X-Analysis  
User Authorities

Software version 13.3.01, 20230403

Contents

[Contents 2](#_Toc131161971)

[Publication Information 3](#_Toc131161972)

[Preface 4](#_Toc131161973)

[About this guide 4](#_Toc131161974)

[Version 4](#_Toc131161975)

[How to use this guide 4](#_Toc131161976)

[What is new in the latest release? 5](#_Toc131161977)

[Managing User Authorities 6](#_Toc131161978)

[Set the Library list 7](#_Toc131161979)

[User Authority Scenarios 10](#_Toc131161980)

[X-Analysis Client 12](#_Toc131161981)

[Application Area Restrictions 14](#_Toc131161982)

[Securing XREFMENU command and programs that modify the X-Analysis authorities 16](#_Toc131161983)

[Protecting the XUSRPRF table 17](#_Toc131161984)

[Index 18](#_Toc131161985)

Publication Information

© 2023 Fresche Solutions Inc.

**Published by:**

Fresche Solutions Inc.  
995 Wellington Suite 200  
Montreal, QC  
Canada, H3C 1V3

Telephone numbers:

(514) 747.7007  
(toll-free in US and Canada): 1.800.361.6782  
(toll-free in Belgium, France, Germany, UK): 00 800 361 67 82 0  
(toll-free in Australia): 0011 800 361 6782 0

E-mail for support: [support@freschesolutions.com](mailto:support@freschesolutions.com?subject=Support)

E-mail for inquiries: [info@freschesolutions.com](mailto:inquiry@freschesolutions.com?subject=inquiry)

Web: [www.freschesolutions.com](http://www.freschesolutions.com/)

Title: X-Analysis User Authorities, software version 13.3.01

Publication Date: April 2023

**Trademarks**

X-Analysis and X-Analysis Professional are trademarks or registered trademarks of Fresche Solutions Inc. <iSeries, Power Systems, Power8> are registered trademarks of IBM Corporation. Microsoft and Microsoft Windows are registered trademarks of Microsoft Corporation. All other brand and product names are trademarks or registered trademarks of their respective companies.

No part of this document may be reproduced or transmitted in any form or by any means, without prior permission in writing from Fresche Solutions.

The information in this manual is believed to be correct at the time of publication. However, Fresche Solutions Inc. makes no warranty, express or implied, about the accuracy of this information and reserves the right to revise this document or make changes to the products described herein at any time without notice and without obligation. Fresche Solutions Inc. is not liable for any loss of data, damage to databases or other software, or any other losses arising from the use of this manual.

Preface

About this guide

This guide, X-Analysis User Authorities, describes how to set specifications depending on the user. The following topics are discussed:

* Managing User Authorities
* Design and Security level settings
* Application area restrictions

Version

This guide describes X-Analysis User Authorities, Software version 13.3.01.

How to use this guide

This guide has one chapter. It has three sections dedicated to the user authorities, design and security levels, and other specifications restricting user access at the application area level.

The X-Analysis suite of products contains a total of eight modules. This guide only covers the following module: X-Analysis User Authorities. For information about the other modules, please contact your Fresche Solutions representative, or visit us at:  
<https://freschesolutions.com/products/x-analysis-suite/>

What is new in the latest release?

|  |  |
| --- | --- |
|  | For this release, we updated this Help. This release has the following changes: |

* Replaced all the existing X-Analysis Server screens with the new 5250 Emulator screens.

Managing User Authorities

This section explains how an administrator can control the user authorities and access the different X-Analysis features. The user can check/modify the user authorities from the “Work with X-Analysis/4 Applications” interface.

Start 5250 session on the IBM i server.

Set the Library list

Most importantly, ensure that the library list is correctly set in the following sequence:

**XAPROD**  
**QGPL**  
**QTEMP**

Use the EDTLIBL command on the IBM i to set the library list. Refer to the Edit Library List screen below that displays the correct libraries and sequence:

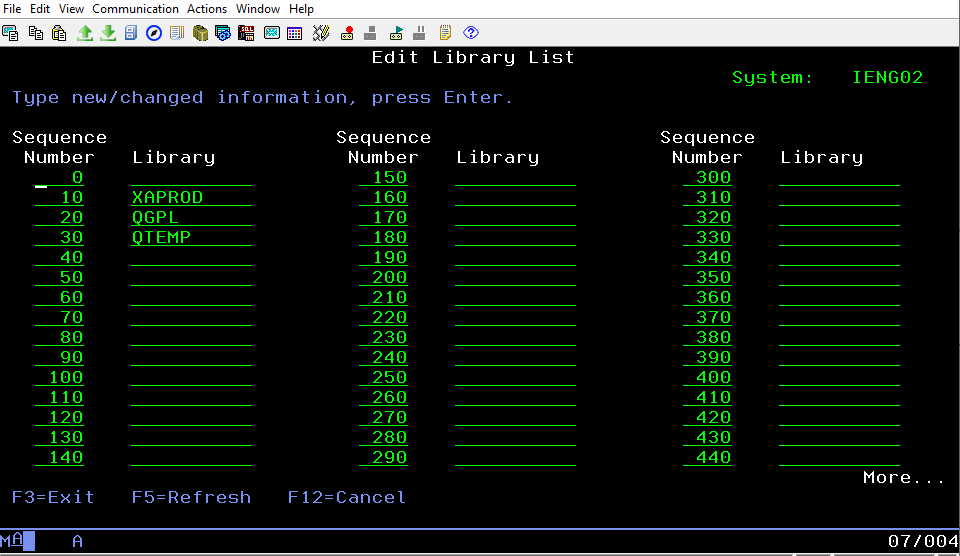


Fig. 1.1.1 – EDTLIBL command screen

Now return to the main command screen and type master command XREFMENU and press ENTER. This command manages all the X-Analysis repositories. The following screen gets displayed.

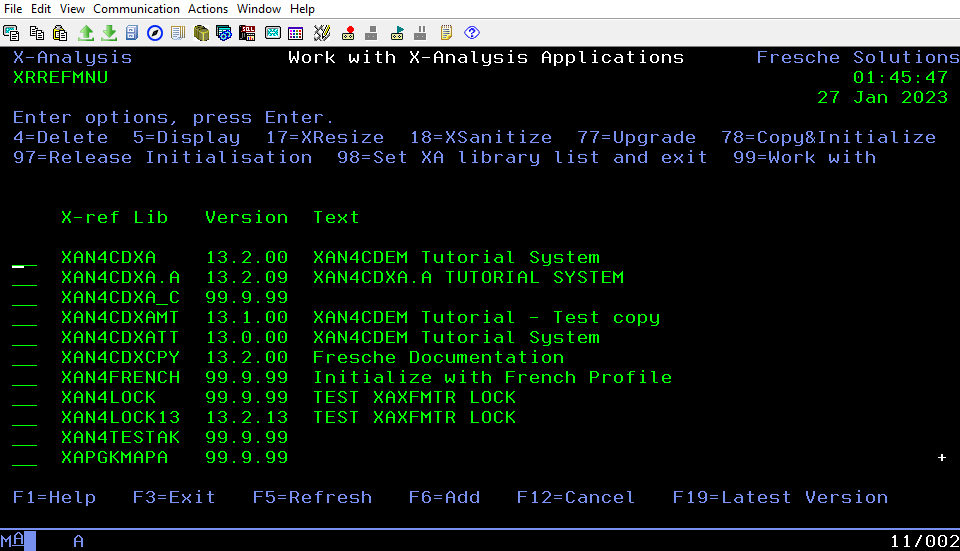


Fig. 1.1.2 – XREFMENU Command Screen

Select option 99 on the X-Ref library you want to work with, and press ENTER.

The following screen displays the Work with X-Analysis/4 Applications interface.

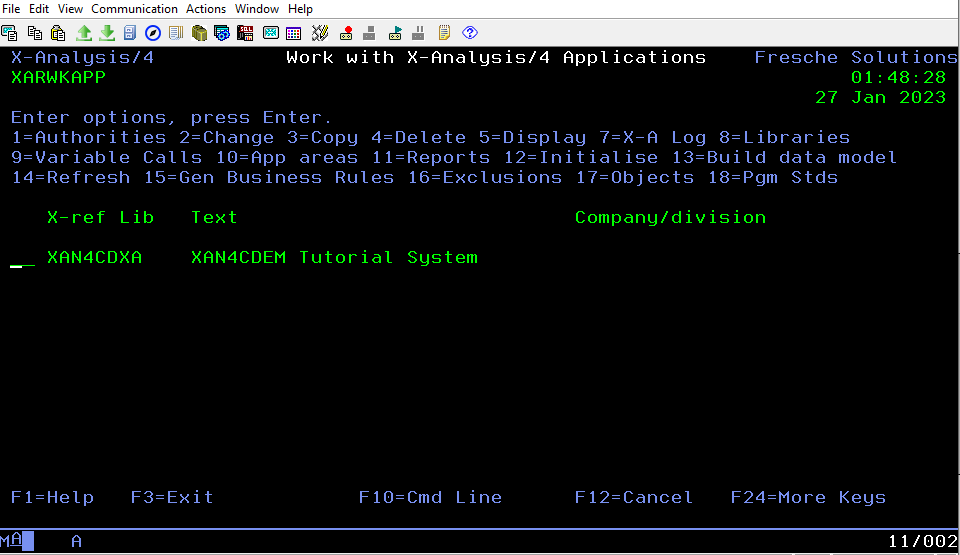


Fig. 1.1.3 – Work with X-Analysis/4 Applications interface

Select Option 1 against the selected tutorial application and press ENTER.

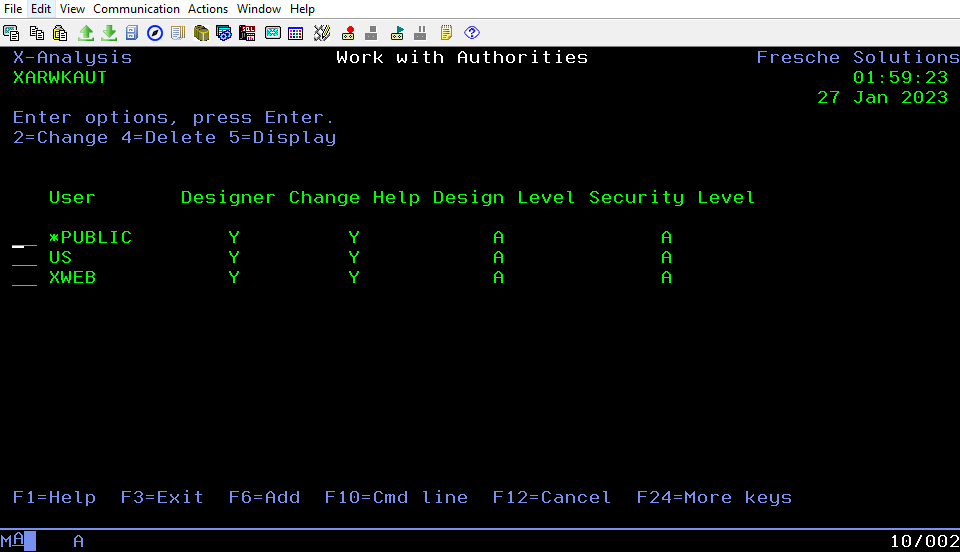


Fig. 1.1.4 – Work with Authorities

The screen facilitates maintaining the following authority information:

1. User  
   Name of the user to whom the specified authorities apply. XA4INIT includes three entries here: US, XWEB, and \*PUBLIC.
2. Designer  
   This field is currently not in use. Changing the value does not have any effect.
3. Change Help  
   This field is currently not in use. Changing the value does not have any effect.
4. Design level  
   This field identifies the authority level assigned to the user.  
   Select one of:
   * ‘A’ – The user has access to all X-Analysis features.
   * Blank limits the use of the X-Analysis features.
5. Security level  
   This field identifies the security level assigned to the user.  
   Select one of:
   * ‘A’ – The user has all security rights.
   * Blank limits the use of the X-Analysis features.

User Authority Scenarios

There are the two scenarios regarding setting the user authorities to access the X-Analysis features:

1. Default entries– Set the default user authority to \*PUBLIC. It means that both the Design Level and the Security Level are set to ‘A’. It implies that all the users have full access to use the X-Analysis repository.

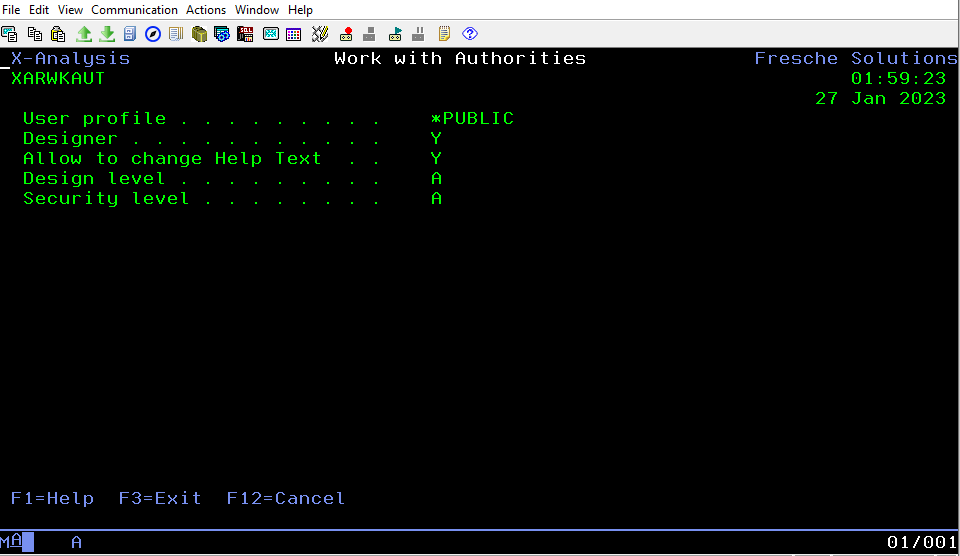


Fig. 1.2.1 – Work with Authorities

1. Restrict User Profile:
   * To prevent users from using X-Analysis, delete the \*PUBLIC user. The user profiles that are named on this list will be able to use this repository. If this is done for all repositories, then unspecified users cannot use X-Analysis.

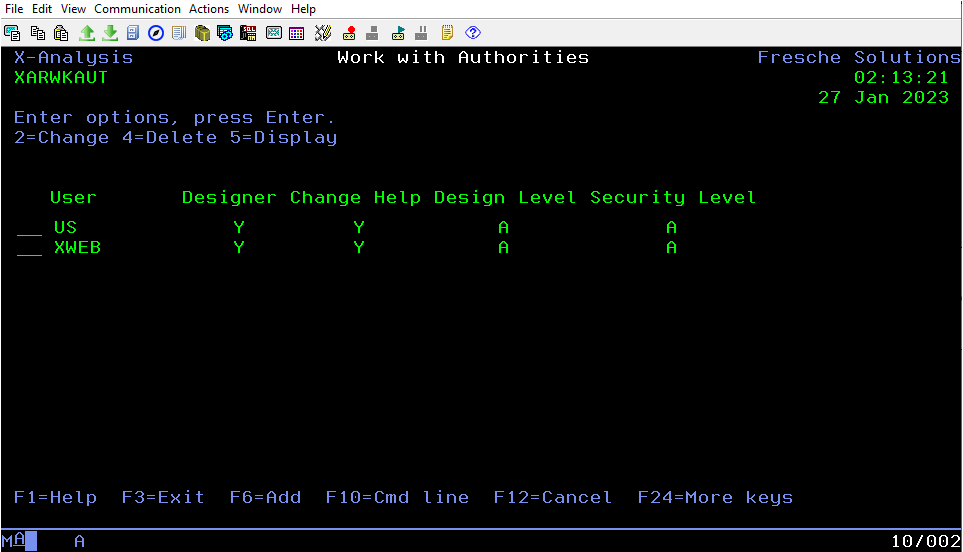


Fig. 1.2.2 – Work with Authorities

* + Change the Design Level and Security Level for \*PUBLIC from ‘A’ to blank. This limits the X-Analysis features for the general users and allows only partial access to the X-Analysis repository.

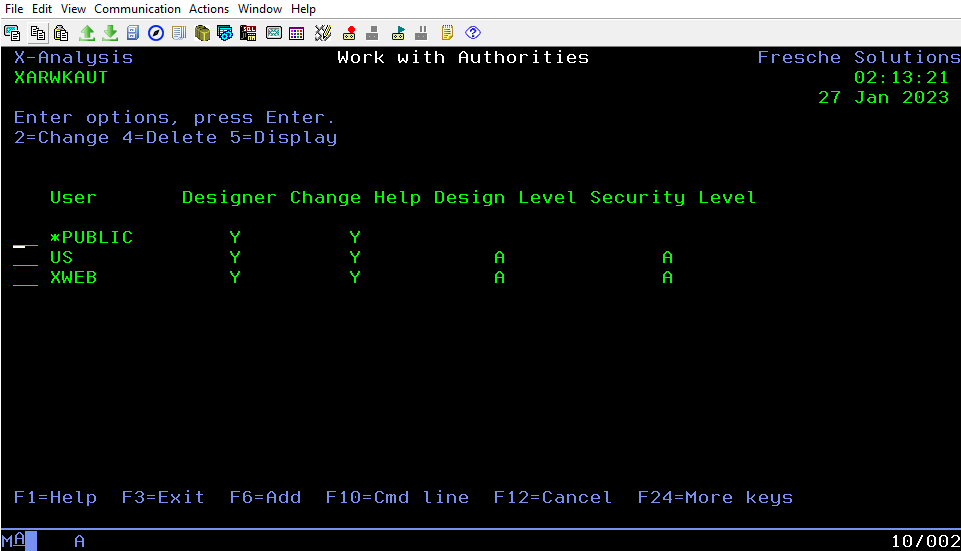


Fig. 1.2.3 – Work with Authorities

* + Designate a user with the Design Level and Security Level set to ‘A’. This allows the user to have full access to the X-Analysis repository.

X-Analysis Client

The Design and Security Level settings control various X-Analysis features as follows:

|  |  |
| --- | --- |
|  | The options listed below as ‘disabled’ assume that the user is entitled to the complete License available for all X-Analysis product sets. |

**Design Level**

The following options are only allowed on the cross-reference context menu when the Design Level is set to ‘A’:

* New Application Area
* Derive Business Rules
* Export Options
  + Export as DDL
  + Export as Web Query Metadata
  + Export as Web Query Application
  + Convert DDS to SQL
  + Generate Database Server Programs
  + Export CRUD Spreadsheet
* Database Migration
* Inter-Repository Options
  + Manage Linked Repositories
* Audit Options
  + Initialize Source Archiving
  + Generate Metrics Analysis
  + Generate Problem Analysis
* Refresh Options
  + Refresh Cross-Reference
  + Rebuild Data Model

The following options are only allowed on the object context menu when the Design Level is set to ‘A’ .

|  |  |
| --- | --- |
|  | The options listed below are based on complete license authority and the All Objects list. |

* Application Area Options
  + Add to Application Area
  + Add to Application Area with Related Objects
  + Omit from Application Area
* Modernization Options
  + Reengineer Programs
* Derive Business Rules

The following options are only allowed on the Application Area context menu when the Design Level is set to ‘A’.

* Test Management Options
  + Create Checkpoint Definition
  + Create Test Result Definition
  + Create Test Process Definition
  + Test Result Field Execution

|  |  |
| --- | --- |
|  | Application Area and Cross-reference context menus share some menu options and the same behavior. |

**Security Level**

The following options are only allowed when the Security Level is set to ‘A’:

* Source, Flowchart and Business Rules inclusion in the System Document.

Application Area Restrictions

X-Analysis has the provision to restrict user access at the application area level. The users who have the appropriate authorities on the specific application area can edit the application area description or add/remove objects from any application area.

The application area user level authorities for the individual users can be maintained from the IBM i screen) (that is, reached via XREFMENU -> 99 -> X4WRKAPP -> 10 -> 15).

The X-Analysis client first checks the user level authority. If it is not found, the \*PUBLIC authority is checked for that application area to decide whether, the user can perform operation on that application area or not.

When the application area authority is set to ‘Y’, users can perform the following operations:

* Update Application Area
* Application Area Rules
* Add to Application Area
* Omit from Application Area

To apply the application area restrictions:

* Log in to the IBM i session and add the XAPROD and XAOBJXXXXX library to the library list. Through the master command XREFMENU screen, select option 99 to work with an X-ref library. Then from the X4WRKAPP screen, select option 10 for application areas.
* Press ENTER. The application areas under the X-Ref will be displayed.

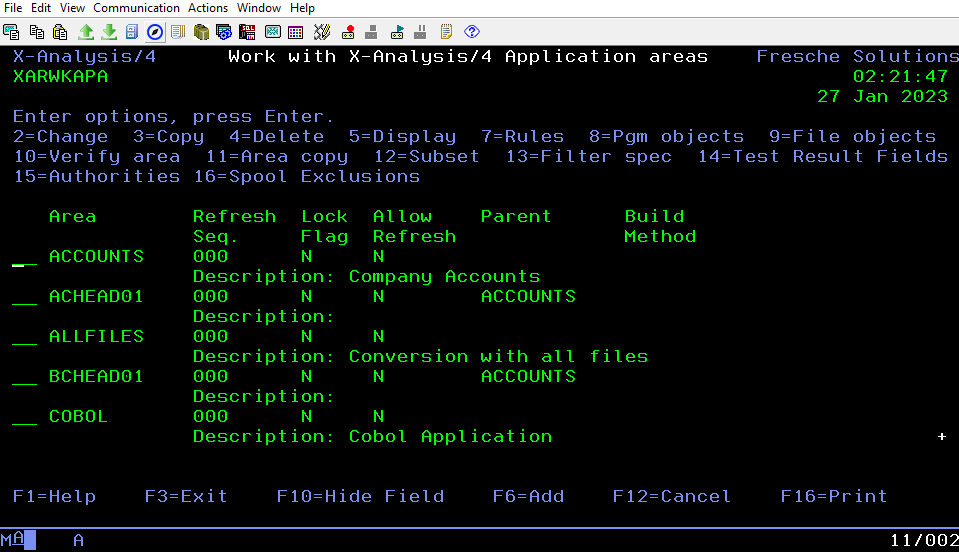


Fig. 1.3.1 – Work with X-Analysis/4 Applications

* Select Option 15 to display User Authorities for an application area and press ENTER. The Work with Application Area Authorities screen are displayed.
* Press F6 to add the Authorities (individual or \*PUBLIC) on the Work with Application Area Authorities screen.

In the screen below, the \*PUBLIC profile is set to have all the authorities (that is, Display, Update, and Delete). Press ENTER to confirm adding the Authorities.

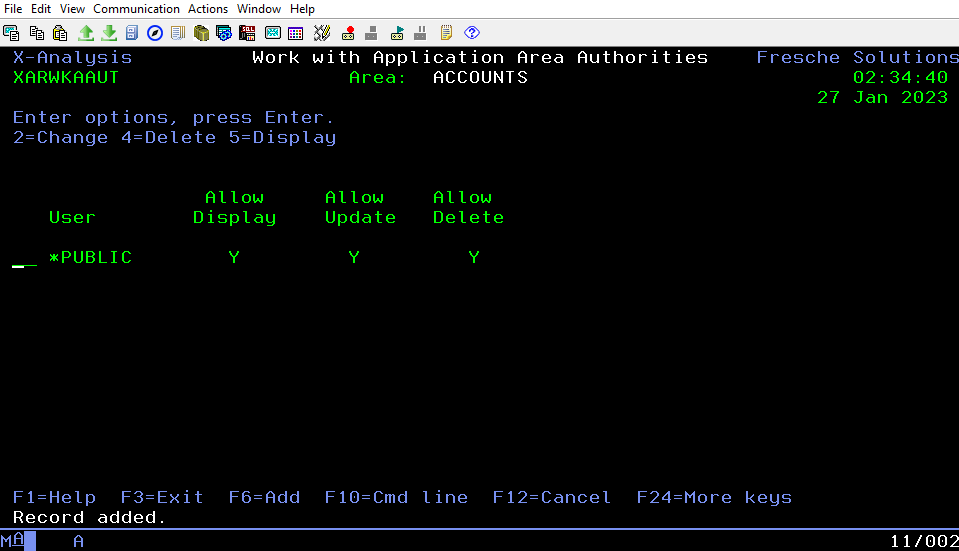


Fig. 1.3.2 – Work with Application Area Authorities

* Select Option 2 to change authorities to ‘Y’ or ‘N’. Based on the application area authorities entered, the Application Area Options (related to updates or deletions) on the GUI will appear as enabled or disabled.

|  |  |
| --- | --- |
|  | If all the authorities are entered as ‘N’, the application area will not show up on the GUI. |

Securing XREFMENU command and programs that modify the X-Analysis authorities

From version 13.2.15, a new feature gets introduced where X-Analysis applications and Application Area authorities get secured from the modification using the XREFMENU command.

To perform this feature new authorization list named XAADMLST is now used on the programs changing the authorities.

The programs called by the following XREFMENU command should be restricted by the authorization list XAADMLST:

* XACWKAUT and XARWKAUT: From Option 1=Authorities of XARWKAPP (Work with application)
* XARWKAAUT: From Option=15 Authorities of XARWKAPA (Work with Application area)

During X-Analysis installation these programs will be secured under authorization list XAADMLST. The authorization list XAADMLST will have a default entry, i.e., setting the default user authority to \*PUBLIC for compatibility.

If the user requires to change X-Analysis authorities. In that case user must have \*RUN to administer the authorities (execute the programs). To secure, remove \*RUN from the user-defined authorization list XAADMLST.

By removing \*RUN, the user will get an error while invoking the options 1=Authorities or 15=Authorities.

|  |  |
| --- | --- |
|  | If a non-authorized user attempt to use any of the XREFMENU options that he is not authorized to, i.e., which are restricted by the authorization list XAADMLST, an error message gets displayed related to the restriction, and no changes gets take place. |

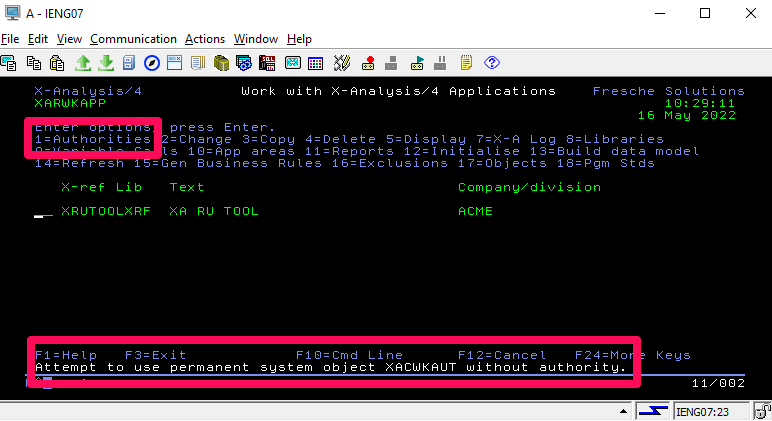


Fig. 1.4.1 – Error message displayed for non-authorized User

After installing X-Analysis for the first time or installing a new version of X-Analysis with this feature for the first time, no change in the behavior of X-Analysis should impact any users until the administrator of X-Analysis alters the definition of the XAADMLST authorization list. But, upgrading to a new version of X-Analysis should retain the previous installation process.

Protecting the XUSRPRF table

X-Analysis users can now protect the Application Authority table XUSRPRF by using the authorization list XAADMAPLST. This protection of the Application Authority table has some limitation mentioned below at the table / file level.

At X-Analysis installation, this authorization list XAADMAPLST will have default user authority, including \*PUBLIC set to \*ALL for compatibility.

If a user wants to change the X-Analysis authorities (change the table) must have \*ALL to administer the authorities. To secure this, change the user authority from \*ALL to \*USE in the authorization list XAADMAPLST.

|  |  |
| --- | --- |
|  | Limitation: To have the XUSRPRF table readable, all X-Analysis users must have \*USE in the user authority level. User having \*USE cannot Initialize, Upgrade, and Copy&Initialize the cross-reference. |

Index

5250 Emulator, 5

application area, 4, 12, 14, 16

Application Area Authorities, 15, 16

Application Area Options, 12, 15

Application Area Rules, 14

Audit Options, 12

Business Rules, 12

Checkpoint, 13

Client, 12, 14

data model, 12

DDL, 12

Design Level, 9, 10, 12

Export Options, 12

Flowchart, 13

IBM, 3, 6, 7, 14

IBM i, 6, 7, 14

Initialize, 12, 17

Initialize Source Archiving, 12

Inter-Repository Options, 12

Level, 4, 9, 10, 12, 14, 17

libraries, 7

Library List, 7, 14

Manage Linked Repositories, 12

metadata, 12

Metrics Analysis, 12

Problem Analysis, 12

repository, 10, 12

Security Level, 4, 9, 10, 12

Server, 5, 6, 12

SOURCE, 12

Suite of products, 4

Test Management Options, 13

Test Process, 13

user authorities, 1, 3, 4, 6, 10, 15

X-Analysis, 1, 3, 4, 5, 6, 7, 10, 12, 14, 16

X-Analysis Client, 12, 14

XAPROD, 7, 14

XREFMENU, 7, 14, 16