Infor IDF for Infor LX Security Maintenance Guide for 8.3.5

Important Notices

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 IDF for Infor LX 8.3.5

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

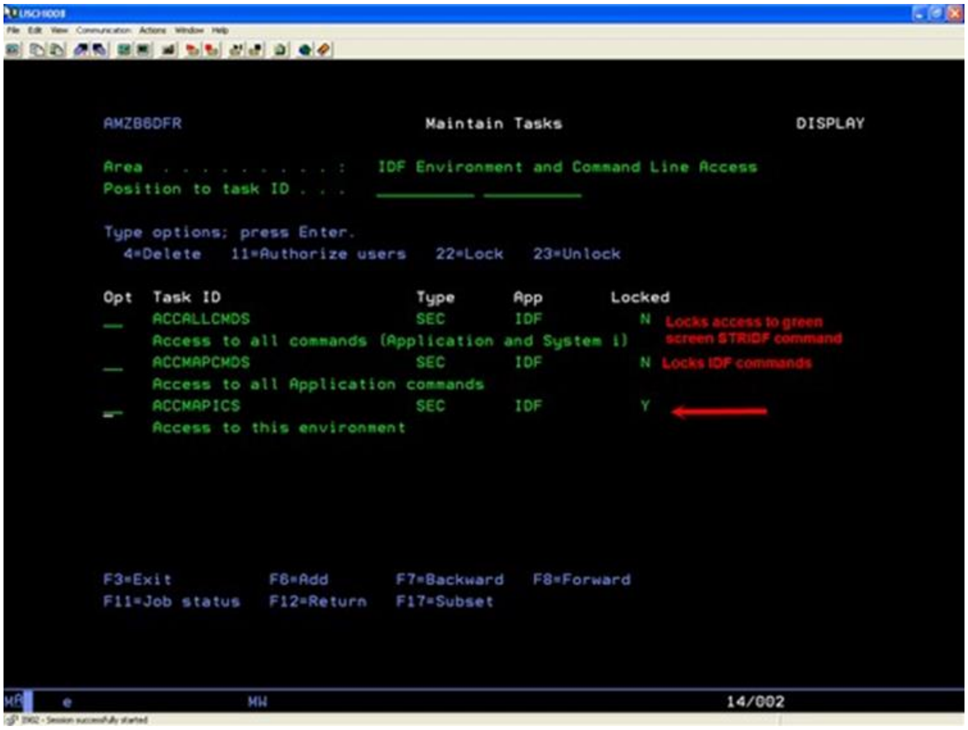
To start security maintenance:

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.



```
 AMZB8DFR                          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
```

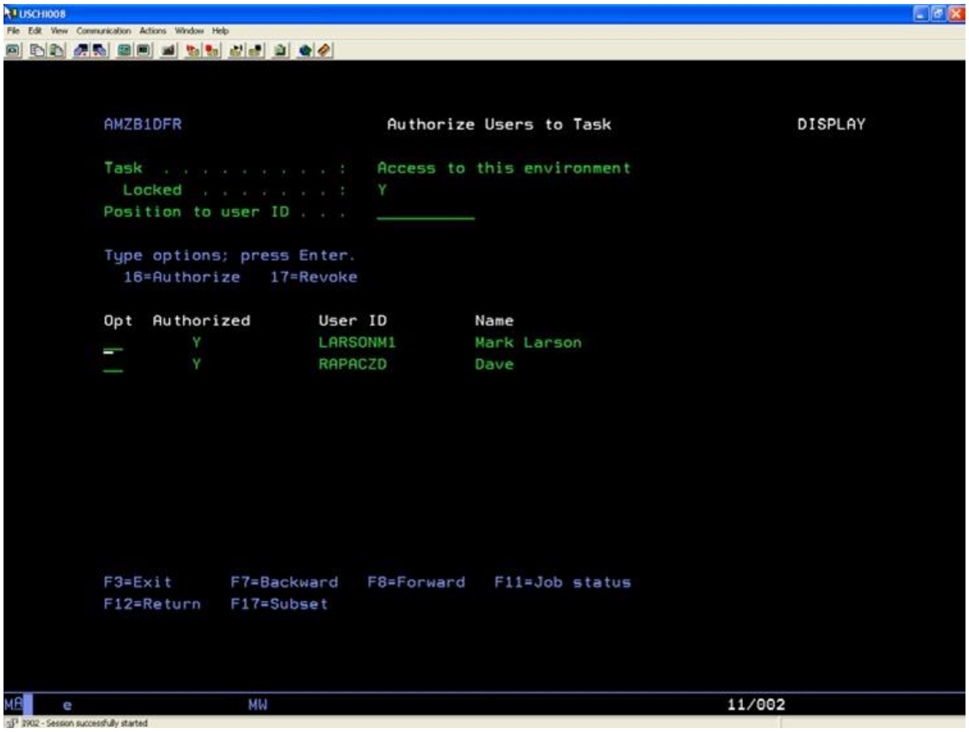
USCH008
File Edit View Communication Actions Window Help
Locks access to green screen STRIDF command
Locks IDF commands
Session successfully started

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**.



```
 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
```

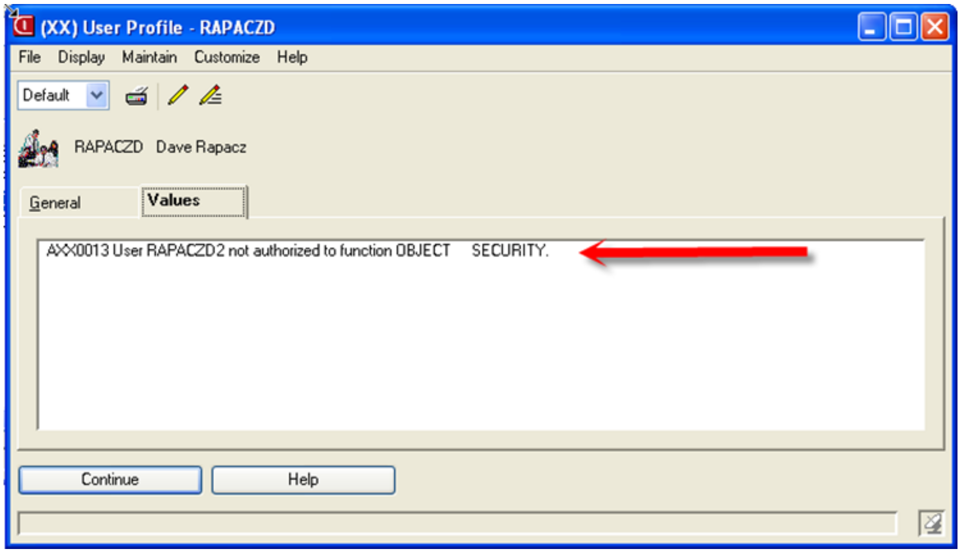
1902 - Session successfully started

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

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.



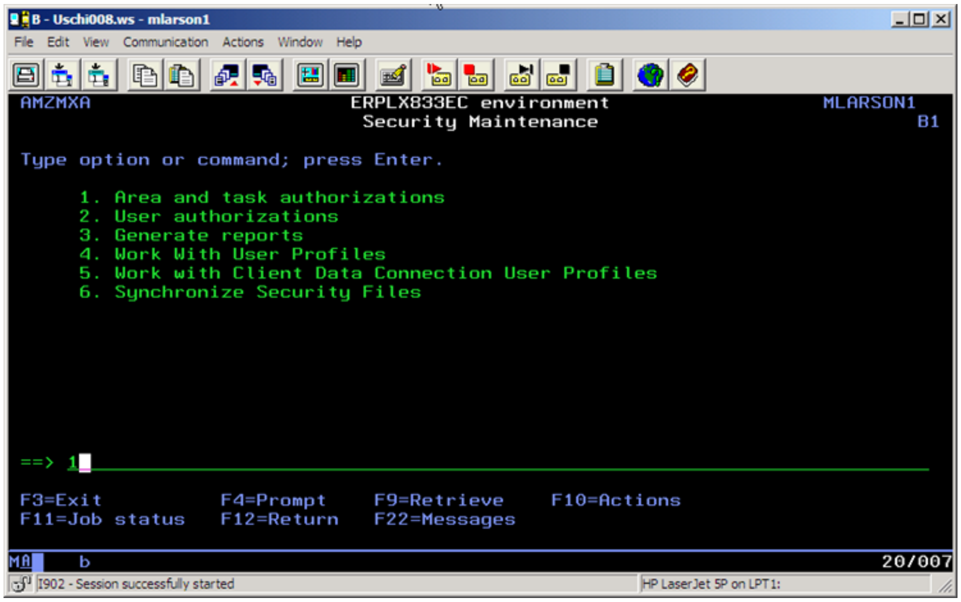
AXX0013 User RAPACZD2 not authorized to function OBJECT SECURITY.

To allow access:

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

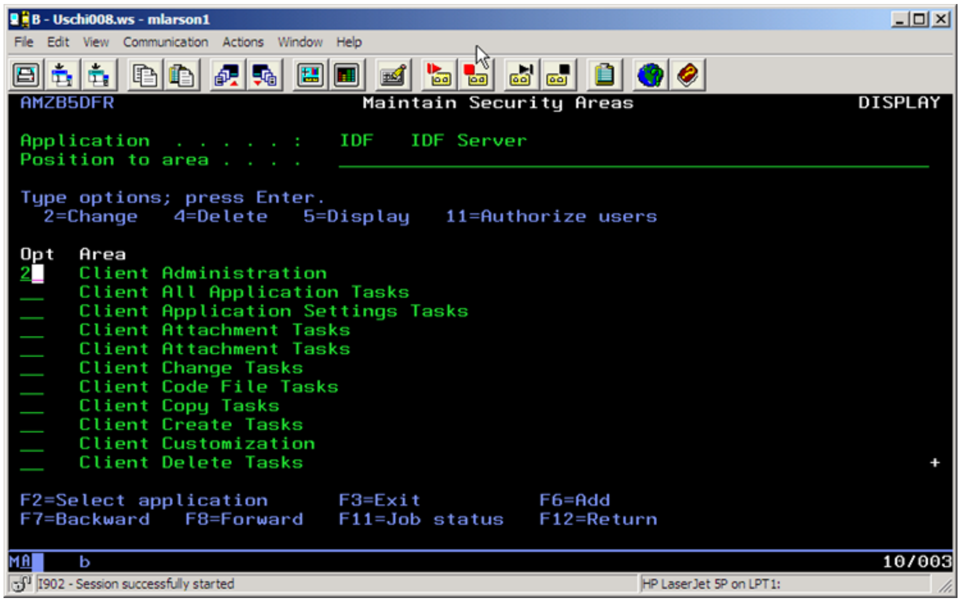
2 Specify **10**, **Security Maintenance**.

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


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

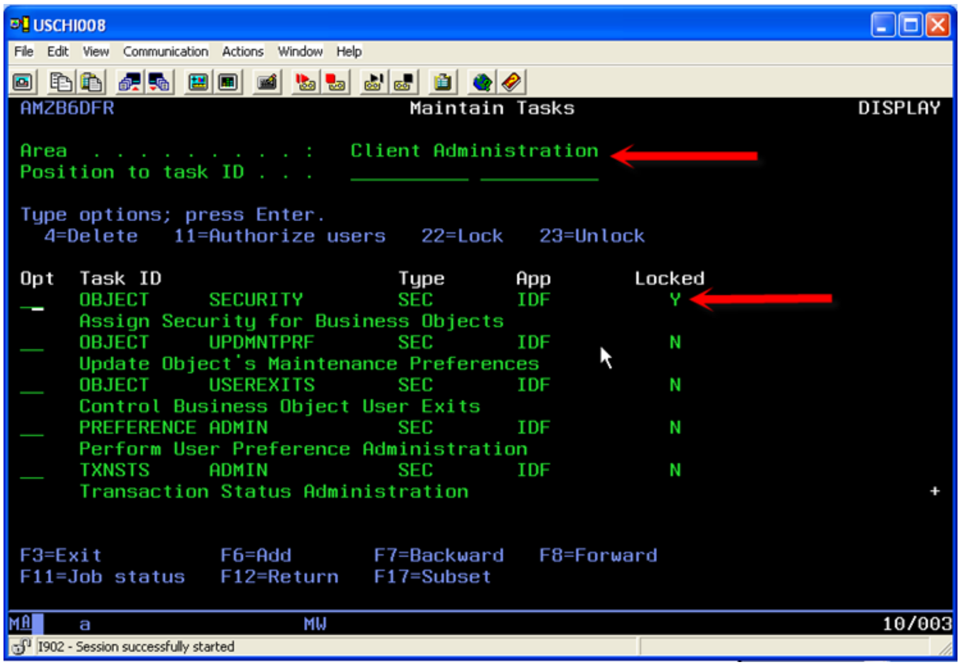
```
 AMZMXA                        ERPLX833EC environment                 MLARSON1
                                Security Maintenance                        B1

 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
```

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
```

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

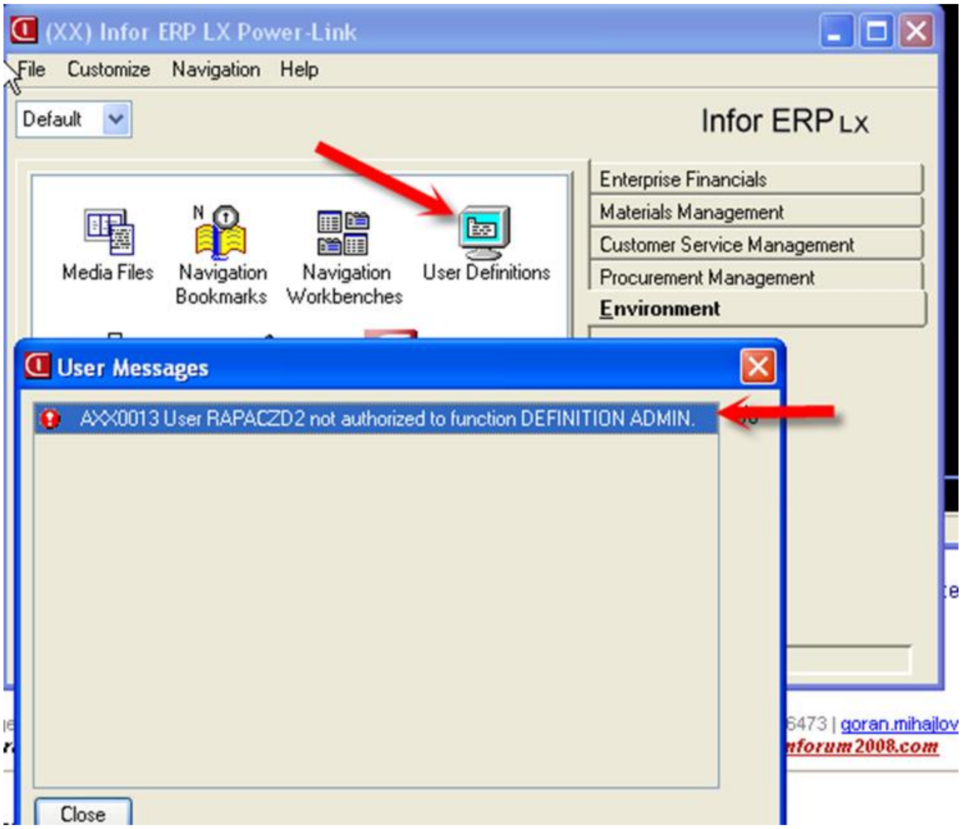


```
AMZB6DFR                         Maintain Tasks                          DISPLAY

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.

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.

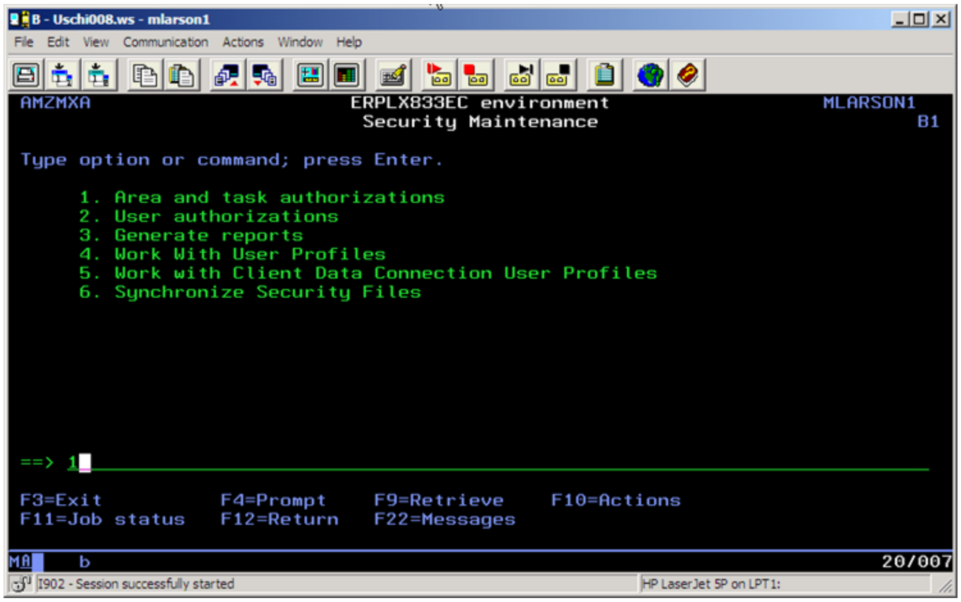


AXX0013 User RAPACZD2 not authorized to function DEFINITION ADMIN.

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

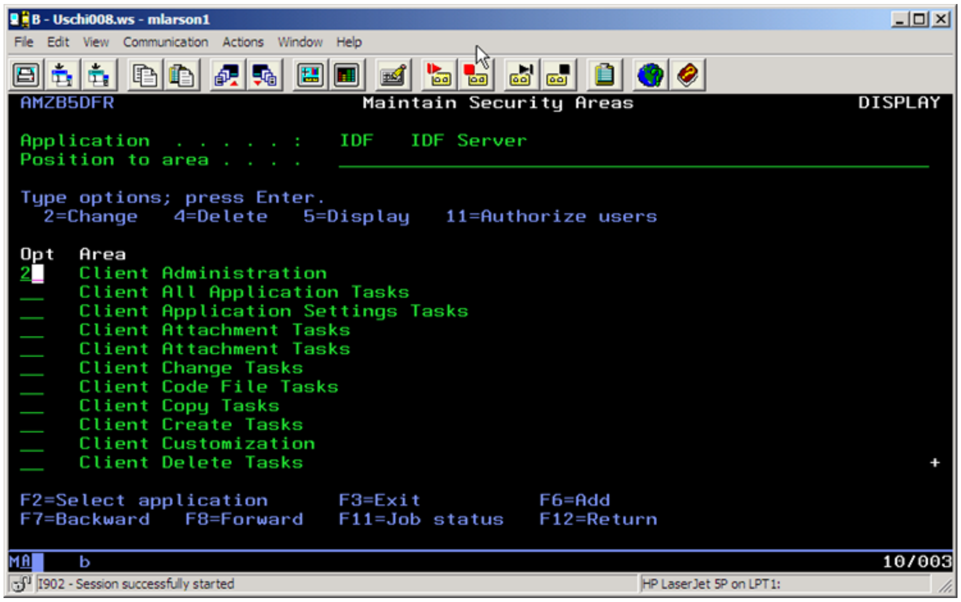
2 Specify **10**, **Security Maintenance**.

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


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

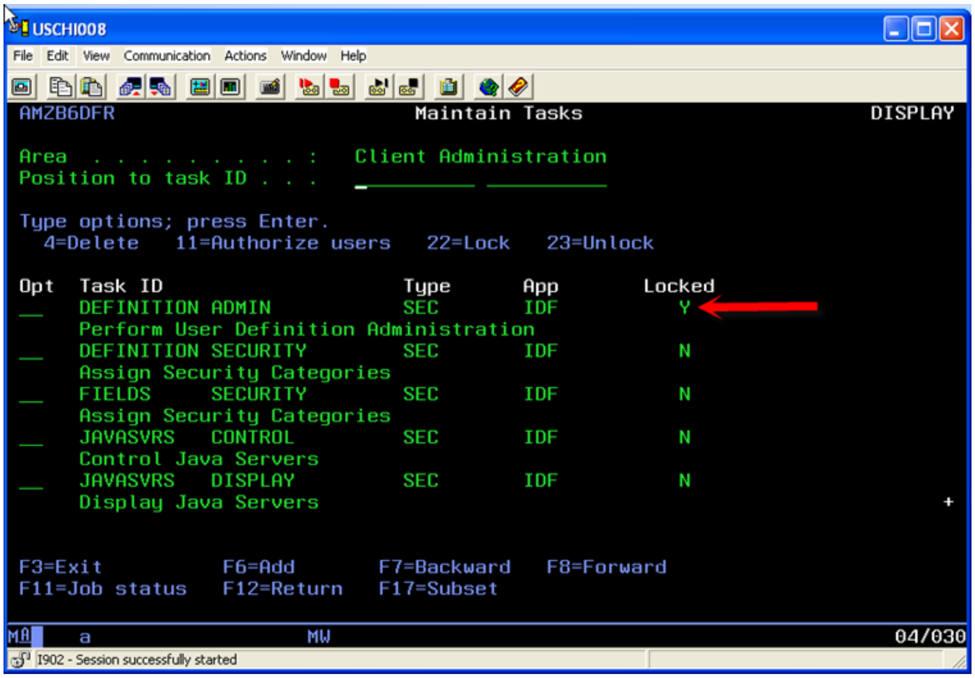
```
AMZMXA                   ERPLX833EC environment                   MLARSON1
                          Security Maintenance                          B1

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.

Chapter 6 Security to change data on all Business Objects

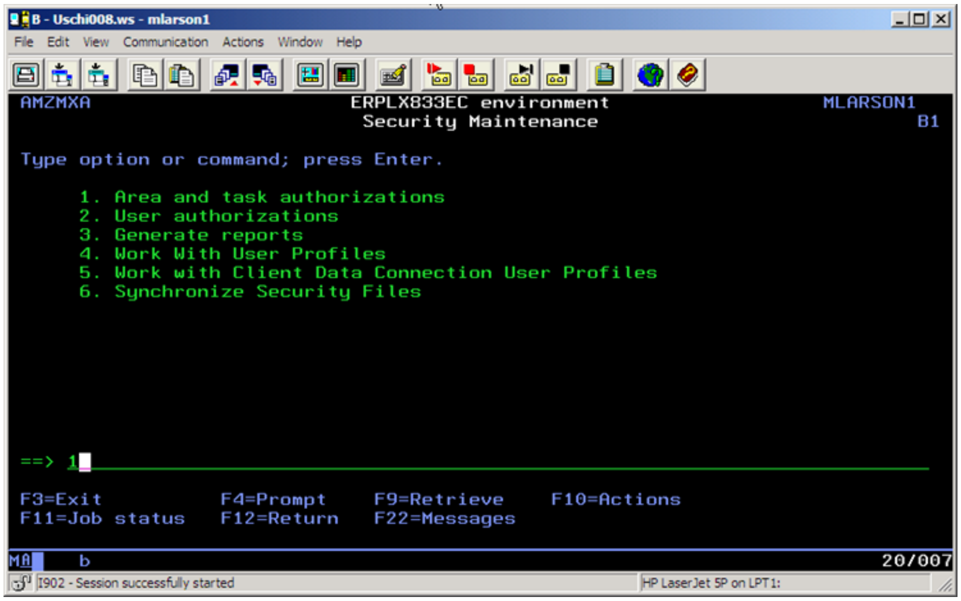
If you want to verify a user can only use Business Objects for inquiry, use the Maintain Business Objects option under Client Administration.

Note: This is Global for all Business Objects.

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

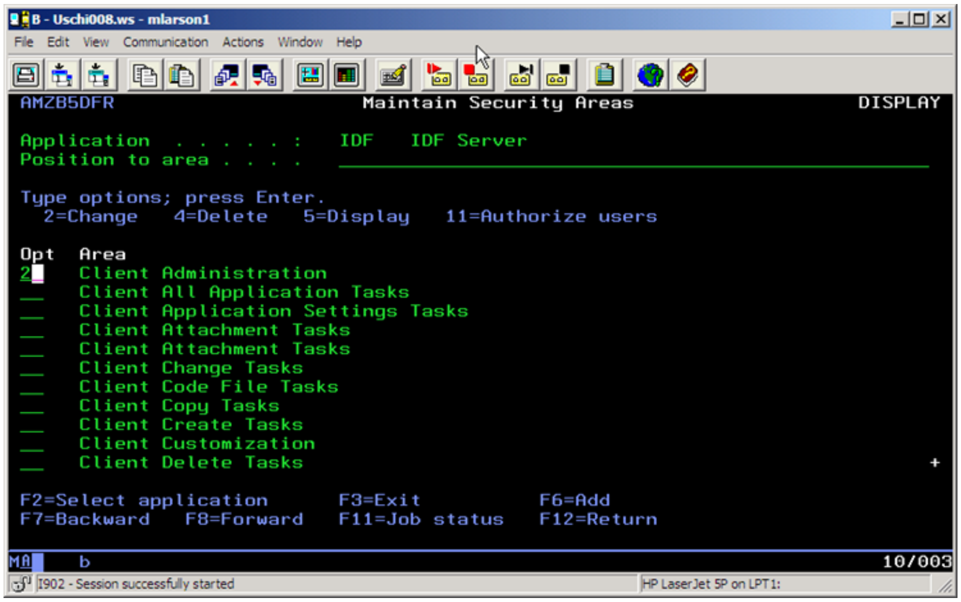
2 Specify **10**, **Security Maintenance**.

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


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
```

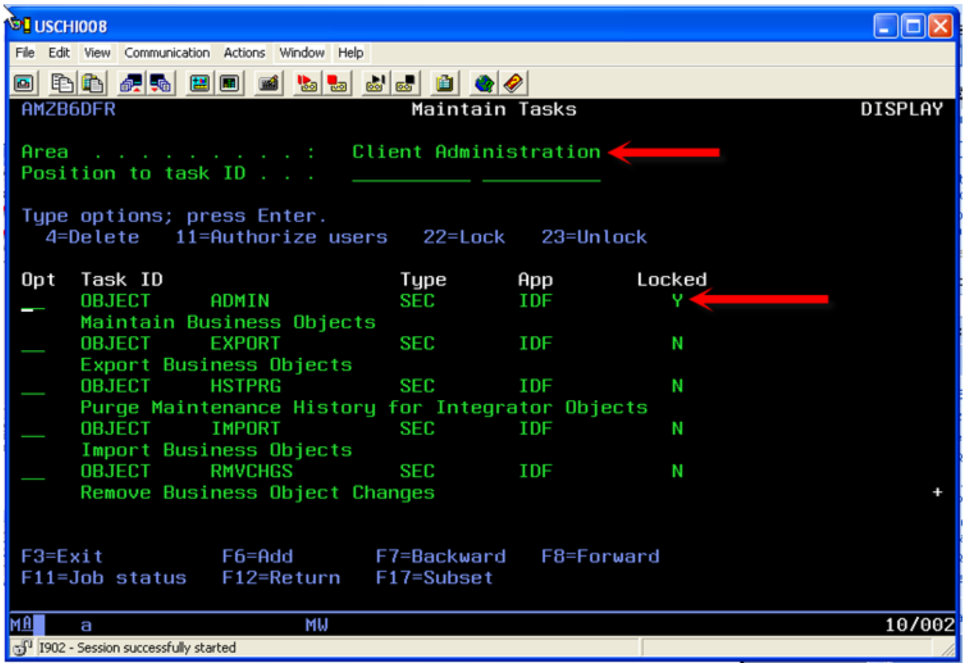
4 Specify **2** for **Client Administration**.



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.

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!

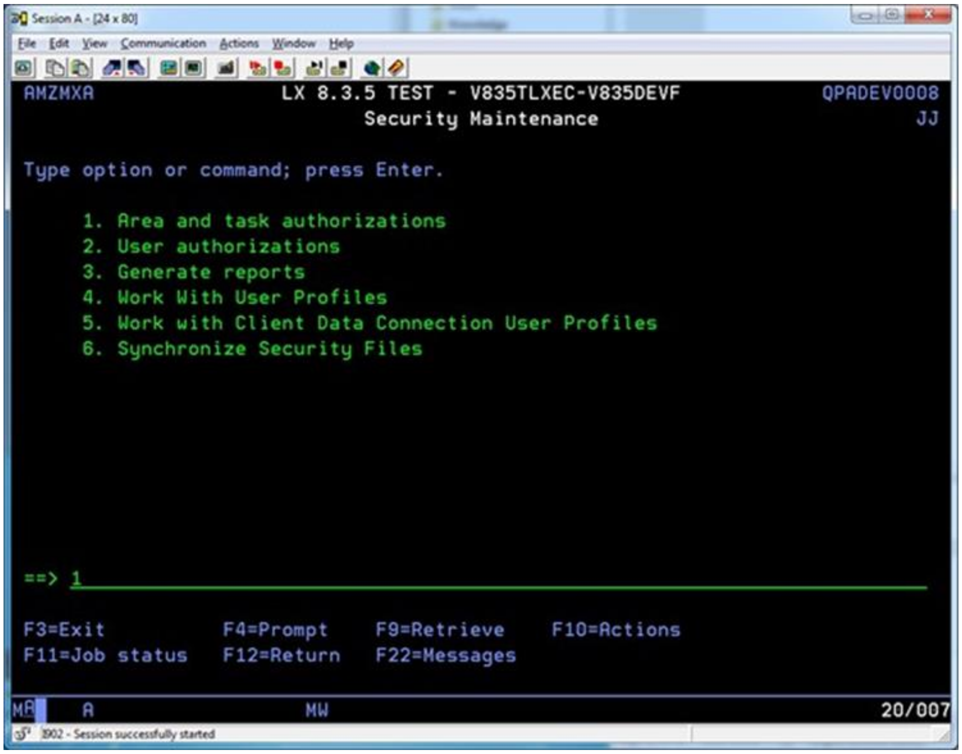
There are two types of Public definitions, cards, for example, Company owned (the definitions shipped with the product, Infor in this case) or User owned. If you want to stop users modifying only Company owned cards, you should lock only MNTPUBLIC tasks.

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.

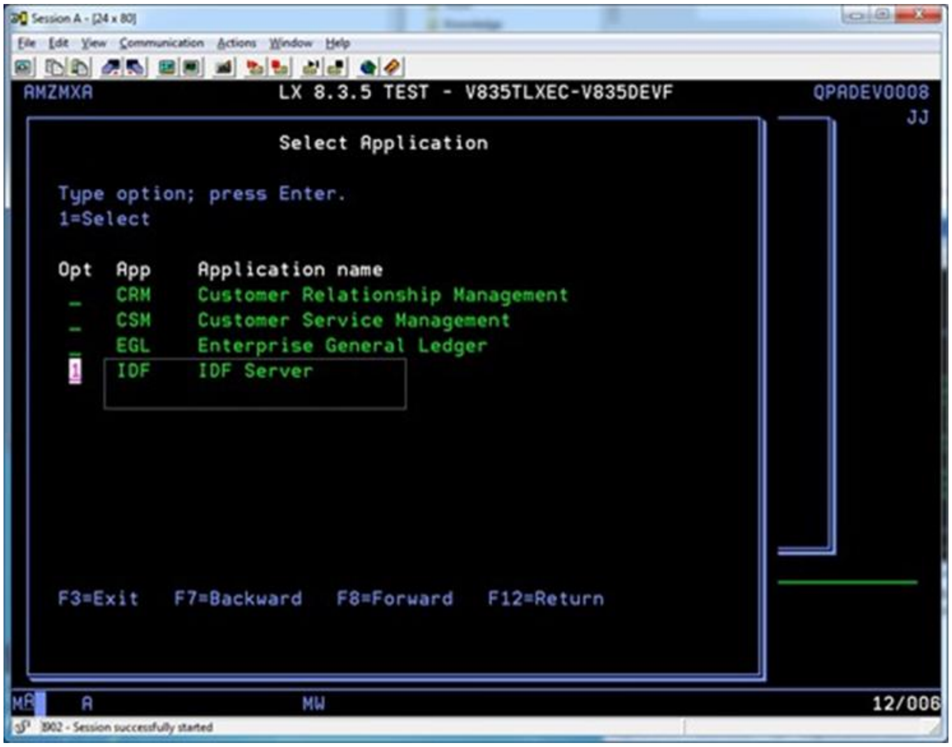
Note: This is Global for all Business Objects.

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.



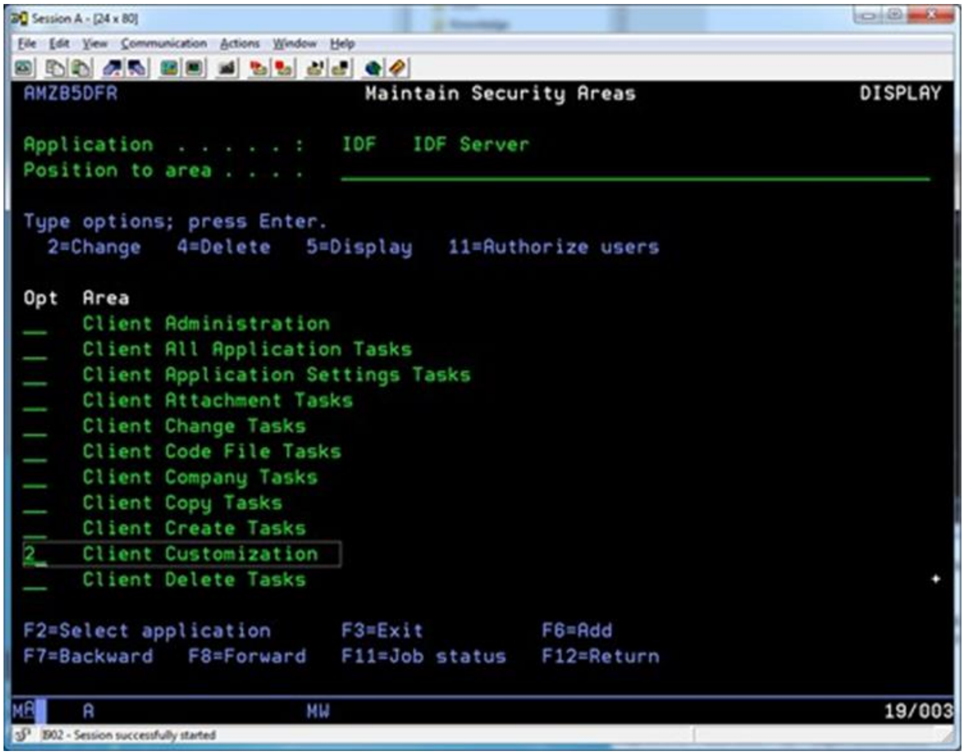
```
AMZMXA                 LX 8.3.5 TEST - V835TLXEC-V835DEVF              QPADEV0008
                               Security Maintenance                            JJ

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     A                  MW                                               20/007
902 - Session successfully started
```

a Select **IDF Server**.



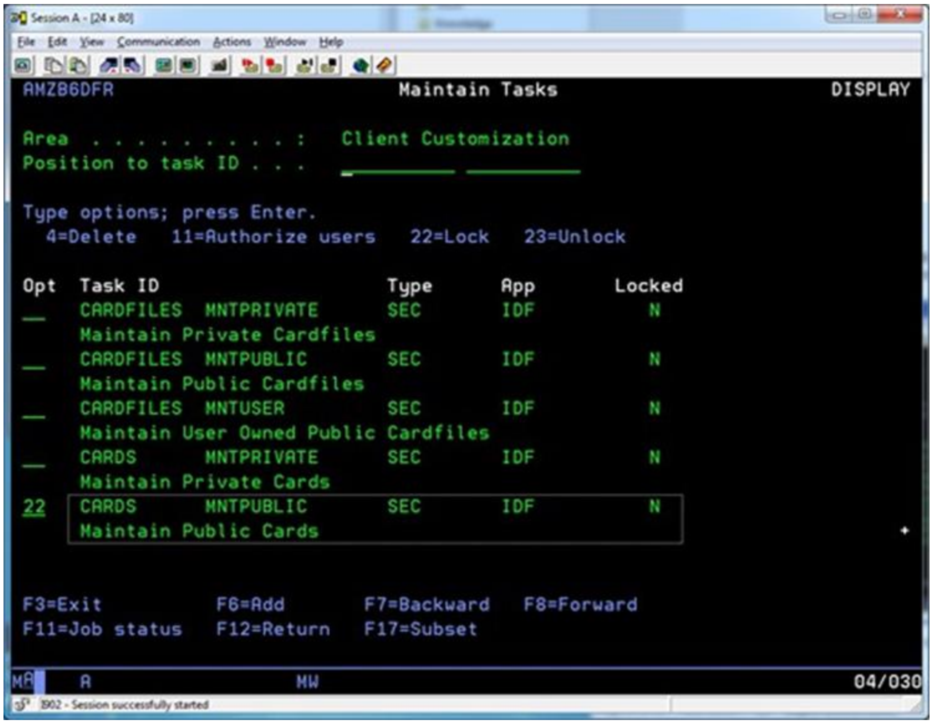
```
AMZMXA                 LX 8.3.5 TEST - V835TLXEC-V835DEVF              QPADEV0008
                                                                               JJ
                        Select Application

   Type option; press Enter.
   1=Select

   Opt  App    Application name
    _   CRM    Customer Relationship Management
    _   CSM    Customer Service Management
    _   EGL    Enterprise General Ledger
    1   IDF    IDF Server







   F3=Exit   F7=Backward   F8=Forward   F12=Return

MA     A                  MW                                               12/006
902 - Session successfully started
```

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

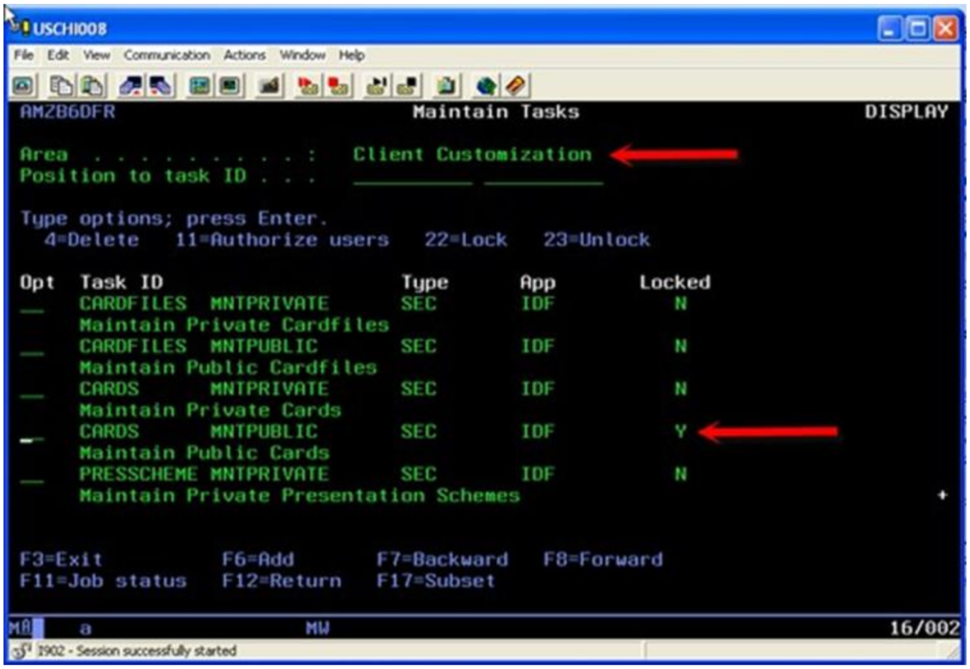

Session A - [24 x 80]
File Edit View Communication Actions Window Help
MA A MW 19/003
I902 - Session successfully started

```
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 Change Tasks
__   Client Code File Tasks
__   Client Company 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
```

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.


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

```
AMZB6DFR                     Maintain Tasks                         DISPLAY

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

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

Opt  Task ID                     Type      App       Locked
__   CARDFILES  MNTPRIVATE       SEC       IDF          N
     Maintain Private Cardfiles
__   CARDFILES  MNTPUBLIC        SEC       IDF          N
     Maintain Public Cardfiles
__   CARDFILES  MNTUSER          SEC       IDF          N
     Maintain User Owned Public Cardfiles
__   CARDS      MNTPRIVATE       SEC       IDF          N
     Maintain Private Cards
22   CARDS      MNTPUBLIC        SEC       IDF          N
     Maintain Public Cards                                               +

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



```
AMZB6DFR                      Maintain Tasks                        DISPLAY

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

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

Opt  Task ID                    Type      App        Locked
__   CARDFILES  MNTPRIVATE      SEC       IDF          N
     Maintain Private Cardfiles
__   CARDFILES  MNTPUBLIC       SEC       IDF          N
     Maintain Public Cardfiles
__   CARDS      MNTPRIVATE      SEC       IDF          N
     Maintain Private Cards
_    CARDS      MNTPUBLIC       SEC       IDF          Y
     Maintain 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    a               MW                                             16/002
1902 - Session successfully started
```

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

Maintain Public Subsets (SUBSETSMNTPUBLIC) – for Subsets

Maintain Public Cardfiles (CARDFILES MNTPUBLIC) – for Cardfiles

Maintain Public Presentation Schemes (PRESSCHEME MNTPUBLIC) for PresentationSchemes

Maintain Public Sorts (SORTSMNTPUBLIC) – for Sorts

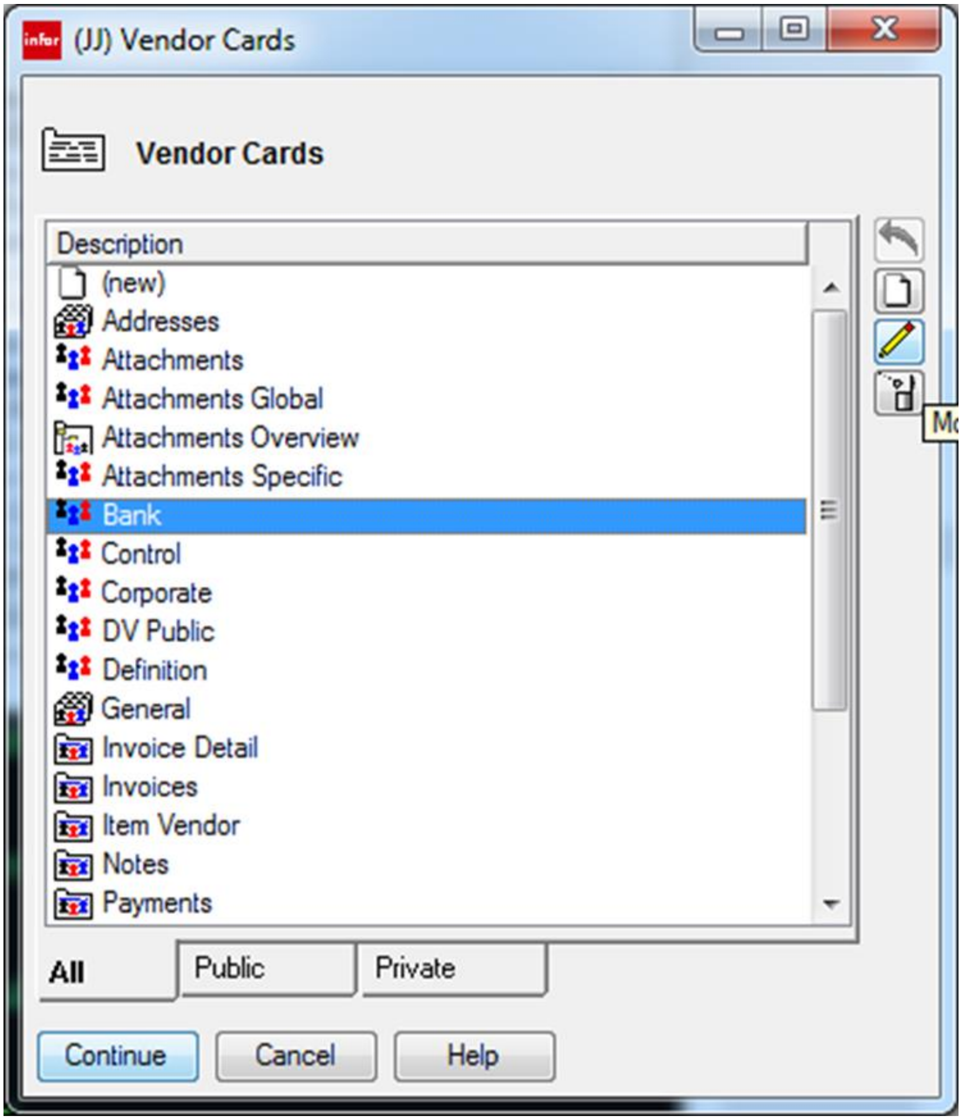
Maintain Public Templates (TEMPLATES MNTPUBLIC) – for Templates

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:

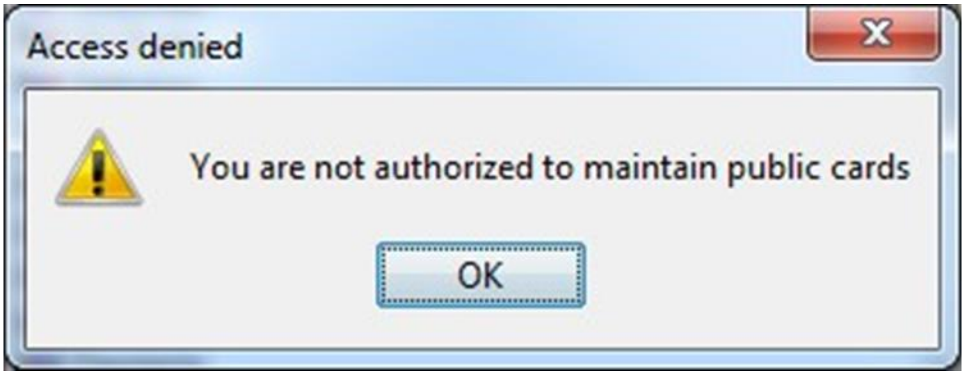


(JJ) Vendor Cards

Vendor Cards

Description

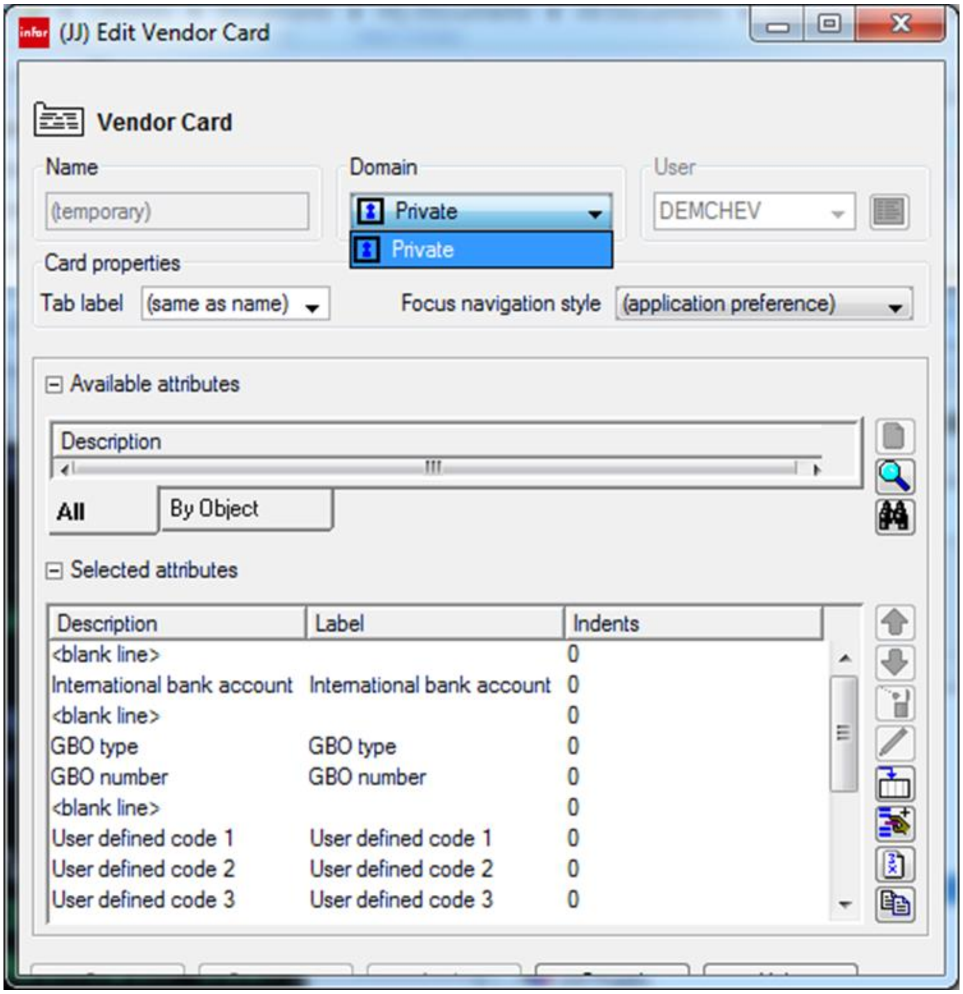
(new)
Addresses
Attachments
Attachments Global
Attachments Overview
Attachments Specific
Bank
Control
Corporate
DV Public
Definition
General
Invoice Detail
Invoices
Item Vendor
Notes
Payments



Access denied

You are not authorized to maintain public cards

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



(JJ) Edit Vendor Card

Vendor Card

Name: (temporary)

Domain: Private

User: DEMCHEV

Card properties

Tab label: (same as name)

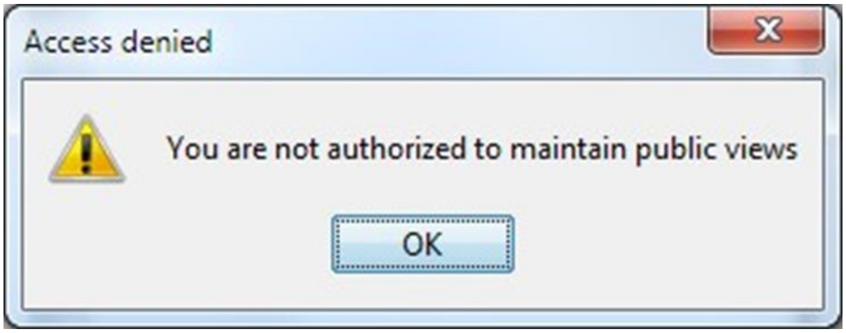
Focus navigation style: (application preference)

Available attributes

Selected attributes

Description	Label	Indents
<blank line>		0
International bank account	International bank account	0
<blank line>		0
GBO type	GBO type	0
GBO number	GBO number	0
<blank line>		0
User defined code 1	User defined code 1	0
User defined code 2	User defined code 2	0
User defined code 3	User defined code 3	0

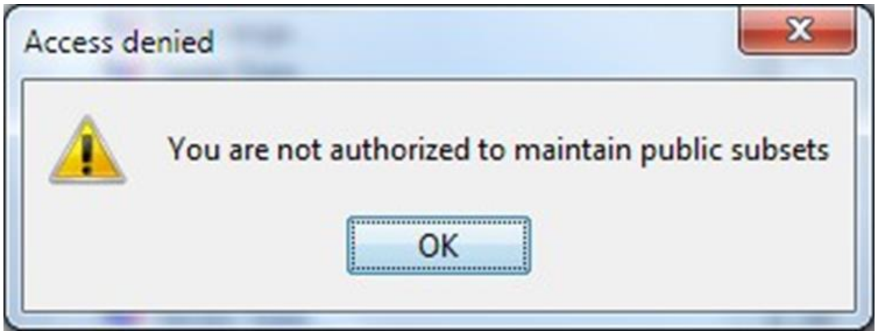
The similar messages will be displayed when you try to maintain public views:



Access denied

You are not authorized to maintain public views

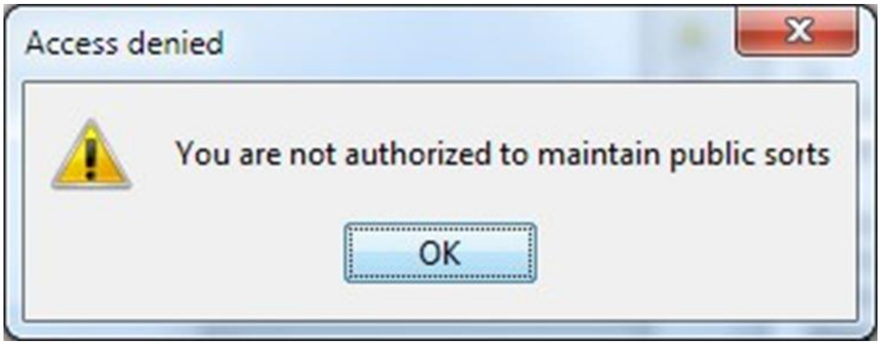
Public Subsets:



Access denied

You are not authorized to maintain public subsets

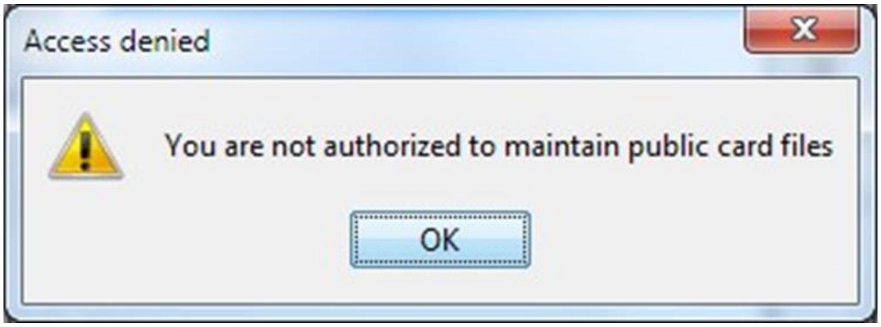
Public Sorts:



Access denied

You are not authorized to maintain public sorts

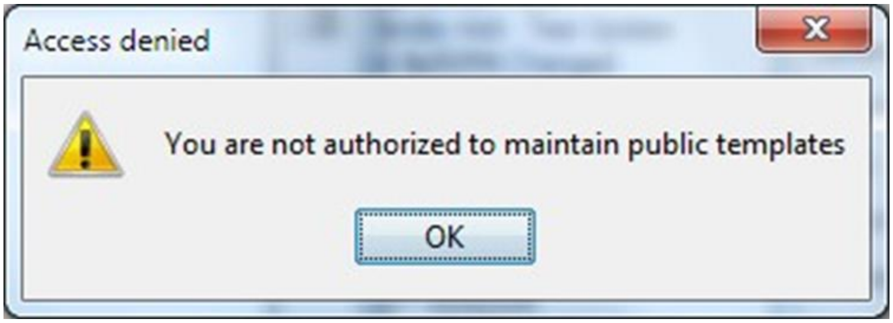
Public Card files:



Access denied

You are not authorized to maintain public card files

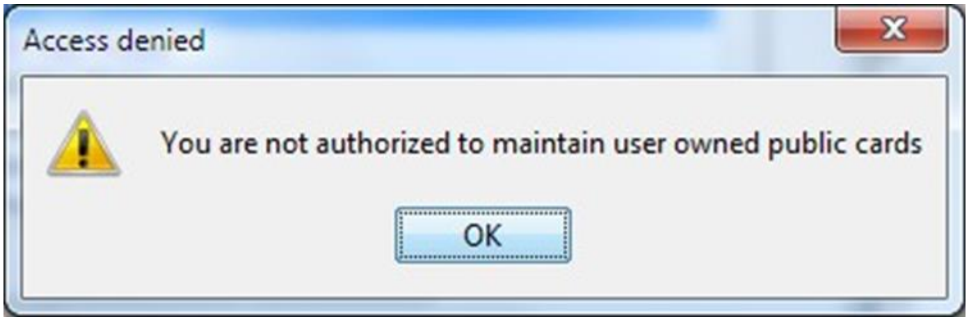
Public Templates:



Access denied

You are not authorized to maintain 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:



Access denied

You are not authorized to maintain user owned public cards

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.

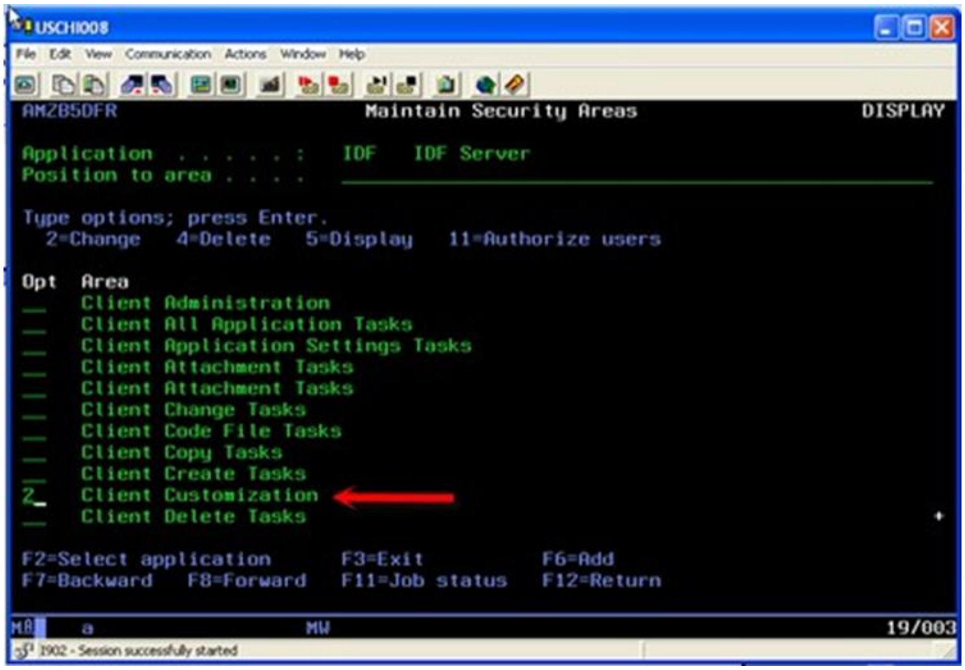
Note: This is Global for all Business Objects.

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

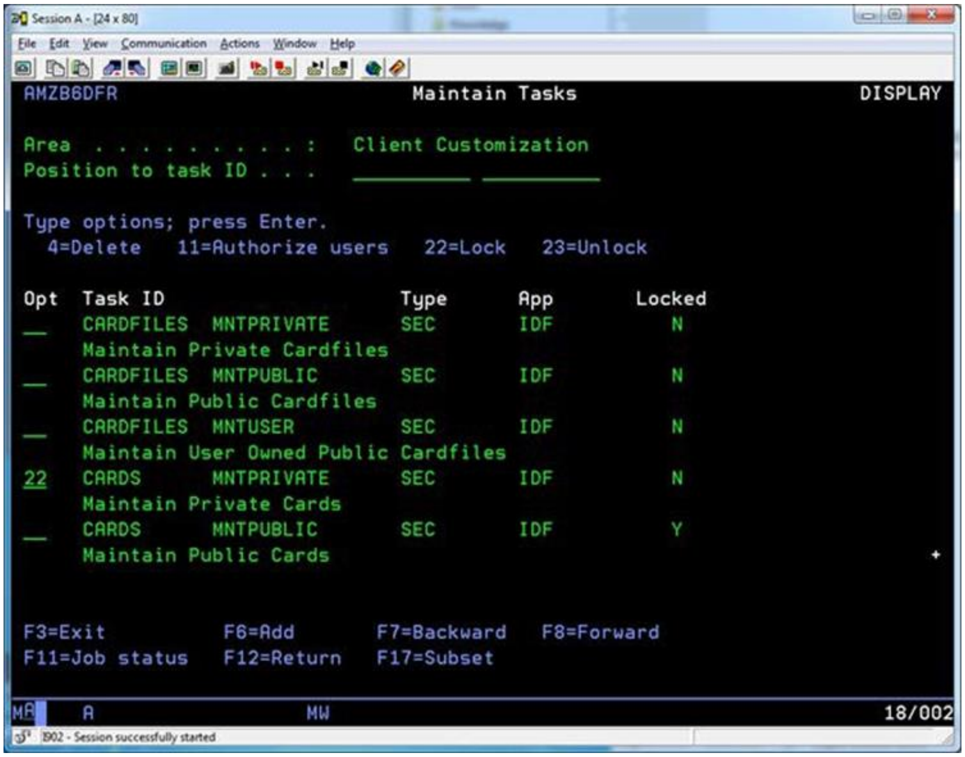
2 Specify **10**, **Security Maintenance**.

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

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



```
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
1902 - Session successfully started
```



```
AMZB6DFR                     Maintain Tasks                          DISPLAY

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

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

Opt  Task ID                  Type      App       Locked
__   CARDFILES  MNTPRIVATE    SEC       IDF          N
     Maintain Private Cardfiles
__   CARDFILES  MNTPUBLIC     SEC       IDF          N
     Maintain Public Cardfiles
__   CARDFILES  MNTUSER       SEC       IDF          N
     Maintain User Owned Public Cardfiles
22   CARDS      MNTPRIVATE    SEC       IDF          N
     Maintain Private Cards
__   CARDS      MNTPUBLIC     SEC       IDF          Y
     Maintain Public Cards                                               +


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

MA   A              MW                                              18/002
I902 - Session successfully started
```

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

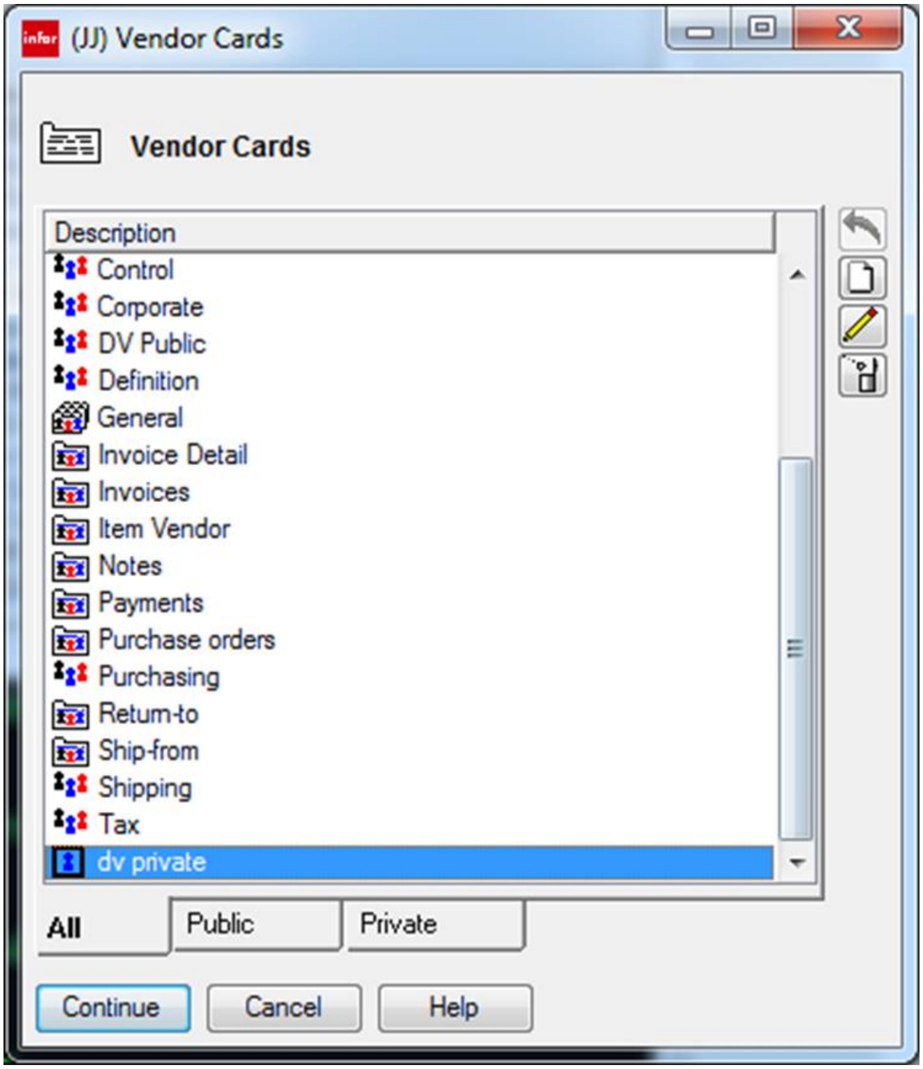
Maintain private Presentation Schemes (PRESSCHEME MNTPRIVATE) for Presentation Schemes

Maintain private Sorts (SORTSMNTPRIVATE) – for Sorts

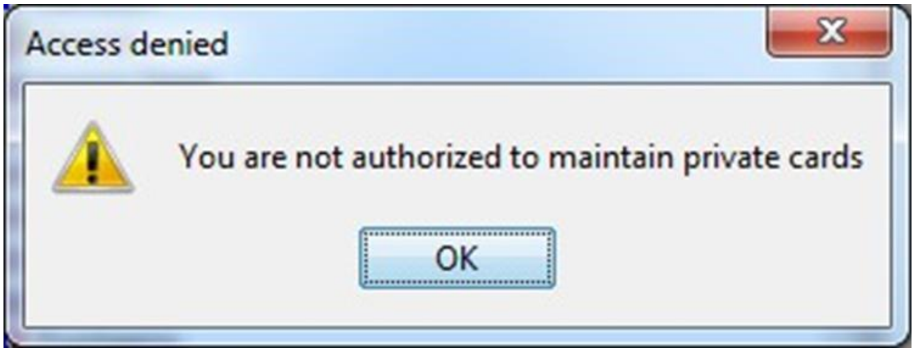
Maintain private Templates (TEMPLATES MNTPRIVATE) – for Templates Maintain private Views (VIEWSMNTPUBLIC) – for Views

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.


Access denied

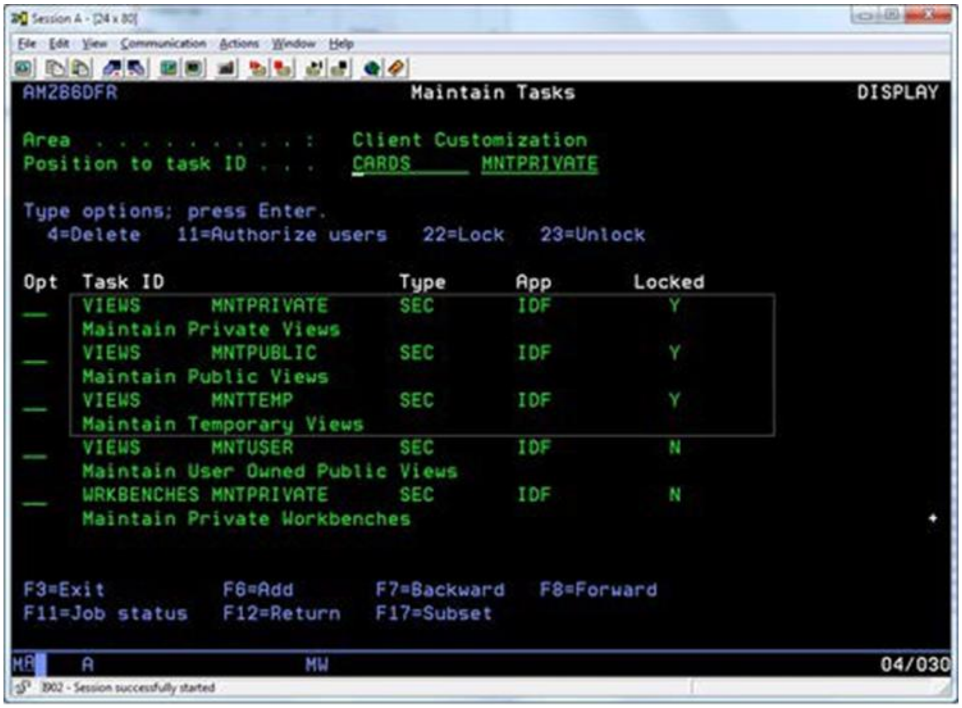
You are not authorized to maintain private cards

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.

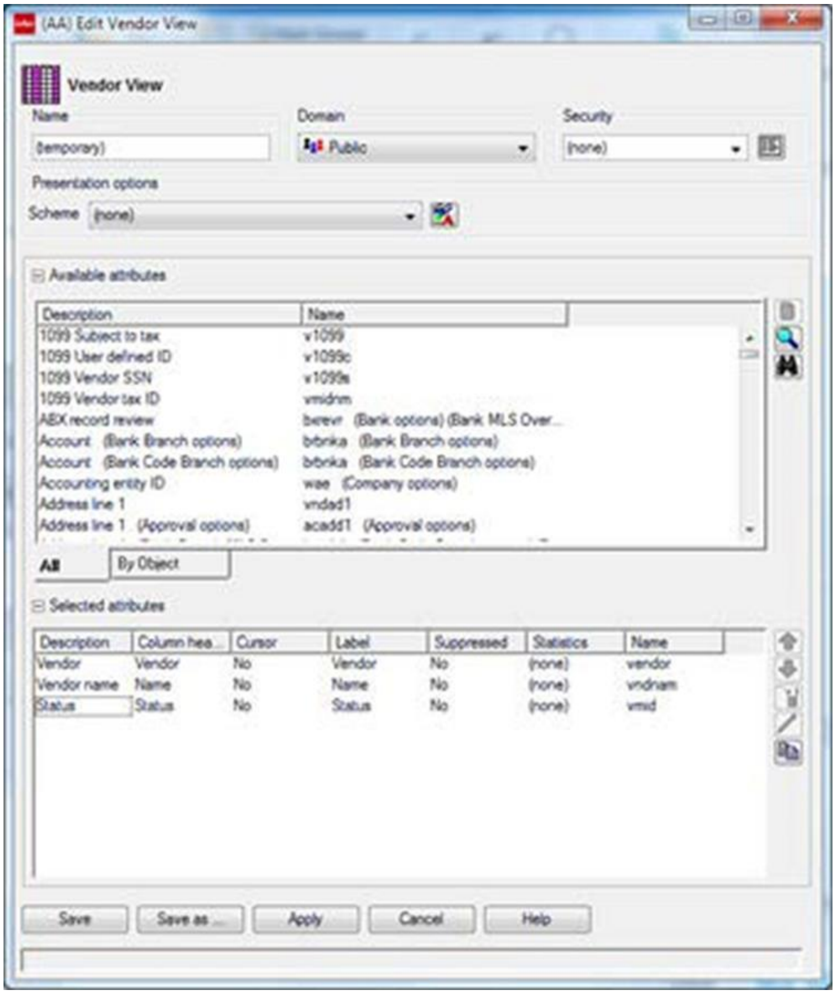


```
AMZB6DFR                       Maintain Tasks                        DISPLAY

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

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

Opt  Task ID                    Type      App       Locked
 __  VIEWS      MNTPRIVATE      SEC       IDF          Y
     Maintain Private Views
 __  VIEWS      MNTPUBLIC       SEC       IDF          Y
     Maintain Public Views
 __  VIEWS      MNTTEMP         SEC       IDF          Y
     Maintain Temporary Views
 __  VIEWS      MNTUSER         SEC       IDF          N
     Maintain User Owned Public Views
 __  WRKBENCHES MNTPRIVATE      SEC       IDF          N
     Maintain Private Workbenches                                          +


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

MA     A                 MW                                           04/030
```

3902 - Session successfully started

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

For the example, we will create a temporary view:



Vendor View

Name: (temporary)

Domain: Public

Security: (none)

Presentation options

Scheme: (none)

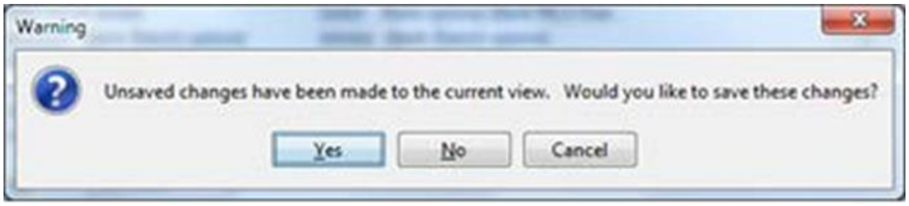
Available attributes

Description	Name
1099 Subject to tax	v1099
1099 User defined ID	v1099c
1099 Vendor SSN	v1099s
1099 Vendor tax ID	vmidnm
ABX record review	bxrevr (Bank options) (Bank MLS Over...
Account (Bank Branch options)	bfbnka (Bank Branch options)
Account (Bank Code Branch options)	bfbnka (Bank Code Branch options)
Accounting entity ID	wae (Company options)
Address line 1	vndad1
Address line 1 (Approval options)	acadd1 (Approval options)

Selected attributes

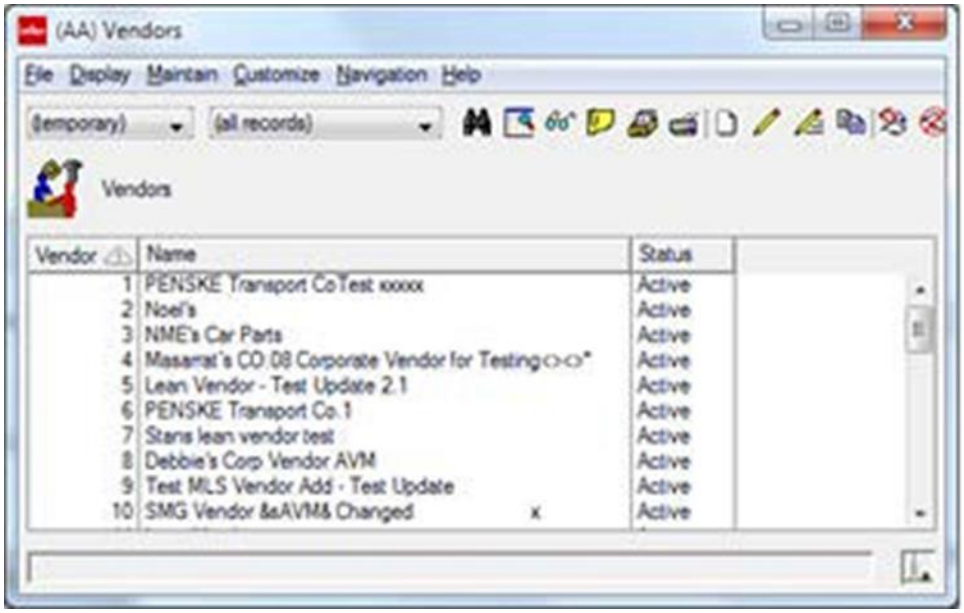
Description	Column hea...	Cursor	Label	Suppressed	Statistics	Name
Vendor	Vendor	No	Vendor	No	(none)	vendor
Vendor name	Name	No	Name	No	(none)	vndnam
Status	Status	No	Status	No	(none)	vmid

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



Unsaved changes have been made to the current view. Would you like to save these changes?

The temporary has been used:

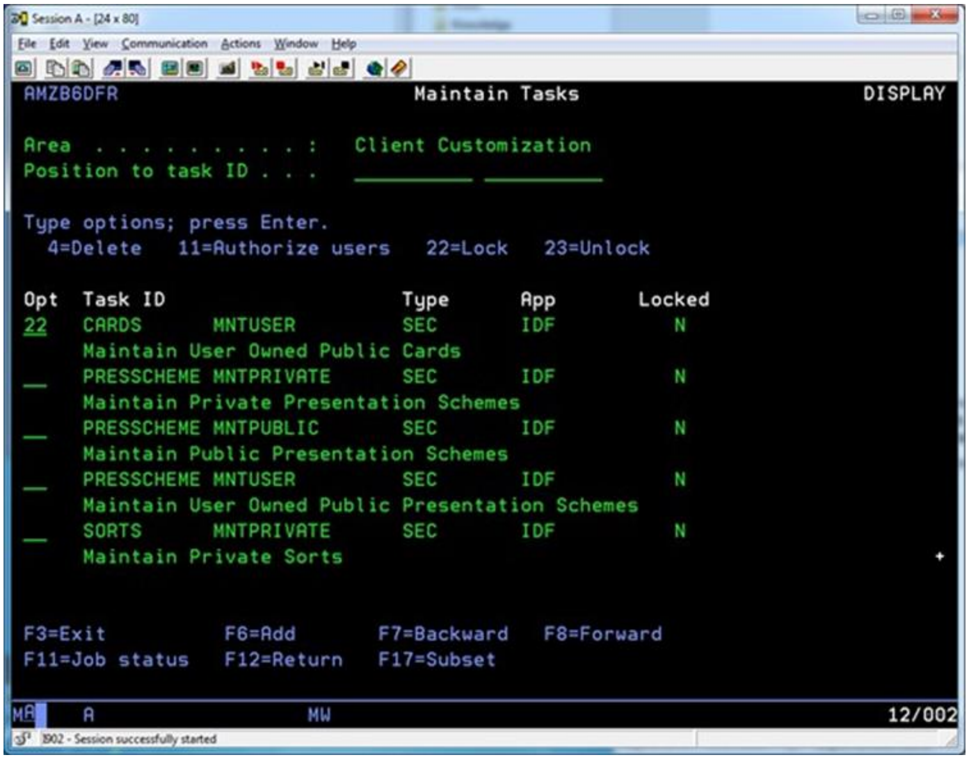


Vendor	Name	Status
1	PENSKE Transport CoTest xxxxx	Active
2	Noel's	Active
3	NME's Car Parts	Active
4	Masarrat's CO 08 Corporate Vendor for Testing<><>*	Active
5	Lean Vendor - Test Update 2.1	Active
6	PENSKE Transport Co.1	Active
7	Stans lean vendor test	Active
8	Debbie's Corp Vendor AVM	Active
9	Test MLS Vendor Add - Test Update	Active
10	SMG Vendor &aAVM& 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.**

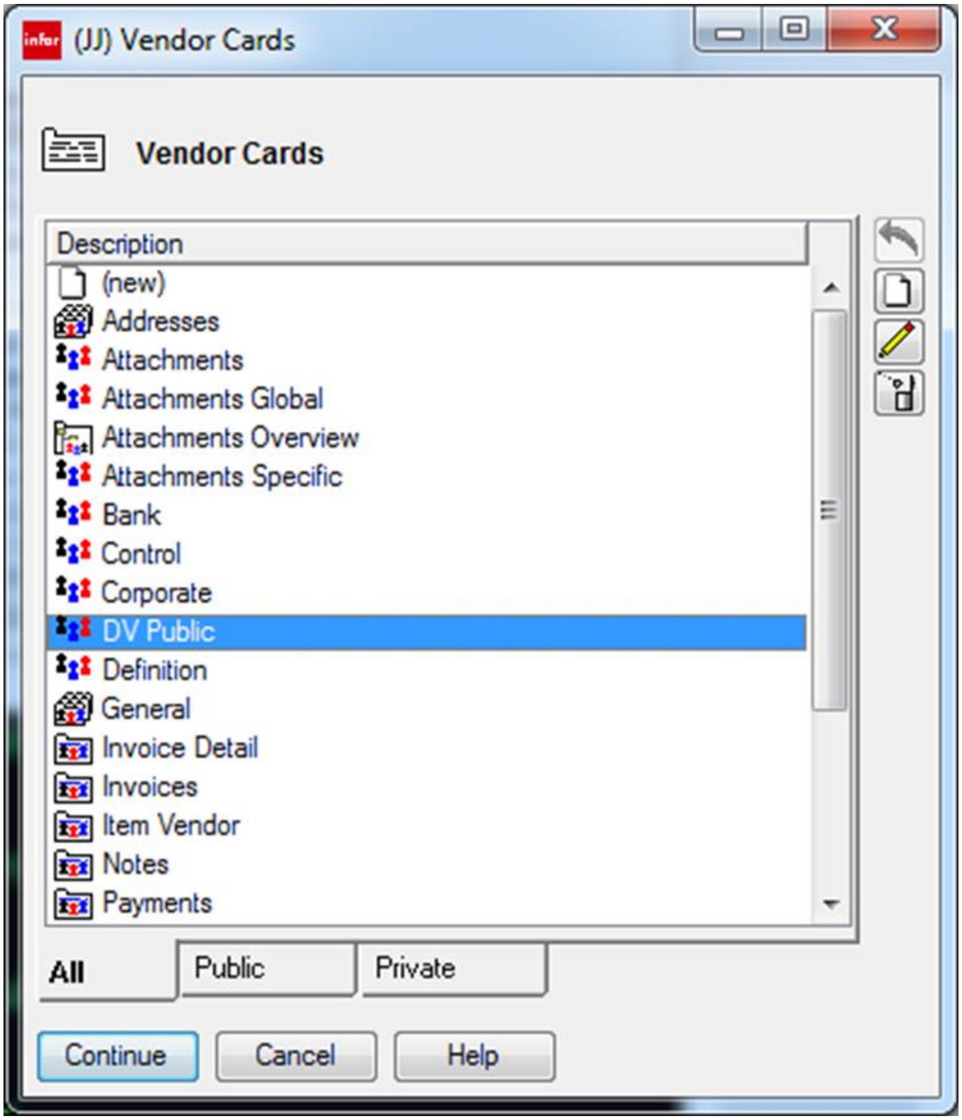
To activate the security use option 22 for these two tasks. Then, specify **11** to select the individual users that should have access to this function.

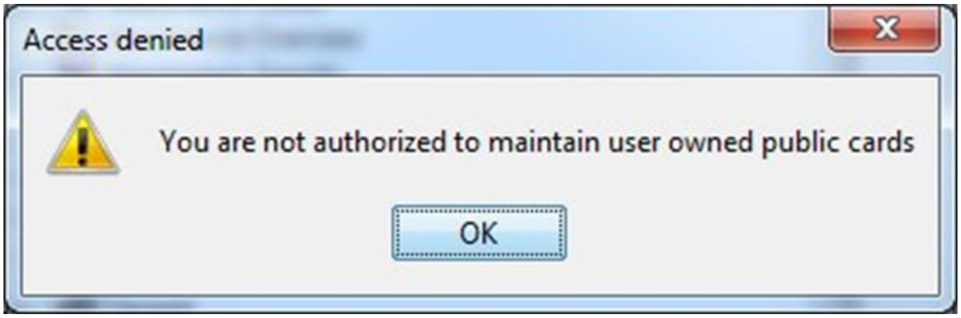


```
 AMZB6DFR                         Maintain Tasks                          DISPLAY

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

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

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


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

 MA     A                   MW                                        12/002
```

1902 - Session successfully started

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





You are not authorized to maintain user owned public cards

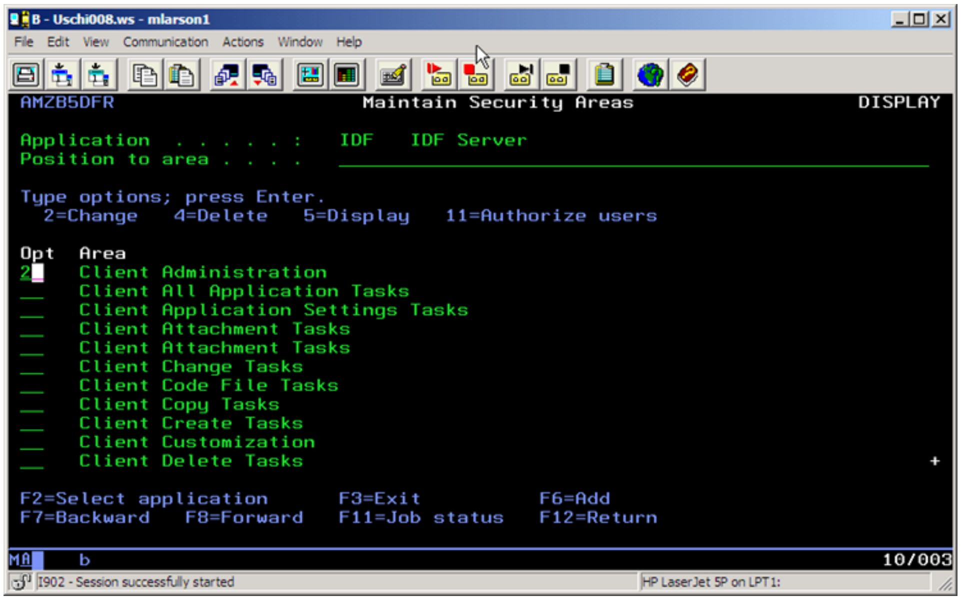
Chapter 10 Preventing end users from using Link Manager

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

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

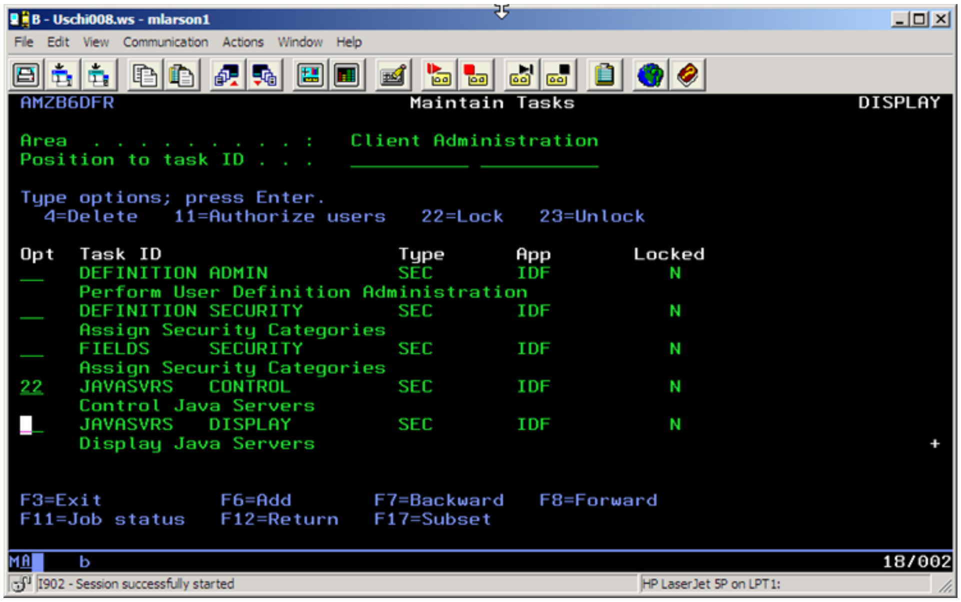
2 Specify **1** for Area and task authorizations.

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


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.

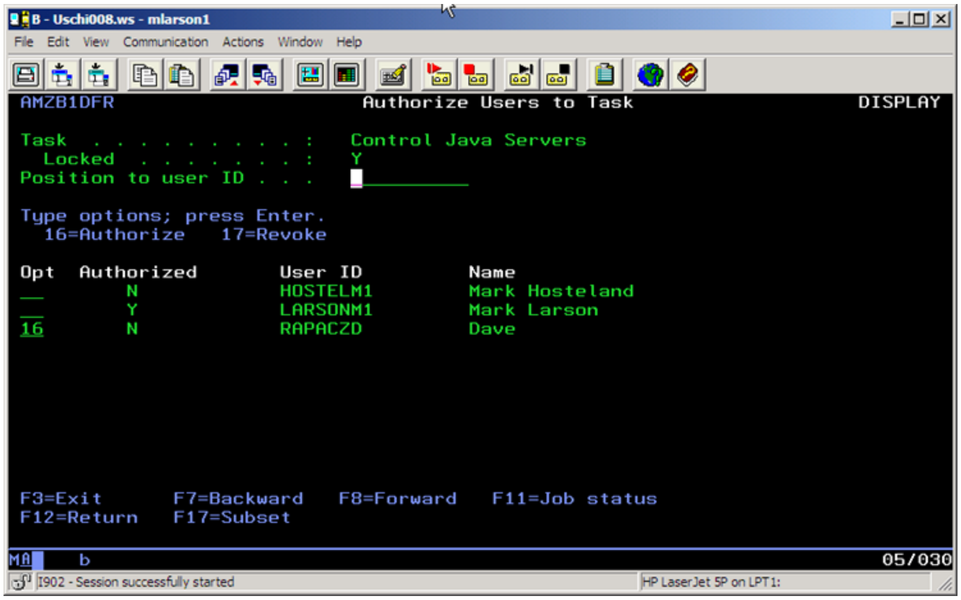


B - Uschi008.ws - mlarson1
File Edit View Communication Actions Window Help

```
 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

```
 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
```

I902 - Session successfully started
HP LaserJet 5P on LPT1:

Chapter 11 Secure IDF object's tasks

LX 8.3.5 IDF objects do not use CAS security, they use Deployment Profiles. However, other products do use CAS Security. 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 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:

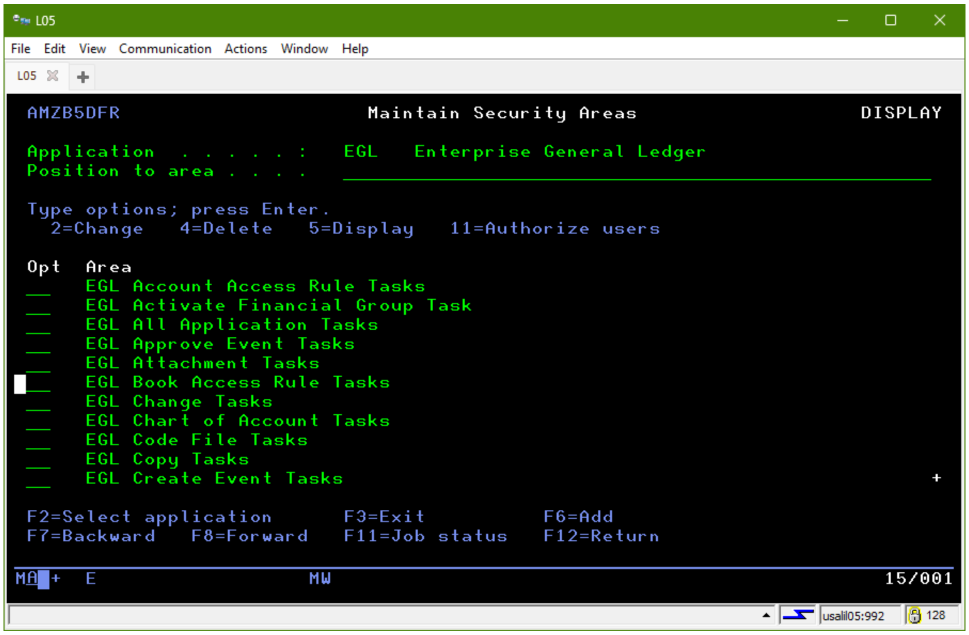
CRM Customer Relationship Management

CSM Customer Service Management

For EGLi use the following product applications to secure objects:

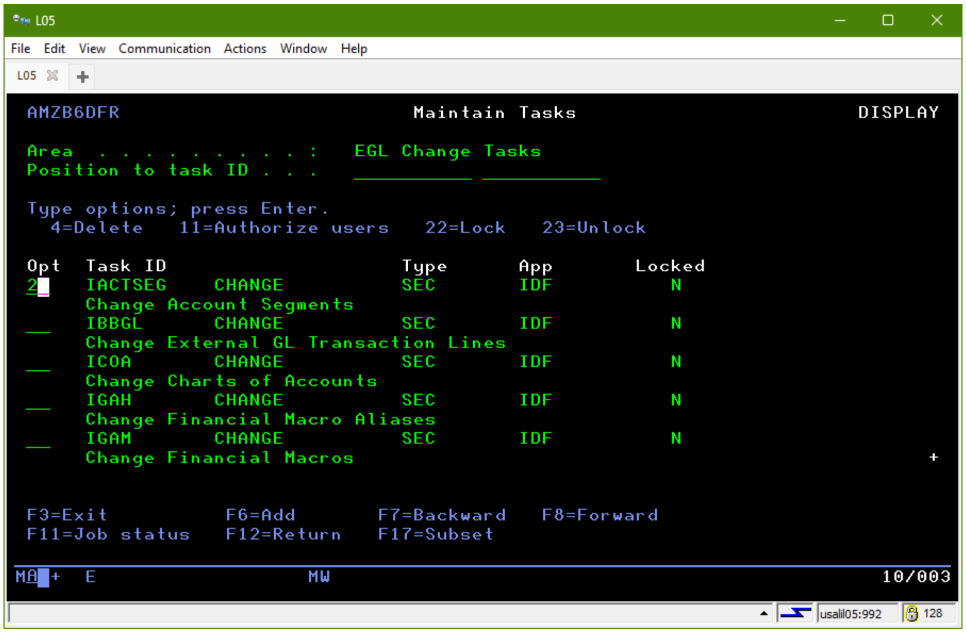
EGL Enterprise General Ledger

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



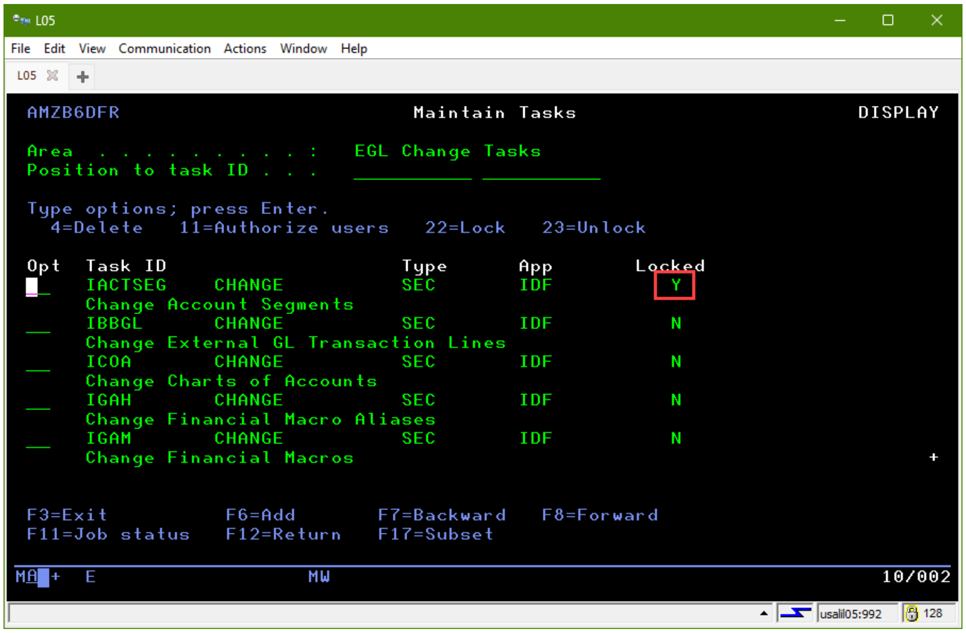
```
AMZB5DFR                    Maintain Security Areas                     DISPLAY

Application  . . . . . :   EGL   Enterprise General Ledger
Position to area . . . .   __________________________________________________

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

Opt  Area
__   EGL Account Access Rule Tasks
__   EGL Activate Financial Group Task
__   EGL All Application Tasks
__   EGL Approve Event Tasks
__   EGL Attachment Tasks
__   EGL Book Access Rule Tasks
__   EGL Change Tasks
__   EGL Chart of Account Tasks
__   EGL Code File Tasks
__   EGL Copy Tasks
__   EGL Create Event Tasks                                                   +

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

MA + E                    MW                                               15/001
```

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



```
AMZB6DFR                         Maintain Tasks                       DISPLAY

Area . . . . . . . . . . :   EGL Change Tasks
Position to task ID . . .    __________ __________

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

Opt  Task ID                    Type      App       Locked
2    IACTSEG     CHANGE         SEC       IDF          N
     Change Account Segments
__   IBBGL       CHANGE         SEC       IDF          N
     Change External GL Transaction Lines
__   ICOA        CHANGE         SEC       IDF          N
     Change Charts of Accounts
__   IGAH        CHANGE         SEC       IDF          N
     Change Financial Macro Aliases
__   IGAM        CHANGE         SEC       IDF          N
     Change Financial Macros                                           +


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

MA + E                  MW                                          10/003
```

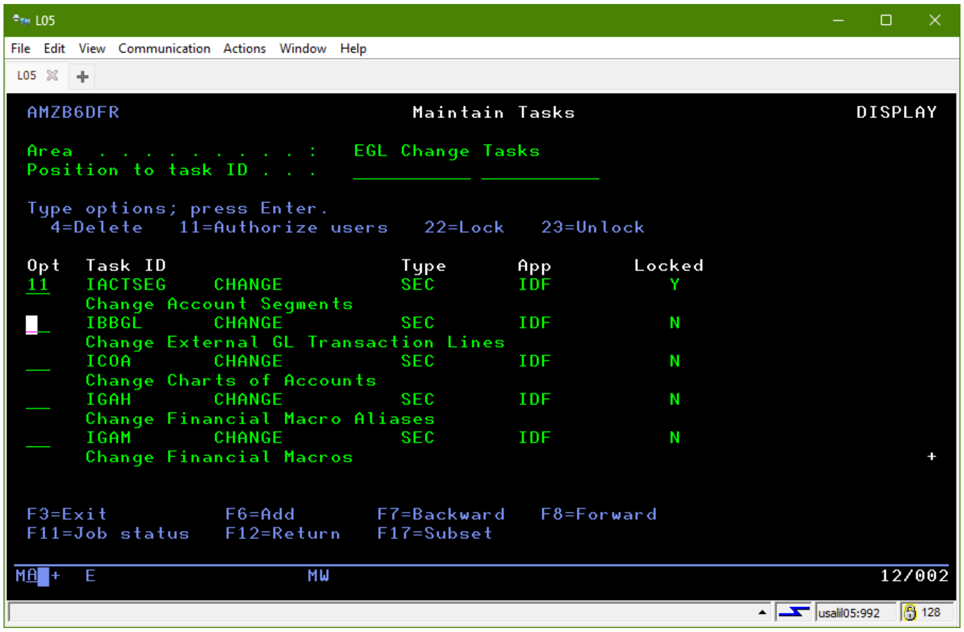
7 Use option **22=Lock** to activate task's security. The Locked flag is set to **Y**.



```
AMZB6DFR                         Maintain Tasks                       DISPLAY

Area . . . . . . . . . . :   EGL Change Tasks
Position to task ID . . .    __________ __________

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

Opt  Task ID                    Type      App       Locked
_    IACTSEG     CHANGE         SEC       IDF          Y
     Change Account Segments
__   IBBGL       CHANGE         SEC       IDF          N
     Change External GL Transaction Lines
__   ICOA        CHANGE         SEC       IDF          N
     Change Charts of Accounts
__   IGAH        CHANGE         SEC       IDF          N
     Change Financial Macro Aliases
__   IGAM        CHANGE         SEC       IDF          N
     Change Financial Macros                                           +


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

MA + E                  MW                                          10/002
```

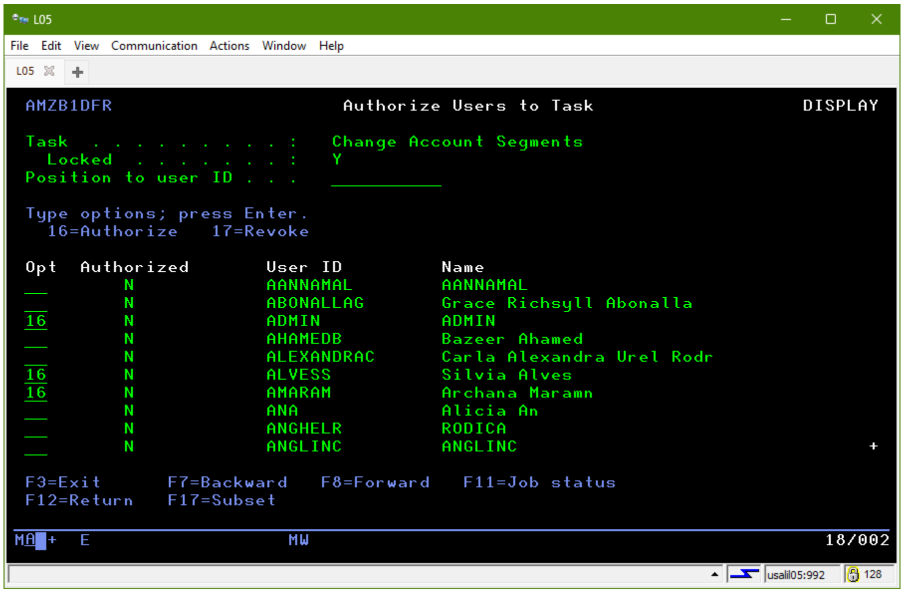
As a result, the User will not be able to execute this task. In this example, user will not be able to open Enterprise Item object.

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



```
AMZB6DFR                      Maintain Tasks                          DISPLAY

Area . . . . . . . . . . :  EGL Change 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   IACTSEG     CHANGE         SEC       IDF          Y
     Change Account Segments
__   IBBGL       CHANGE         SEC       IDF          N
     Change External GL Transaction Lines
__   ICOA        CHANGE         SEC       IDF          N
     Change Charts of Accounts
__   IGAH        CHANGE         SEC       IDF          N
     Change Financial Macro Aliases
__   IGAM        CHANGE         SEC       IDF          N
     Change Financial Macros                                              +


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

MA + E                        MW                                      12/002
```

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



```
AMZB1DFR                 Authorize Users to Task                  DISPLAY

Task . . . . . . . . . . :  Change Account Segments
  Locked . . . . . . . . :  Y
Position to user ID . . .   __________

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

Opt  Authorized          User ID          Name
__       N               AANNAMAL         AANNAMAL
__       N               ABONALLAG        Grace Richsyll Abonalla
16       N               ADMIN            ADMIN
__       N               AHAMEDB          Bazeer Ahamed
__       N               ALEXANDRAC       Carla Alexandra Urel Rodr
16       N               ALVESS           Silvia Alves
16       N               AMARAM           Archana Maramn
__       N               ANA              Alicia An
__       N               ANGHELR          RODICA
__       N               ANGLINC          ANGLINC                       +

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

MA + E                     MW                                     18/002
```

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 Areas that have these tasks:

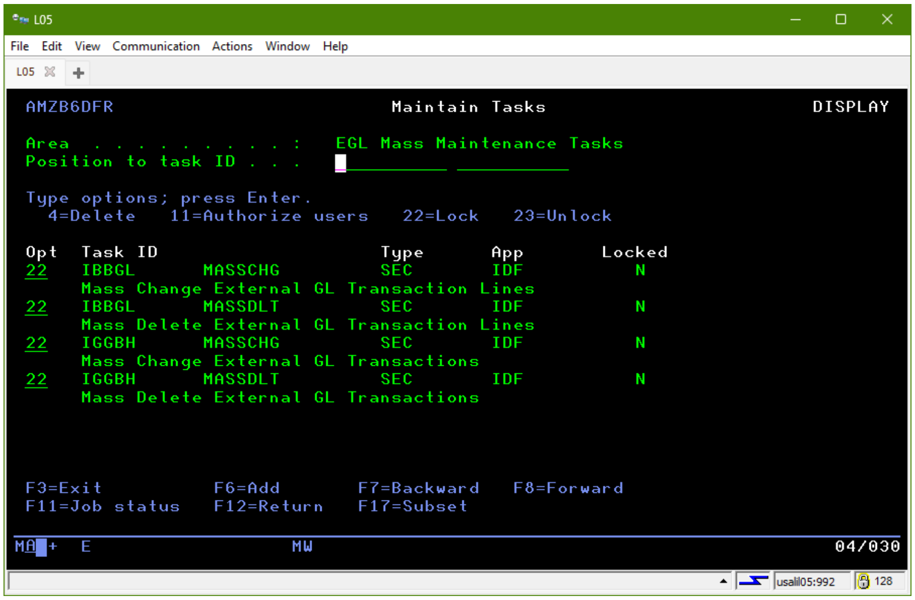
EGL Mass Maintenance Tasks

CRM Mass Maintenance Tasks

STTi Mass Maintenance Tasks

Client Mass Maintenance Tasks

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 . . . . . . . . . . :   EGL Mass Maintenance Tasks
 Position to task ID . . .    __________ __________

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

 Opt  Task ID                Type      App       Locked
 22   IBBGL      MASSCHG      SEC       IDF           N
      Mass Change External GL Transaction Lines
 22   IBBGL      MASSDLT      SEC       IDF           N
      Mass Delete External GL Transaction Lines
 22   IGGBH      MASSCHG      SEC       IDF           N
      Mass Change External GL Transactions
 22   IGGBH      MASSDLT      SEC       IDF           N
      Mass Delete External GL Transactions



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

MA +  E                    MW                                          04/030
```

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:

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 Deployment Profiles for each user's authorizations it finds in LX security for users in SYS600.

See "Appendix A LX to IDF Security Cross Reference" on page 45 for details on the files used by CPYSECIDF to map LX programs and products to IDF Business Objects.

Acquiring and installing the CPYSECIDF tool

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

Extract the CPYSECIDF SAVF from the zip file and upload to your IBM i system, then restore the CPYSECIDF 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 CPYSECIDF library to your *LIBL ADDLIBLE CPYSECIDF

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 to import or *ALL
REPLACE	*YES or *NO to replace security already imported for the named user(s).
PROFILES	Select *YES to create IDF deployment profiles based on LX user security and assign IDF users to the profiles. Management of deployment profiles requires Infor Integrator. If an LX user is not authorized to any LX products or programs that are related to IDF Business Objects then a deployment profile will be created that has no Business Objects assigned. This will allow users to log into the IDF environment, but they will not have access to any of the LX Inquiry Business Objects. Select *NO to bypass deployment profile processing.
INACTIVE	When copying users from LX to IDF if a user record is found in LX that is inactive (delete action in SYS600 was taken) then there are two options for how this user will be handled in IDF. Select *DELETE to delete the user in IDF if it exists. Select *RETAIN to leave the user in IDF if it exists.

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

8 Two 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 Start a Power-Link session and add the new environment.

10 Open the User business object to make any desired changes.

Dynamically executing the CPYSECIDF tool

With the User Provisioning capability added to LX 8.3.5 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 CPYSECIDF, or command CPYSECIDF and all of its supporting objects must be copied from library CPYSECIDF to one of the libraries already in the LX library list.

Appendix A LX to IDF Security Cross Reference

LX security is mapped to IDF business objects so that Deployment Profiles can be created.

Uses the CPYSECIDF/XISXR file. The product and program authorities relate to settings in SYS600 to access each business object. Editing this file is limited as the business objects require a key value that is not available for other objects.

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.