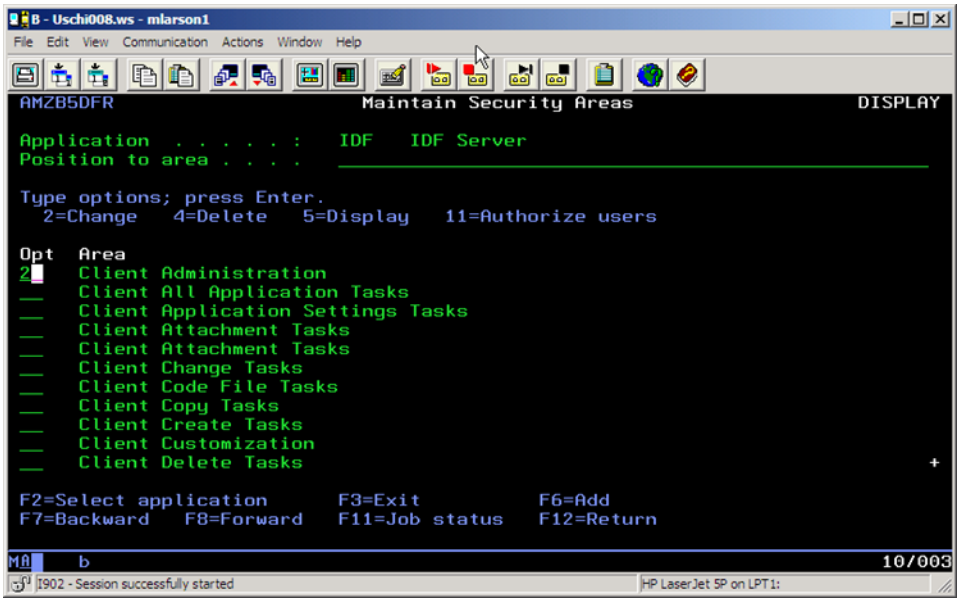
1 Start IDF (STRIDF) and select the environment you want to secure.

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

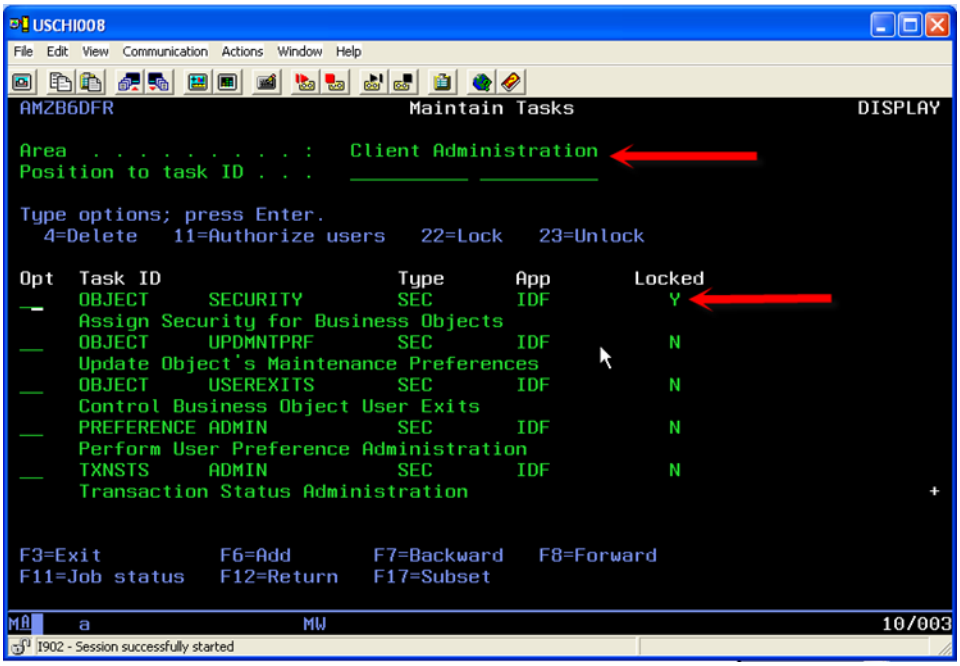
3 Specify **1** for Area and task authorizations.



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



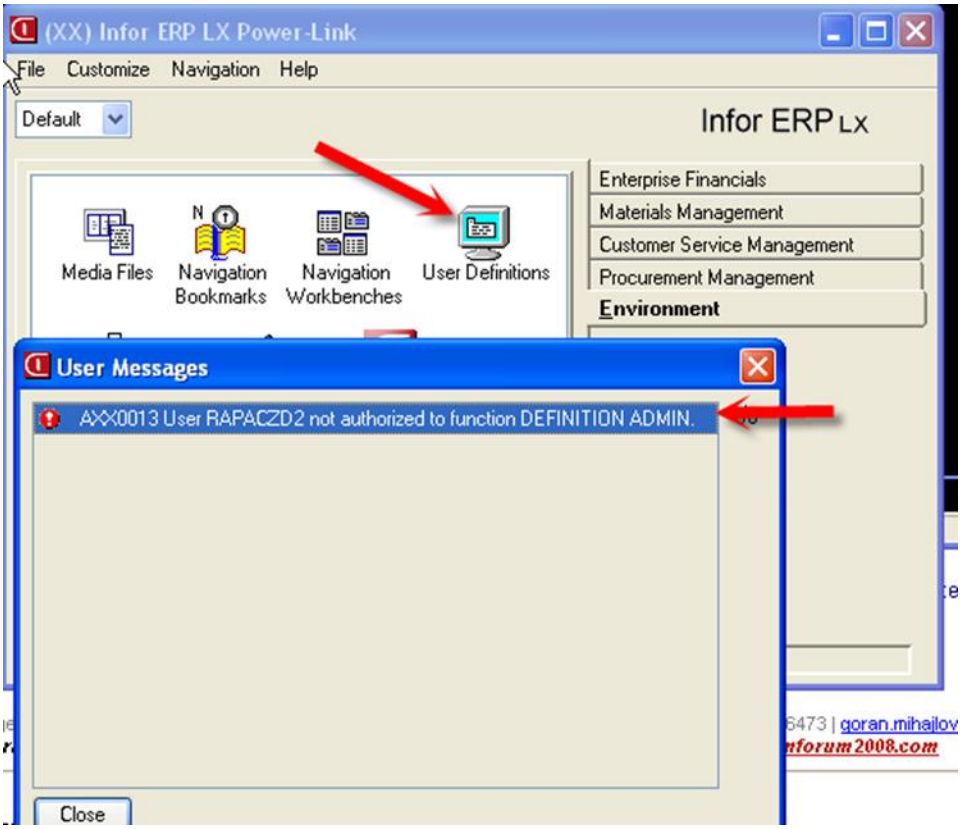
5 Specify **22** for the **OBJECT SECURITY** task to activate security.



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

Chapter 5 User Definitions

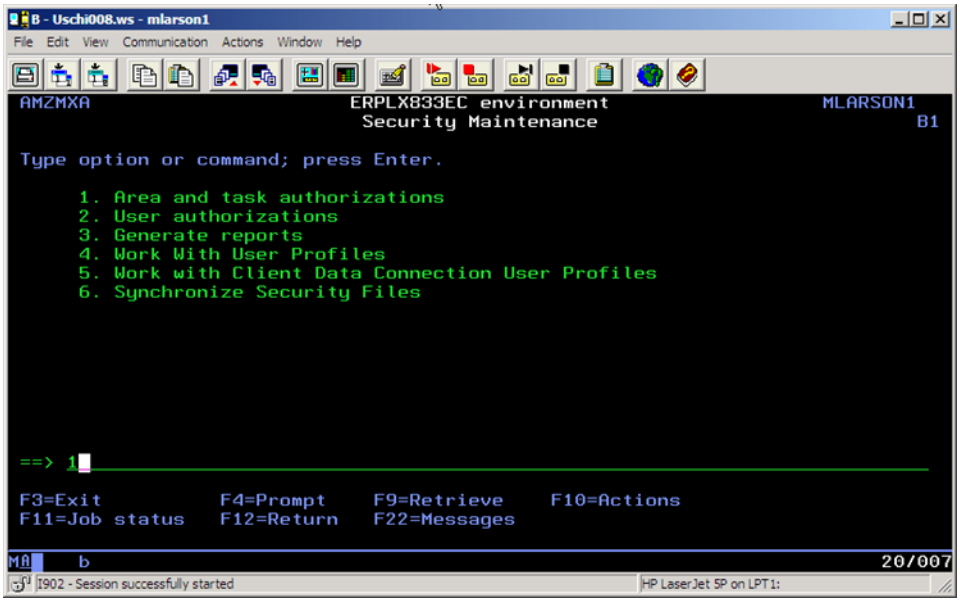
To configure the users that can update User Definitions, use the Perform User Definition Maintenance option under Client Administration in IDF.



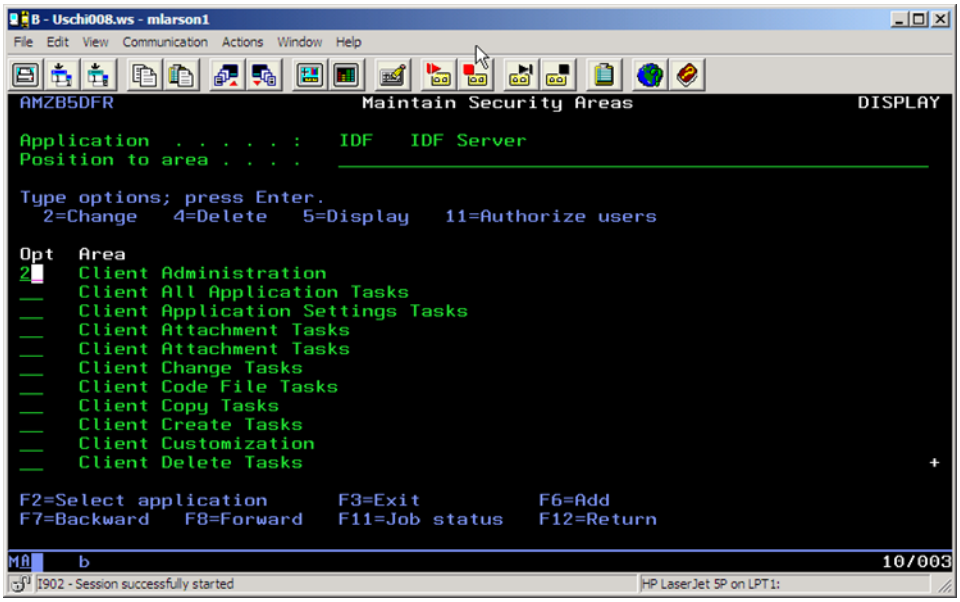
1 Start IDF and select the environment you want to secure.

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

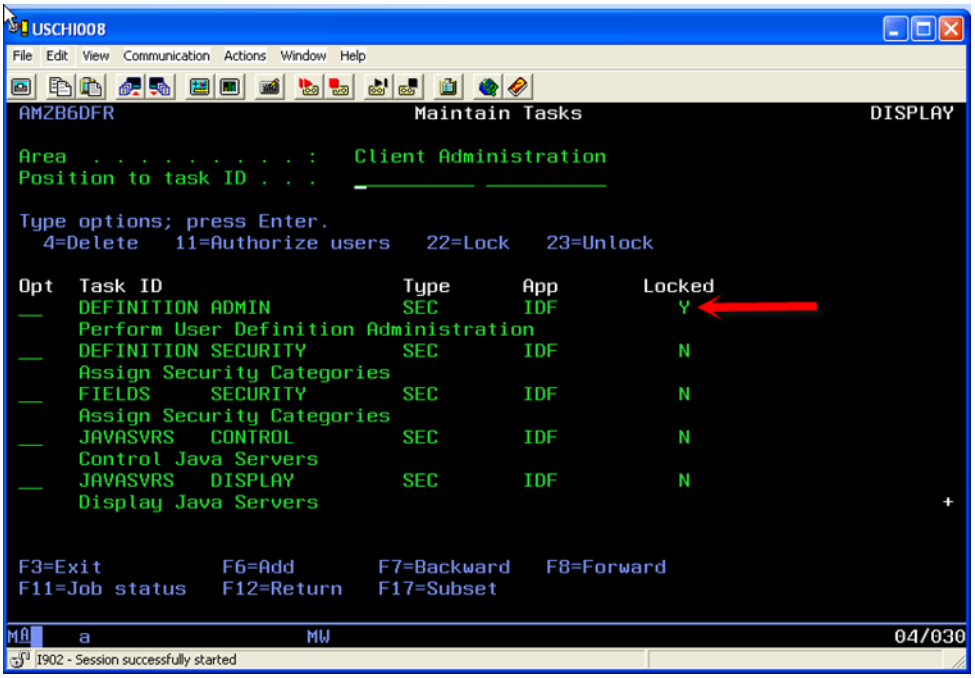
3 Specify **1** for Area and task authorizations.



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



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



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

Chapter 6 Security to change data on all Business Objects

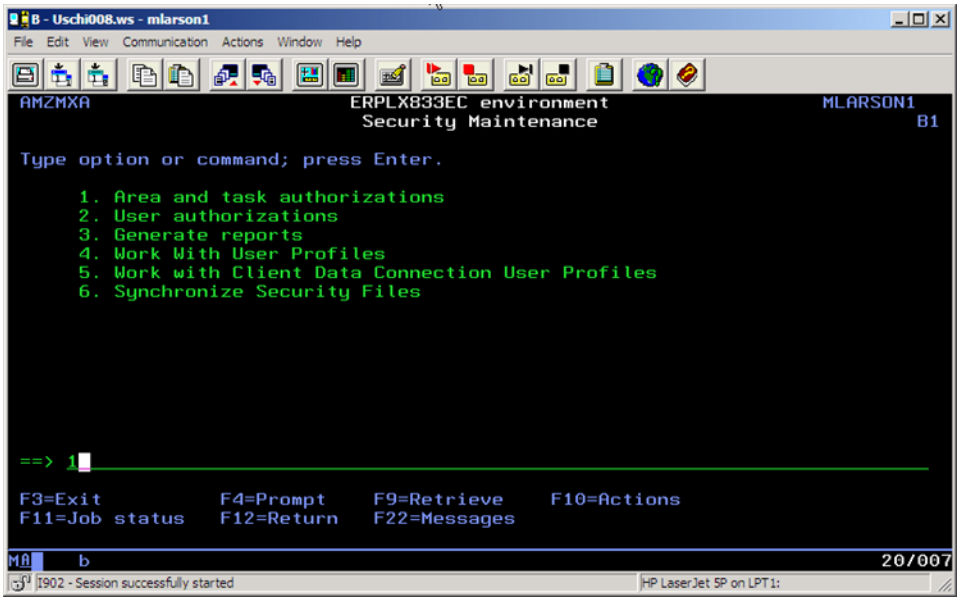
If you want to verify a user can only use Business Objects for inquiry, use the Maintain Business Objects option under Client Administration.

Note: This is Global for all Business Objects.

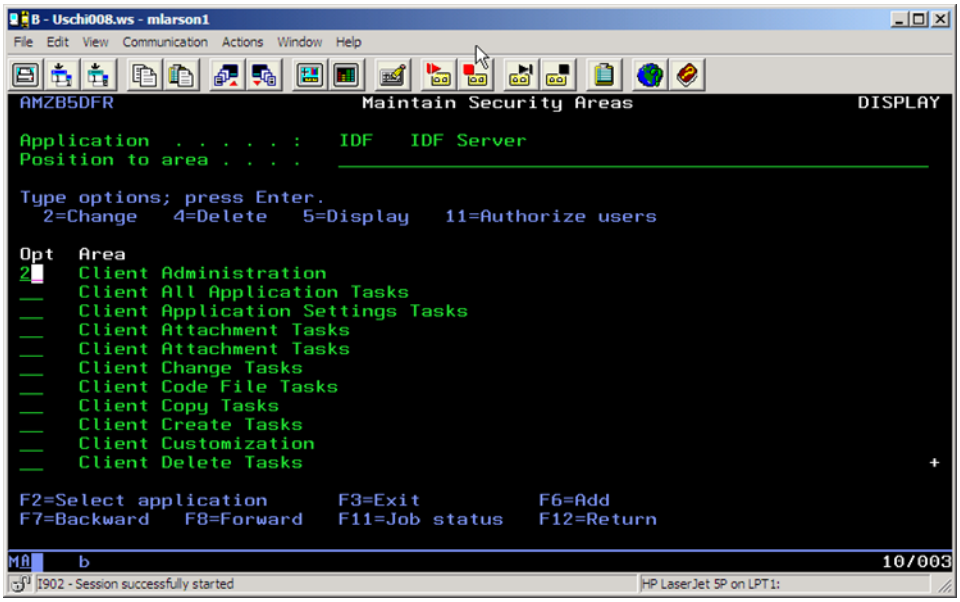
1 Start IDF and select the environment you want to secure.

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

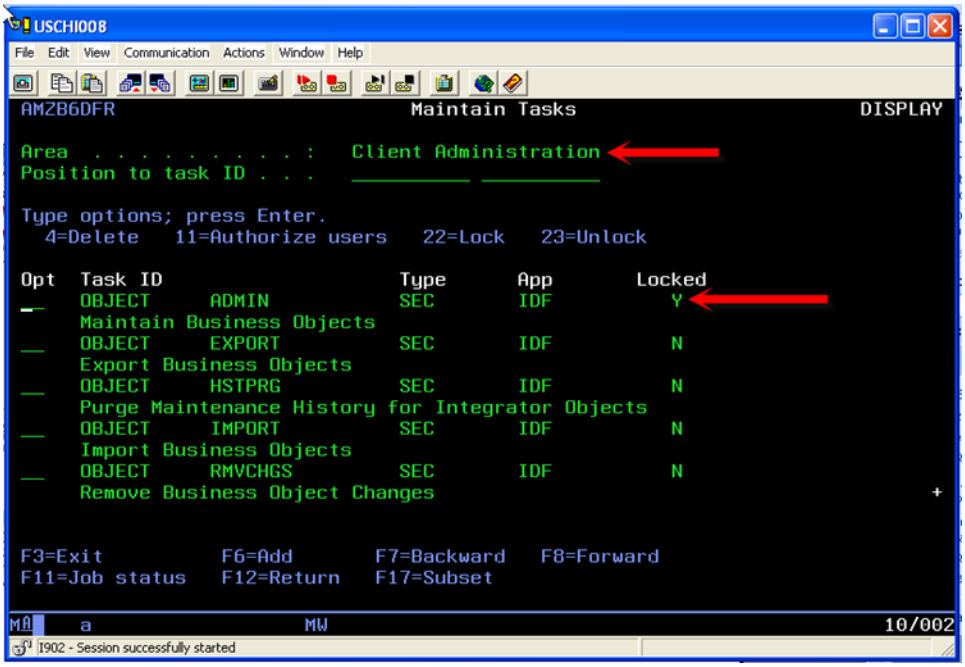
3 Specify **1** for Area and task authorizations.



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



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



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

Chapter 7 Preventing end users from changing public cards

In order to prevent users from changing public cards, cardfiles, presentation schemes, sorts, subsets, templates, views , workbenches and workspaces, you have to lock corresponding tasks in IDF CAS security and provide authority only to the users who may use them.

The procedure is the same for all types of public definitions. Important!

There are two types of Public definitions, cards, for example, Company owned (the definitions shipped with the product, Infor in this case) or User owned. If you want to stop users modifying only Company owned cards, you should lock only MNTPUBLIC tasks.

To stop users modifying any public card (owned by company and created by users) you will need to lock both MNTPUBLIC and MNTUSER tasks. If users are authorized to MNTPUBLIC they can modify all public cards, Infor and user. With MNTUSER they can only modify public user owned. If both tasks locked, users are not able to modify any public cards unless have authority to do this. See Chapter 9 for details.

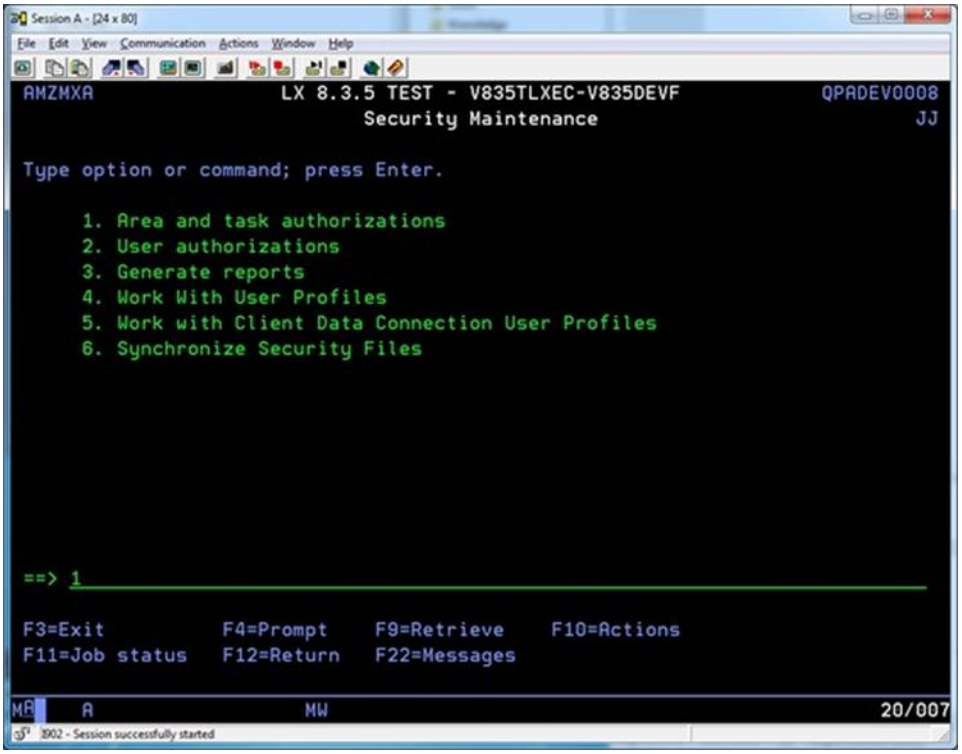
For example, in order to prevent users from changing Infor owned public cards, use the Maintain Public Cards option under Client Customization.

Note: This is Global for all Business Objects.

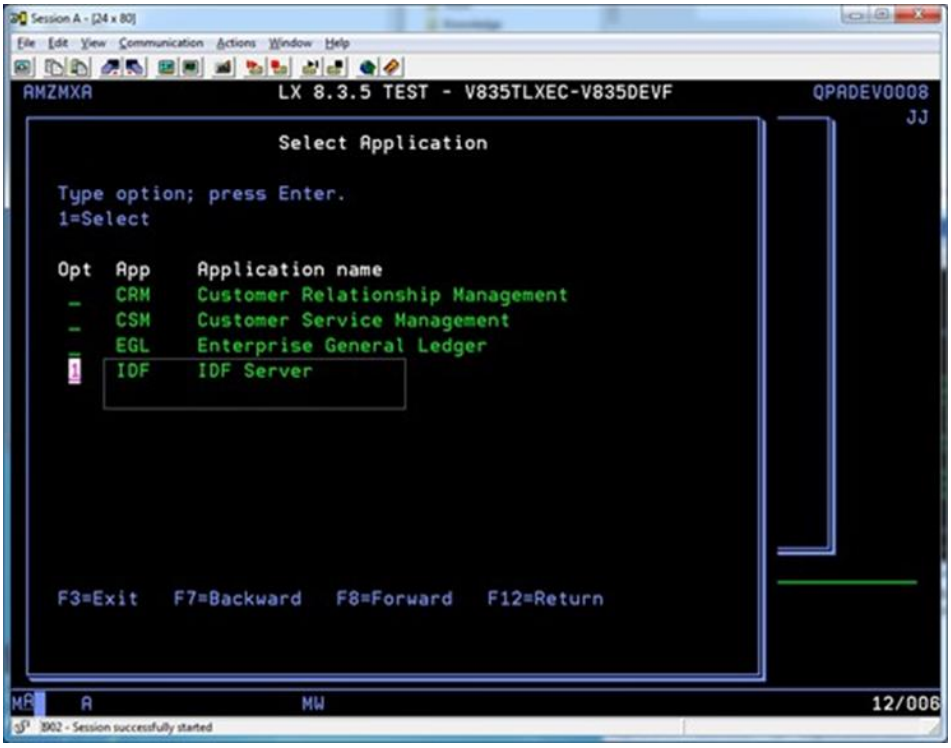
1 Start IDF and select the environment you want to secure.

2 Take option **10**, **Security Maintenance**.

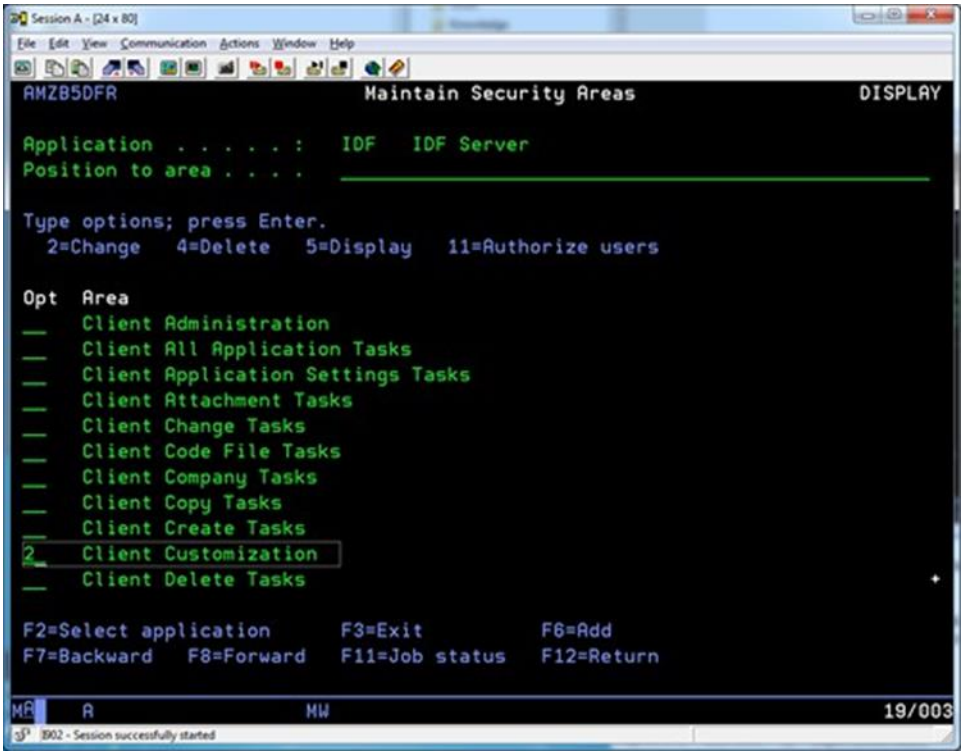
3 Take option **1** for Area and task authorizations.



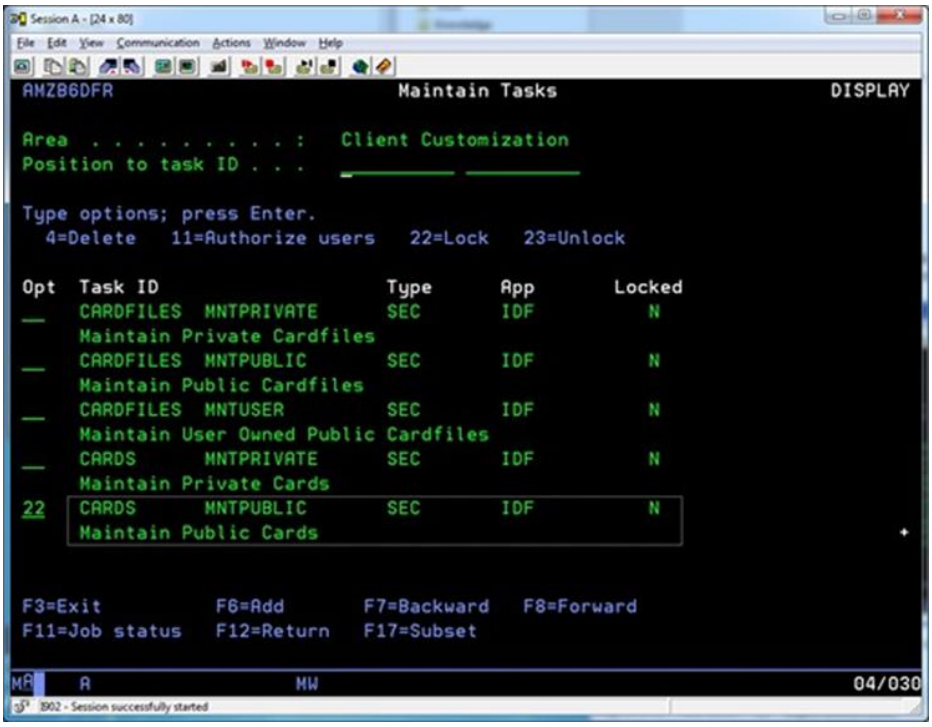
a Select **IDF Server**.

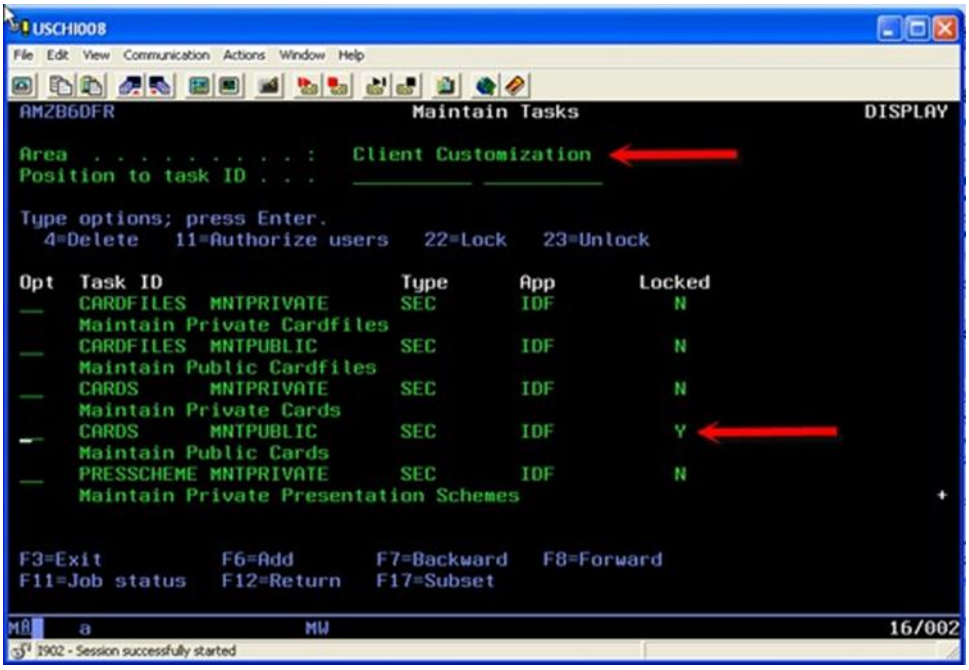


4 Take option **2** for C**lient Customizations**.



5 Take option **22** for **CARDS MNTPUBLIC - Maintain Public Cards** to activate the security. Then, specify **11** to select the individual users that should have access to this function.





For another type of the public definitions, you should use corresponding records, for example

Maintain Public Subsets (SUBSETSMNTPUBLIC) – for Subsets

Maintain Public Cardfiles (CARDFILES MNTPUBLIC) – for Cardfiles

Maintain Public Presentation Schemes (PRESSCHEME MNTPUBLIC) for Presentation Schemes

Maintain Public Sorts (SORTSMNTPUBLIC) – for Sorts

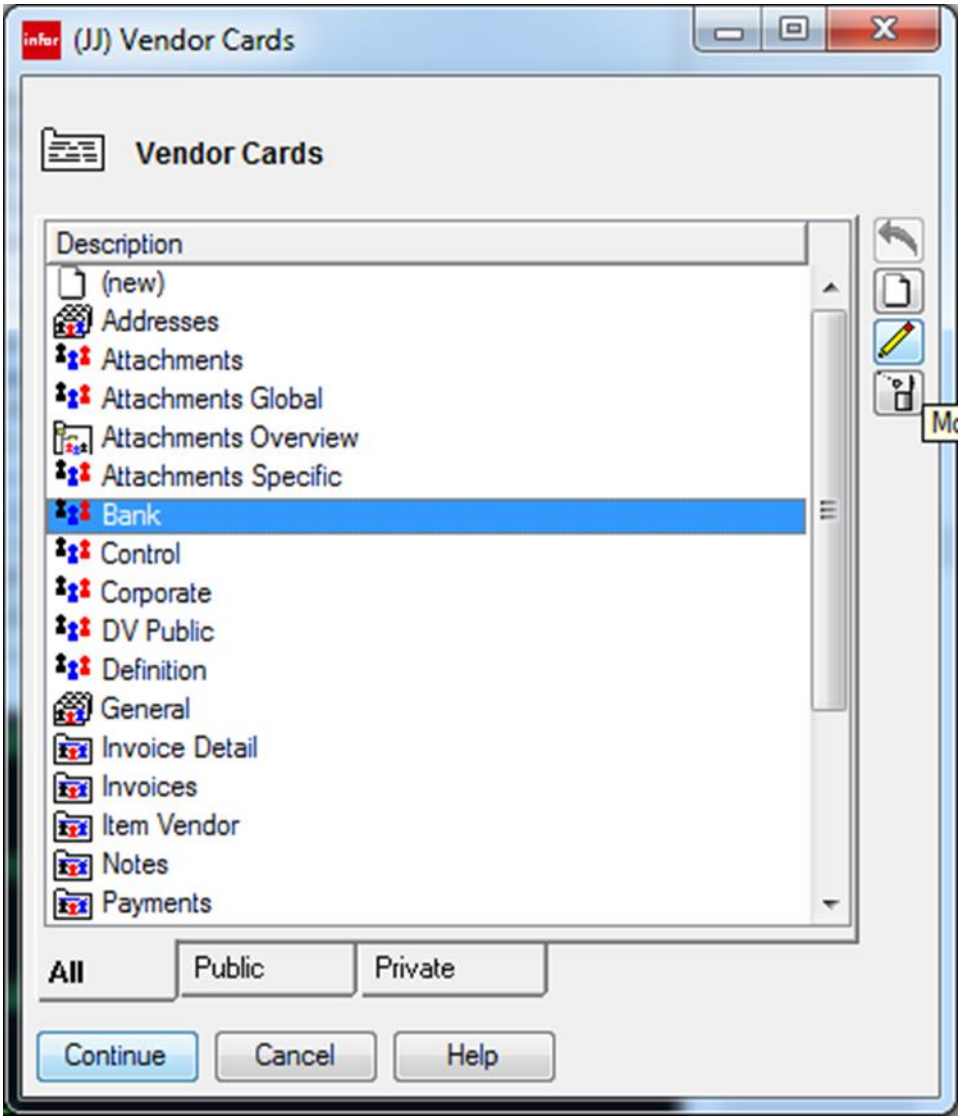
Maintain Public Templates (TEMPLATES MNTPUBLIC) – for Templates

Maintain Public Views (VIEWSMNTPUBLIC) – for Views

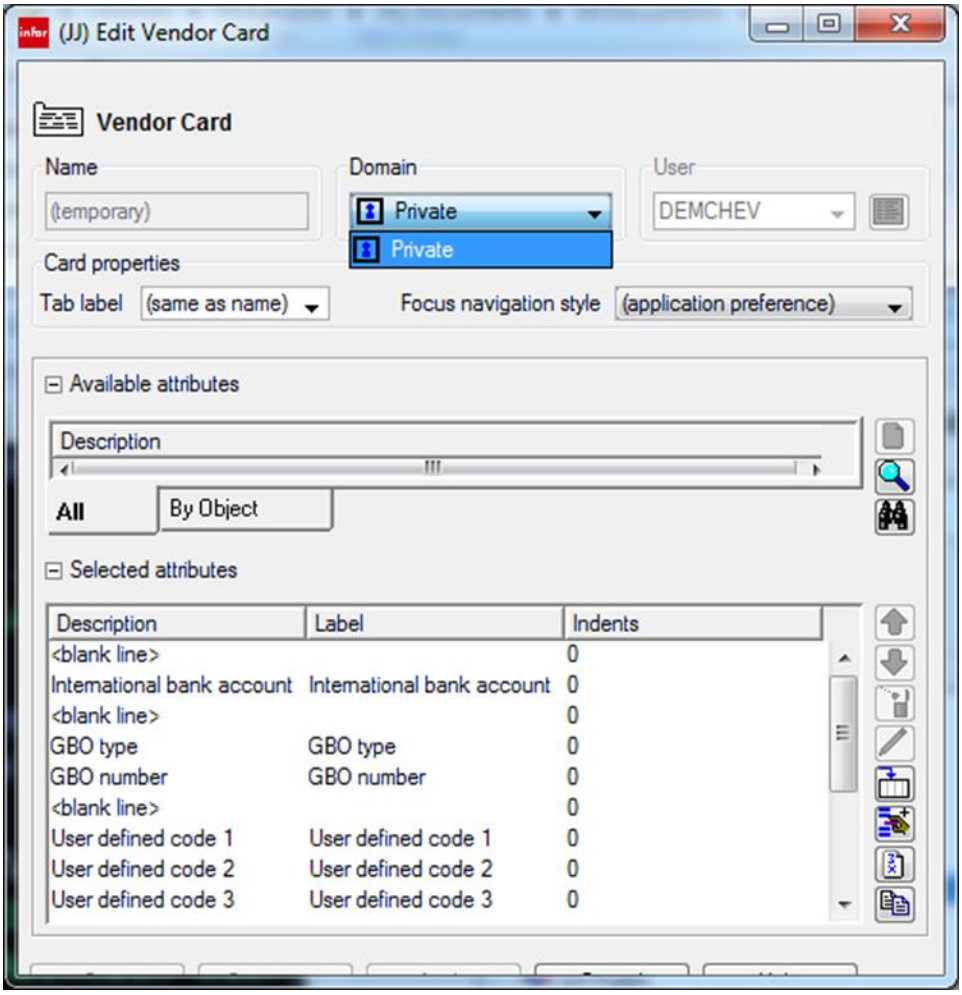
Maintain Public Workbenches (WRKBENCHES MNTPUBLIC) – for Workbenches

Maintain Public Workspaces (WRKSPACES MNTPUBLIC) for Workspaces

6 To see the security in action, try to change any public card and receive error message:



The only security domain available when you create a new card is Private:

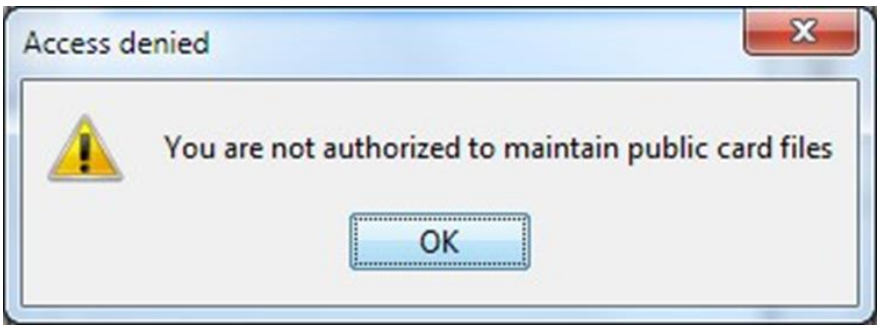


The similar messages will be displayed when you try to maintain public views:

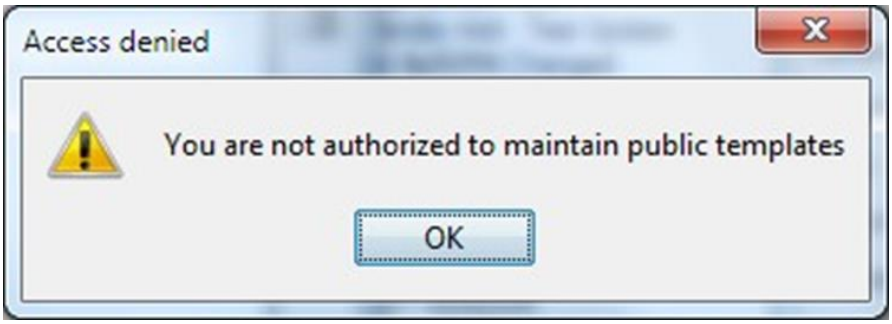
Public Subsets:

Public Sorts:

Public Card files:



Public Templates:



If you now lock the Maintain User Owned Public Cards (CARDSMNTUSER), the user will not be able to maintain public cards created by any user getting the message:

The same is valid for all other public definitions listed before.

Chapter 8 Preventing end users from changing private cards, Cardfiles, Presentation Schemes, Sorts, Subsets, Templates, Views, Workbenches and Workspaces

In order to prevent users from changing Private cards, cardfiles, presentation schemes, sorts, subsets, templates, views , workbenches and workspaces, you have to lock corresponding tasks in IDF CAS security and provide authority only to the users who may use them.

The procedure is the same for all types of private objects.

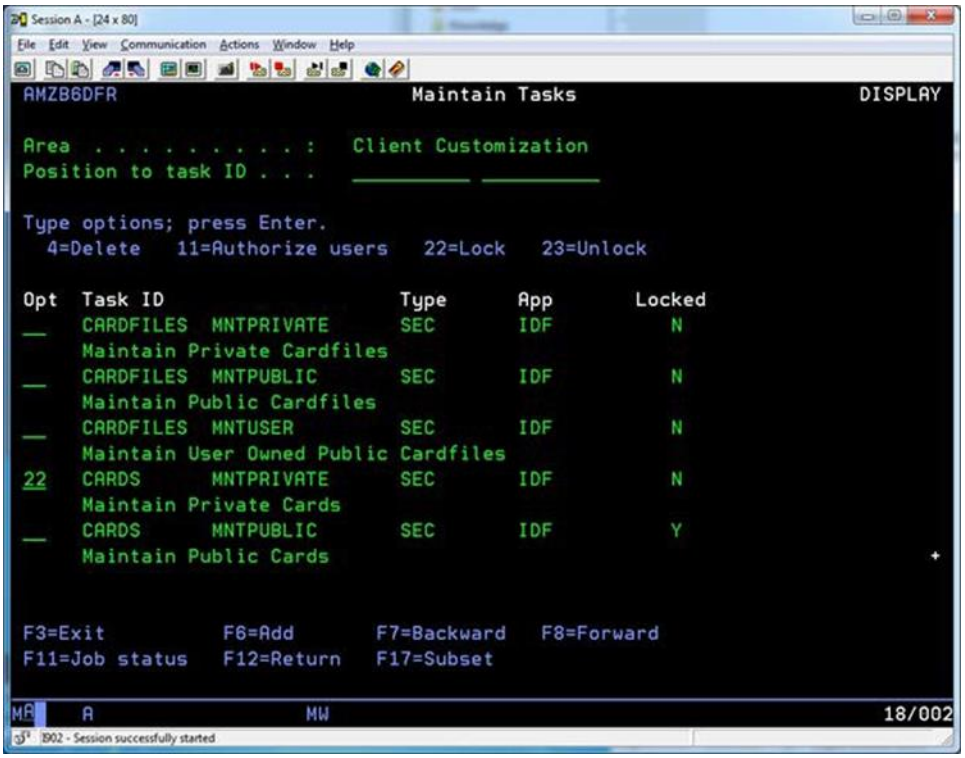
Note: This is Global for all Business Objects.

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

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

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

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



Take option **22** for **CARDS MNTPRIVATE - Maintain Private Cards** to activate the security. Then, specify **11** to select the individual users that should have access to this function

For another type of the private definitions, you should use corresponding records, for example

Maintain private Subsets (SUBSETSMNTPRIVATE) – for Subsets

Maintain private Cardfiles (CARDFILES MNTPRIVATE) – for Cardfiles

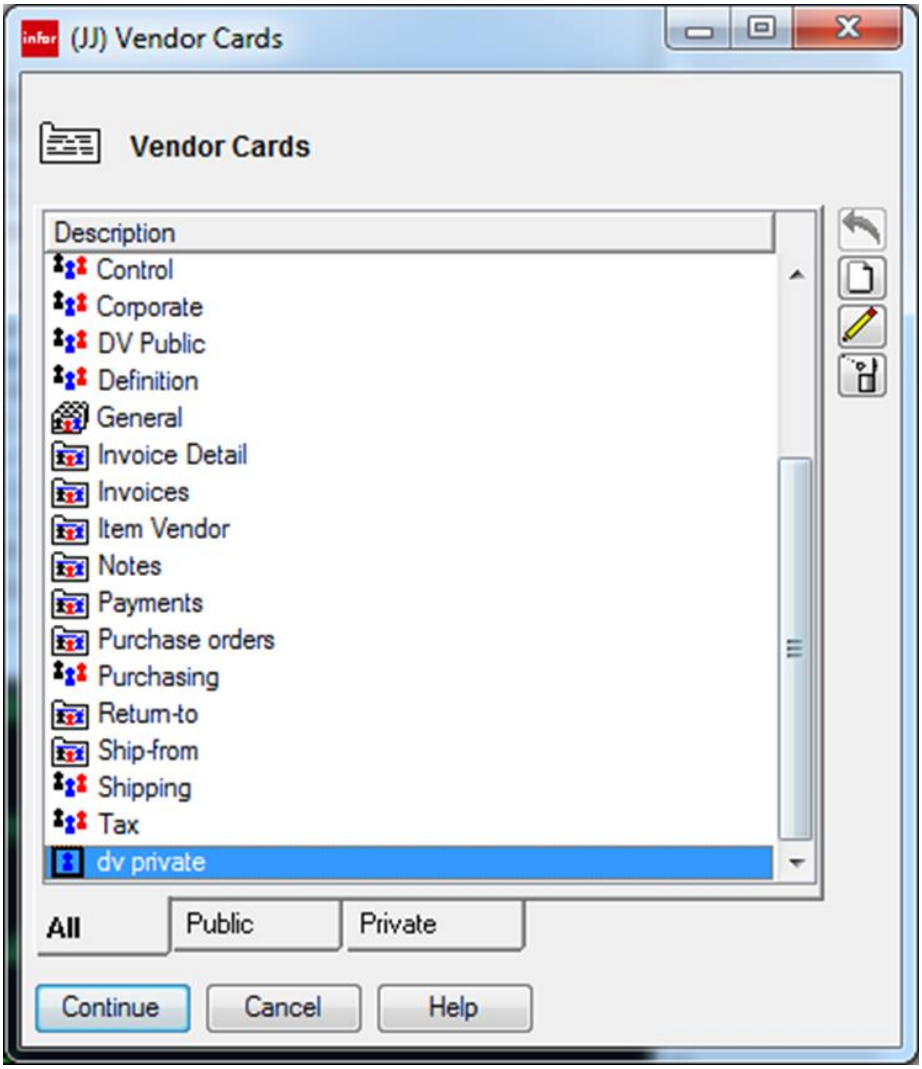
Maintain private Presentation Schemes (PRESSCHEME MNTPRIVATE) for Presentation Schemes

Maintain private Sorts (SORTSMNTPRIVATE) – for Sorts

Maintain private Templates (TEMPLATES MNTPRIVATE) – for Templates Maintain private Views (VIEWSMNTPUBLIC) – for Views

Maintain private Workbenches (WRKBENCHES MNTPRIVATE) – for Workbenches Maintain private Workspaces (WRKSPACES MNTPRIVATE) for Workspaces

To see the security in action, specify any private card to change and click on the pencil icon.



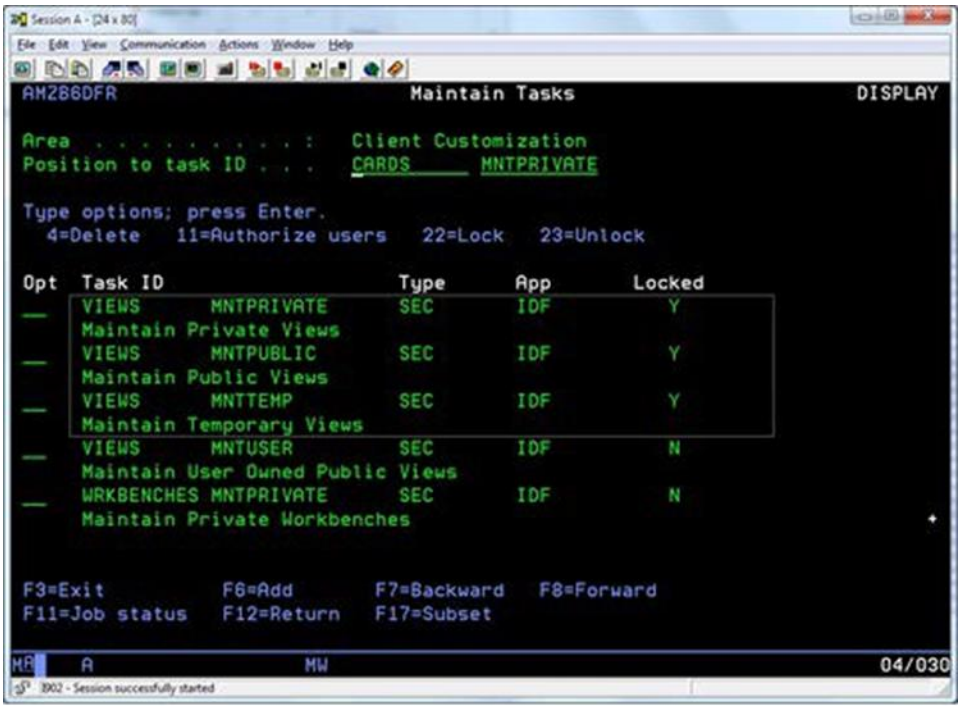
The error message will be displayed preventing you to maintain private card.

The same is valid for other private definitions listed before.

There is one more type of the definitions – Temporary.

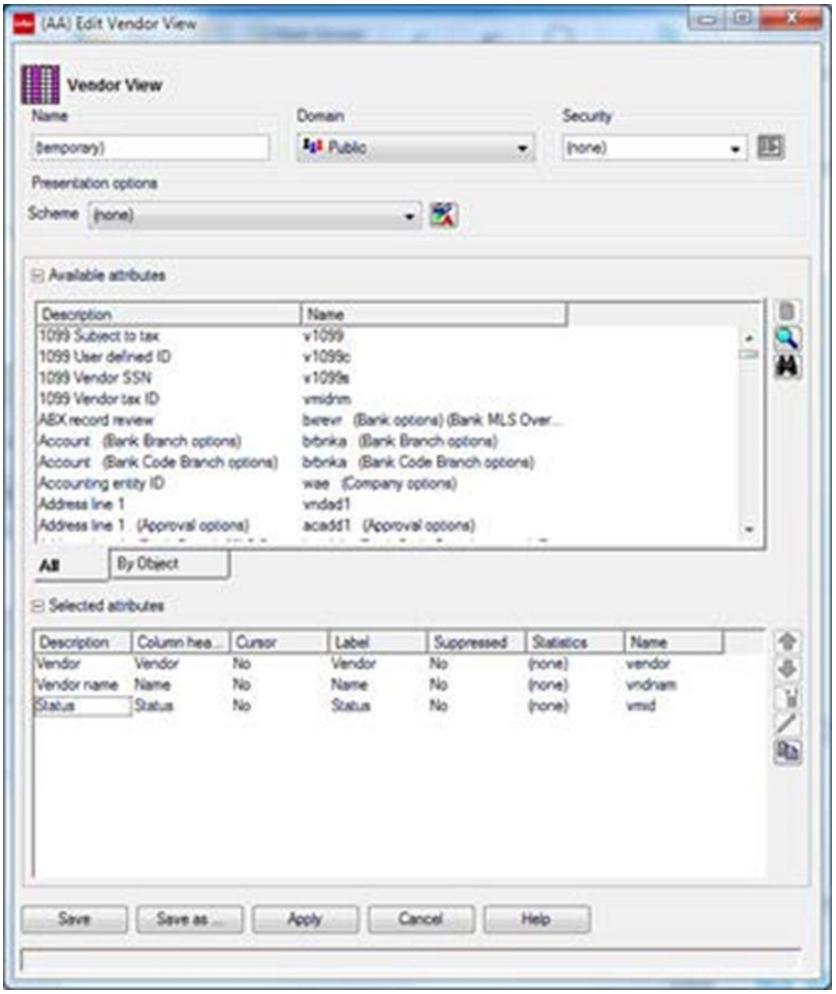
The Temporary definitions can be created, used but not saved. For the test we can take a views.

To test, restrict access from MNTPUBLIC, MNTPRIVATE , MNTTEMP and MNTUSER.

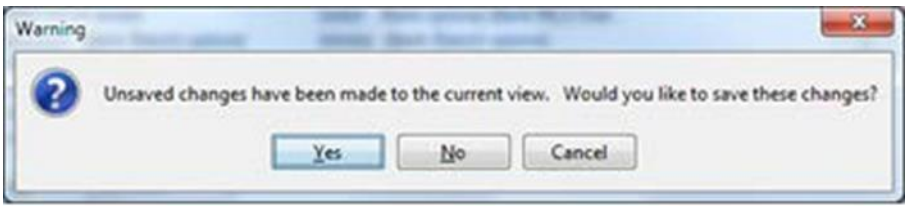


You can still create and apply a definition just not save.

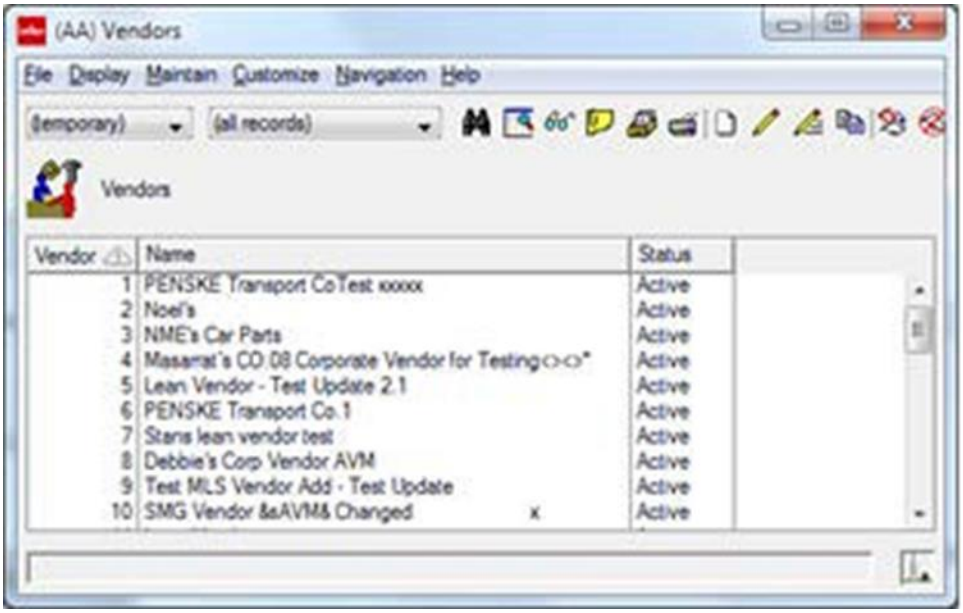
For the example, we will create a temporary view:



Click on Apply leaving the name as (temporary). Click on No in pop up asking for saving:



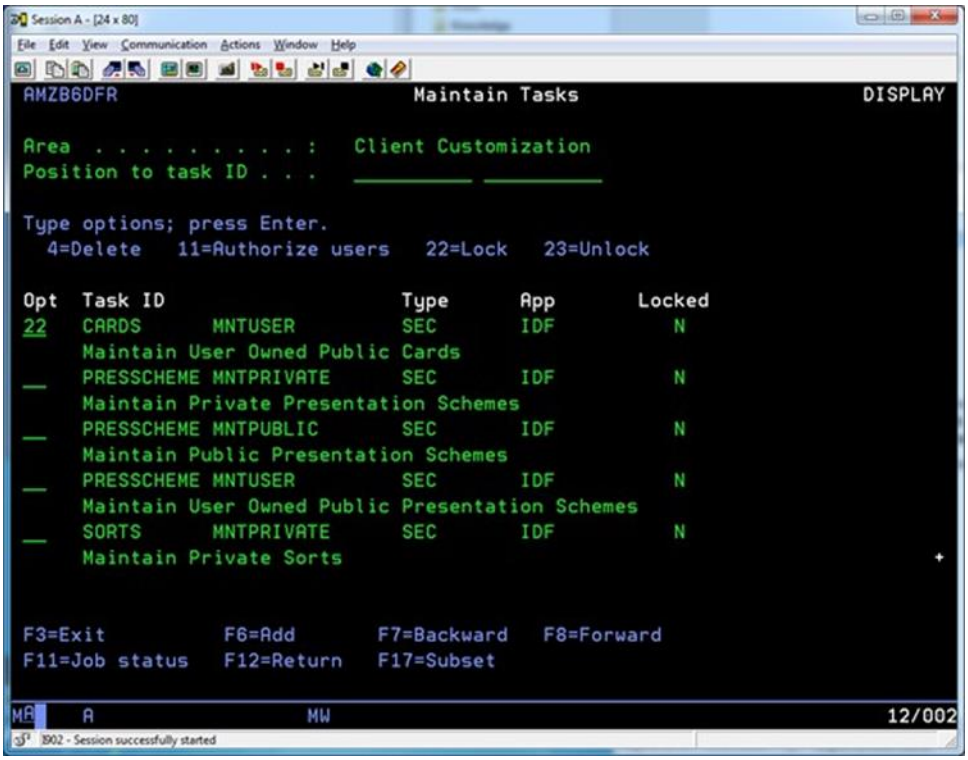
The temporary has been used:


(AA) Vendors
File Display Maintain Customize Navigation Help
(temporary)
(all records)
Vendors
Vendor
Name
Status
1 PENSKE Transport CoTest xxxxx Active
2 Noel's Active
3 NME's Car Parts Active
4 Masarrat's CO 08 Corporate Vendor for Testing Active
5 Lean Vendor - Test Update 2.1 Active
6 PENSKE Transport Co.1 Active
7 Stans lean vendor test Active
8 Debbie's Corp Vendor AVM Active
9 Test MLS Vendor Add - Test Update Active
10 SMG Vendor &AVM& Changed x Active

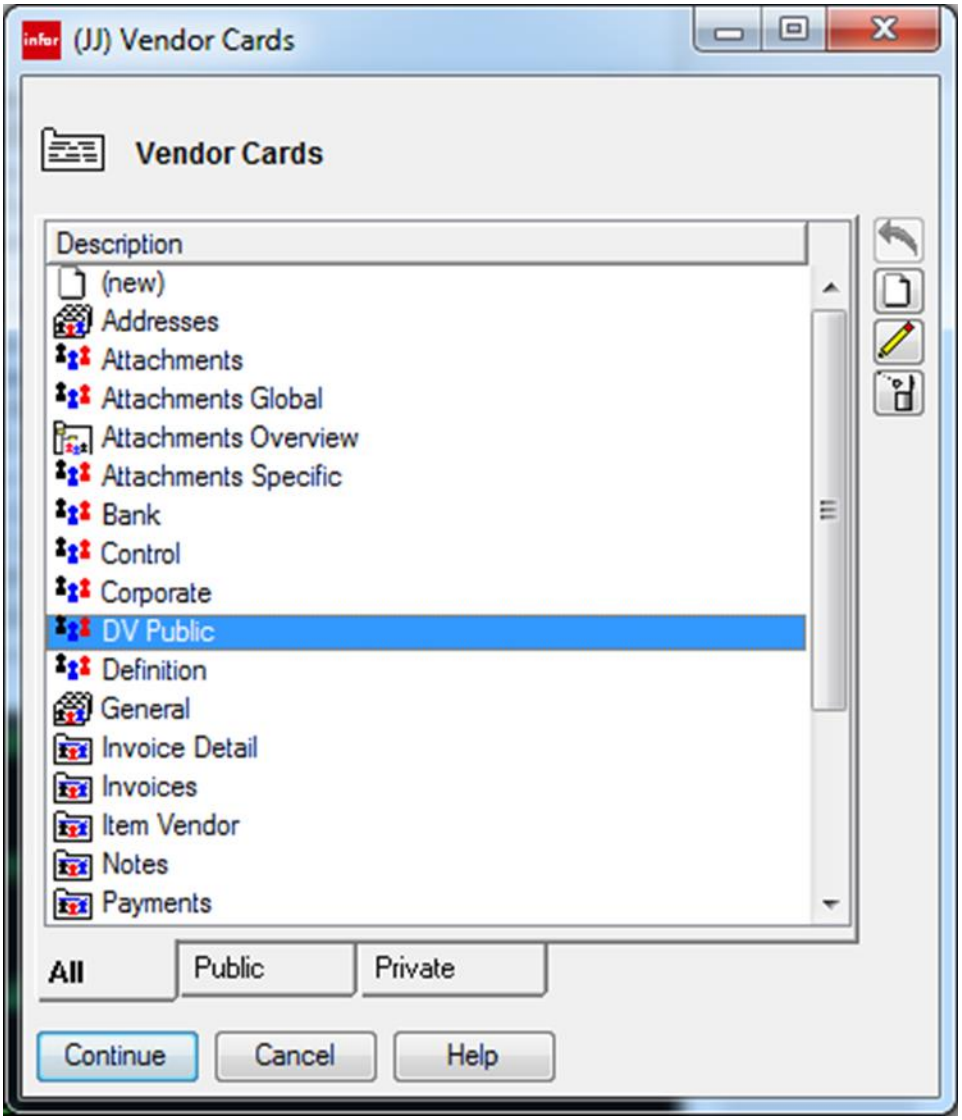
Chapter 9 Preventing end users from changing User owned public cards

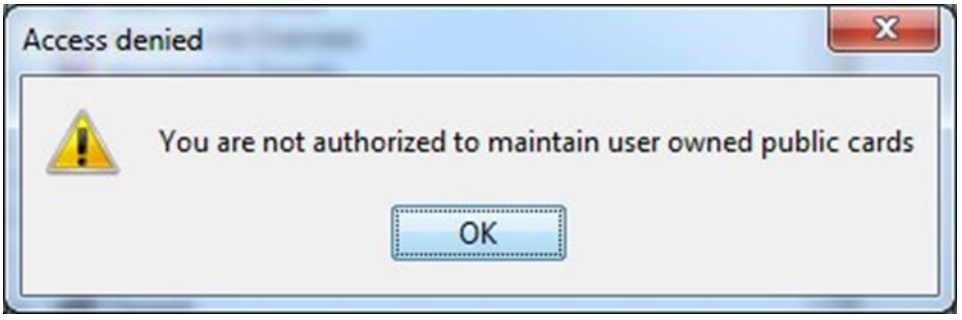
In order to prevent user modifying any public cards including the public cards created by users, you have to lock both **CARDS MNTPRIVATE - Maintain Private Cards** and **CARDS MNTUSER - Maintain User Owned Public Cards.**

To activate the security use option 22 for these two tasks. Then, specify **11** to select the individual users that should have access to this function.



Try to change any Public card created by user – you will get this error message:


(JJ) Vendor Cards
Vendor Cards
Description
(new)
Addresses
Attachments
Attachments Global
Attachments Overview
Attachments Specific
Bank
Control
Corporate
DV Public
Definition
General
Invoice Detail
Invoices
Item Vendor
Notes
Payments
All
Public
Private
Continue
Cancel
Help


Access denied
You are not authorized to maintain user owned public cards
OK

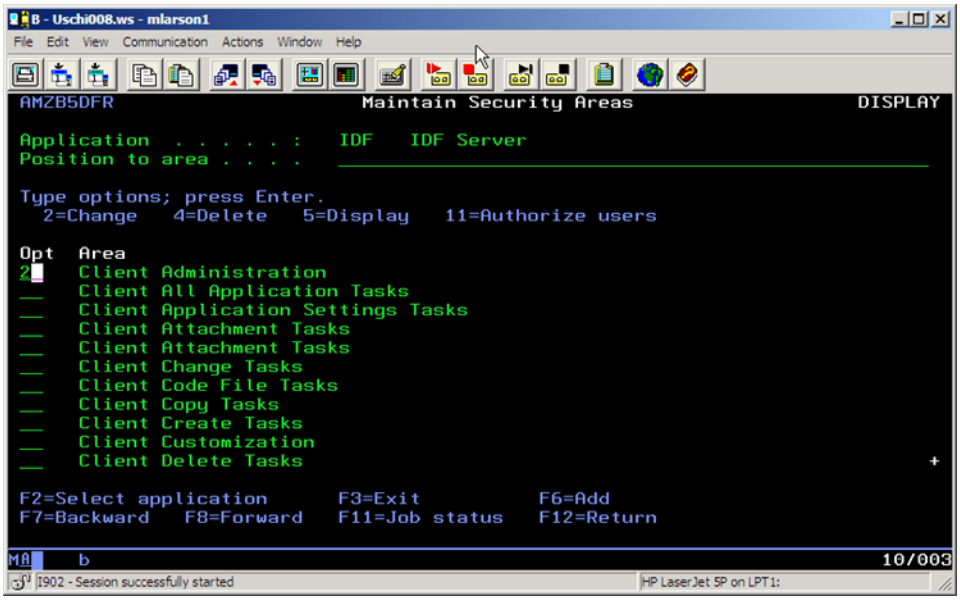
Chapter 10 Preventing end users from using Link Manager

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

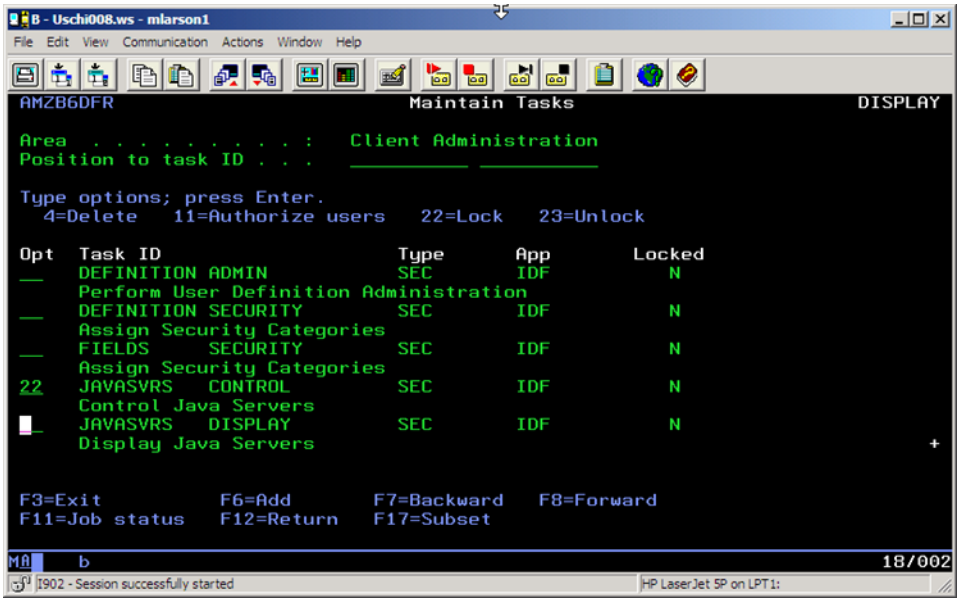
1 Start IDF and select the environment you want to secure.

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

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

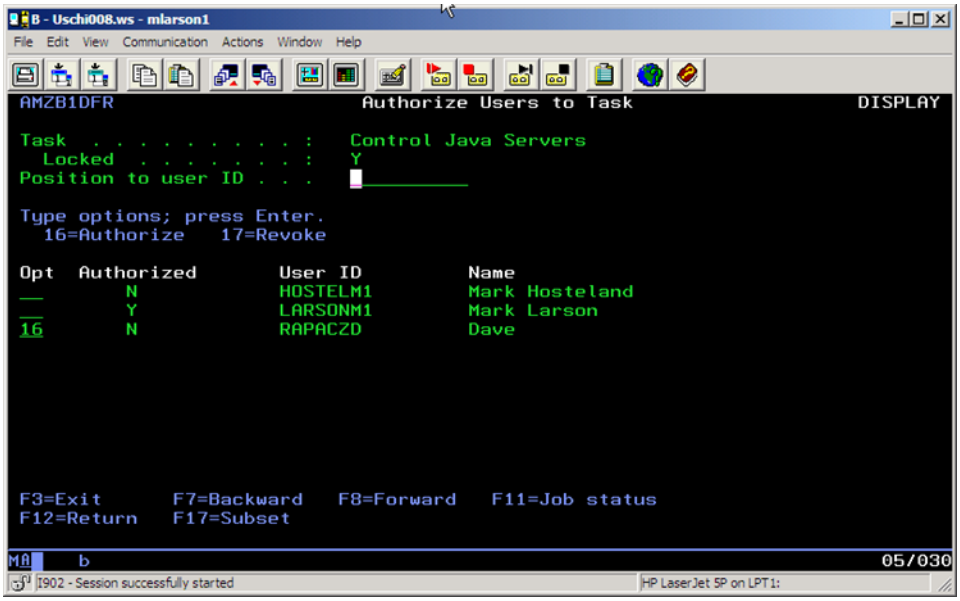


4 Specify **22** on **JAVASVRS CONTROL** to lock the task.



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.



Chapter 11 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

LCS LX Customer Service Management

LEFLX Enterprise Financials

LPD LX Enterprise Product Data Mgt

LMMLX Materials Management

LOP LX Order-Based Production Mgt

LPMLX Procurement Management

LRBLX Rate-Based Production Mgt

LX CBO (LX Common Business Objects) have been added into IDF Server product application and may be found and secured under this product.

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:

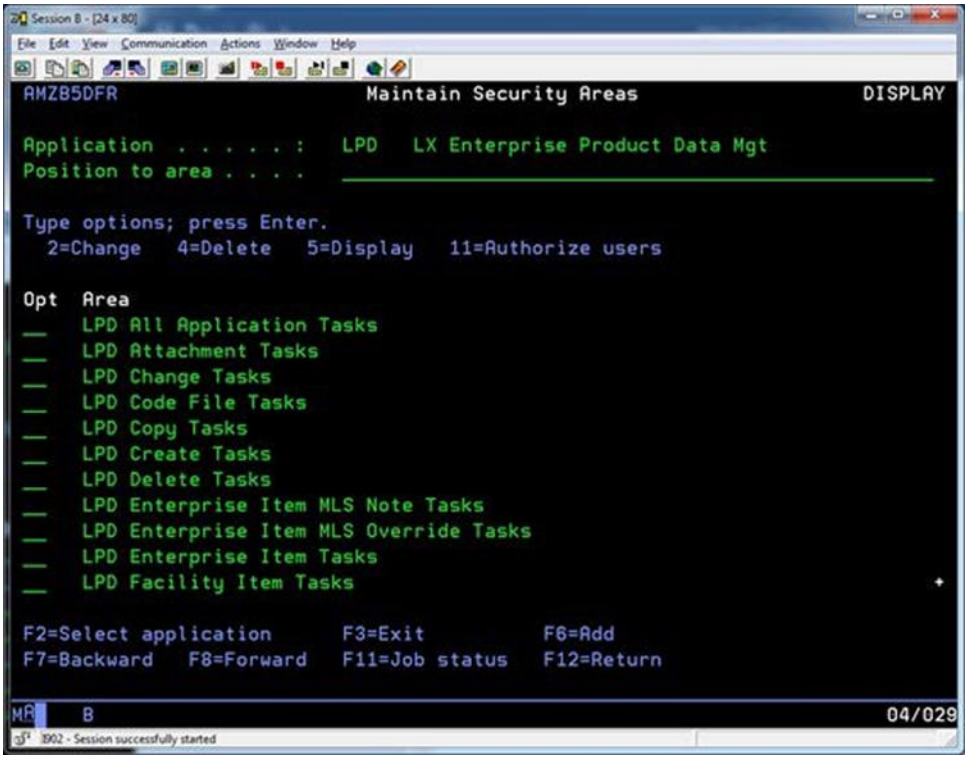
CRM Customer Relationship Management

CSM Customer Service Management

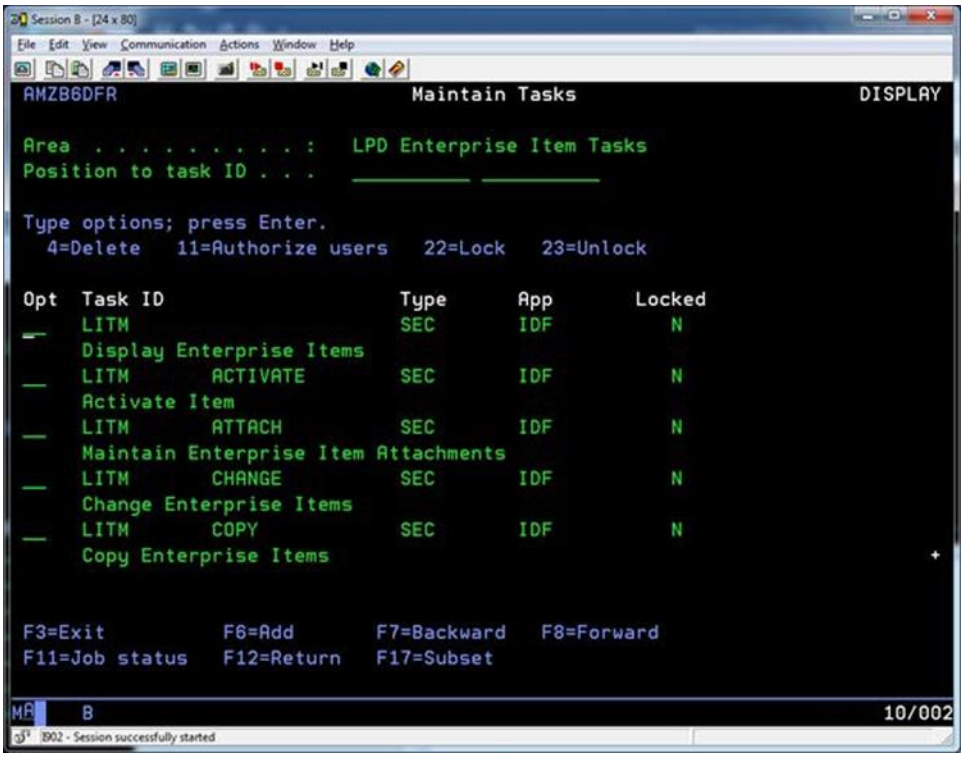
For EGLi use the following product applications to secure objects:

EGLEnterprise General Ledger

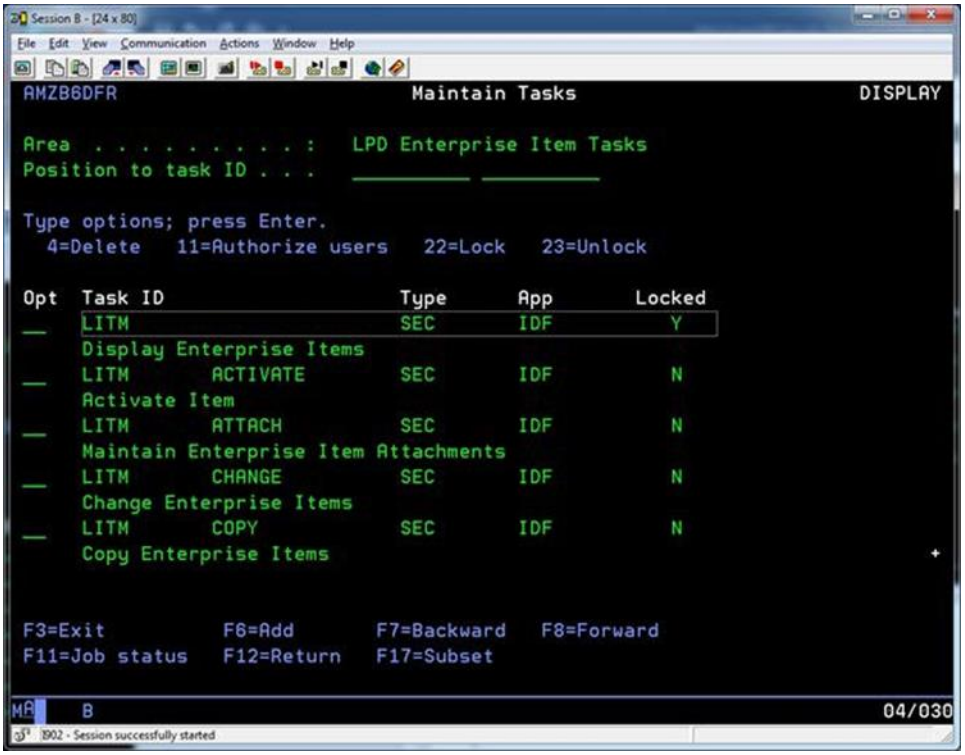
5 Select an application. The **Maintain Security Areas** screen lists all available application tasks.



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

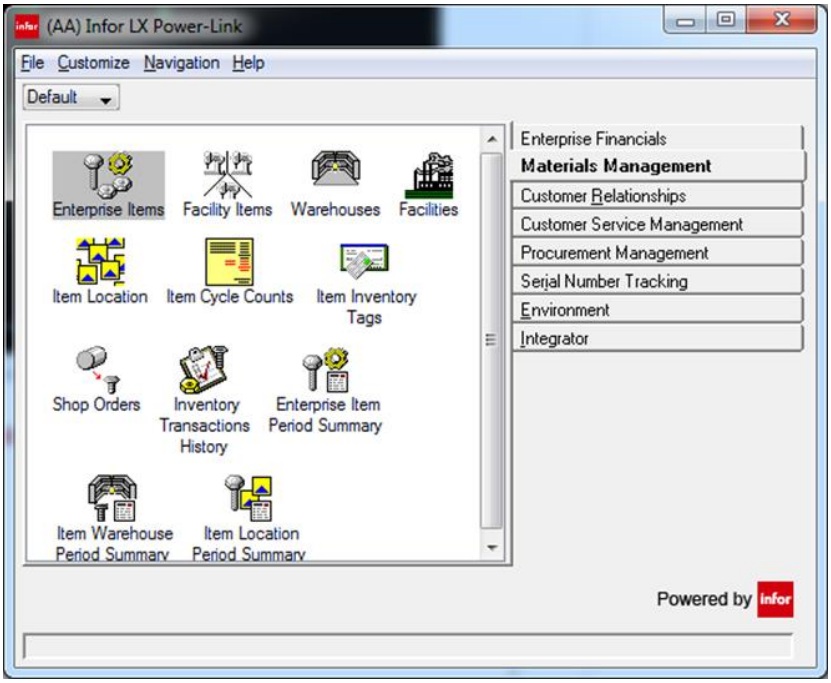


7 Use option **22=Lock** to activate task's security. The Locked flag is set to **Y**.

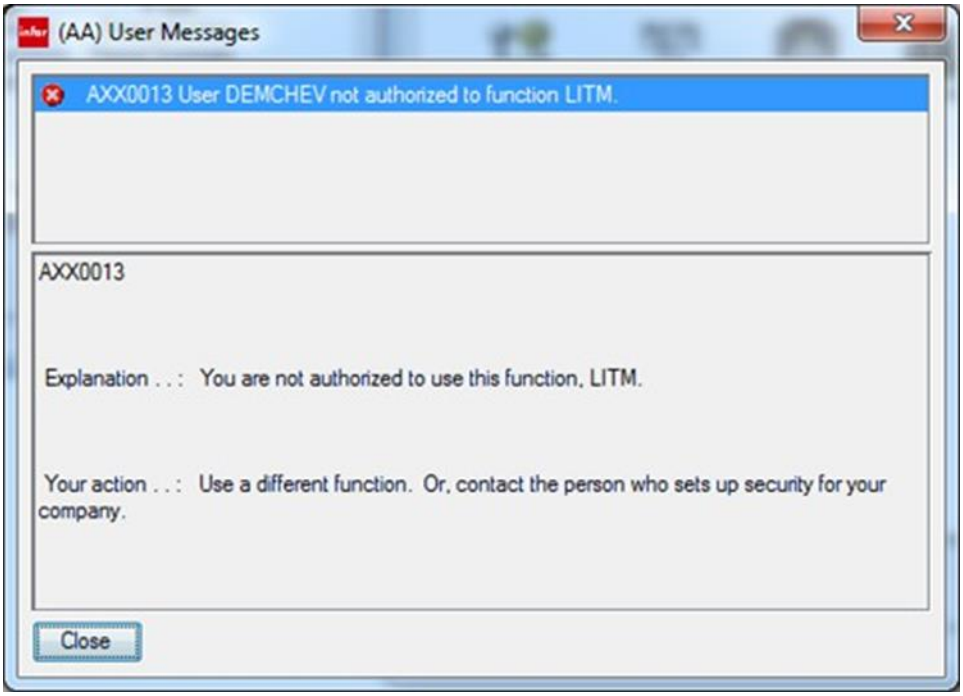


As a result, the User will not be able to execute this task. In this example, user will not be able to open Enterprise Item object.

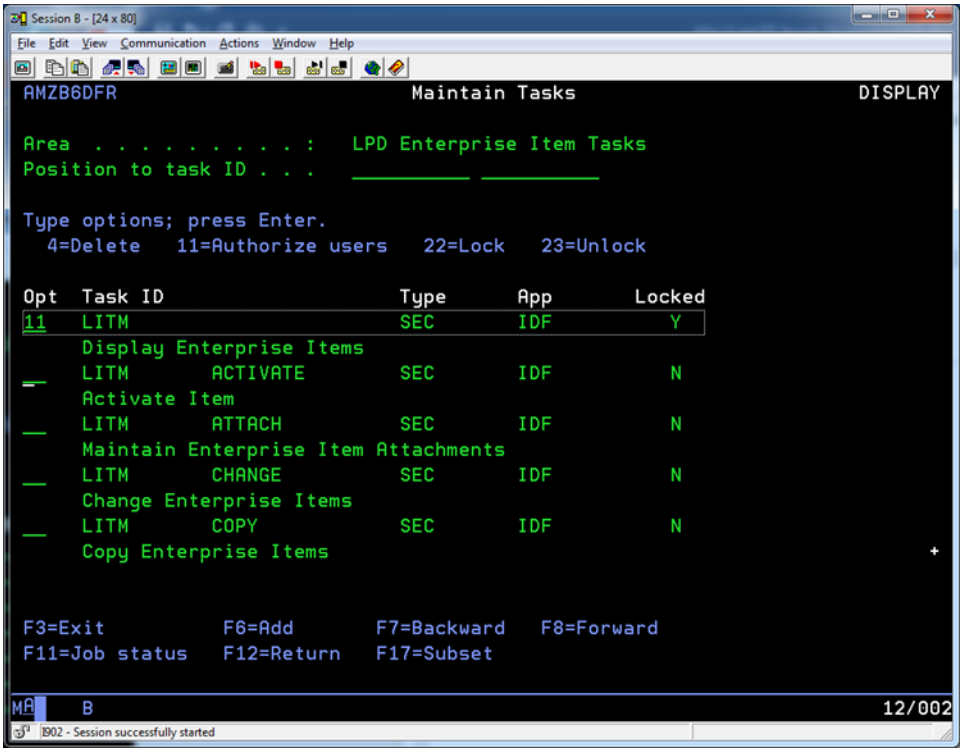
8 Start IDF and try to open Enterprise Item object:



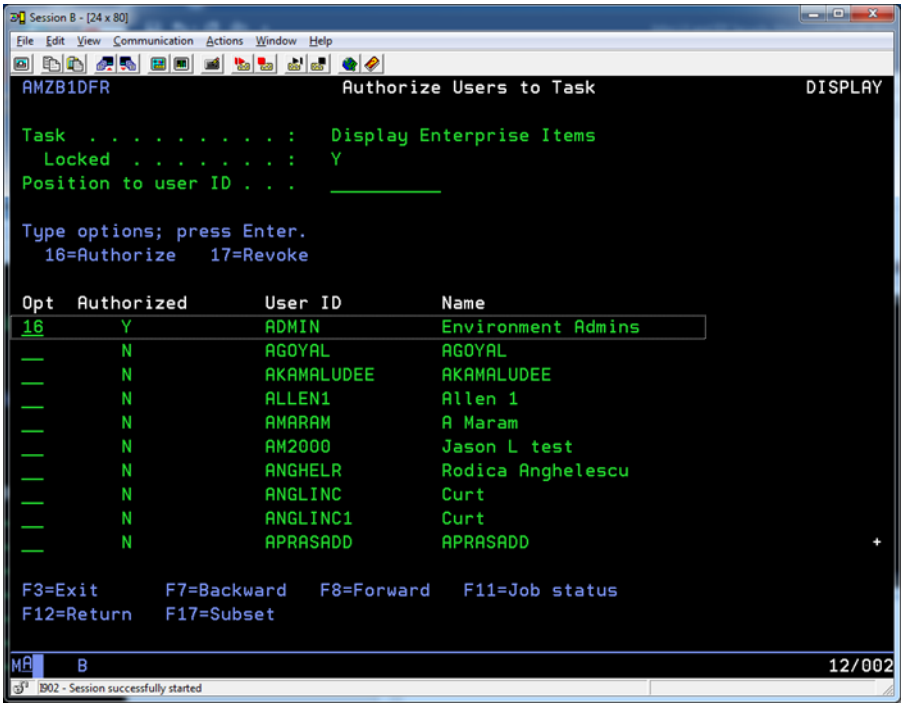
The error message is displayed:



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



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



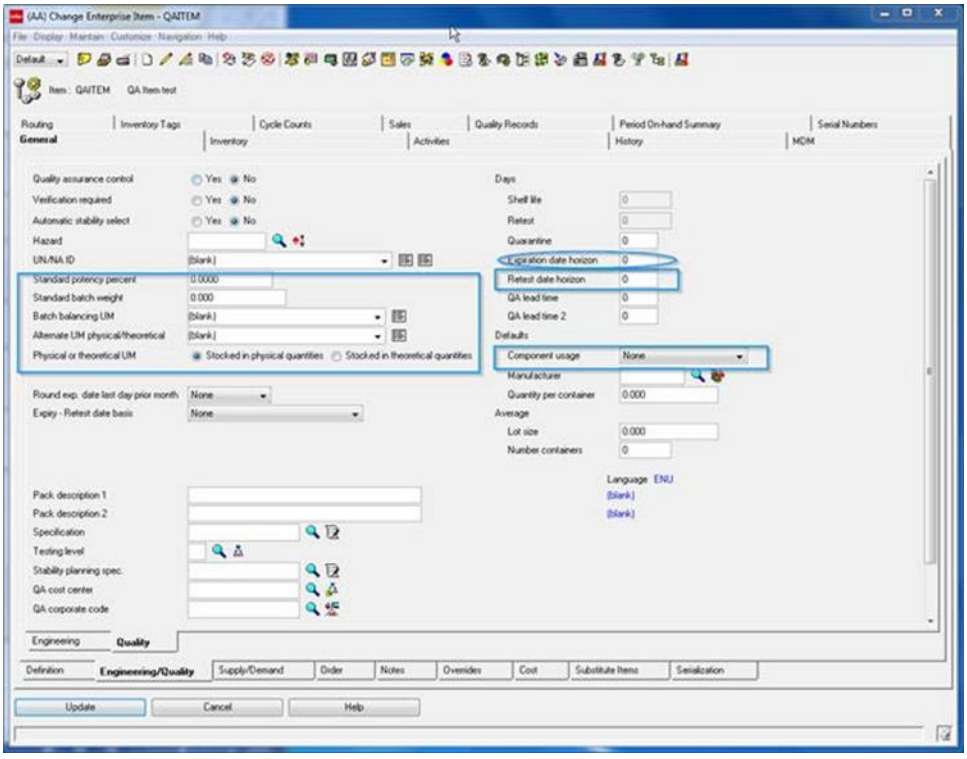
Locate LPD Field Level Security. It has two tasks that secures two sets of attributes:

- Maintain LX QMS fields
- Maintain LX API fields

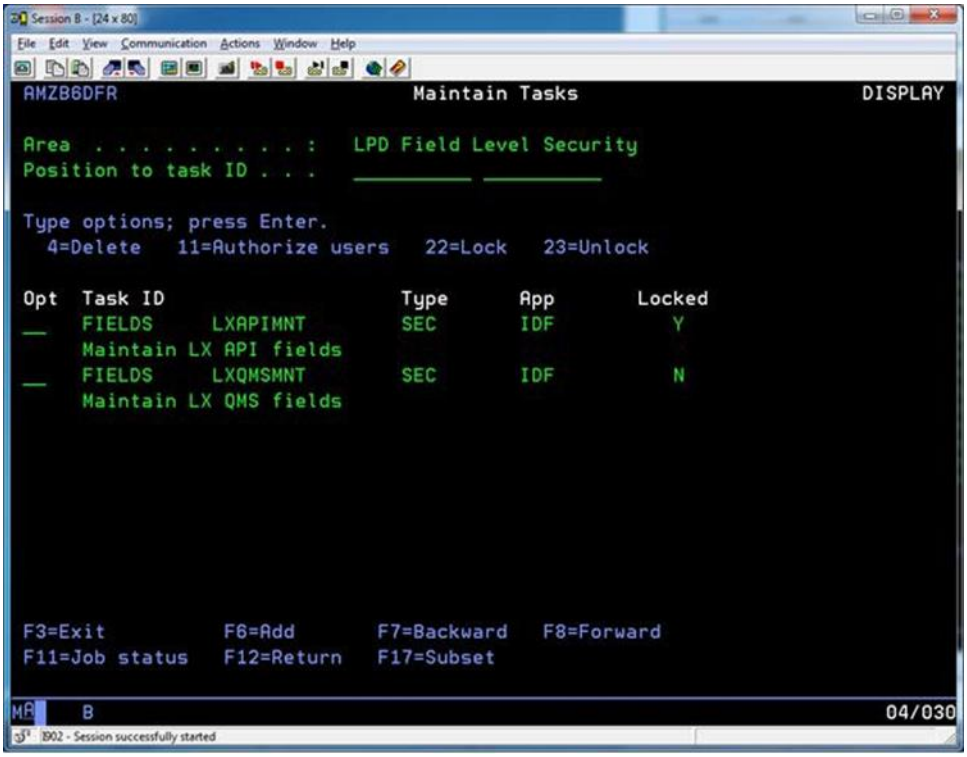
If you locked the task, only authorized users can maintain the group of the attributes.

When a user is authorized to the task:

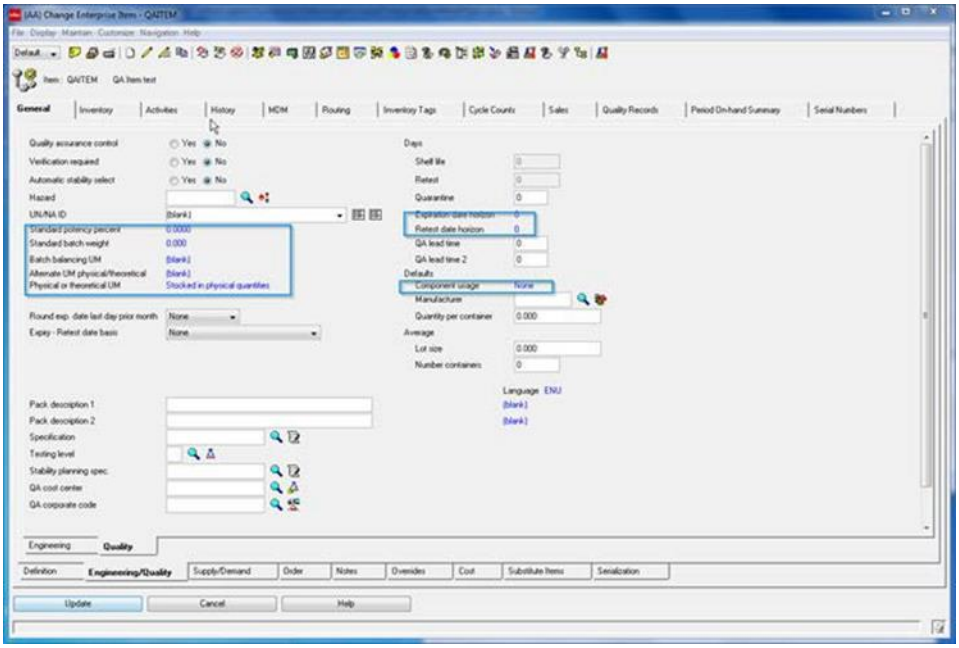
Open Item. The attributes are input allowed and you can change them.



Lock LPD Field Level Security/Maintain LX API fields.



The attributes become protected.


General
Inventory
Activities
History
MDM
Routing
Inventory Tags
Cycle Counts
Sales
Quality Records
Period On-hand Summary
Serial Numbers
Quality assurance control
Verification required
Automatic stability select
Hazard
UN/NA ID
Standard potency percent
Standard batch weight
Batch balancing UM
Alternate UM physical/theoretical
Physical or theoretical UM
Round exp. date last day prior month
Expiry - Retest date basis
Days
Shelf life
Retest
Quarantine
Expiration date horizon
Retest date horizon
QA lead time
QA lead time 2
Defaults
Component usage
Manufacturer
Quantity per container
Average
Lot size
Number containers
Language ENU
Pack description 1
Pack description 2
Specification
Testing level
Stability planning spec
QA cost center
QA corporate code
Engineering
Quality
Definition
Engineering/Quality
Supply/Demand
Order
Notes
Overrides
Cost
Substitute Items
Serialization
Update
Cancel
Help

Chapter 12 Securing Mass Change and Mass Delete actions

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

Mass Change Customers

Mass Change Item Costs

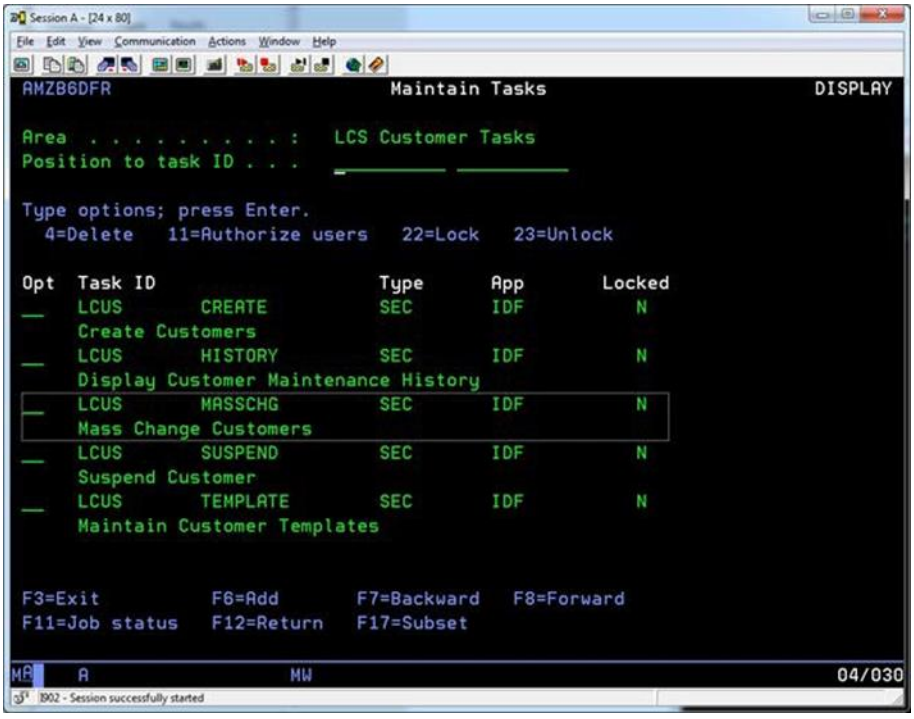
Mass Change Vendors

Mass Change Enterprise Items

Mass Delete Item Costs and

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.



Chapter 13 Using CPYSECIDF

The Copy LX Security to IDF command is a tool that is designed to simplify the setup of user security in IDF for LX. There are several areas of LX security that the tool imports from an LX environment into an IDF environment.

These LX security areas can be mapped to IDF security:

LX Security	IDF 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
Program Security: Products	CAS Security Tasks
Program Security: Programs	CAS Security Tasks
Program Security: Function Keys/Action Codes (FKAC)	CAS Security Tasks
User Identity:User exists in LX Security	CAS Security Task for access to IDF environment

Data security for Company, Facility, and Warehouse in LX is setup in SYS600 for each user. Data security for CEA Ledger, Book, and Year in LX is set up in CLD175 Book Security for each group.

Only group codes 1 – 100 in CLD170 are migrated to IDF. These same values are migrated to IDF and can be viewed and modified in the User Profiles business object.

The CPYSECIDF tool creates CAS Security entries for each user's authorizations it finds in LX security for users in SYS600. Function key/Action code settings for a user are defined by the user's SYS600 group and that group's settings in SYS603. Additionally, users can be authorized to access the IDF environment. CPYSECIDF will add active LX users to the IDF environment's access. See Chapter 3 step 2c above for details.

See "Appendix A LX to IDF Security Cross Reference" on page 48 for details on the files used by CPYSECIDF to map LX programs, products, and FKAC to IDF Business Objects and CAS Security Tasks.

Acquiring and installing the CPYSECIDF tool

The CPYSECIDF tools are available from the Infor Support Portal in KB 2158293.

Extract the CPYSECID84 SAVF from the zip file and upload to your IBM i system, then restore the CPYSECID84 library.

Running the CPYSECIDF tool

1. Start a Link Manager session and import an Infor LX environment.
2. Start a 5250 session with a user profile that has *ALLOBJ authority and access the LX environment from which you plan to copy the security from.
3. Press **F21** to access a command line.
4. Add the CPYSECID84 library to your *LIBL ADDLIBLE CPYSECID84
5. Run the CPYSECIDF command and prompt it. CPYSECIDF (F4)
6. You need to provide these parameters:

Parameter	Description
LXENV	Source ERPLX Environment Control library
IDFENV	Target IDF Environment
USER	User profile, generic*, or *ALL to copy LX security to IDF
AUTHENV	Select *YES to authorize user to the IDF environment. Inactive LX users will have their IDF environment authority removed. Select *NO to bypass authorizing user to the IDF environment.

Parameter	Description
UPDCAS	Select *YES to create IDF CAS Security records to allow user to use Business objects and perform selected functions within the objects. File ZXYP contains mappings between LX Security settings and IDF CAS Security Tasks/Sub-Tasks. Select *NO to bypass updating CAS Security.
UPDAUTO	Select *YES to update IDF Auto-Content security from the LX security settings. The Warehouse, Company, Facility security settings are exported to IDF. IDF settings that do not match LX settings will be removed. Inactive users will have all settings removed. Select *NO to bypass updating Auto-Content Security.
UPDCEA	Select *YES to update CEA Auto-Content security from the LX security settings. The CEA Ledger, Book, and Year security settings are exported to IDF based on the users SYS600 Group value. Note, only groups that are assigned an SOCODE value from 1 to 100 in GSO will be processed. Inactive users will have all settings removed. Select *NO to bypass updating CEA Auto- Content Security.
UPDEGLI	Select *YES to update EGLI Auto-Content security from the LX security settings. The CEA Ledger, Book, and Year security settings are exported to IDF based on the users SYS600 Group value. Note, only groups that are assigned an SOCODE value from 1 to 100 in GSO will be processed. Inactive users will have all settings removed. Select *NO to bypass updating EGLI Auto- Content Security.

Parameter	Description
UPDGRUP	Select *YES to update the EGLI Finance Group to match the user group in SYS600. A Finance Group record will always be created if it doesn't exist, but this parameter will force an update to EGLI if they don't match. Inactive users will have their Finance Group removed. To view/change the EGLI Finance Group in IDF use the User Profiles object. For each user access the Finance tab to change the user's group. Select *NO to bypass updating EGLI Finance Group.

7 Specify the appropriate values and press **Enter**.

8 Three reports are generated that provide details on the actions performed by the command. Find the reports by typing **WRKSPLF** and review the actions taken by the tool.

9 To make any additional Auto-Content or Financial Group changes start a Power-Link session and login to the IDF new environment. Open the User business object and select the Values and Financial tabs.

10 To change CAS Security settings, start a 5250 session, add AMCESLIB to your *LIBL, execute command STRIDF. Option 10 on the main menu is the Security menu where you can make additional CAS security changes.

Dynamically executing the CPYSECIDF tool

With the User Provisioning capability added to LX 8.4.0 via BMR 78589, if the new SYS802D parameter “Synchronize IDF users existence with LX users” is set to 1=Yes, then SYS600 User Maintenance attempts to dynamically execute the CPYSECIDF command which must exist in the active LX library list. Either the LX library list (INLIBL data area and job descriptions) need to be updated to include library CPYSECID84, or command CPYSECIDF and all of its supporting objects must be copied from library CPYSECID84 to one of the libraries already in the LX library list.

Appendix A LX to IDF Security Cross Reference

LX security settings are mapped to IDF CAS Security by the CPYSECID84/ZXYP file. Edit this file to change those settings as needed. 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.

Setting the XYRCID value to 'XX' will inactivate a record from being processed by CPYSECIDF. The notes and last maintenance fields (XYNOTES, XYLMUS, XYLMDT, XYLMTM) have no impact on processing.

SYS600 based settings

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

Function Key Action Code settings

Records with XYSEQ <> 0 map Function Key Action Code settings from ZAUP to IDF CAS Security Tasks and Subtasks. For these settings the full program name is used for XYPGM.

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 XYPROD and XYPGM fields are left blank and no LX security is mapped. If you wish to map LX security to these tasks update the XYPROD and/or XYPGM fields for those tasks you wish to map. Note that records with duplicate XYTASK and XYSUBT are allowed for different LX products and programs. For example, task "LPOR" with sub-task *blanks is authorized if the PUR product or PUR300, PUR312, PUR520, PUR550, or PUR651 are authorized. Additionally, if you create custom IDF objects that have CAS Security task created you can add records to ZXYP to map SYS600 products and/or programs or FKAC options to those tasks.

Any CAS security settings that do not have records in ZXYP with XYPROD or XYPGM populated are not impacted by CPYSECIDF and will need to be managed through IDF Security Maintenance. The one exception is the ACCMAPICS task that allows users access to the environment which is controlled for LX users via the AUTHENV parameter of CPYSECIDF.

In ZXYP many IDF objects are mapped to LX programs for display access which typically has a named task (XYTASK) and a blank sub-task (XYSUBT). For these objects many will also have sub-tasks ATTACH, HISTORY, and/or TEMPLATE. These sub-tasks allow users to perform specific actions and may be useful to include in the security mappings. Since there is no LX setting for these functions no default mapping is included. For each of these objects/tasks adding XYPROD and or XYPGM values will include user access to these sub-tasks.

ATTACH – Allows user to view and maintain attached files for the selected entries. HISTORY – Allows user to view and navigate to entries they have taken in the past. TEMPLATE – Allows users to maintain templates used to create, change, or copy entries.

A couple extra copies of ZXYP are included in library CPYSECID84. ZXYP_ORIG is an exact copy of ZXYP in case changes are made to ZXYP and the original settings are needed. ZXYP_MORE is an example of adding security settings for the ATTACH, HISTORY, and TEMPLATE tasks based on product authority.