Security zSecure Visual
Version 2.1.0

Client Manual

SC27-5647-00

Security zSecure Visual
Version 2.1.0

Client Manual

SC27-5647-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 151.

September 2013

This edition applies to version 2, release 1, modification 0 of IBM Security zSecure Visual (product number 5655-N20) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

IBM® Security zSecure™ Visual enables administrators to manage mainframe security and administration from a Microsoft Windows workstation through a Windows interface to the mainframe server. IBM Security zSecure Visual has two components: IBM Security zSecure Visual Server and IBM Security zSecure Visual Client. This publication describes how to install, configure, and use IBM Security zSecure Visual Client.

Note: Information about setting up and configuring a Visual Server on a z/OS® system is available in the *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide*.

Intended audience

This publication is for administrators and system programmers responsible for RACF® administration and security.

Readers need to be familiar with RACF administrative tasks and using Microsoft Windows-based applications. This publication assumes that the IBM Security zSecure Visual server mainframe component is installed and configured.

What this publication contains

This publication contains these chapters:

- Chapter 1, "IBM Security zSecure Visual customization and primary tasks," on page 1

  Provides the basic operating procedures for using IBM Security zSecure Visual.
- Chapter 2, "RACF database operations," on page 19

  Describes the different options to work in the database.
- Chapter 3, "User management," on page 39

  Explains how IBM Security zSecure Visual manages users.
- Chapter 4, "Group management," on page 63

  Describes how IBM Security zSecure Visual manages groups.
- Chapter 5, "Connect management," on page 73

  Explains the connection relationship between users and groups.
- Chapter 6, "Resource management," on page 85

  Describes how to manage resource profiles.
- Chapter 7, "Segment management," on page 103

  Explains application segments and how to manage these segments.
- Chapter 8, "Running REXX scripts," on page 127

  Describes how to use the Visual Client interface to run a REXX script that is configured on the Visual Server.
- Chapter 9, "Maintenance," on page 129

  Describes how to maintain client definitions.
- Chapter 10, "Setup and configuration," on page 133

  Describes the installation, configuration, maintenance, and removal of IBM Security zSecure Visual from the client side.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security zSecure library."
- Links to "Online publications" on page viii.
- A link to the "IBM Terminology website" on page viii.

IBM Security zSecure library

The following documents are available online in the IBM Security zSecure library:

- *IBM Security zSecure Release information*

  For each product release, the release information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information for the IBM Security zSecure products. You can obtain the most current version of the release information at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.htm.

- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide*, SC27-5638

  Provides information about installing and configuring the following IBM Security zSecure components:

  – IBM Security zSecure Admin
  – IBM Security zSecure Audit for RACF, CA-ACF2, and CA-Top Secret
  – IBM Security zSecure Alert for RACF and ACF2
  – IBM Security zSecure Visual for RACF
  – IBM Tivoli® Compliance Insight Manager Enabler for z/OS

- *IBM Security zSecure Admin and Audit for RACF Getting Started*, GI13-2324

  Provides a hands-on guide introducing IBM Security zSecure Admin and IBM Security zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new users develop both a working knowledge of the basic IBM Security zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.

- *IBM Security zSecure Admin and Audit for RACF User Reference Manual*, LC27-5639

  Describes the product features for IBM Security zSecure Admin and IBM Security zSecure Audit. Includes user instructions to run the features from ISPF panels, RACF administration and audit user documentation with both general and advanced user reference material for the CARLa command language and the SELECT/LIST fields. This manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS component. This publication is only available to licensed users.

- *IBM Security zSecure Audit for ACF2 Getting Started*, GI13-2325

  Describes the IBM Security zSecure Audit for ACF2 product features and provides user instructions for performing standard tasks and procedures such as analyzing Logon IDs, Rules, and Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.

- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640

  Explains how to use IBM Security zSecure Audit for ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using ACF2 and accessing functionality from the

ISPF panels. For advanced users, the manual provides detailed reference information including message and return code lists, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup. This publication is only available to licensed users.

- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641

  Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures.

- *IBM Security zSecure Alert User Reference Manual*, SC27-5642

  Explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS systems protected with the Security Server (RACF) or CA-ACF2.

- *IBM Security zSecure Command Verifier User Guide*, SC27-5648

  Explains how to install and use IBM Security zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.

- *IBM Security zSecure CICS Toolkit User Guide*, SC27-5649

  Explains how to install and use IBM Security zSecure CICS® Toolkit to provide RACF administration capabilities from the CICS environment.

- *IBM Security zSecure Messages Guide*, SC27-5643

  Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.

- *IBM Security zSecure Quick Reference*, SC27-5646

  This booklet summarizes the commands and parameters for the following IBM Security zSecure Suite components: Admin, Audit, Alert, Collect, and Command Verifier. Obsolete commands are omitted.

- *IBM Security zSecure Visual Client Manual*, SC27-5647

  Explains how to set up and use the IBM Security zSecure Visual Client to perform RACF administrative tasks from the Windows-based GUI.

- *IBM Security zSecure Documentation CD*, LCD7-5373

  Supplies the IBM Security zSecure documentation, which contains the licensed and unlicensed product documentation. The *IBM Security zSecure: Documentation CD* is only available to licensed users.

- *Program Directory: IBM Security zSecure CARLa-Driven Components*, GI13-2277

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CARLa-Driven Components: Admin, Audit, Visual, Alert, and the IBM Tivoli Compliance Insight Manager Enabler for z/OS. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

- *Program Directory: IBM Security zSecure CICS Toolkit*, GI13-2282

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CICS Toolkit. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation

website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

- *Program Directory: IBM Security zSecure Command Verifier*, GI13-2284

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure Command Verifier. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

- *Program Directory: IBM Security zSecure Admin RACF-Offline*, GI13-2278

  This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of the IBM Security zSecure Admin RACF-Offline component of IBM Security zSecure Admin. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security zSecure library
: The product documentation site (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
: IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
: The IBM Publications Center site (http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Related documentation

For additional information about using IBM Security zSecure Visual Client, see these publications:

- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide, SC27-5638*

  Provides reference information for installing, configuring, and deploying IBM Security zSecure Visual server on a z/OS system.

- *IBM Security zSecure Admin and Audit for RACF User Reference Manual, LC27-5639*

Provides information about the Security zSecure Admin and Audit for RACF components and explains how to use the features from the ISPF panels. It also describes RACF administration and audit user documentation, including general user reference material and advanced reference material for the CARLa and CKGRACF command languages and the SELECT/LIST fields. The manual also provides troubleshooting resources and instructions for installing the zSecure Collect for z/OS component. This publication is only available to licensed users.

If you are using IBM Security zSecure products in a RACF environment, you can find RACF user and reference information in several IBM manuals. The RACF commands and the implications of the various keywords can be found in the *RACF Command Language Reference* and the *RACF Security Administrator's Guide*. Information about writing other RACF exits can be found in the *RACF System Programmer's Guide*. Information about auditing RACF can be found in the *RACF Auditor's Guide*. You can access this documentation from the z/OS internet library available at http://www.ibm.com/systems/z/os/zos/bkserv/.

For information about incompatibilities, see the **Incompatibility** section under **Release Information** on the IBM Security zSecure documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

Table 1. Further information about RACF administration, auditing, programming, and commands

Manual	Order Number
z/OS V1 Security Server RACF Command Language Reference	SA22-7687
z/OS V1 Security Server RACF System Administrator's Guide	SA22-7683
z/OS V1 Security Server RACF Auditor's Guide	SA22-7684
z/OS V1 Security Server RACF System Programmer's Guide	SA22-7681
z/OS MVS™ System Commands	SA22-7627

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. IBM Security zSecure Visual customization and primary tasks

IBM Security zSecure Visual maintains an IBM RACF security database from a Windows workstation. Some customization and primary tasks are described in the following topics.

Release information

The zSecure Release information topics include details on new features and enhancements, incompatibility warnings, and documentation update information. You can download the most current version of the release information from the following link in the zSecure Information Center: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html.

Selecting to work locally or in a multisystem environment

To limit or expand the scope of your task, you can work with users and resources on the local RACF database or with users and resources that are defined in multiple nodes across multiple systems.

Before you begin

To work with users and resources in a multisystem environment, the administrator must first complete these tasks:

1. Configure the zSecure server and the Visual server to manage multiple RACF databases on multiple systems. See the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

2. Create and verify a server definition on the Visual client that connects to the Visual server. See "Configuring IBM Security zSecure Visual" on page 139.

Procedure

- To work locally, ensure that the **Use zSecure Server for multi-system services** option is *not* selected in the Options dialog of the Visual client. By default, this option is not selected. When operating in local mode, the Visual client does not request node details from the zSecure server.
- To work with users and resources in a multi-system environment, set the Visual client to operate in multi-system mode. Use these steps to specify multi-system mode:
  1. Select **Start > Programs > Security zSecure Visual** to start the Visual client.
  2. Select **View > Options** to start the Options dialog (see "Setting display preferences" on page 9).
  3. Select **Use zSecure Server for multi-system services > OK**.

     You are prompted to accept the list of systems that are configured for the multi-system environment or to specify the systems to which your actions will apply for the session.

     Note: If the client cannot establish a session with the zSecure server, the client issues a message indicating that the server is not active. It begins operation in local mode.

Logging on

You log on to the Visual client so that the program can determine your scope of operation.

About this task

After starting the program, you must logon to RACF so that IBM Security zSecure Visual can inform the CKGRACF program on the mainframe to report your access to certain commands. This access loads schedule names and disables certain features. The CKG profiles control your access. It continues to load the class descriptor table to present a list of all classes defined on the complex.

Procedure

Follow these steps to logon to RACF on the mainframe:

1. Select **File > Logon** from the main menu to access IBM Security zSecure Visual, or click **Logon** from the toolbar. The **Logon to RACF** dialog is displayed.

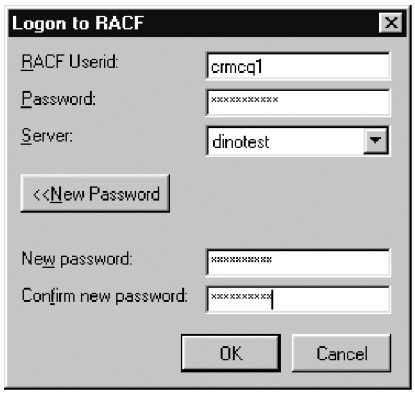


Figure 1. Logon dialog

2. Enter your mainframe user ID and password. Or,
3. Select **New Password** to change your password.
4. Confirm your new password.
5. Click **OK** to continue.

   Note: If this logon is your first logon to the mainframe, it takes time to set up a cryptographically secure communication channel.
6. If you log on in multi-system mode, you are prompted to select the nodes that you want to work with. See "Selecting available nodes"
7. After a successful logon, the **Find** dialog displays. Use the **Find** dialog to display or change the users, groups, or resources. See "Viewing connect properties as a first task" on page 5.

Selecting available nodes

If you log on in multisystem mode, the zSecure server is queried for a list of available nodes. The nodes that are defined in the zSecure server are made available to the Visual client. Select the zSecure and RRSF nodes that you want to work with.

The list of nodes includes zSecure nodes and RRSF nodes, which are displayed in the **Node selection** dialog. Use these guidelines to help determine which nodes you want to work with:

- You must select at least one zSecure node to continue. The Visual client sends your request to the server, which directs it to the zSecure node. The node returns data from the associated RACF database. After the client receives data, it can send requests to the zSecure node to change the data.
- Nodes that you can operate on only as zSecure nodes are listed only in the **zSecure Nodes** column.
- Nodes that you can operate on only as RRSF nodes are listed in the **RRSF Nodes** column.
- Nodes that are listed in the same row under the **zSecure Nodes** column and the **RRSF Nodes** column are available in both environments.
- The nodes you select become your list of preferred nodes. You change your preferred zSecure and RRSF nodes using the Select Nodes dialog (see "Select Nodes dialog: multi-system options" on page 20). You can also change your preferred list of zSecure nodes by selecting **>>Advanced** in the **Find** dialog.

- Operations that you perform on RRSF nodes are not verified for successful completion. You can send edit requests to a RACF database through an RRSF node. However, the client does not receive feedback on the final outcome of the action. Consequently, the software assumes that RRSF operations are successful.

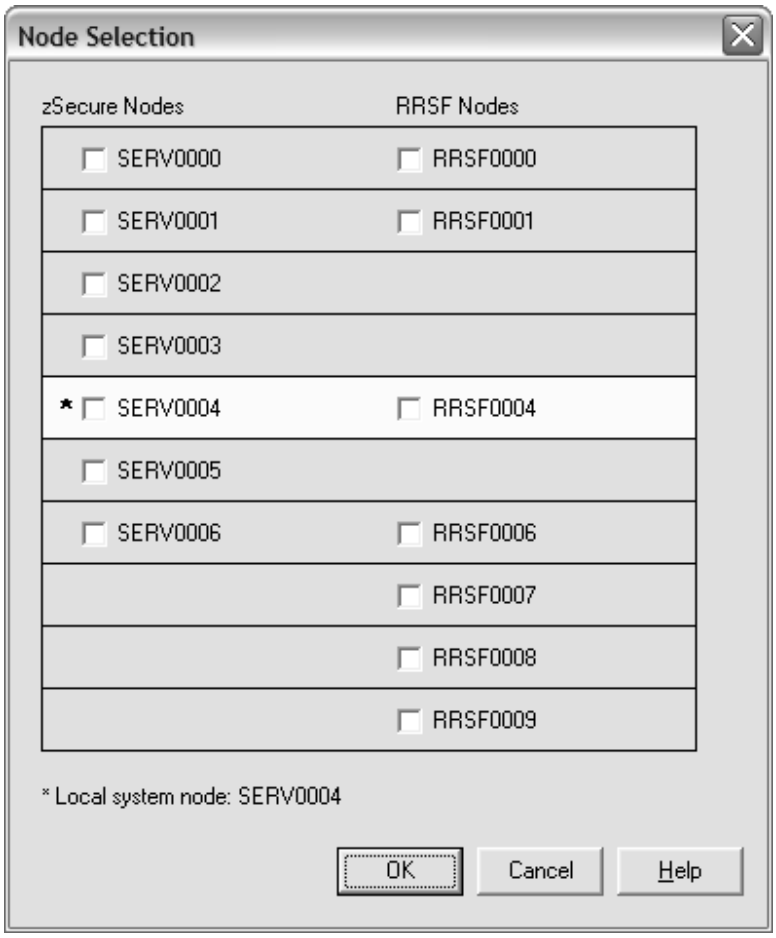


Figure 2. Node Selection dialog

Viewing connect properties as a first task

This procedure gives an example of how to use the interface to look at the connections between users and groups.

About this task

Use this task as an example first task to view the connections between user and groups. See Chapter 5, "Connect management," on page 73 for more information on performing connect tasks.

Procedure

1. In the **Find** dialog window, select **User** or **Group** from the **Class** drop-down list.
2. Type a user or group in the **Search** field and click **OK**. A search results window is displayed.
3. To view what the connections are for the selected user or group, follow these steps:

a. Select a specific user or group from the search results window.
b. Select **Navigate > Connects**. A Connects window displays all groups or users related to this specific user or group.
c. Double-click any of the user or group in the **Connects** window to see its properties.

Logging off

You log off the Visual client after completing your tasks.

Procedure

Select **File > Logoff** from the main menu to log off IBM Security zSecure Visual.

Exiting

You exit the Visual client after logging off the Visual Server.

Procedure

1. To exit IBM Security zSecure Visual, select **File > Exit** from the main menu.
2. Specify whether the program prompts for a confirmation on exit in the **Option** dialog.

   For more information, see the section "Setting display preferences" on page 9. If you press **Exit** while you are still on IBM Security zSecure Visual, the program logs off before exiting.

Turning off the server definition name

You can create a simple file and entry to turn off the displaying of the server definition name in the Visual client.

About this task

The IBM Security zSecure Visual client includes the server definition name in the application title. The server definition name is enclosed between square brackets. By default, the application turns on the server name definition during logon and turns it off during logoff, but you can turn off this feature.

Procedure

To turn off the server definition name in the application title, follow these steps:

1. Go to the application folder. The default directory is `C:\Program Files\IBM\Security zSecure Visual\2.1\`.
2. Create a text file named `c2racv.cfg`.
3. Add this option:`ShowHost=No`
4. Save the file.
5. Exit and log on again for the change to take effect.

Viewing the log files

You can view logged information about the Visual application in the `cesys` and `ceaud` files.

About this task

The zSecure Visual client provides log files to capture errors, warnings, and informational messages that can help locate the source of a problem and diagnose its severity.

Procedure

Follow these steps to access the log files:

1. Navigate to the log directory:
   user_profile\Application Data\IBM\Security zSecure Visual*version*\Servers*ServerName*\ClientLogs

   Example directory: C:\Documents and Settings\Administrator\Application Data\IBM\Security zSecure Visual\2.1\Servers\Server_A\ClientLogs

   Various logs are recorded in this directory. The log files include the process identifier in the titles, so multiple versions from different runs of the client can be stored in the same directory. Here is an example of same-named files that are differentiated by process identifiers:

   ```
   About0480.log
   CKGPRINT0480.log
   Requests0480.log
   SYSPRINT0480.log
   SYSTERM0480.log

   About6412.log
   CKGPRINT6412.log
   Requests6412.log
   SYSPRINT6412.log
   SYSTERM6412.log
   ```

   You must provide these log files when reporting problems related to the zSecure Visual client.
2. Navigate to the other log file directory:
   All Users\Application Data\IBM\Security zSecure Visual*version*\Servers*ServerName*

   Example directory: C:\Documents and Settings\All Users\Application Data\IBM\Security zSecure Visual\2.1\Servers\Server_A

   The log files named cesys and ceaud are stored in this directory. These log files provide information about the communication layer between the client and server. Though this information is not for user interpretation, it is useful to diagnose communication-related problems. You must also provide these log files when reporting problems related to the zSecure Visual client.
3. View the latest updates contained in these log files from the tabs of the Communication window GUI.

   Note: When you start the client it clears log files that are older than 7 days.

   For information about the messages and possible resolutions, see *IBM Security zSecure: Messages Guide*.

Using the Communication window

You use the Communication window to view information exchanged between the zSecure Visual client and the components and programs on the mainframe side.

About this task

The **Communication** window enables you to view most of the information exchanged between the zSecure Visual client and the components and programs on the mainframe side, including the zSecure Visual server, CKRCARLA, CKGRACF, and RACF. In general, the client issues requests for the CKRCARLA and CKGRACF programs to obtain information about the client and to modify the RACF database. You can use the **Communication** window to view real-time logs for the client requests and their results.

You can print the information found in the **Communication** window and export it to rich text format (.rtf). See "Printing" on page 16 and "Saving and exporting printable data" on page 15.

Procedure

Follow these steps to view the **Communication** window:

1. Display the **Communication** window, using one of these options:
   a. From the main menu, select **View > Communication**; or,
   b. Select the **Communication** button on the toolbar. This button always puts the **Communication** window on top.

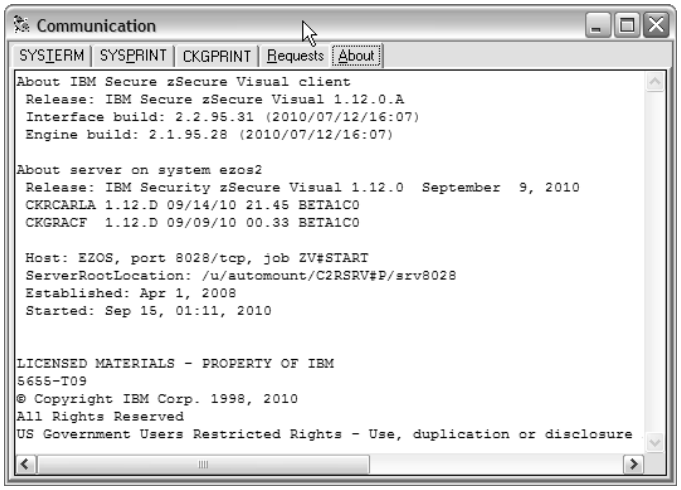


Figure 3. Communication window

2. Select the **Requests** tab to see all requests issued by the client, which include the latest CARLa commands, CKGRACF commands, and commands sent to the server. You can find the commands that are sent to the server under the *extension* section of this tab.
3. Select the **SYSTERM** tab to view status messages and messages with a return code (RC) of 12 or higher.
   - If the most recent request is for CKRCARLA, the *SYSPRINT* tab contains the detailed SYSPRINT output of the CKRCARLA program. The SYSPRINT output includes CKRCARLA listings and critical and informational messages. This information helps locate the command causing problems.
   - If the most recent request is for CKGRACF, the *CKGPRINT* tab contains the detailed CKGPRINT output of the CKGRACF program. The CKGPRINT

output includes CKGRACF commands and messages. This information can help you locate a command causing problems. You can also view messages returned directly from RACF.

4. Select the **About** tab to see aggregated client and server information. You can copy and paste this information as text. From this tab, you can find:
   - Client information: the specific version of zSecure Visual client and information about the building of the GUI and its engine.
   - Server information. See "Server Information dialog" on page 17.
   - Copyright notice.

Setting display preferences

Use the **Option** dialog to specify how you want to display IBM Security zSecure Visual.

Procedure

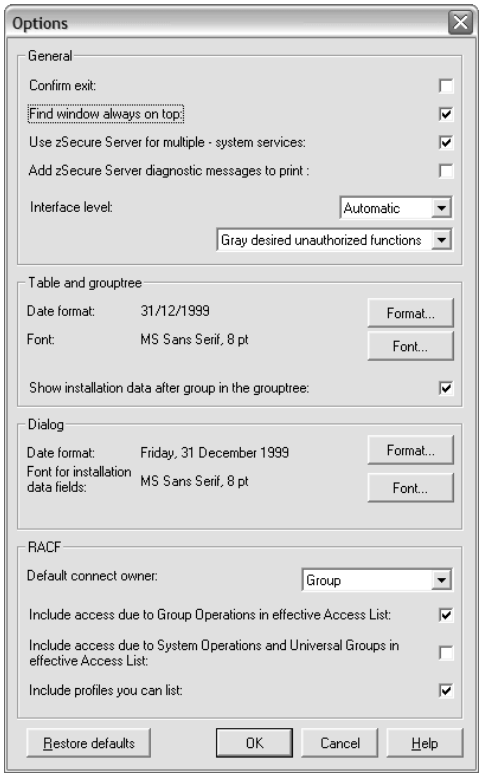


Figure 4. Options dialog

1.
Follow these steps to set the options:

2. Select **View > Options** from the main menu.
3. (Optional) Change any of the general behaviors:

   Confirm exit
   Specifies whether the program has to prompt for confirmation on exit or exit directly.

Find window always on top
Specifies whether the **Find** dialog remains on top or closes after every search.

Use zSecure Server for multi-system services
Specifies whether to operate the Visual client in local mode only or multi-system mode. The default is local mode (unchecked). You must specify the operational mode before you log on. You cannot change from one mode to another while you are logged on. See "Selecting to work locally or in a multisystem environment" on page 2 for information about operating in multi-system mode.

Add zSecure diagnostic messages to print
Select this option to include a DEBUG statement in the requests to remote nodes. The DEBUG statement generates information to assist in debugging node problems. Leave this option unchecked if you do not want to generate troubleshooting information.

Interface level
Determines which functions are available and shown to the user.

4. (Optional) Change any of the table and grouptree behaviors:

   Date format
   You can specify two date formats: one format for all tables, where the width of the columns is an issue, and one date format for all dialogs. Select a date format from the list to get the wanted date format.

   Font selection
   You can specify two different fonts, one for the table and the grouptree, the other for the dialogs. A font size must be 8 - 12 points.

5. (Optional) Change any of RACF behaviors:

   Default connect owner
   Specify who is the default owner for new connects. If you leave the **Owner** field blank in the connect dialog, zSecure Visual uses the owner specified here.

   Include access due to Group Operations in effective Access List
   Specifies whether the Group Operations attributes determine the effective access list. By default, this option is on.

   Include access due to System Operations and Universal Groups in effective Access List
   Specifies whether the System Operations attributes and Universal Group access determine the effective access list. By default, this option is off.

   CAUTION:
   If you select this option, zSecure Visual must read the entire RACF database to create an Effective Access List. It can cause a significant drop in performance.

   Include profiles you can list
   Determines which profiles you can see and edit. When this option is on, you see the profiles you can edit and the profile in your CKGLIST and group-auditor scope. When it is off, you see only the profiles you can edit. By default, this option is on.

6. When you finish the changes, perform one of these steps:

a. Click **Restore defaults** to set the options to factory defaults.
b. Click **OK** to accept the changes.
c. Click Cancel to close the **Options** dialog window without changing the settings.

Setting interface options according to your access level

You can adjust the interface to display specific groups of options, according to the access level you are assigned.

About this task

Use the **Options** dialog to adjust the interface according to your role as a user.

Procedure

- You can select one administration level from the **Interface level** drop-down list. If you are not authorized to perform all functions of the particular level, the options that you cannot access are either hidden or displayed in gray. If you change the administration level, the **Find** dialog changes to adapt to that level. These options are the administration levels for you to select:

  Helpdesk
  Helpdesk is the lowest level, the functionality is limited to:
  - List users
  - Resume a user
  - Set password
  - Manage schedules
  - List mapping profiles
  - View the mapping profiles of a user

  Connect
  This level expands the functionality from the **Helpdesk** level to:
  - List groups
  - List connects
  - View the grouptree
  - Create connects
  - Change connect attributes
  - Remove connects

  User This level expands the functionality from the **Connect** level to:
  - Duplicate user
  - Change properties of user
  - Mark user for deletion

  Access list
  This level expands the functionality from the **User** level to:
  - List resources
  - List Access List
  - List effective Access List
  - Change access lists (RACF command: permit)

  Group This level expands the functionality from the Permit level to:
  - Add subgroup

- Duplicate group
- Change group properties
- Delete group

Full Full is currently the highest level, functionality for this level includes:

- List member list
- List scope
- Create resource profile
- Duplicate resource profile
- Modify resource profile
- Delete resource profile
- Change member list
- Segment management

Automatic
Displays the highest administration level to which the user has access. The CKGRACF SHOW MYACCESS command determines access.

- In the right field, you can select how the interface looks. If you are not authorized on the mainframe for all commands in your administration level, you can select either of these options:

  Gray desired unauthorized functions
  Display all unauthorized functions in gray.

  Hide desired unauthorized functions
  Do not display all unauthorized functions. You can use this setting for further customization between different levels. You can select the higher level and remove undesired functions by refusing access to their corresponding CKG profiles on the mainframe.

  CKG profiles cannot control the availability of the list commands, which are based on the administration level only.

Setting the date format

You can choose a predefined format to display dates or define your own format.

About this task

The date format dialog specifies how dates are displayed. You can select one of the predefined formats or build your own format.

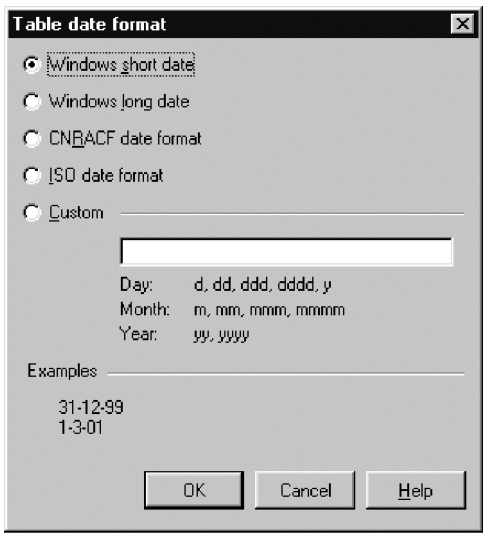


Figure 5. Date format dialog

Procedure

- Use these options specify the predefined formats.

  Windows short date
  The Windows date formats are taken from the Windows configuration settings. You can change these formats by selecting **Control Panel > Regional Settings > Date**. The modified format affects all applications that use the format.

  Windows long date
  See description of Windows short date.

  CKRCARLA date format
  This format is used by the CKRCARLA program on the mainframe, which is *dd mmm yyyy*. This format has no special meaning or advantages.

  ISO date format
  This format is *yyyy-mm-dd*.

- If you want to change from the predefined formats, select **Custom** and build your own format using these characters in the format string.

  Note: You can use the characters **/** and **-** as separators, but the separator character defined in the Windows **Control Panel > Regional Settings > Date** can replace them. You can prevent replacement by placing a **/** before the character.

Table 2. Date formatting characters

d	one-digit day, two digits only if necessary
dd	two-digit day
ddd	day of week, three characters
dddd	day of week, full name
m	one-digit month, two digits only if necessary
mm	two-digit month
mmm	three-character month name

Table 2. Date formatting characters (continued)

mmmm	full month name
yy	two-digit year
yyyy	four-digit year

Drag and drop function

You can use the drag and drop function to change users or connects in the RACF database.

Use drag-and-drop to change users or connects in the RACF database, instead of using menus, pop-up menus, or the toolbar. After every drop, a dialog or a pop-up window for confirmation displays to avoid accidental changes. With dragging and dropping you can delete and change users, and delete, change, copy, merge, and move connects. You can also change subgroups and modify access lists and member lists.

Copy and paste function

You can use the **Copy**, **Paste,** and **Paste Special** functions to perform various copy, merge, and move tasks.

Use **Copy**, **Paste,** and **Paste Special** options on the main menu to perform these tasks:

- Copy users, groups, connects, access lists, and member lists
- Create, merge, move, and copy connects

Toolbar buttons

You can use the Visual client toolbar buttons to show the most frequently used menu options.

The toolbar buttons show the most frequently used menu options. When you hover the mouse cursor over each button, a yellow pop-up with the description displays.

Right mouse button

You can right-click a row to display **Navigate** and **Action** options.

In most tables and the group tree, right-click a row to display a pop-up menu with frequently used **Navigate** and **Action** options.

Naming conventions

Use these guidelines to create names for users and groups.

When you add new users or groups, follow these naming conventions:

- The name must be from 1 to 8 characters long.
- The characters must be the letters A-Z, number 0-9, or #, $, @.
- The name cannot start with a number.
- A group cannot have the same name as another group.

- A group name cannot have same name as an existing user ID.

Changing column sequences

You can use click and drag to change the arrangement of a table column or to change the border of a column.

Procedure

You can rearrange the columns in a table and change the size of a column.

- To change the arrangement of the columns in a table, drag a column to where you want it so you can compare columns. The column arrangement you make becomes the default when you start the program next time.
- To change the size of a column, click a vertical border and move it left or right. Double-clicking gives you the required size of a column.

Site-specific columns and fields

The site administrator can customize zSecure Visual to display user information that is defined by your organization.

For example, a site might want to display employee IDs and department numbers. These fields are displayed in front of or instead of the `INSTDATA` column for `USER` profiles.

Your administrator defines the number, order, and characteristics of site-specific fields; you do not configure these fields in the Visual client. Configuration instructions are in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

If defined, site-specific fields are in the User properties dialog, User table, and the Find dialog:

User properties
: Site-specific columns can replace the `InstData` field or be included in addition to the `InstData` field. Depending on the number of site-specific fields, these fields can be displayed under a separate tab. The contents of the fields are read-only.

User table
: Scroll right to view site-specific columns. Depending on the configuration of your site, you might be able to search on some fields.

Find dialog
: If site-specific columns are specified with a search capability, the dialog displays the fields when you select the **>>Advanced** button.

Saving and exporting printable data

You can save a printable table in CSV format and export the communication window to RTF format.

About this task

You can save all printable tables as Comma Separated Values format (CSV). Different programs, such as Microsoft Excel, can read this format. You can also

export the communication window to an RTF format. See “Using the Communication window” on page 7.

Procedure

To save table information in CSV or RTF format, perform these steps:

1. Select **File > Save As**.
2. In the **Save as** dialog, enter a file name. If this name exists, a warning box displays. If you do not change the name, it overwrites the original file.
3. Click **Save**.

Printing

You can print data and see print previews in the Visual client.

About this task

You can print data and see print previews.

Procedure

To print data, perform these steps:

1. From the main menu, select **File > Print**, or click the printer icon on the toolbar.
2. In the print dialog, select the options you want. The **Current Page** option is only enabled if you print from the print preview.
3. Click **OK**.

   Every printout has these elements:

   - Page header with the name of the data list on the left and the product *version number* on the right
   - Date
   - Page number

   You can print every list and export to CSV, see “Saving and exporting printable data” on page 15.

Previewing a print file

You can preview and change the layout of a print file in the Visual client.

Procedure

1. To get a print preview, select **File >Print Preview** from the main menu or click the print preview icon on the toolbar.
2. Select **PgUp** or **PgDown** on your keyboard to scroll through the preview.
3. Select the desired printing option from the list of icons:
   - Click the print icon to print the information as shown. All pages are printed.
   - Select the zoom icon to specify the size of the text that is included on the print page. The percentage values are: 10, 25, 50, 75, 100, 150, 200, and 500 percent.
   - Select one of the page icons to view the page layout of 1 (default), 2, 3, 4, or 6 pages of the print file.
   - Click **Close** to go back to the main program.

Tables available for printing

You can print these tables and lists in the Visual client.

You can print the tables described in these topics:

- "User table" on page 39
- "Group table" on page 63
- "Connects table" on page 73
- "Resource profiles" on page 86
- "Selecting resources for a specific user ID or group with the Permits function" on page 29.
- "Viewing an Access List" on page 37
- "Viewing an Effective Access List" on page 37
- "Using Scope *" on page 34
- "Viewing a member list" on page 38.

If you cannot print a table, the print and preview options are not active.

Server Information dialog

You can use the **Server Information** dialog to view information about the server you are currently logged on to.

To view the server information, select **Help > Server Information** from the main menu. The following information is available:

- Release information of the server CKRCARLA and CKGRACF
- Host name of the server and its IP port
- The possibly resolved value of the C2RSERVE parameter in the zSecure configuration
- Time that the server established itself as a certificate authority
- Time that the server was last started.

See your server documentation for additional information.

Display of the ? character

The question mark (?) is displayed if a field is not within the scope of the user.

If you find a ? in a field of a table, it means that this field is not loaded because it is out of your scope.

Chapter 2. RACF database operations

Use the Visual client **Navigate** option to find and view users, groups, and resources and their connects, permits, and schedules.

This chapter explains the different options you can use to work with the databases. Click **Navigate** to go to the databases that you want to see. You can find individual users, groups, and resources and their relations such as connects, permits, schedules, and so on.

Select Nodes dialog: multi-system options

Specify the systems and nodes you want to work with in the **Select Nodes** dialog.

If you select to work with multiple systems when you start the Visual client, the **Select Nodes** dialog is displayed each time you start an action. For example, if you select **Duplicate** to duplicate a user or group, the **Select Nodes** dialog displays your preferred list of nodes.

Note: If you select a single node (which becomes your preferred list) to work in multi-system mode, the Select Nodes dialog is *not* displayed before your request is processed. You must select at least two nodes to view the Select Nodes dialog before the processing of a client request.

If you have performed an action already, the nodes you selected for the previous action are displayed. If needed, you can change the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.

If a node is defined as a zSecure node and an RRSF node, you can select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select an alternative user ID to run the command.

For RRSF nodes, if other user IDs are associated with your user ID (using the RACLINK command), those associated IDs are displayed.

When you click **OK**, the selected list of nodes is verified, then the specified action is performed for each selected node.

Click **Cancel** to return to the previous dialog without selecting any nodes.

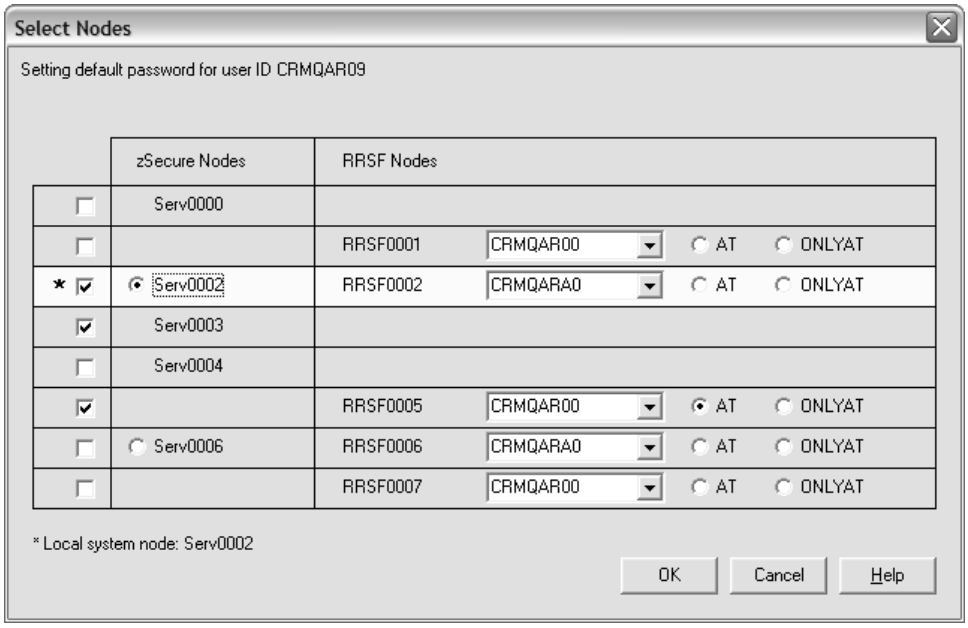


Figure 6. Select Nodes dialog

The **Select Nodes** dialog has these fields and options:

Check box column
The left check boxes enable you to select the nodes to which you want to apply your request.

zSecure Nodes
Lists the available zSecure nodes in your preferred nodes list.

Radio button
If the row contains entries for zSecure and RRSF nodes, a radio button is displayed beside the zSecure node. This button enables you to select or clear the zSecure node. If you select the row and the radio button, your request is processed for the zSecure and RRSF nodes. If you select the row and clear the button, your request is processed only for the RRSF node.

System_name
Displays the name of the available zSecure system. You can select and clear the systems to which the action applies.

RRSF Nodes
Lists the available RRSF nodes in your preferred nodes list.

System_name
Displays the name of the available RRSF system. You can select and clear the systems to which the action applies.

Alternative ID (drop-down list column)
Select this dropdown option to specify a different ID than the associated user ID to perform the action on the selected RRSF system. Associated IDs on RRSF systems are defined using the RACLINK command.

Specify only IDs that are defined with the authority to execute your action. If the specified ID does not have the authority on the selected system to issue the command corresponding to your action, RACF will reject the command.

The alternative user IDs that you specify are saved in the drop-down list for your reuse during a logon session. The alternative IDs are *not* saved between logon sessions.

AT Specifies how the instruction is processed at the selected RRSF node. If you select the **AT** option, it is used to build the command, for example, `AT(RRSF0000.userid)`.

ONLYAT
Specifies how the instruction is processed at the selected RRSF node. If you select the **ONLYAT** option, it is used to build the command, for example, `ONLYAT(RRSF0000.userid)`.

Verification of actions across multiple systems

You can use the **Status of** progress form to verify actions for each selected node in a multi-system task.

If you execute an action for multiple systems, the **Status of** progress form is displayed to show the progress of the action for each selected node.

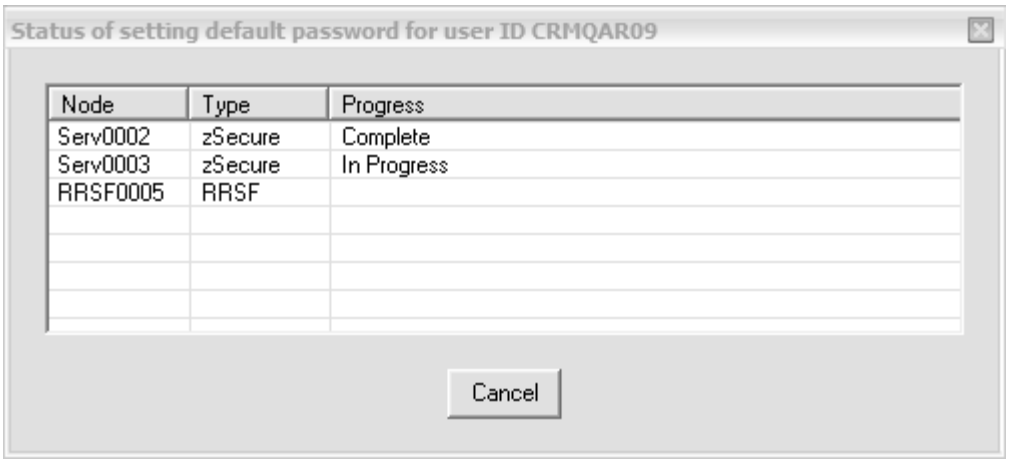


Figure 7. Multiple system progress Status form

As each action completes, the progress form is updated to indicate the status of the action on each node. For example, the **Progress** field indicates if the action completes, fails, or is in progress for each node. You can click **Cancel** to prevent starting the action on nodes where the action has not begun. You cannot cancel an action in progress.

If an action fails, you can review any error messages before closing the form. Click **Close** when the action completes successfully on all listed nodes.

Note: The completion status cannot be determined for RRSF nodes. Consequently, all RRSF node requests are assumed to be successful.

Using the Find dialog

Use the **Find** dialog to view users, groups, or resources for one or more RACF databases.

Procedure

Follow these steps to open the **Find** dialog:

1. Select **Navigate > Find**.
2. Enter the class and the search string.
3. Specify how the search string value is interpreted, such as Exact, Filter, or Mask.
4. Select the scope of the nodes for which you are searching.
5. Click **OK**.

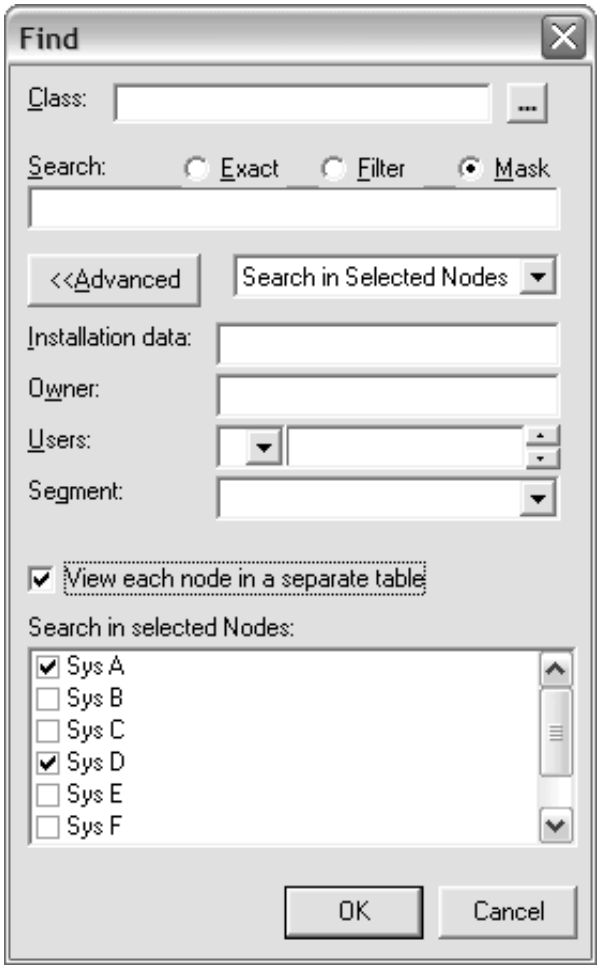


Figure 8. Find dialog

Depending on your configuration, you might see one or more site-specific fields in conjunction with user information. This information is either at the bottom of the dialog or on the right of the dialog. If installation data (`INSTDATA`) is displayed, up to three site-specific search fields are added to the bottom of the dialog. If there is no installation data, up to four site-specific search fields are added to the bottom of the dialog. If there are more than four site-specific search fields, the fields are displayed on right side of the dialog.

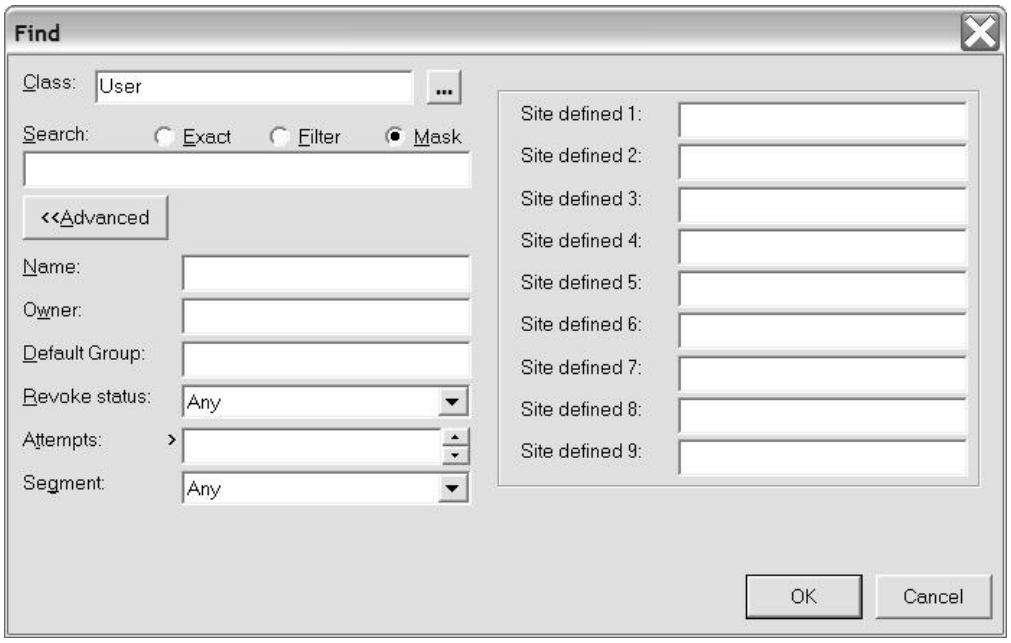


Figure 9. Find dialog with site-specific fields

The Find dialog presents these fields and options:

Class Specifies the name of the class. If you do not know the class, click the button next to the class field to open the **Select class** dialog. See "Finding classes with the Select class dialog" on page 26. When you leave the class field empty, you receive all records except users or groups.

You can use keyboard shortcut keys to specify the class field:

Table 3. Shortcut keys for the class

Shortcut keys	Class
Ctrl + D	Dataset
Ctrl + G	Group
Ctrl + U	User

Exact The search string is the only user ID, group ID, or profile that is loaded.

If you have site-specific fields, do not specify values in these fields if you want to search on an exact match to the specified string in the search field. If you select **Exact** and specify one or more values in the site-specific fields, the Visual client returns message C2RU163. This message warns that you cannot specify values in the site-specific fields when searching for an exact match.

Filter If the search string is used as a filter, all characters of the profile key must match. The percentage (%) character matches any character and the asterisk (*) character matches all succeeding characters. The * character is only accepted as a last character. For example:

- "IBMUSER" matches "IBMUSER" only.
- "I%MUSER" matches "IBMUSER," "ICMUSER," "IDMUSER" and so on.

- "IBM*" matches "IBM," "IBMUSER," "IBMGROUP," "IBMSYS" and so on.

The only exception is that an empty string used as a filter selects all, just as an empty mask does.

Mask When the string is used as a mask, the first characters of the item must match the string. "IBM" matches "IBMUSER," "IBMGROUP," "IBMSYS" and so on.

Advanced

When clicking **<<Advanced**, you get additional criteria, which you can use to reduce the selection. Only profiles that match all criteria can be selected.

- See Chapter 3, "User management," on page 39 for a description of the extra fields for users.
- See Chapter 4, "Group management," on page 63 for a description of the extra fields for groups.
- See Chapter 6, "Resource management," on page 85 for a description of the extra fields for resources.

Your list of preferred nodes is maintained in the **<<Advanced** search options. You can change the preferred nodes using the **<<Advanced** option.

Mode selection listbox

This drop-down field is displayed only if you are operating in multi-system mode.

Search All Nodes

Select this mode to perform operations on all preferred zSecure nodes. You cannot include RRSF nodes in the search because they do not return data.

Search in Selected Nodes

Default. Select this mode to perform operations on specific zSecure nodes. Nodes are searched in the order in which they are listed. The **Search in Selected Nodes** listbox is enabled when you specify **Search in Selected Nodes**.

Segment

The segment option lets you refine the class you open. Select only the profiles that have the segment you have chosen. The default option is any, which gives you the complete profile list including the profiles that have no segments.

If you are not authorized to view segments, or if there are no segments present, the Segment option is shaded in grey to indicate that it is not available.

The **Find window always on top** option in the **Options** dialog specifies whether the dialog disappears after you click **OK**. The interface options determine which fields and options are available in this dialog.

Site-specific fields

Site-specific fields with user information can be configured by your organization. If so, one or more fields with site-specific names and content are on the right.

View each node in a separate table

This option is displayed only if you are operating in multi-system

mode. Select this option to view the search results for each node in a separate table. If you do not select this option, all nodes are shown in the same table.

Search in Selected Nodes
Your list of preferred nodes is displayed here if you select **Search in Selected Nodes** in the drop-down list next to **<<Advanced**. The list contains only preferred nodes. You can change the list of search nodes as needed. The nodes are not selected for your current request but your changes are used for the next action you specify.

Ambiguous Class selection

To view the desired search results, specify the exact class name in the **Find** dialog.

If you open the **User** or **Group** table and make a mistake in the **Find** dialog (for example, you enter `Users` instead of `User`), the software displays the `Ambiguous Class selection "`*`class_name`*`"` warning. If you continue the search, the program tries to find resources of the class you type. Typically this results in the message `No matching resources found`.

Figure 10. Ambiguous Class specification

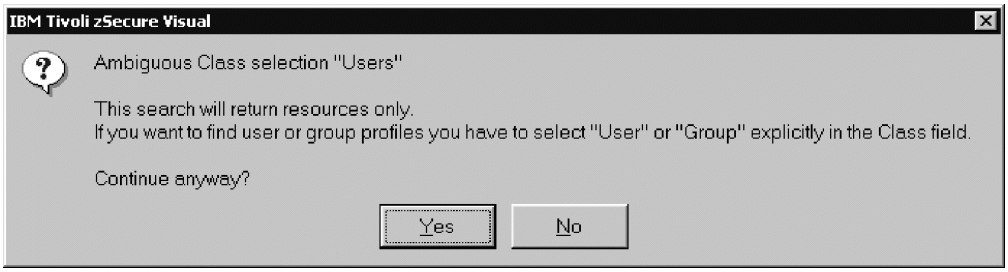


Figure 11. Warning

To view the **User** table, select **No**, then select the right class.

Finding classes with the Select class dialog

You can use the **Select class** dialog to find a specific class.

About this task

The **Select class** dialog helps you find the class you need.

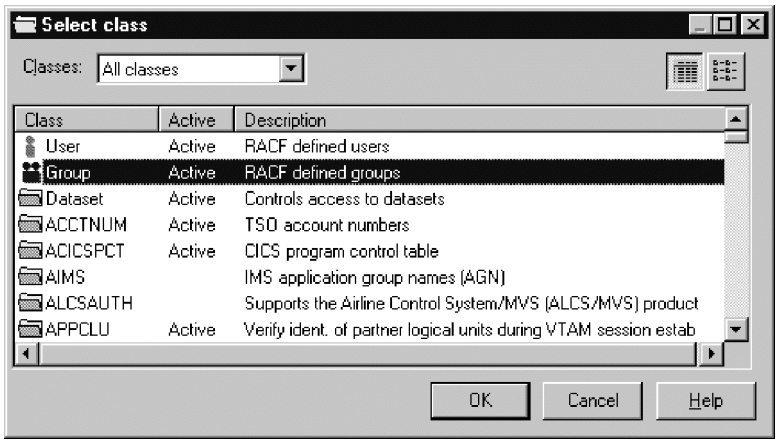


Figure 12. Select class dialog

Procedure

- Click **OK** to select the desired class.

  The table contains these columns:

  Class: Name of the class.

  Active:
  Flag indicating whether RACF protection for the class is active.

  Description:
  Description of the purpose of the class.
- To limit the list of classes, use the Classes field:

  All classes
  Displays all classes that have been read from the class descriptor table during logon.

  Active classes
  Displays only classes that are active, as set by SETROPTS CLASSACT and SETROPTS NOCLASSACT commands on the mainframe.

  Authorized classes
  Displays only classes that you are authorized to change, according to your class authorizations or system-wide special attribute.

Viewing connected users and groups

You can select **Navigate > Connects** to view connect relationships for users and groups.

Procedure

1. To see the connected users or groups, select a user or group.
2. Select **Navigate > Connects** from the main menu. You can find the explanation of the columns of the resulting table in these topics:
   - Chapter 3, “User management,” on page 39
   - Chapter 4, “Group management,” on page 63
   - Chapter 5, “Connect management,” on page 73

Viewing the groups

You can view a group tree to understand the hierarchy of groups and subgroups.

About this task

A superior group can have zero or more subgroups. A group always belongs to only one superior group except for the group SYS1. SYS1 does not have a superior group because it is the root of the tree.

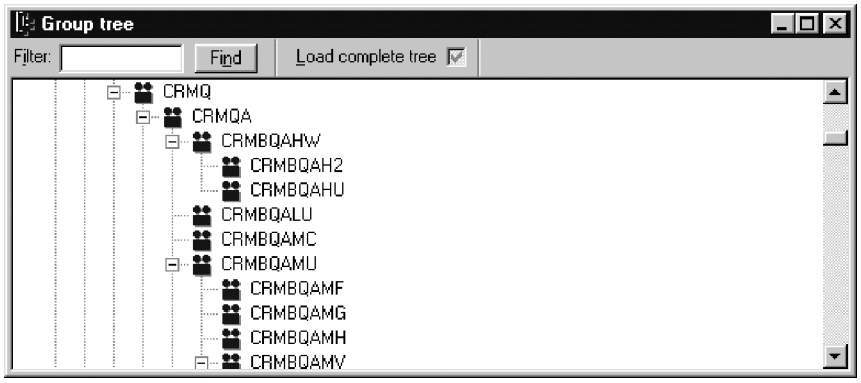


Figure 13. Group tree

To display the group tree, use one of these methods:

Procedure

1. Select **Navigate > Group tree** from the main menu, or
2. Click the **Group tree** button from the toolbar.

   If you are operating in multi-system mode, a **Select Node** dialog displays the list of zSecure complex nodes. You can select only one zSecure complex. Select the complex that you want to display in the group tree.

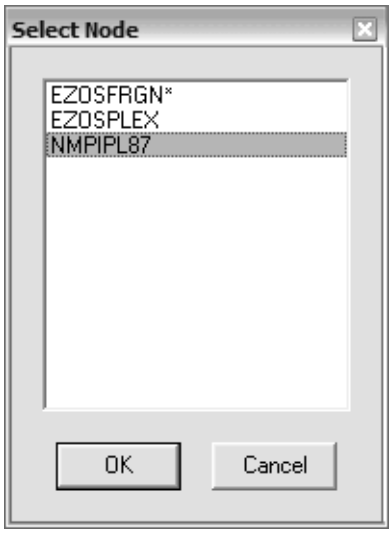


Figure 14. Select complex for group tree

If you close and reopen the session, you must reopen the group trees for the nonlocal nodes.

The **Group tree** window normally does not contain all groups defined in the RACF database. It contains only the groups that are in your scope and their superior groups up to SYS1. Though you can see the superior groups displayed, you are not able to see any information about any superior group that is out of your scope.

Load Complete is a time saving feature of . It loads all groups in your scope and their superior ones from the mainframe. It stores them in the memory of your PC, so you can use them during this session. This loading is only possible if your PC has enough memory capacity.

3. To select groups, enter a filter in the filter box in the grouptree window.
4. Click **Find**.

   The grouptree is extended with the wanted groups. The first one that matches the filter is highlighted. If you select just one group, use its name for a filter. The **Find** command loads the wanted information directly from the mainframe except when the **Load Complete** option is used. Then it looks into the memory of your PC.

   In the **Options** dialog, you can specify whether the available installation data of the group is shown in the tree.

Selecting resources for a specific user ID or group with the Permits function

You can select resources related to a specific user ID or group so that you can see the resource profiles.

Procedure

Follow these steps to select the resources:

1. Select the user ID or group.
2. Select **Navigate > Permits**.

Figure 15. Permits

When you use Permits, select these profiles:

- Resource profiles that contain the user ID or group on their Access List
- Resource profiles that are owned by the user ID or group
- DATASET profiles that have the user ID or group as first qualifier. This qualifier is often referred as the high level qualifier (HLQ). These profiles are selected because RACF users and groups need to alter the data sets that have the user ID or group as the HLQ.

Note: This procedure does not select all resources that the user has access to because the connects of the user are not taken into account. To get a list that takes into account the connects, use View Scope.

In addition to the columns of a resources table explained in Chapter 6, "Resource management," on page 85, the table contains these columns:

Access
This field contains the access the user or group has to the resource. It can be an access level between None and Alter, and one of the values:

Owner
The user ID or group is the owner of the resource profile.

QualOwner
The user ID or group is the first qualifier of a DATASET profile.

When If this field is not blank, the access is only granted if the condition is met. If the field is blank, the access is granted without restriction.

Using Scope

Use the various filtering options in the **Scope** dialog to view users, groups, and resources that can be accessed by a specific user ID or group.

About this task

Users, groups, and resources that can be accessed by a specific user ID or group are in *scope* of the user ID or group. To find the resources that every user can select, use **Scope ***. See "Using Scope *" on page 34.

Procedure

To select users, groups, or resources in scope of a user or group, perform these steps:

1. Select the user or group.
2. Select **Navigate > Scope** from the main menu.

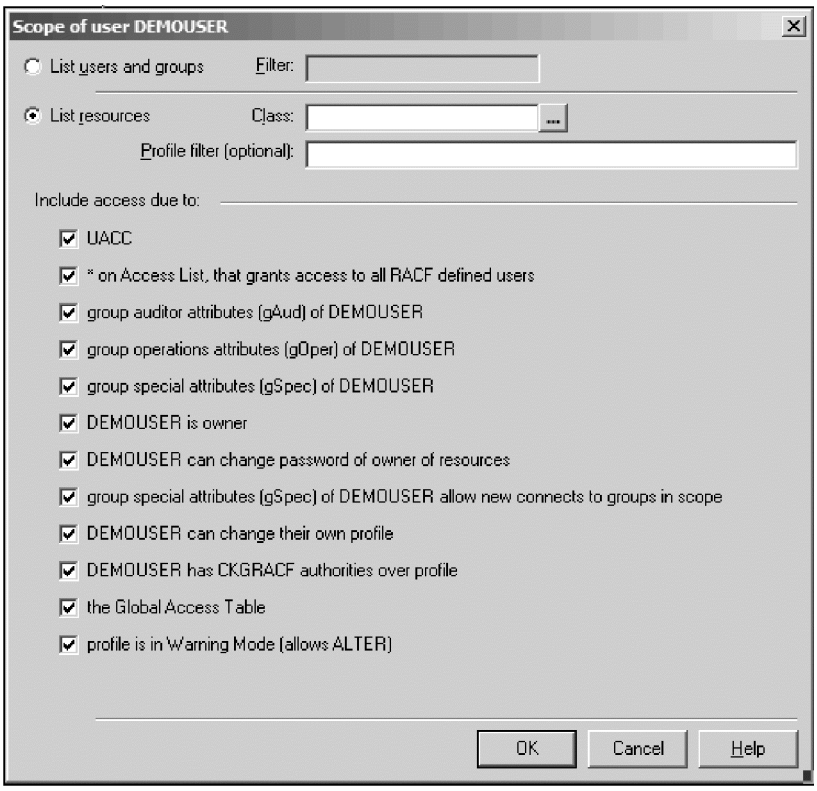


Figure 16. Scope dialog

The Scope dialog displays these fields and options:

List users and groups
Select this option to get a list of users and groups that are in scope of the specified user ID or group. When you select this option, some of the other options become disabled because they do not apply to these users and groups.

Filter Use this field only if you select **List users and groups**. You can enter a user or group filter, for example, IBM,* to select only users and groups that are in scope and match the filter. When you leave this field empty, all users and groups in scope are selected. It leads to a large table.

List resources
Select this option to get a list of resources that are in scope of the specified user ID or group.

Class Use this field only if you select **List resources**. You can enter a class name or class filter to select only resource profiles in a class that matches the filter. If you leave this field empty, no class filter is used. It leads to a large table.

Profile filter
Use this field only if you select **List resources**. You can enter a profile filter to select only resource profiles that match the filter. If you leave this field empty, no profile filter is used. It leads to a large table.

UACC When selecting this option, resources that have a UACC other than None are considered in scope.

*** on Access List, that grants access to all RACF defined users**
When selecting this option, resources that have * on the Access List with an access other than None are considered in scope.

group auditor attributes (gAud) of *ID*
By selecting this option, the group auditor attributes of the selected user are taken into account when determining whether a user, group, or resource is within scope. If you select a group, this option is disabled because groups have no auditor attributes.

group operations attributes (gOper) of *ID*
By selecting this option, the group operations attributes of the selected user are taken into account when determining whether a user, group, or resource is within scope. If you select a group, this option is disabled because groups have no group auditor attributes.

group special attributes (gSpec) of *ID*
By selecting this option, the group special attributes of the selected user are taken into account when determining whether a user, group, or resource is within scope. If you select a group, this option is disabled because groups have no group special attributes.

ID **is owner**
When selecting this option, user, groups, or resources owned by the ID you select are considered in scope.

ID **can change password of owner of ...**
When selecting this option, users, groups, or resources owned by the ID you select are considered in scope. It is because ID might change the password, logon, user, group or resource, and set the password back to the previous value.

ID **can self-connect**
By selecting this option, the user ID *ID* can connect to a group in scope of the user ID. The user ID has group special attribute (gSpec) to the groups in scope. If you select a group, this option is disabled because groups have no such group special attributes.

ID **can change their own profile**
When selecting this option, users, groups, or resources, which become within scope when ID has changed their own profile, are considered within scope.

ID **has CKGRACF authorities over ...**
When selecting this option, users, group, or resources within the CKGRACF scope are considered in scope.

Global Access Table
When selecting this option, a resource is considered in scope if the Global Access Table allows access.

Profile is in Warning Mode (allows ALTER)
When selecting this option, all resources protected by profiles in Warning Mode are considered within scope. Warning Mode implies all access is accepted, but a warning message is generated where a violation occurs.

3. Click **OK.**

The requested table displays the columns that are found in user, group, and resources tables, which are described in Chapter 3, "User management," on page 39

page 39, Chapter 4, “Group management,” on page 63, and Chapter 6, “Resource management,” on page 85. The table also contains these columns:

Access
This field contains the access to the user, group, or resource. It can be in the range Execute-Read-Update-Control-Alter and has these options:

Owner
The user or group that owns the user, group, or resource.

QualOwner
The user ID or group that is the first qualifier of a DATASET profile.

Alter-Operations
The user that can alter the resource using their operations attribute.

CKGOwner
Access granted by the CKGRACF authorized component of IBM Security zSecure Admin.

CKGList
Read access granted by the CKGRACF authorized component of IBM Security zSecure Admin.

Alter-M
The user can alter 'myself' - a user can alter some fields in their own user profile.

Alter-P
Alter access on a discrete profile, enabling you to issue PERMIT.

When If this field is not blank, the access is only granted if the condition is met. If the field is blank, the access is granted without restriction.

Via This field contains the user ID, group, or connected group that was granted the specified access, or it contains one of these options:

Warning
Access is granted because the profile is in warning mode.

***** Access is granted because * is on the Access List with access other than *None*.

UACC Access is granted because the UACC is not *None* or the Global Access Table allows access.

Auditor
Access is granted because the user has a group auditor attribute.

Operations
Access is granted because the user has a group operations attribute.

SCP.G Access is granted because the group or the owner of the user, group, or resource lies in the CKGRACF scope, according to a CKG.SCP.G.... scope profile.

SCP.U Access is granted because the user or the owner of the user, group, or resource lies in the CKGRACF scope according to a CKG.SCP.U... scope profile.

SCP.ID
The access is granted because the user or group, or the owner of the user, group, or resource lies in the CKGRACF scope according to a .SCP.ID... scope profile.

Global
Access is granted because the Global Access Table allows access.

Note:

- When the **Via** column shows *Global*, the Access List and Effective Access List options are deactivated. These lists do not yield any usable information.
- This list is a snapshot. If you want to see any changes made after you display the list, you must close it and display it again.

A related function for resources is the effective Access List, which results in a list of all users and groups that have access according to the profile.

Using Scope *

Use the various filtering options in the **Scope *** dialog to view users, groups, and resources that can be accessed by every user.

About this task

You can use the **Scope *** function to view a list of resources that can be accessed by every user. To find the users, groups, or resources that can only be accessed by a specific user, use the **Scope** function. See "Using Scope" on page 30.

Procedure

1. To find the **Scope *** function, select **Navigate > Scope *** from the main menu.

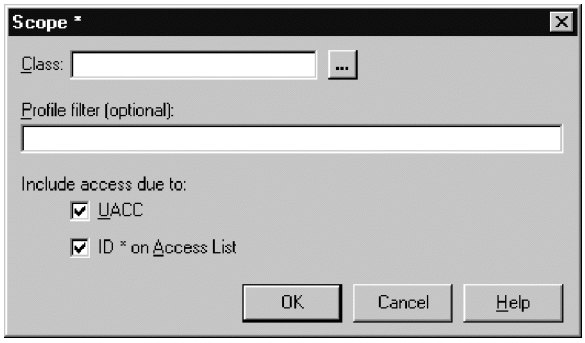


*Figure 17. Scope **

The Scope * dialog displays these fields and options:

Class You can enter a class name or class filter to select only resource profiles in a class that matches the filter. If you do not know the class, click the button next to the class field to view the **Select class** dialog. See "Finding classes with the Select class dialog" on page 26. If you leave this field empty, no class filter is used, which can result in a large table.

Profile filter
You can enter a profile filter to select only resource profiles that match the filter. If you leave this field empty, no profile filter is used, which can result in a large table.

UACC When selecting this option, resources that have a UACC other than **None** is in scope.

ID * on Access List
When selecting this option, resources that have * on the Access List with an access other than **None** are in scope.

2. Click **OK** to view the requested table.

The table contains columns found in resources tables, which are described in Chapter 6, "Resource management," on page 85. The table also contains these columns:

Access
This field contains the access to the user, group, or resource. It can be in the range Execute-Read-Update-Control-Alter and has these options:

Owner
The user or group that owns the user, group, or resource.

QualOwner
The user ID or group that is the first qualifier of a DATASET profile.

Alter-Operations
The user that can alter the resource using their operations attribute.

CKGOwner
Access granted by the CKGRACF authorized component of IBM Security zSecure Admin.

CKGList
Read access granted by the CKGRACF authorized component of IBM Security zSecure Admin.

Alter-M
The user can alter 'myself' - a user can alter some fields in their own user profile.

Alter-P
Alter access on a discrete profile, enabling you to issue PERMIT.

When If this field is not blank, the access is only granted if the condition is met. If the field is blank, the access is granted without restriction.

Via This field contains the user ID, group, or connected group that was granted the specified access, or it contains one of these options:

Warning
Access is granted because the profile is in warning mode.

***** Access is granted because * is on the Access List with access other than *None*.

UACC Access is granted because the UACC is not *None* or the Global Access Table allows access.

Auditor
Access is granted because the user has a group auditor attribute.

Operations
Access is granted because the user has a group operations attribute.

SCP.G Access is granted because the group or the owner of the user, group, or resource lies in the CKGRACF scope, according to a CKG.SCP.G.... scope profile.

SCP.U Access is granted because the user or the owner of the user, group, or resource lies in the CKGRACF scope according to a CKG.SCP.U... scope profile.

SCP.ID
The access is granted because the user or group, or the owner of the user, group, or resource lies in the CKGRACF scope according to a .SCP.ID... scope profile.

Global
Access is granted because the Global Access Table allows access.

Note:

- When the **Via** column shows *Global*, the Access List and Effective Access List options are deactivated. These lists do not yield any usable information.
- This list is a snapshot. If you want to see any changes made after you display the list, you must close it and display it again.

A related function for resources is the effective Access List, which results in a list of all users and groups that have access according to the profile.

Viewing RACF SETROPTS settings

Use the RACF SETROPTS Settings report to view the system-wide RACF options as set or as retrieved by the SETROPTS command.

About this task

The RACF SETROPTS Settings report is read-only.

Procedure

To view the RACF SETROPTS Settings report, Select **Navigate > System Audit > RACF SETROPTS Settings** from the main menu.

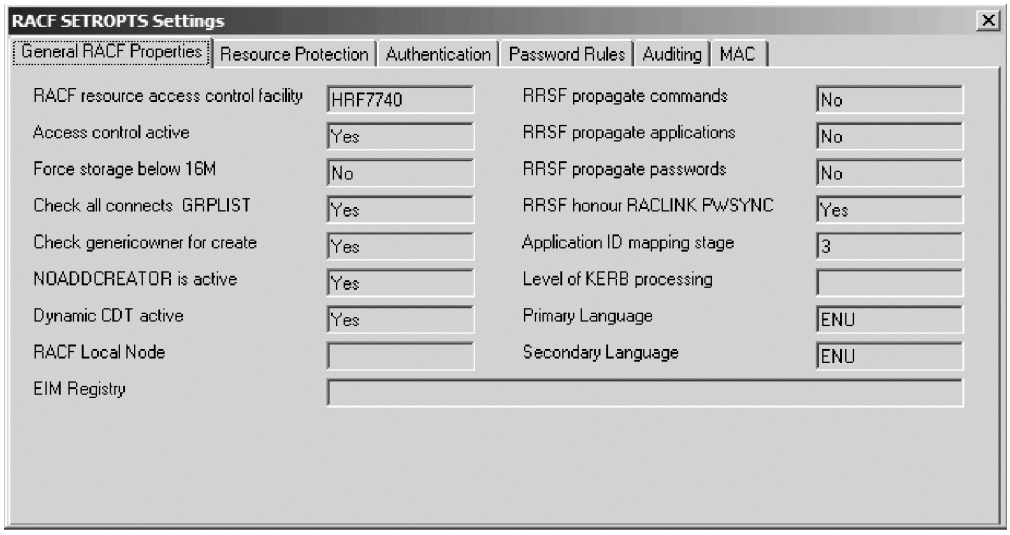


Figure 18. RACF SETROPTS Settings

Viewing an Access List

You can use the **Access List** window to view the access list for all user IDs of a resource profile.

About this task

The access list contains user IDs and groups. When a group is in an access list, all its users get access.

Follow these steps to view the access list of a resource profile.

Procedure

- To view the access list of a resource profile, select a resource profile then select **Navigate > Access List**. The columns of the resulting table are explained in "Modifying an Access List (ACL)" on page 94.
- To view the users in groups that are in your scope, select the **Effective Access List** option. See "Viewing an Effective Access List"

Viewing an Effective Access List

You can use the **Effective Access List** window to view the access list for groups of users of a resource profile that are in your scope.

About this task

The **Effective Access List** contains all user IDs of the access list and all users that are in the groups on the access list. If a user is in more than one group on the access list, the highest access is displayed, just as RACF displays the access.

Procedure

To view the **Effective Access List** of a resource profile, follow these steps:

1. Select a resource profile from the main menu.
2. Select **Navigate > Effective Access List**.

   "Modifying an Access List (ACL)" on page 94 explains all columns of the resulting table except the **Via** column, which contains the connect group of the user that results in the access.

   Note:

   - In the **Options** dialog, you can specify whether Group Operations or System Operations (together with Universal Groups) are used when determining the **Effective Access List**.
   - When activated, the last option might cause a significant drop in performance while creating the Effective access list.
   - If a group on the access list is out of your scope, the access list displays the group but does not display its users.
   - When you load **Effective Access List**, the access list is loaded as well, so you can quickly switch to the access list.
   - This list is a snapshot. If you want to see any changes made after you display the list, you must close it and display it again.

Viewing a member list

You can use the **Members** window to view the member list of a general resource profile.

Procedure

1. To view the member list of a general resource profile, select the profile from the main menu.
2. Select **Navigate > Members**. See "Viewing and changing a member list" on page 99 for information about the columns of the resulting table.

Chapter 3. User management

The administrator uses IBM Security zSecure Visual to view the user table and properties, delete, duplicate, and resume users, set passwords, and use schedules. These tasks are described in the following topics.

"User table"
The administrator reviews user data, such as owner and status, in the User table.

"Viewing user properties" on page 42
The administrator uses the User properties window to view and edit the attributes and status of users.

"Duplicating a user" on page 46
The administrator uses the **Duplicate user** window to create a new user from existing users.

"Deleting a user" on page 49
The administrator uses the **Delete user** dialog to revoke access for one or more users.

"Resuming a user" on page 50
The administrator uses the **Resume user** dialog to resume a user that has revoked status.

"Disabling a user" on page 51
The administrator uses the **Disable user** dialog to prevent a user from logging on.

"Enabling a user" on page 51
The administrator uses the **Enable user** dialog to enable a revoked or disabled user to log on.

"Setting passwords" on page 53
The administrator uses the **Set Password** dialog to set or reset the user password.

"Setting a default password" on page 54
The administrator uses the **Edit default password** dialog to set the default password for a user.

"Removing the default password" on page 56
The administrator uses the **Edit default password** dialog to remove the default password for a user.

"About Schedules" on page 57
The administrator uses schedules to specify intervals during which a user is revoked or resumed.

User table

The administrator reviews user data, such as owner and status, in the User table.

The User table consists of a list of users and their properties. Use the **Find** dialog to open the User table. Every icon in the list can be either red or green. When an icon is green, it means that the user is active; when it is red, the user is revoked or inactive.

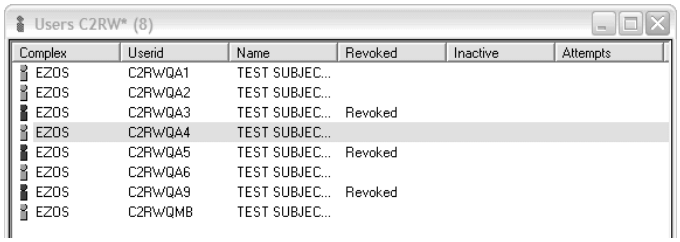


Figure 19. User table

Note: If your organization has configured site-specific fields with user information, those fields are on the right side of the dialog. Scroll right to view site-specific fields.

The User table has these columns:

Complex
The name of the complex where the result was found. This column is displayed only if you are operating in multi-system mode.

Userid
The RACF user ID.

Name Real name of the user, or any other description.

Site-specific fields
If configured, you might see fields with user information that have site-specific names and content. Site-specific fields are on the right of the `InstData` field if the `InstData` field is not replaced by the configured site-specific fields.

InstData
This field has a site-defined layout and purpose. Typically it contains organizational data on the user ID. The `InstData` field might be replaced by site-specific fields, depending on the configuration used by your organization.

Owner
The owner can change the user definition.

DefaultGrp
The default group is the group that the user automatically connects at logon.

Revoked
A revoked user cannot log on, but the profile is still present. A user can be revoked for these reasons:

- An administrator revokes the user.
- The user makes too many unsuccessful password attempts and is revoked automatically.
- An administrator schedules the revocation on a specified date.
- The user does not log on in a specified timeframe and is revoked automatically.

The status is derived from the revoke status flag, the current date, the revoke date, the resume date, and the date the user last logged on.

Inactive
A user ID becomes inactive when it is not used for a period of time set by

the SETROPTS INACTIVE command on the mainframe. An inactive user who tries to logon is revoked immediately. The field presented takes into account the RACF inactive setting and the last use date.

Note: If a user ID has never been used, it does not become inactive.

Expired
This field indicates whether the password has expired. When the password has expired, the user must change the password at the next logon. The field presented takes into account the current date, the password interval of the user, the system-wide password interval, and the most recent password change date.

Interval
The period in days after which the user needs to change the password.

Attempts
Count of logon attempts with an invalid password. This count is only kept if the RACF user revoke setting has been activated with the RACF SETROPTS PASSWORD(REVOKE(nn)) command on the mainframe. After nn invalid password attempts, the user is revoked.

LastConnect
This field contains the last RACINIT date for any group that the user is connected to.

Note: RACF uses a different date to calculate the inactivity interval of the user.

LastPwdChange
The most recent date the password is changed.

Created
Date on which the user is defined.

MappingsCount
The number of distributed identity filters that are associated with the user ID.

The extra selection fields for users in the **Find** dialog are:

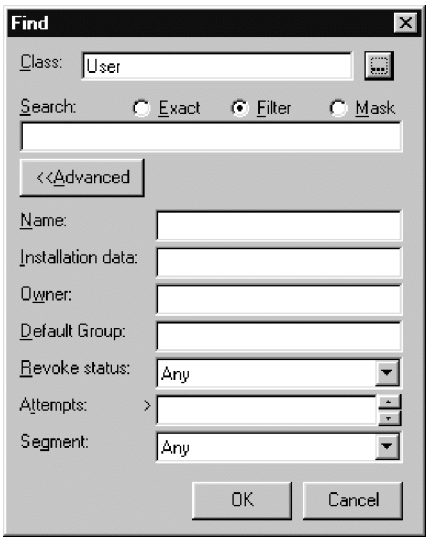


Figure 20. Find dialog for users

Name A substring that must exist in the name.

Installation data
A substring that must exist in the installation data.

Owner
Select users by owner. The field is used as a filter.

Default Group
Select users by default group. The field is used as a filter.

Revoke status
Select users that are revoked, not revoked, or independent of the revoke status.

Attempts
Select users that have more or less than a certain number of password attempts. A blank field selects users independent of the number of password attempts.

Segment
Select the users that have the segment you specify. If this option is grayed out, you cannot view segments or there are no segments. If you select Any, you have the complete user list, whether the profiles have segments or not.

Viewing user properties

The administrator uses the User properties window to view and edit the attributes and status of users.

About this task

The user property dialog presents the user properties in three categories: Attributes, More attributes, and Status.

Follow these steps to view the properties of a user.

Procedure

1. Select **Navigate > Properties** from the main menu. You can also start with these actions:
   - Select and double-click the user.
   - Select the user from the user table and press **Enter**.
   - Right-click a user and select **Properties** from the pop-up menu.
   - Click **Properties** on the toolbar.

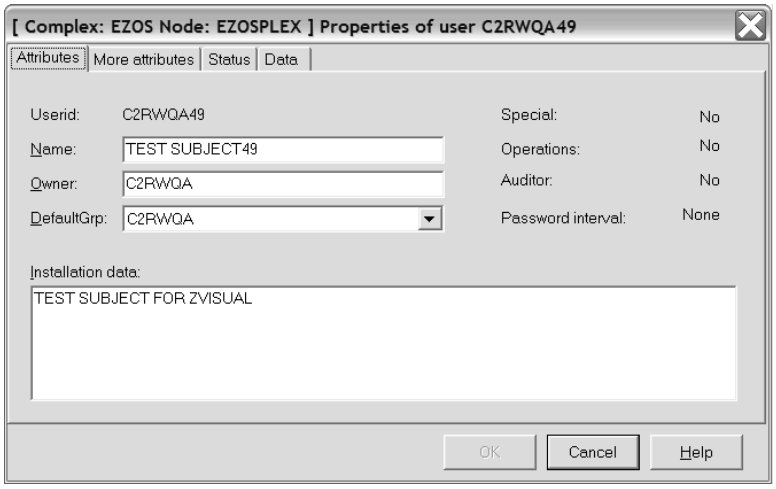


Figure 21. User properties dialog

If your organization configured four or less site-specific fields as a replacement for the installation data field, those fields are at the bottom of the dialog:

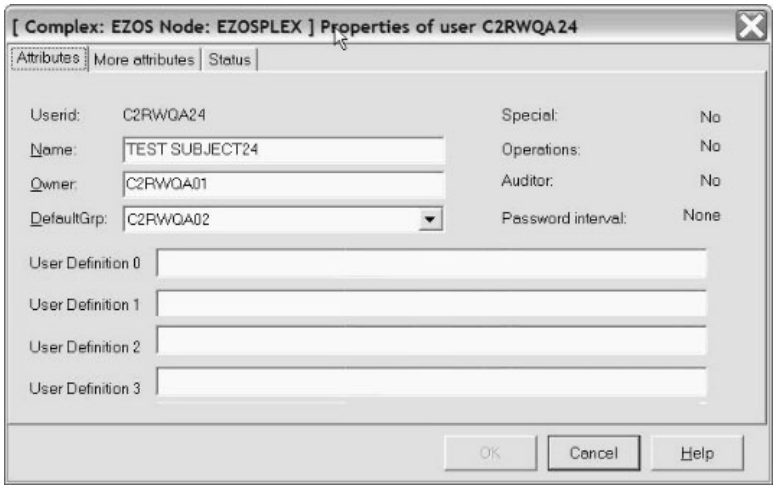


Figure 22. User properties dialog with site-specific fields

Note: If more than four site-specific fields are configured, or they are configured in addition to Installation data, those fields are shown in a panel with the separate tab named **Data**.

2. View or edit the fields as needed and click **OK** to accept the changes.

   Note: Your level of authorization determines whether you can edit the user properties.

The following information is included in the header of the dialog only if you are operating in multi-system mode:

Complex
The name of the complex associated with the user ID.

Node The name of the node associated with the user ID.

These fields are displayed in the **Attributes** tab:

Userid
The RACF user ID.

Name Real name of the user, or any other description.

Owner
The owner can change the user definition.

DefaultGrp
The *defaultgroup* is the group that the user automatically connects to at logon.

Site-specific fields
If configured, displays one or more fields with user information that have site-specific names and content. The contents are read-only.

Installation data
The purpose and layout of this field are site-defined. Typically it contains organizational data on the user ID. The installation data field can contain as much as 255 characters. The field is displayed in multiple lines as it is when displayed by the RACF LISTUSER command: the first line contains 62 characters and the succeeding lines contain 80 characters. A changed installation data field can be composed of the separate lines. It is possible to change the font of this field, see "Setting display preferences" on page 9.

The Installation data field might be replaced by site-specific fields, depending on the configuration used by your organization.

Special
System-wide special attribute.

Operations
System-wide operations attribute.

Auditor
System-wide auditor attribute.

Password interval
The period in days after which the user must change the password.

In the **More attributes** tab, you see these fields:

Security level
Security level.

Categories
Security categories to which the user has access.

Security label
Security label.

Class authorizations
Class in which the user is ed to define profiles.

In the **Status** tab, you see these fields or buttons:

Revoked
Revoked users cannot logon, but their profiles are still present. An administrator revokes the user, or the user is revoked automatically due to too many unsuccessful password attempts, or by scheduled actions. The status is derived from the revoke status flag, the current date, the revoke date, the resume date, and the last used date.

Inactive
An inactive user that tries to logon is revoked immediately. A user ID becomes inactive when it is not used for a period set by the SETROPTS INACTIVE command on the mainframe. The field presented takes into account the RACF inactive setting and the last use date.

Note: If a user ID is not used yet, it does not become inactive.

Expired
This field indicates whether the password expires. When the password expires, the user must change the password at the next logon. The field presented takes into account the current date, the password interval of the user, the system-wide password interval, and the most recent password change date.

Password attempts
Count of logon attempts with an invalid password. This count is only kept when the RACF user revoke setting is activated with the RACF SETROPTS PASSWORD(REVOKE(*nn*)) command on the mainframe. After *nn* invalid password attempts, the user is revoked.

Last password change
The most recent date the password is changed.

Last connect
This field contains the last RACINIT date for any group the user is connected to.

Note: RACF uses a different date to calculate the inactivity interval of the user.

Last logon
The last time the user logs on to RACF.

Created
Date on which the user is defined.

Mappings count
The number of distributed identity filters that are associated with the user ID.

The **Data** tab is displayed only if your organization has configured the use of site-specific fields in addition to the use of the **Installation data** field or when more than four site-specific fields have been configured. If site-specific fields are used as a replacement to the **Installation data** field, and there are four or less site-specific fields configured, the site-specific data is displayed in the **Attributes** tab.

When you execute the corresponding commands on the mainframe, you can use these buttons and check box for actions on the user ID.

Resume
Displays the **Resume** dialog. See “Resuming a user” on page 50.

Set Password
Displays the **Set Password** dialog. See “Setting passwords” on page 53.

Schedules
Displays the **Schedules** dialog. See “About Schedules” on page 57.

Mappings
Displays the Mappings window. See “Mappings” on page 60.

Duplicating a user

The administrator uses the **Duplicate user** window to create a new user from existing users.

About this task

You can generate new users by duplicating an existing user. You can take the existing user as the prototype user.

Note: If you are operating in multi-system mode, you can duplicate users across zSecure nodes only; you cannot duplicate users across multiple RRSF nodes.

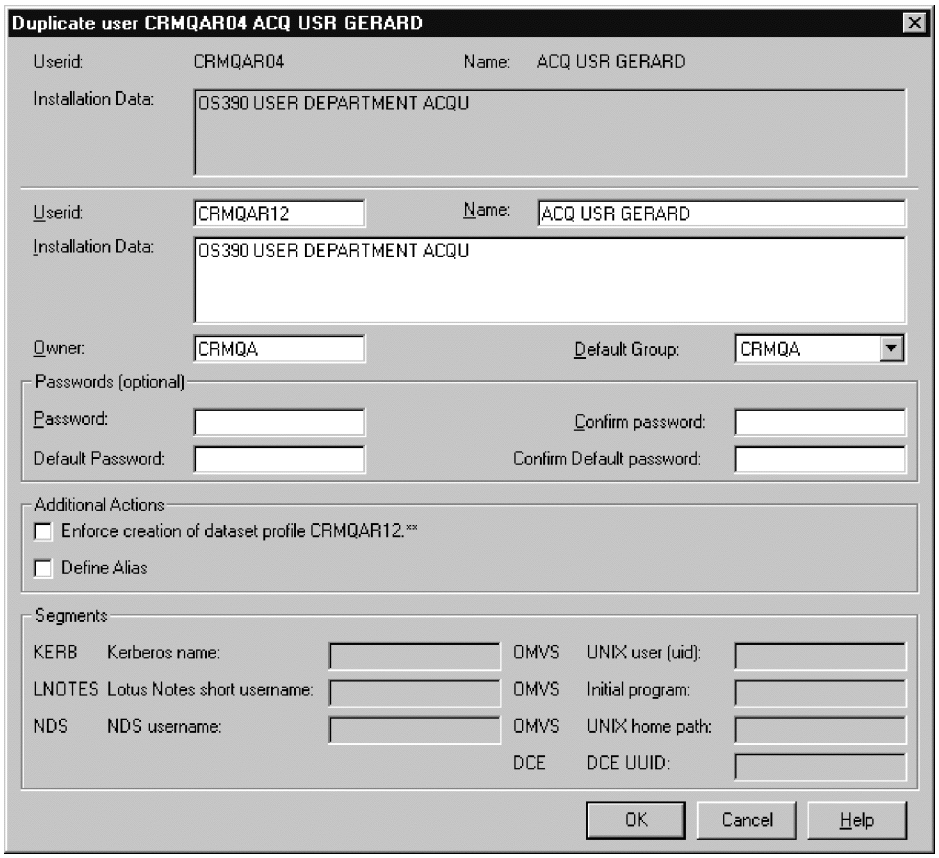


Figure 23. Duplicate user dialog

Procedure

To duplicate a user, follow these steps:

1. Select the prototype user in a user window and click **Action > Duplicate** in the main menu. You can also start with these actions:

- Select a user and click **Duplicate** on the toolbar.
- Right-click a user and select **Duplicate** from the pop-up menu.

2. Complete the fields in the dialog.

Userid
User ID of the new user.

Name Name of the new user.

Installation data
Installation data of the new user.

Owner
Owner of the new user.

Default Group
Default group of the new user. The default group must be one of the connected groups of the prototype user.

Passwords (optional)
The password fields are optional.

Password
Password of the new user.

Confirm password
Confirmation of the password of the new user.

Default password
Optional. Default value that you can set for the new user password. For more information, see "Setting a default password" on page 54.

Confirm default password
Confirms the value specified for the default password. Must be equal to the default password.

Additional Actions

Enforce creation of dataset profile
Create a generic data set profile with the new user ID as High Level Qualifier or HLQ. It has the new user ID as owner and a UACC of none. This command is also available on the Action menu.

Note: If the existing, prototype user already has one or more data set profiles with the HLQ equal to the user ID, these profiles can be copied instead. It is done regardless whether the check box here is on or off.

Define Alias
Defines an alias for the user pointing to the user catalog. You must know the user catalog data set name to use this option. This command is also available on the Action menu.

Note: This action attempts to retrieve the user catalog data set name by searching the XFACILIT class or the class configured as the Site Module general resource class during the server setup, as described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. It looks for profiles with names starting with "CKG.UCAT." using the SHOW MYACCESS command. If one or more such profiles are

found, this option can be activated. If more than one data set name is found, you are prompted to select one of them when activating the option.

Do not duplicate OMVS Segment
Prevents the duplication of the OMVS Segment of the existing user.

Segments
Use the segment fields to store information about specific subsystems or components of z/OS. If these segments are present for the original profile, the values are copied to the new user profile.

Some of these values must be changed while others can remain the same. If no value exists for the duplicated user or the segment is not in your scope, the field is disabled. For more information about authorities needed to manage segments, see "Authorities and settings required to manage segments" on page 103.

The fields shown in the panel are just a subset of all fields that are present in the segments. All other fields in your scope are copied unchanged. The segment fields are divided into two columns.

In the left column, you can find the segments that need **unique** values; you must change the value for the new user profile:

KERB Kerberos name
KERB KERBNAME field that defines the local Kerberos principal name of the user.

LNOTES Lotus® Notes® short username
LNOTES SNAME field indicating the short name as found in the Lotus Notes address book.

NDS username
NDS UNAME field defining the user name as stored in the Novell Directory Services for OS/390® directory.

In the right column, you can find the other segment fields. These values do not need to be unique per user profile:

OMVS UNIX user (uid)
OMVS UID field with the user identifier. To have the system assign an unused value, use "auto." If you want more than one user to share the UID, add "s" at the end of the UID value.

OMVS Initial program
OMVS PROGRAM field describing the path name of the first program to be started when an OMVS session is started.

OMVS UNIX home path
OMVS HOME field defining the hierarchical file system (HFS) directory path name of the working directory.

DCE UUID
DCE UUID field indicating the principal name of the user as defined in the DCE registry.

3. Click **OK** to start the duplication, or click **Cancel** to quit the dialog without changes. The field values are validated to determine whether the unique fields differ from the original values. If no field is changed, this warning displays and the dialog is not closed:

```
Please change the <Name> field. It needs to be unique for this system.
```

Note: There is no check whether the value is unique in the RACF database. Checking on this scale triggers a full database read, which can consume system and network resources for an extended period.

4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of zSecure nodes. You cannot duplicate a user across multiple RRSF nodes. If you have performed an action already, the zSecure nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
   b. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Deleting a user

The administrator uses the **Delete user** dialog to revoke access for one or more users.

About this task

You cannot delete users from the RACF database if you are using zSecure Visual. However, you can revoke their access by marking them for deletion. You can revoke access for one or more selected users.

Follow these steps to revoke user access.

Procedure

1. Select a user ID and click **Action > Delete** in the main menu. You can also revoke user access using these actions:
   - Right-click a user ID to display the pop-up menu and select **Delete**.
   - Select a user ID and click **Delete** from the toolbar.
   - Drop the users on the Recycle Bin.
2. Enter a reason for the deletion. This reason is displayed if you undo a **Delete**.
3. Click **OK**, or click **Cancel** to quit the dialog to discard any changes. The selected user IDs are disabled in the $DELETE schedules of the users.

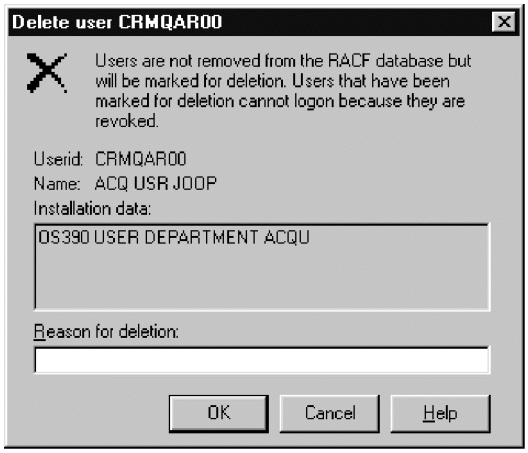


Figure 24. Mark user for deletion dialog

If you are using multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:

a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the drop-down list an alternative user ID to run the command.
c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Results

To undo **Delete**, go to the schedules of the user and delete the disabled action in the $DELETE schedule. If there are no other scheduled actions, you must also resume the user. A related dialog is displayed in that case.

Resuming a user

The administrator uses the **Resume user** dialog to resume a user that has revoked status.

About this task

A resume resets the revoke status of the user. It succeeds only if the revoke is not due to scheduled actions. In that case, you must delete the scheduled action.

To resume one or more users in single-node mode, complete these steps.

Procedure

1. Select the user IDs and click **Action > Resume** from the main menu. You can also use these actions:
   - Right-click the user IDs to display the pop-up menu and select **Resume**.
   - Select the user IDs and click **Resume** on the toolbar.

   The **Resume user userid *userid*** dialog is displayed for one of the users you selected:

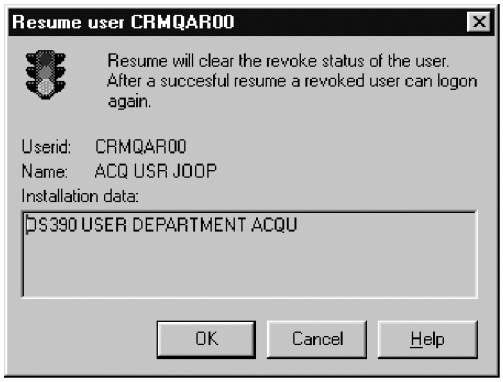


Figure 25. Resume user dialog

2. Click **OK** to invoke the resume, or click **Cancel** to return to the previous dialog.
3. If you are resuming two or more users, the **Resume user** ***userid*** dialog is displayed for each user you select. Click **OK** in each dialog to finish resuming all selected users.

Disabling a user

The administrator uses the **Disable user** dialog to prevent a user from logging on.

About this task

You can disable a user from logging on. The disabling schedule starts the same day you set the option. To use this option, you need UPDATE or better on resource CKG.CMD.USER.REQ.SCHEDULE and at least one schedule in your scope, excluding the reserved $DELETE schedule.

To disable a user, follow these steps:

Procedure

1. Select a user ID from the main menu.
2. Select **Action > Disable**, or right-click a user ID and select **Disable** from the pop-up menu:

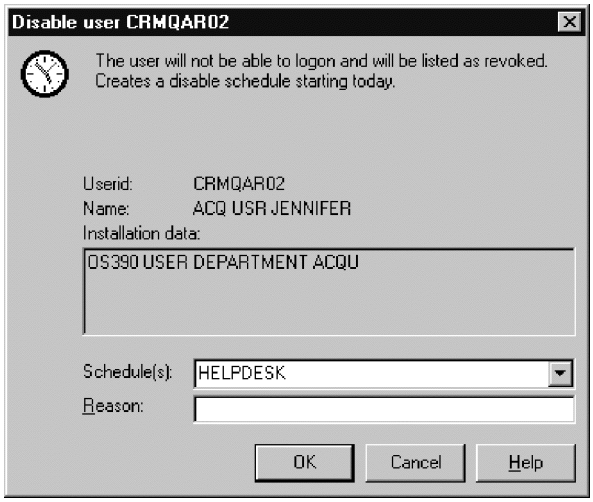


Figure 26. Disable user dialog

   If you are operating in multi-system mode, the node associated with the user is displayed in the header of the dialog.
3. Enter the reason for disabling the user. If the user is already disabled, the reason can be shown in the **Details** field.
4. Click **OK** to finish.

Enabling a user

The administrator uses the **Enable user** dialog to enable a revoked or disabled user to log on.

About this task

You can enable a revoked or disabled user to log on again. When enabling a user, any schedule that disables the user expires. If there is more than one schedule available to enable the user, you can select any one of them from the selection list.

To use this option, you need UPDATE or better on resource CKG.CMD.USER.REQ.SCHEDULE and at least one schedule in your scope, excluding the reserved $DELETE schedule.

To enable a user, follow these steps:

Procedure

1. Select a user ID and select **Action > Enable** from the main menu, or right-click a user ID and select **Enable** from the pop-up menu:

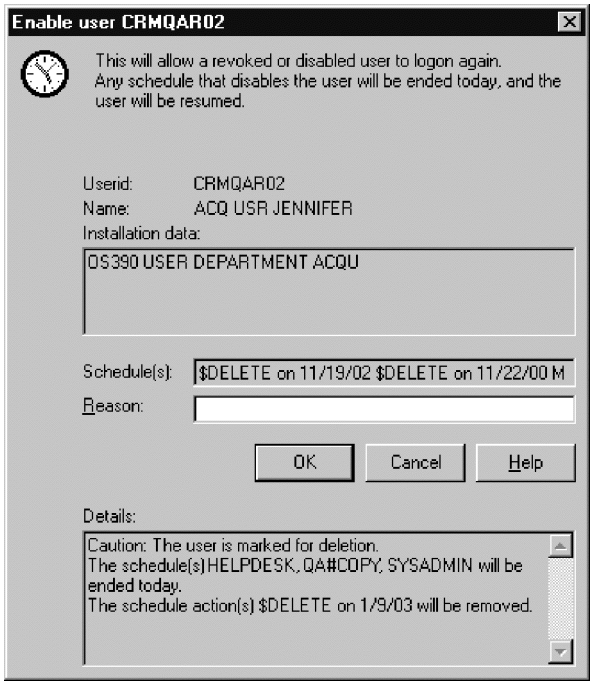


Figure 27. Enable user dialog

   If you are operating in multi-system mode, the node associated with the user is displayed in the header of the dialog.
2. Enter the reason for enabling the user. If a future schedule disables the user again, the reason can be shown in the **Details** field. If no schedules exist to disable the user, a dialog is displayed to do a normal resume.

   Note: The **Enable** user dialog is displayed even if you do not have the authority to resume.
3. If the user is marked for deletion, confirm the enabling action. Once confirmed, the user is no longer marked for deletion. If the user is disabled with one or more schedules that are out of your scope, an error message is displayed that lists the out-of-scope schedules.
4. Click **OK** to finish.

5. To enable users on multiple systems, select each user individually in the list of users, then repeat these steps.

Setting passwords

The administrator uses the **Set Password** dialog to set or reset the user password.

About this task

The **Set Password** dialog lets you set the user password. To set a password, follow these steps:

Procedure

1. Select a user ID and select **Action > Set Password** from the main menu. You can also start with these actions:
   - Right-click a user ID to display the pop-up menu and select **Set Password**.
   - Select a user ID and click **Set Password** on the toolbar.

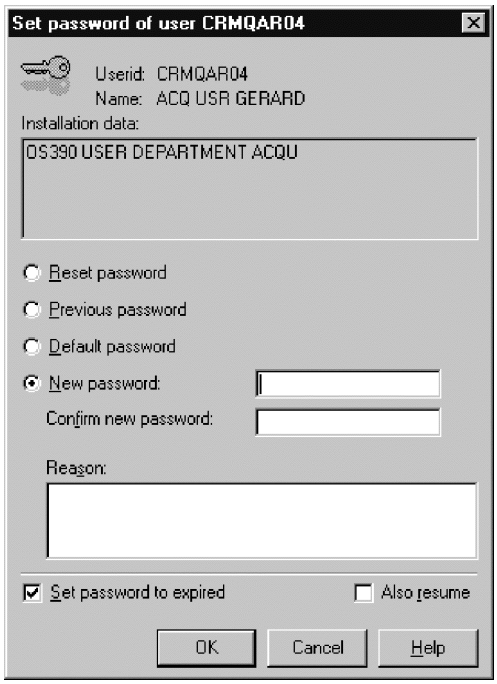


Figure 28. Set password dialog

If you are operating in multi-system mode, the complex and node associated with the user is displayed in the header of the dialog.

The available options and checkboxes depend on your update access level. If your client display is set to **Gray desired unauthorized functions**, you can view the unavailable options. If your client display is set to **Hide desired unauthorized functions**, you see only the available options and checkboxes. See "Setting interface options according to your access level" on page 11. The next step describes all possible options and checkboxes.

2. Complete the appropriate fields in the dialog.

Reset Password
Sets the password to the default password and sets the password to "expired."

Previous password
Sets the password back to the previous password. This setting works only if a password history is maintained in RACF and the user remembers the previous password.

Default password
Sets the password to the default password that the administrator set previously.

New password
Sets the password to a new value. You must confirm the new value by retyping it in the **Confirm new password** field. This value must be compliant with the password rules. It must not occur in the password history unless you have the necessary access to the corresponding resources to bypass these checks. See *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide* for more information about specifying passwords.

Reason
Logs the reason why the password is changed. Depending on company policy, input might be required. Examples are: *Forgotten password*, *Never used*, and *Revoked*.

Set password to expired
When this option is active, the new password becomes expired. When the user logs on, the user has to specify a new password.

Also resume
Resumes the user ID when resetting the password. When the user is revoked due to too many unsuccessful password attempts, a resume is required to enable the logon again. Use Resume to avoid setting the password.

3. Click **OK** to finish, or click **Cancel** to quit the dialog without changes. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed.
4. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the drop-down list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Setting a default password

The administrator uses the **Edit default password** dialog to set the default password for a user.

About this task

The default password is a fixed value the user can set. By default, the default password is set system-wide. It is outside the scope of zSecure Visual. However, it is more secure to set an individual default password for each user, especially for users with important roles.

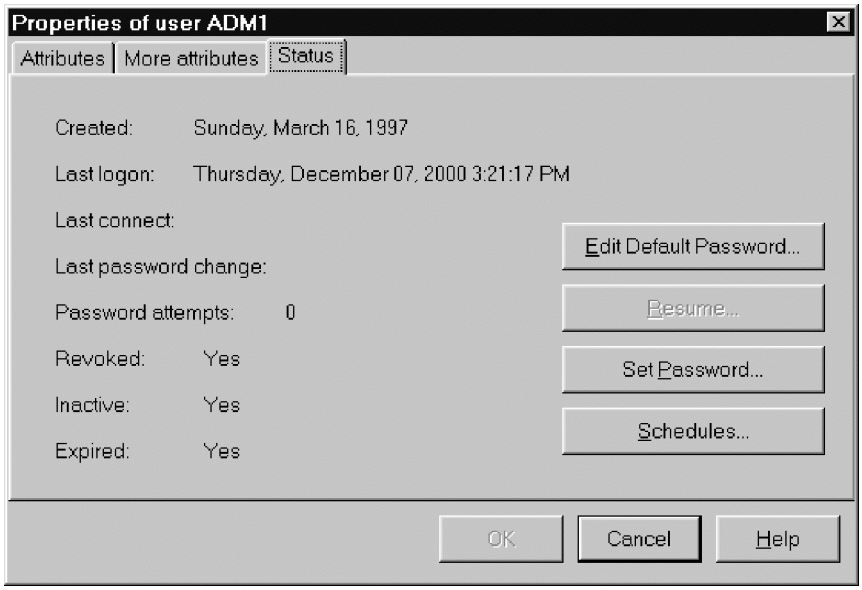


Figure 29. Status

To set the default password, perform these steps:

Procedure

1. Select a user ID and select **Navigate > Properties** from the main menu to open the properties dialog.
2. Select the **Status** tab.
3. Click **Edit Default Password** to open the **Edit Default Password** dialog.

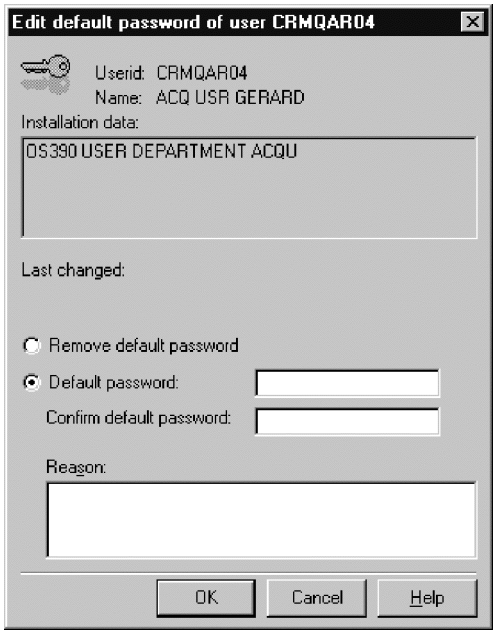


Figure 30. Edit default password dialog

4. Check the **Default Password** box.
5. Type and confirm the default password.
6. Optionally, enter the reason why the default password is changed.
7. Click **OK** to finish, or click **Cancel** to quit the dialog without changes.
8. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the drop-down list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Removing the default password

The administrator uses the **Edit default password** dialog to remove the default password for a user.

About this task

Removing or changing the default password does not affect the normal password. The normal password changes to the default password only if it is reset to it. If you change the default password after resetting, it does not affect the normal password; it retains the old default value.

Procedure

You can remove the default password using these steps:

1. Select a user ID and select **Navigate > Properties** from the main menu to open the properties dialog.
2. Select the **Status** tab.
3. Click **Edit Default Password** to open the **Edit Default Password** dialog.
4. Select the **Remove Default Password** box.
5. Optionally, enter the reason why the default password is removed.
6. Click **OK**. When a default password is set, the **Edit default password** dialog displays this information:
   - The user ID of the person who changed the password
   - The date and time of the change

About Schedules

The administrator uses schedules to specify intervals during which a user is revoked or resumed.

The only way to revoke a user in zSecure Visual is to use schedules. Schedules are a facility provided by the CKGRACF mainframe program that enables different groups of administrators to set the revoke status of a user.

You can separately revoke and resume a user, or you can combine these two actions. These are called intervals. The CKGRACF program updates the revoke flags of the user based on the schedules. A disabling interval starts with a revoke and ends with a resume. An enabling interval starts with a resume and ends with a revoke. A single revoke or resume corresponds with an interval without an end date. All actions of an interval are written to the RACF database, together with the schedule name, date, author, and reason. The schedule name is categorize intervals. New intervals wipe previous conflicting actions only in the same schedule. When all past scheduled actions are deleted, CKGRACF leaves the user's revoke status unchanged.

The equivalent of revoking a user is Disable from today forever. The equivalent of deleting a user is Disable from today forever with schedule name $DELETE. The deletion is sent to the mainframe after you click OK in the schedules dialog.

Users are only able to log on when all scheduled actions enable them to. Schedules can be set by centralized and decentralized administrators. When given access to just a part of the defined schedule names while others reserved for centralized administrators only, decentralized administrators cannot undo intervals set by a centralized administrator.

Viewing and editing schedules

The administrator uses the **Schedules** dialog to view, set, or edit schedules that revoke or resume users.

Procedure

- To view the schedules of a user, perform one of these steps:
  1. Select the user and select **Navigate > Schedules** from the main menu.
  2. Right-click the user to display the pop-up menu and select **Schedules**.

3. Select the user and click **Schedules** on the toolbar.

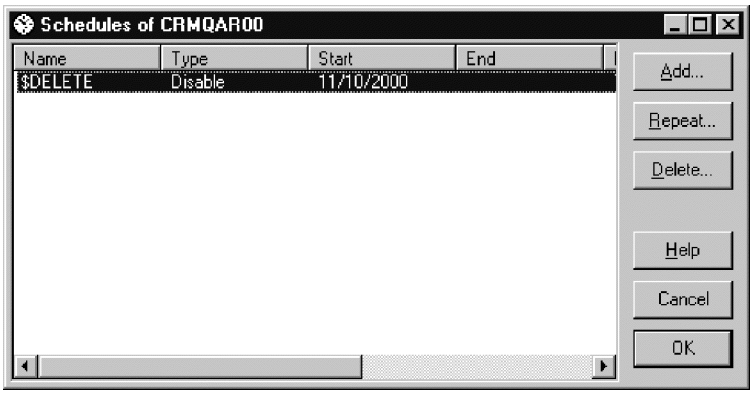


Figure 31. Schedules dialog

A schedule dialog window displays these columns:

Name Name of the schedule.

Type Type of the interval, either Enable or Disable.

Start Start date of the interval.

End End date of the interval.

Reason column
Reason of the schedule.

Author
Administrator who enters the schedule.

Created
Date and time the author enters the interval.

- To edit schedules, perform these steps:
  1. Click **Add** to add an interval to the table.
  2. Select an interval and click **Repeat** to enter a similar interval in the table.
  3. Select an interval and click **Delete** or press the **Delete** key to delete an interval from the table.
  4. After you edit schedules, click **OK** to apply the changes to the RACF database, or click **Cancel** to cancel the changes.

Adding a schedule interval

The administrator uses the **Add schedule** dialog to add a new schedule that enables or disables a user.

Procedure

To add a schedule interval, follow these steps:

1. Select a user and select **Navigate > Schedules > Add** from the main menu. The **Add schedule interval** dialog displays.

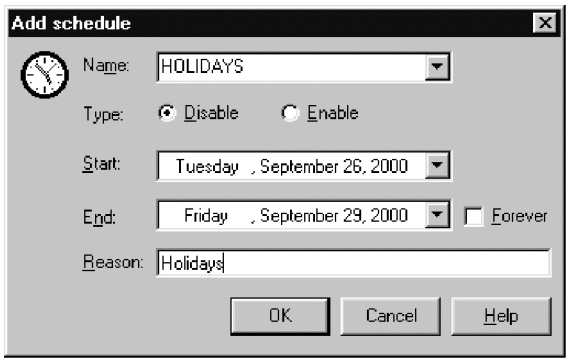


Figure 32. Add schedule interval dialog

2. Enter the fields and click **OK** to add the schedule to the table. The new schedule interval becomes active after clicking **OK** in the **Schedules** dialog.

   The dialog contains these fields:

   Name Name of the schedule. You can select one of the predefined names or type a new name.

   Type Select **Disable** to disable the user for a certain period, select **Enable** to enable the user.

   Start Enter the start date of the interval. The start date is included in the interval.

   End Either enter an end date, or select **Forever** to indicate there is no end date for this interval. The end date is included in the interval.

   Reason
   Enter a reason for the enabling or disabling the user.

Repeating a schedule interval

The administrator uses the **Repeat** function to make a new schedule based on an existing schedule.

You cannot edit an existing schedule, but with the **Repeat** function, you can make a new schedule based on the existing one. If the existing schedule and the new schedule overlap, the program creates a new schedule. The new schedule begins at the earliest start date and ends at the last termination date.

To create a new schedule using the existing schedule, select **Navigate > Schedules > Repeat** from the main menu.

Deleting a schedule interval

The administrator uses the **Delete schedule** dialog to delete an existing schedule interval.

Procedure

To delete a schedule, follow these steps:

1. Select a schedule interval and click **Delete**.

   The **Delete schedule** interval dialog displays the properties of the schedule.

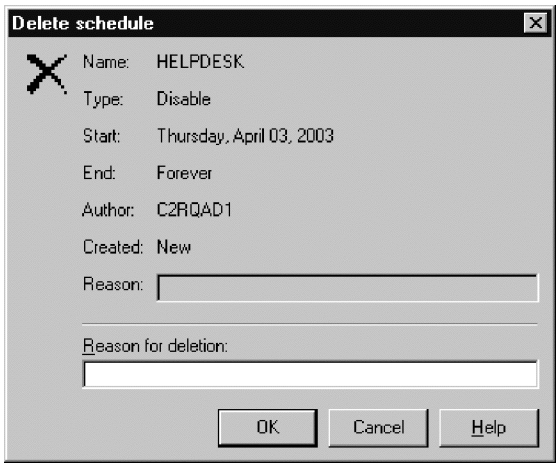


Figure 33. Delete schedule interval dialog

2. For auditing purposes, enter a reason for the deletion.
3. Click **OK** to delete the schedule interval. The deletion is sent to the mainframe after you click **OK** in the schedules dialog.

Mappings

The administrator uses mapping profiles to determine the distributed identity filters associated with RACF user IDs.

RACF supports distributed identity filters which are mapping associations between a RACF user ID and one or more distributed user identities, as they are known to Web-based application servers and defined in distributed user registries. The **Mappings** window provides the information about distributed identity filters associated with the RACF user ID. These filters are in fact the IDIDMAP profiles. For the remainder of this chapter, such profiles are referred as mapping profiles.

Viewing mappings

The administrator uses the various **Mappings** selections to view information about the mapping profile of a user.

Procedure

To view mapping information of a user, perform one of these steps:

- Select the user and select **Navigate > Mappings** from the main menu.
- Right-click the user to display the pop-up menu and select **Mappings**.
- Click the **Mappings** button on the **User Properties** dialog.

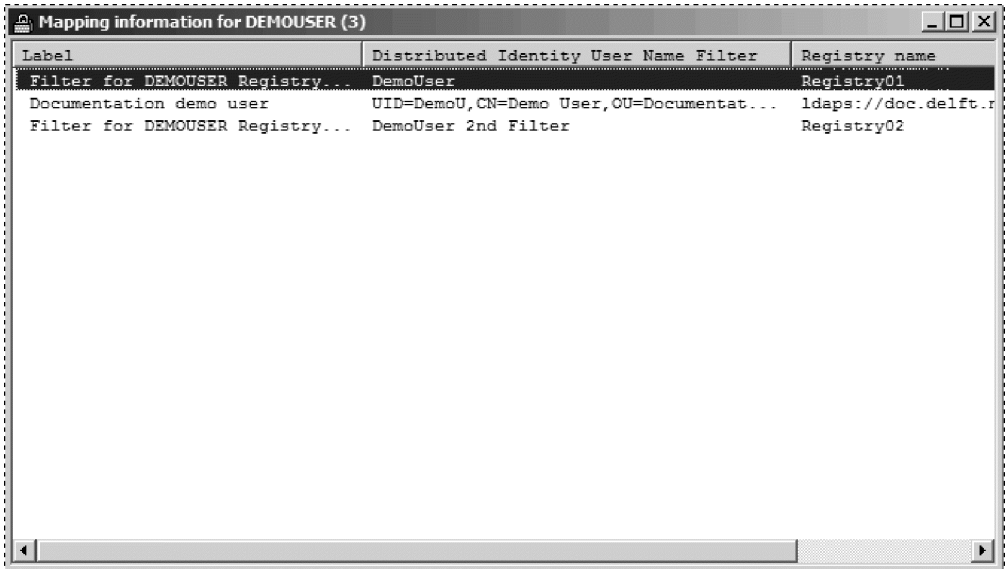


Figure 34. Mapping information for a user

A Mappings window displays these columns:

Label The label associated with this mapping profile.

Distributed Identity User Name Filter
The name of the mapping profile.

Registry name
The registry name of the mapping profile.

Chapter 4. Group management

The administrator uses IBM Security zSecure Visual to display, add, duplicate, and delete groups. These tasks are described in the following topics

"Group table"
The administrator reviews group data, such as owner and connected users, in the Groups table.

"Viewing group properties" on page 65
The administrator uses the **Properties of group** window to view and edit the attributes and status of groups.

"Adding a subgroup" on page 67
The administrator uses the **Add subgroup** dialog to add a new subgroup to a group.

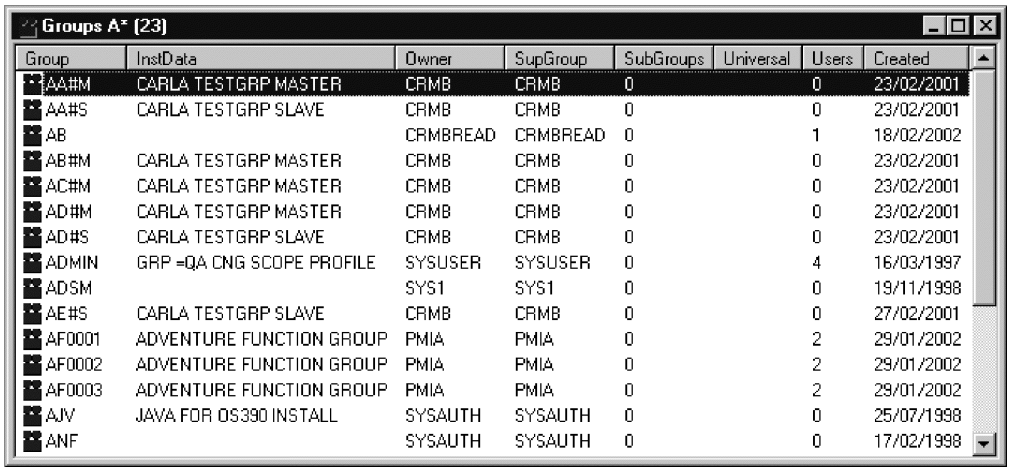
"Duplicating a group" on page 69
The administrator uses the **Duplicate group** window to create a new group from an existing group.

"Deleting a group" on page 71
The administrator uses the **Delete group** dialog to delete a group or to prevent users from using the group (incomplete deletion).

Group table

The administrator reviews group data, such as owner and connected users, in the Groups table.

Use the **Find** dialog to view a list of groups. A group is displayed in two colors, blue as default and gray when the installation data of the group is not yet loaded.



Group	InstData	Owner	SupGroup	SubGroups	Universal	Users	Created
AA#M	CARLA TESTGRP MASTER	CRMB	CRMB	0		0	23/02/2001
AA#S	CARLA TESTGRP SLAVE	CRMB	CRMB	0		0	23/02/2001
AB		CRMBREAD	CRMBREAD	0		1	18/02/2002
AB#M	CARLA TESTGRP MASTER	CRMB	CRMB	0		0	23/02/2001
AC#M	CARLA TESTGRP MASTER	CRMB	CRMB	0		0	23/02/2001
AD#M	CARLA TESTGRP MASTER	CRMB	CRMB	0		0	23/02/2001
AD#S	CARLA TESTGRP SLAVE	CRMB	CRMB	0		0	23/02/2001
ADMIN	GRP =QA CNG SCOPE PROFILE	SYSUSER	SYSUSER	0		4	16/03/1997
ADSM		SYS1	SYS1	0		0	19/11/1998
AE#S	CARLA TESTGRP SLAVE	CRMB	CRMB	0		0	27/02/2001
AF0001	ADVENTURE FUNCTION GROUP	PMIA	PMIA	0		2	29/01/2002
AF0002	ADVENTURE FUNCTION GROUP	PMIA	PMIA	0		2	29/01/2002
AF0003	ADVENTURE FUNCTION GROUP	PMIA	PMIA	0		2	29/01/2002
AJV	JAVA FOR OS390 INSTALL	SYSAUTH	SYSAUTH	0		0	25/07/1998
ANF		SYSAUTH	SYSAUTH	0		0	17/02/1998

Figure 35. Groups table

The list of groups has these columns:

Complex
The name of the complex where the result was found. This column is displayed only if you are operating in multi-system mode.

Group The ID of the RACF group.

InstData
The purpose and layout of this field are site-defined. Typically it contains organizational data on the group.

Owner
The owner can change the group definition.

SupGroup
The superior group of the group. All groups except group SYS1 belong to one superior group.

SubGroups
Number of subgroups of the group. A subgroup is a group that belongs to another group.

Universal
A universal group can have an unlimited number of users with USE authority connected to it.

Note:

1. A group can be created as a universal group. It is not possible to change the attribute after creation.
2. In most cases, it is not possible to delete a universal group.
3. The old limitation of 5957 connections is still valid for users with authority higher than USE or with the attributes SPECIAL, OPERATIONS, or AUDITOR at the group level.
4. For universal groups, the Connected Users table shows only the users with authority higher than USE or with the attributes SPECIAL, OPERATIONS, or AUDITOR at the group level.
5. On sites where universal groups are not yet supported, the Universal column or field stays empty and disabled.

Users Number of users connected to the group.

Created
Date of creation of the group.

The extra selection fields for groups in the **Find** dialog are:

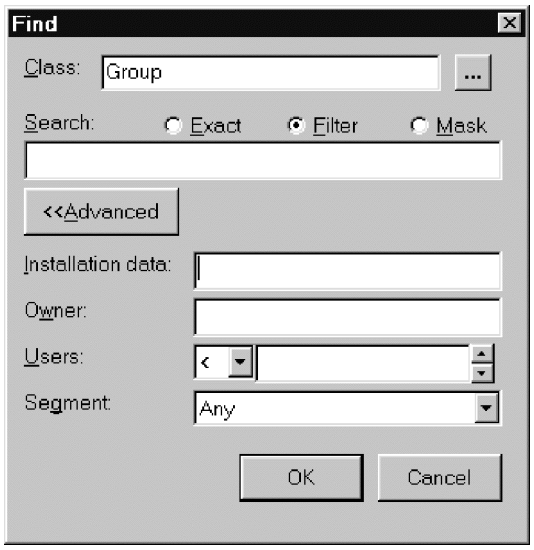


Figure 36. Find dialog for groups

Installation data
A substring that appears in the installation data.

Owner
Select groups by owner. The field is used as a filter.

Users Select groups that have more or less than a certain number of connected users. A blank in the number field selects groups independently of this number. Typing < or > in the number field selects the corresponding operator.

Segment
Select the groups that have the segment you specified. If this option is grayed out, you cannot view segments or there are no segments. The option ANY gives you the complete group list, whether the profiles have segments or not.

Viewing group properties

The administrator uses the **Properties of group** window to view and edit the attributes and status of groups.

About this task

The Group properties dialog provides detailed information about a specific group.

To view the properties of a group, perform one of these steps.

Procedure

1. Select a group and select **Navigate > Properties** from the main menu.

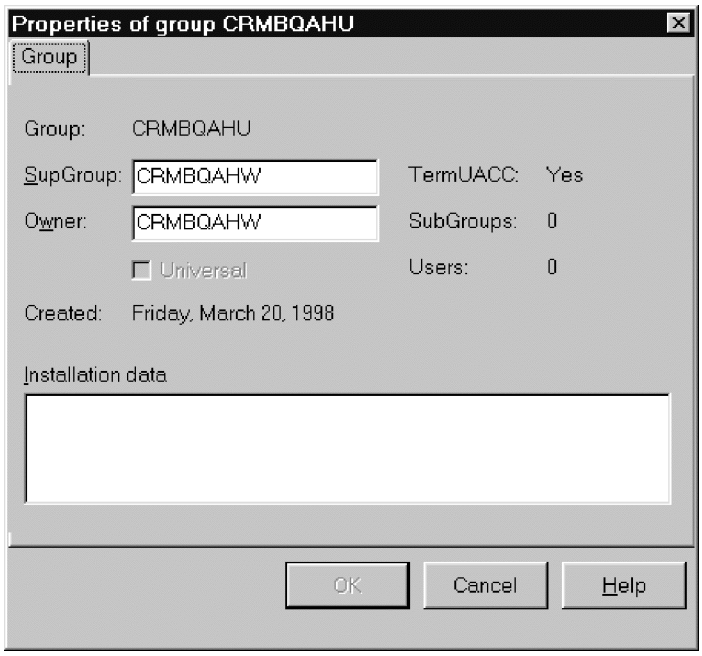


Figure 37. Group properties dialog

2. Double-click on the group.
3. Select a group and press **Enter**.
4. Right-click a group and select **Properties** from the pop-up menu.
5. Select a group and click **Properties** on the toolbar.

   The following information is included in the header of the dialog only if you are operating in multi-system mode:

   Complex
   The name of the complex associated with the user ID.

   Node The name of the node associated with the user ID.

   The **Properties** dialog contains these fields:

   Group The ID of the RACF group.

   SupGroup
   The superior group of the group. All groups except group SYS1 belong to one superior group. You can change this field to another existing group name.

   TermUACC
   Terminal access is granted through the UACC of TERMINAL profiles, as well as through access list entries.

   Owner
   The owner can change the group definition. You can change this field for another existing group name.

   SubGroups
   Number of subgroups of the group. A subgroup is a group that belongs to another group.

   Universal
   A universal group can have an unlimited number of users with USE authority connected to it. This field is read-only.

Note:

a. A group can be created as universal group. It is not possible to change the attribute after creation.

b. In most cases, it is not possible to delete a universal group.

c. The old limitation of 5957 connections is still valid for users with authority higher than USE or with the attributes SPECIAL, OPERATIONS, or AUDITOR at the group level.

d. For universal groups, the Connected Users table shows only the users with authority higher than USE or with the attributes SPECIAL, OPERATIONS, or AUDITOR at the group level.

e. On sites where universal groups are not yet supported, the Universal column or field stays empty and disabled.

Created
Date of creation of the group.

Installation data
The purpose and layout of this field are defined by your organization. You can change the contents of this field.

Adding a subgroup

The administrator uses the **Add subgroup** dialog to add a new subgroup to a group.

Procedure

To add a new subgroup to group, complete these steps:

1. Select a group and select **Action>Add subgroup** from the main menu. You can also start with these actions:
   - Click **Add subgroup** on the toolbar.
   - Right-click a group and select **Add subgroup** from the pop-up menu.

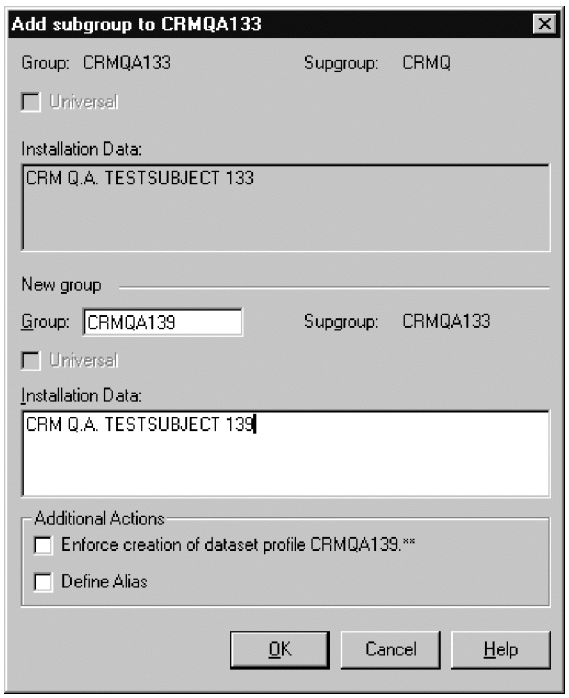


Figure 38. Add subgroup dialog

The following information is displayed for your reference:

Complex: Node
The complex and node names to which this action applies are displayed in the header of the dialog only if you are operating in multi-system mode.

Group Displays the name of the group to which you are adding a subgroup.

Supgroup
Displays the supergroup of the group to which you are adding a subgroup.

Universal
Indicates whether the selected group is a universal group.

Installation Data
Displays the data for the group to which you are adding a new subgroup.

2. Change these fields as needed:

New group

Group Required. You must change the name from the copied name to a new name.

Installation Data
Required. You must change the copied data to new data.

Additional Actions

Enforce creation of data set profile
Optional. Creates a generic data set profile with the new group name as High Level Qualifier or HLQ. It has the new group as owner and a UACC of none. This command is also available on the Action menu.

Define Alias

Optional. Defines an alias for the group pointing to the user catalog. You must know the user catalog data set name to use this option. This command is also available on the Action menu. This action attempts to retrieve the user catalog data set name by searching the XFACILIT class, or the class configured as the Site Module general resource class during the server setup, as described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. It looks for profiles with names starting with "CKG.UCAT." using the SHOW MYACCESS command. If one or more such profiles are found, this option can be activated. If more than one data set name is found, you are prompted to select one of them when activating the option.

Note: Note: If your access is NONE, the profiles with names starting with "CKG.UCAT." are ignored.

3. Click **OK** to create the subgroup, or click **Cancel** to cancel the change.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the drop-down list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Duplicating a group

The administrator uses the **Duplicate group** window to create a new group from an existing group.

About this task

You can create a group by duplicating a group, or by adding a new subgroup to a group. The duplicate group has the same connects, permits, and attributes as the original group. Adding a subgroup to a group is described in “Adding a subgroup” on page 67.

Note: If you are operating in multi-system mode, you can duplicate groups across zSecure nodes only; you cannot duplicate groups across multiple RRSF nodes.

Procedure

To duplicate a group, follow these steps:

1. Select a group and click **Action > Duplicate** in the main menu. You can also start with these actions:
   - Select a group and click **Duplicate** on the toolbar.
   - Right-click a group and select **Duplicate** from the pop-up menu.

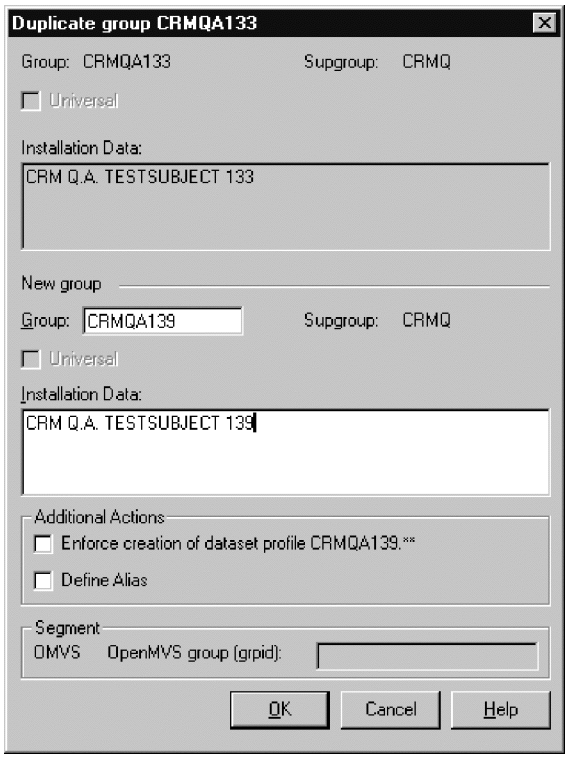


Figure 39. Duplicate group dialog

The following information is displayed for your reference:

Complex: Node
The complex and node names to which this action applies are displayed in the header of the dialog only if you are operating in multi-system mode.

Group Displays the name of the group from which you are creating the new group.

Supgroup
Displays the supergroup of the group from which you are creating a group. This group becomes the supergroup of the new group.

Universal
Indicates whether the selected group is a universal group.

Installation Data
Displays the data for the group from which you are creating a new group.

2. Change these fields as needed:

New group

Group Required. Change the name from the copied name to a new name.

Installation Data
Required. The data shown is copied from the group you are using to create the new group. You can change the copied data to new data.

Additional Actions

Enforce creation of data set profile
Optional. Creates a generic data set profile with the new group name as High Level Qualifier or HLQ. It has the new group as owner and a UACC of none. This command is also available on the Action menu.

Define Alias
Optional. Defines an alias for the group pointing to the user catalog. You must know the user catalog data set name to use this option. This command is also available on the Action menu.

Note: This action attempts to retrieve the user catalog data set name by searching the XFACILIT class, or the class configured as the Site Module general resource class during the server setup, as described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. It looks for profiles with names starting with "CKG.UCAT." using the SHOW MYACCESS command. If one or more such profiles are found, this option can be activated. If more than one data set name is found, you are prompted to select one of them when activating the option.

Do not duplicate OMVS Segment
Prevents the duplication of the OMVS Segment of the existing group.

Segment
If the segment is present in the original group profile, the value is copied to the new group and displayed in this field. If no segment value exists for the duplicated group or if the segment is not in your scope, this field is disabled. If this field is disabled, you cannot create this segment for the new group in this dialog. For more information about the authorities needed to manage segments, see "Authorities and settings required to manage segments" on page 103.

OMVS OpenMVS group (grpid)
The OMVS group identifier. To have the system assign an unused value, use "auto." If you want more than one group to share the group ID, add "s" at the end of the grpid value.

3. Click **OK** to create the duplicate group, or click **Cancel** to cancel the changes.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the zSecure nodes that you selected previously are displayed.

   Complete the following steps if you are using multi-system mode.

   Note: You cannot duplicate a group across multiple RRSF nodes.

   a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
   b. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Deleting a group

The administrator uses the **Delete group** dialog to delete a group or to prevent users from using the group (incomplete deletion).

About this task

You can delete a group only if the group does not own resources. If the group owns resources, the group remains present. However, because all permits and connects have been removed, no user can use the group. A dialog is displayed to inform you about the incomplete deletion.

Procedure

Follow these steps to delete a group:

1. Select the group and click **Action > Delete** in the main menu. You can also use these actions:
   - Select the group and press the **Delete** key.
   - Right-click a group to display the pop-up menu and select **Delete**.
   - Select the group and click **Delete** from the toolbar.

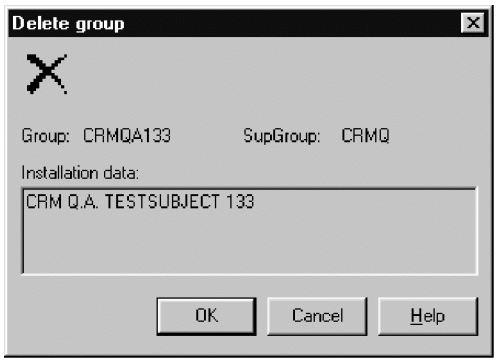


Figure 40. Delete group dialog

   The dialog lists the **Group**, **SupGroup**, and Installation Data of the group to be deleted. If you are operating in multi-system mode, the associated complex and node names are listed at the top of the dialog.
2. Click **OK** to delete the group, or click **Cancel** to quit the dialog without making changes.
3. If you are using multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed.

   Complete these steps if you are using multi-system mode:

   a. Specify the nodes to which the action applies. You must select at least one node to continue. The local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the drop-down list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Chapter 5. Connect management

The administrator performs connect management tasks in the Visual Client to establish and maintain the connection associations between users and groups.

RACF users are connected to one or more groups. Different kinds of connects result in different authorizations for the users. Users get at least some of the authorizations of their groups. Their authorizations depend on the attributes of the connect, but they can use the resources that their groups have access to. Connection relationships between users and groups are described in the following topics.

Connects table

The administrator reviews connects and access levels for a user or group in the Connects table.

The **Connects** table displays the connects of a user or group. Use these methods to open the connects table:

- Select a user or group and select **Navigate > Connects** from the main menu.
- Right-click a user or group and select **Connects** from the pop-up menu.
- Select a user or group and click **Connect** on the toolbar.

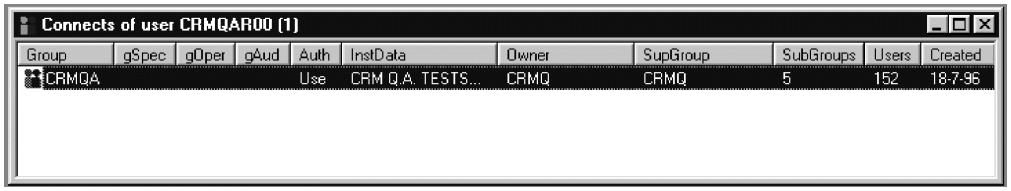


Figure 41. Connects table

The **Connects** table has the following columns.

For groups, the other columns are the same as the group table in “Group table” on page 63.

Note: For universal groups, the Connected Users table shows only the users with authority higher than USE or with the SPECIAL, OPERATIONS, or AUDITOR attributes at the group level.

For users, the other columns are the same as the user table in “User table” on page 39, except the revoked column. The revoked column indicates the users whose connection to the group is revoked.

Complex
The name of the complex where the result was found. This field is displayed only if you are operating in multi-system mode.

Auth Connect authority. The value can be any of these options:

Use The user can access the resources that the group has access to.

Create The user has the same authorizations as with **Use**. The user is also authorized to create data sets and data set profiles that have a High-Level-Qualifier (HLQ) as the name of the group.

Connect
The user has the same authorizations as with **Create** and is also authorized to connect existing users to the group.

Join The user has the same authorizations as with **Connect** and is also authorized to create new subgroups.

gSpec Group special attribute. When a user is connected with the group special attribute, the user can do everything with users, groups, and resources that are in the scope of the group, except changing auditing attributes.

gOper Group operations attribute. When a user is connected to a group with the group operations attribute, the user can do everything with resources that are in the scope of the group.

gAud Group auditor attribute. When a user is connected to a group with the group auditor attribute, the user can change auditing attributes of the users, groups, and resources that are in the scope of the group.

Connects in multi-system mode

The administrator follows these guidelines to create and change connects for users and groups in multi-system mode.

You can connect users and groups only on the same node. You cannot connect users and groups across separate nodes. However, if the same-name groups and users exist in another node, you can propagate the connects to that node.

Note: Use caution if you intend to propagate connects across nodes. You can create unintended consequences if the names and groups are not identical.

Example of unintended consequences:

If you have two users with different names but identical user IDs on separate nodes, you can unintentionally propagate a user's connect properties to a different user. The Visual client does not ensure that user IDs refer to the same user or group names.

Viewing and changing Connect properties

The administrator uses the **Properties** dialogs for users and groups to view or change the properties of a connect.

Procedure

1. To see the properties of the connected users of a group, perform one of these steps:
   - Select the users and select **Navigate > Show Connects** from the main menu.
   - Right-click the users and select **Show Connects** from the pop-up menu.
   - Click **Show Connects** on the toolbar.

   If you want to see the connects between a group and its users, the columns of the resulting table are described in Chapter 3, "User management," on page 39.

   If you want to see the connects between the groups of a user, the columns of the resulting table are described in Chapter 4, "Group management," on page 63.
2. To see or change the properties of a connect, perform one of these steps:
   - Select the connected user or group and select **Navigate > Properties** from the main menu.
   - Right-click a connected user or group and select **Properties** from the pop-up menu.
   - Click **Properties** on the toolbar.

   The resulting dialog depends on whether you select to view properties for a user or group.
3. If you select to view properties for a group, the following dialog is displayed:

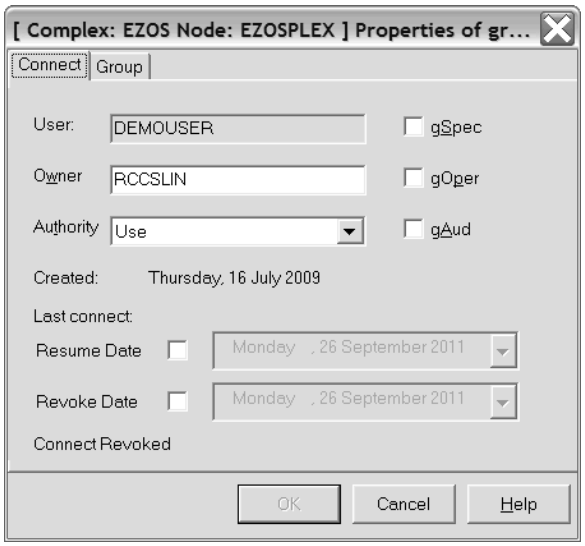


Figure 42. Connect properties dialog for a group

The complex and node names are displayed in the header of the dialog only if you are operating in multi-system mode.

The **Properties** dialog for a group has two tabs: **Connect** and **Group**. Your authorization to create connects on the mainframe determines which of these fields are editable.

The **Connect** tab for group properties displays these fields:

User The connected user of the selected group.

Owner
The user or group that owns the group.

Authority
Connect authority. From the connect authority dropdown list, you can select either **Use**, **Connect**, **Create** or **Join**.

Use The user can access the resources that the group has access to.

Create The user has the same authorizations as with **Use**. The user is also authorized to create data sets and data set profiles that have a High-Level-Qualifier (HLQ) as the name of the group.

Connect
The user has the same authorizations as with **Create** and is also authorized to connect existing users to the group.

Join The user has the same authorizations as with **Connect** and is also authorized to create new subgroups.

gSpec Group special attribute. When a user is connected to a group with the group special attribute, the user can do everything with users, groups, and resources that are in the scope of the group, except changing auditing attributes.

gOper Group operations attribute. When a user is connected to a group with the group operations attribute, the user can do everything with resources that are in the scope of the group.

gAud Group auditor attribute. When a user is connected to a group with the group auditor attribute, the user can change auditing attributes of the users, groups, and resources that are in the scope of the group.

Created
Date that the connect was created.

Last connect
Most recent time that the user was connected to the group.

Resume Date
Specifies the date that the connection to the group is resumed for the user ID in the **User** field. If the RESUME attribute is required, the check box is selected and the calendar (date selector) is enabled. Use the calendar to specify the date.

Revoke Date
Specifies the date that the connection to the group is revoked for the user ID in the **User** field. If the `REVOKE` attribute is required, the check box is selected and the calendar (date selector) is enabled. Use the calendar to specify the date. To change the status from active to revoked, specify a date that is *equal to or prior to the current date*. If you specify today's date or a prior date, the Visual Client issues the `REVOKE` command immediately instead of scheduling it for a future date.

Connect Revoked
Indicates the revocation status of the user in the **User** field. This field is Read-only. **Revoked** indicates the status is currently revoked. No value (blank) indicates the status is active or suspended. To change the revocation status, you must update the revoke and resume dates.

In the Group tab, you see the Group Properties fields. For detailed description, see "Viewing group properties" on page 65.

4. Click **OK** to apply your changes.
5. If you select to view properties for a user, the following dialog is displayed:

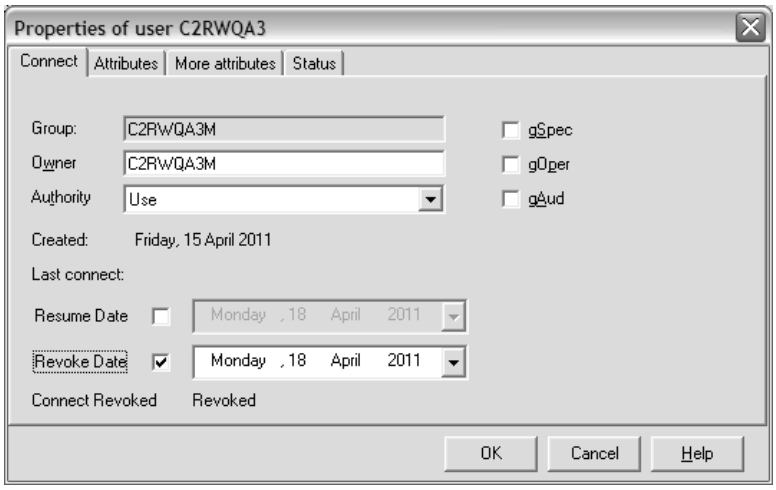


Figure 43. Connect properties dialog for a user

The complex and node names are displayed in the header of the dialog only if you are operating in multi-system mode.

The **Properties** dialog for a user has four tabs: **Connect**, **Attributes**, **More Attributes**, and **Status**. Your authorization to create connects on the mainframe determines which of the fields on these tabs are editable.

The **Connect** tab for user properties displays these fields.

Group The connected group of the selected user.

Owner
The user or group that owns the user.

Authority
Connect authority. From the connect authority dropdown list, you can select either **Use**, **Connect**, **Create** or **Join**.

Use The user can access the resources that the group has access to.

Create The user has the same authorizations as with **Use**. The user is also authorized to create data sets and data set profiles that have a High-Level-Qualifier (HLQ) as the name of the group.

Connect
The user has the same authorizations as with **Create** and is also authorized to connect existing users to the group.

Join The user has the same authorizations as with **Connect** and is also authorized to create new subgroups.

gSpec Group special attribute. When a user is connected to a group with the

group special attribute, the user can do everything with users, groups, and resources that are in the scope of the group, except changing auditing attributes.

gOper Group operations attribute. When a user is connected to a group with the group operations attribute, the user can do everything with resources that are in the scope of the group.

gAud Group auditor attribute. When a user is connected to a group with the group auditor attribute, the user can change auditing attributes of the users, groups, and resources that are in the scope of the group.

Created
Date that the connect was created.

Last connect
Most recent time that the user was connected to the group.

Resume Date
Specifies the date that the connection to the user ID is resumed for the group ID in the **Group** field. If the RESUME attribute is required, the check box is selected and the calendar (date selector) is enabled. Use the calendar to specify the date.

Revoke Date
Specifies the date that the connection to the user ID is revoked for the group ID in the **Group** field. If the `REVOKE` attribute is required, the check box is selected and the calendar (date selector) is enabled. Use the calendar to specify the date. To change the status from active to revoked, specify a date that is *equal to or prior to the current date*. If you specify today's date or a prior date, the Visual Client issues the `REVOKE` command immediately instead of scheduling it for a future date.

Connect Revoked
Indicates the revocation status of the user. This field is Read-only. **Revoked** indicates the status is currently revoked. No value (blank) indicates the status is active or suspended. To change the revocation status, you must update the revoke and resume dates.

The Attributes, More Attributes, and Status tabs are described in "Viewing user properties" on page 42.

6. Click **OK** to apply your changes.

Creating a connect

The administrator uses the **Properties** dialogs for users and groups to view or change the properties of a connect.

About this task

A connect is a relation between a user and a group. The kind of the relation between a user and a group depends on its attributes.

Procedure

1. To create a connect, select either users or groups and perform one of these steps:
   - Select **Action > Connect** from the main menu.
   - Right-click a user or group and select **Connect** from the pop-up menu.
   - Click **Connect** on the toolbar.

Figure 44. Create connect dialog

The complex and node names are displayed in the header of the dialog only if you are operating in multi-system mode.

2. Enter the user ID or group. You can select from these options:

Authority
Connect authority. The connect authority is either Use, Connect, Create, or Join.

Use The user can access the resources that the group has access to.

Create The user has the same authorizations as with **Use**. The user is also authorized to create data sets and data set profiles that have a High-Level-Qualifier (HLQ) as the name of the group.

Connect
The user has the same authorizations as with **Create** and is also authorized to connect existing users to the group.

Join The user has the same authorizations as with **Connect** and is also authorized to create new subgroups.

gSpec Group special attribute. When a user is connected to a group with the group special attribute, the user can do everything with users, groups, and resources that are in the scope of the group, except changing auditing attributes.

gOper Group operations attribute. When a user is connected to a group with the group operations attribute, the user can do everything with resources that are in the scope of the group.

gAud Group auditor attribute. When a user is connected to a group with the group auditor attribute, the user can change auditing attributes of the users, groups, and resources that are in the scope of the group.

Resume Date
Specifies the date that the connection to the group is resumed for the

user ID in the **Userid** field. If the RESUME attribute is required, the check box is selected and the calendar (date selector) is enabled. Use the calendar to specify the date.

Revoke Date
Specifies the date that the connection to the group is revoked for the user ID in the **Userid** field. If the REVOKE attribute is required, the check box is selected and the calendar (date selector) is enabled. Use the calendar to specify the date.

3. Click **OK** to connect.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes.

   If you have performed an action already, the nodes that you selected previously are displayed. If needed, you can change the nodes to which the create-connect action applies. You must select at least one node to continue. Note that local node entry is highlighted.

   Note: You can create a connect for users and groups only on the same node. You cannot create a connect for users and groups across separate nodes. However, if the same-name groups and users exist in another node, selecting multiple systems will propagate the new connect to the specified nodes. Use caution if you intend to propagate new connects across nodes. See "Connects in multi-system mode" on page 74.

   If a node is defined as a zSecure node and an RRSF node, you can select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.

   a. Click **OK**. The selected list of nodes is verified, then the create-connect action is performed for each selected node.
5. Click **Cancel** to return to the previous dialog without selecting any nodes.

Attributes gSpec, gOper and gAud

The **GrpSpecial**, **GrpOperations**, and **GrpAuditor** scope attributes might not be available.

If the attributes **GrpSpecial**, **GrpOperations**, and **GrpAuditor** display in gray, you cannot specify the attributes. The new connect cannot have them unless the connect exists with these attributes.

Drag-and-drop and copy-paste

The administrator can use the drag-and-drop or Copy-Paste functions to create a connect.

Another way to create connects is by drag-and-drop. A pop-up menu is displayed after dropping users from one list on a group in another list, or vice versa. Select **Connect** to create a connect.

Note: All new connects get the same attributes.

You can also use the Copy-Paste function available on the main menu bar. This function copies all the attributes. For more information, see "Copy and paste function" on page 14.

Deleting a connect

The administrator uses the **Delete connect** dialog to delete the connects of a user and a group.

Procedure

To delete connects, follow these steps:

1. Select the connects in a **Connects** table and perform one of these steps:
   - Select **Action > Delete** from the main menu.
   - Right-click the connects and select **Delete** from the pop-up menu.
   - Click **Delete** on the toolbar.
   - Press the **Delete** key.
   - Drag the connects and drop them on the Recycle Bin.

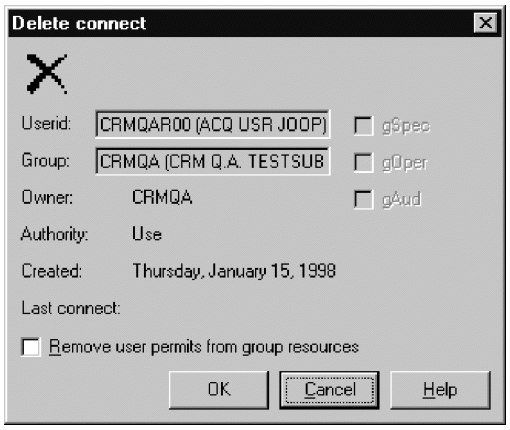


Figure 45. Delete connect dialog

2. Specify that the user must be removed from all access lists of group resources in the **Remove user permits from group resources** option.
3. Click **OK** to delete or remove the connect.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed.
   a. Select the nodes to which the delete-connect action applies. You must select at least one node to continue. Note that the local node entry is highlighted.

      Note: You can delete a connect for users and groups only on the same node. You cannot delete a connect for users and groups across separate nodes. However, if the same-name groups and users exist in another node, selecting multiple systems will propagate the delete-connect action to the specified nodes. Use caution if you intend to propagate the delete connects action across nodes. See “Connects in multi-system mode” on page 74.

      If a node is defined as a zSecure node and an RRSF node, you can select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   b. Click **OK**. The selected list of nodes is verified, then the delete-connect action is performed for each selected node.

c. Click **Cancel** to return to the previous dialog without selecting any nodes.

Copy, merge, and move functions for connects

The administrator uses the **Drag and Drop** and **Copy and Paste** functions to copy, merge, and move connects.

You can copy, merge, and move connects by using **Drag and Drop** or **Copy and Paste**. If you use **Drag and Drop**, you can drag connects from one table and drop them on a similar one. After the drop, a pop-up menu is displayed, listing these options:

Copy The dragged connects are copied to the target table. If a connect exists and has an authority higher than the dragged connect, the user can choose between copying and merging the connects. If copy is selected, the dragged connects replace the target connects. If merge is selected instead, every new connect has the attributes of both connects and have the highest connect authority.

Note: When copying a connect, if the revoke or resume dates are earlier than or equal to the current date, RACF prevents you from copying or entering the dates. Table 4 shows how revoke and resume values are managed for copy-connect actions.

Table 4. Before-and-after revoke-and-resume values for copy-connect operation

Original Values			**Copy Output Values**		
Revoke Flag	**Revoke Date**	**Resume Date**	**Revoke Flag**	**New Revoke Date**	**New Resume Date**
	None	None		None	None
	GT today	None		*Copy revoke date	None
	GT today	GT revoke date		*Copy revoke date	Copy resume date
	LT today	LE today & GT revoke date		(1)None	None
Yes	LE today	None	**Yes	(2)None	None
	LT today	Today		None	None
Yes	LE today	GT today	**Yes	(3)None	Copy resume date
Yes	None	None	**Yes	None	None
	None	LT today		None	None
	None	Today		None	None
Yes	None	GT today	**Yes	None	Copy resume date
Legend: LT = less than, LE = less than or equal to, GT = greater than, None = not specified					

Table 4. Before-and-after revoke-and-resume values for copy-connect operation (continued)

Original Values	Copy Output Values
*For a temporary connect, you must remove the revoke date in order for the copy operation to create a permanent connect. **If the revoke flag is set in the copied values, the initial status of the connect is set to revoked. **Copy outcome examples:** (1)The resume date takes precedence because it is less than or equal to today's date. The new connection is not set to revoke and resume. (2)The connection is already revoked (date in the past), therefore the new connection is set to be revoked with no revoke or resume dates. (3)The connection has a current status of revoked (date in the past), but a resume date later than today is specified. The new connection is revoked and set to resume with the specified date.	

Merge The outcomes of merge-connect operations are based on various combinations of resume and revoke dates. The goal is to prevent a connection from becoming unintentionally active in these circumstances:

- Revoking too late.
- Resuming too soon.
- Resuming when a permanent revocation is wanted.

If the outcome from a merger is unexpected or unwanted, open the user or group properties dialog and change the dates. The following example shows how an outcome is derived.

Merge-connect example:

A merger of connects is executed between these connects:

- The current date is November 1.
- The source connect is active with a revoke date of November 15 and no resume date.
- The target connect is active with a revoke date of November 5 and a resume date of December 1st.

The outcome of this operation is a connect that is currently active until revoked on November 5, with no resumption date.

Move The move action is a combination of a copy or merge followed by a delete of the successfully copied or merged connects. A dialog in which you can specify the move options is displayed. The **Remove user permits from group resources** option specifies whether the user must be removed from the access list of resource profiles of the group on the delete action.

Select **Copy and Paste** from the main menu to perform a copy and paste operation. For more information about **Copy and Paste**, see "Copy and paste function" on page 14.

Chapter 6. Resource management

The administrator performs zSecure resource management tasks to maintain the access rules that different users and groups have to resources.

Resource profiles

Rules for access to various kinds of resources are kept in resource classes as profiles. This section describes these resource profiles.

Access checks are done against specific resource classes, depending on the type of resource the access check is for. For example, DATASET for reading a data set, or TERMINAL to see if you can log on using a particular machine. Profiles within each class describe sets of access settings. The profile name can be generic, such as a mask specification. RACF determines which access settings apply by looking for the profile name that best matches the resource name within the particular class.

In RACF, a distinction is made between DATASET profiles and all other profiles. The DATASET profiles reside in the DATASET class which controls access to data sets. All other profiles are called *General Resource Profiles*. zSecure Visual lets you work with both types of profiles.

To protect a resource with a profile, the profile has to reside in the appropriate class. The name of the profile needs to match the name of the resource. For example, to protect dataset C2R.CKR260.CKRLOAD, you can make a profile named C2R.CKR260.CKRLOAD in the DATASET class.

To avoid creating a resource profile for every resource, RACF enables you to use generic characters in the profile name. You can use character * to represent one qualifier, or the rest of the current qualifier. The ** sequence matches zero or more qualifiers. The following examples show the matches based on the use of the * character:

```
C2R.CKR*.CKRLOAD matches C2R.CKR260.CKRLOAD.
C2R.CKR260.CKRLOAD.* does not match C2R.CKR260.CKRLOAD,
        because it has no fourth qualifier.
C2R.** matches C2R.CKR260.CKRLOAD.
C2R.**.CKRLOAD matches C2R.CKR260.CKRLOAD.
```

If there are different resource profiles that match a certain resource, RACF uses the most specific profile. It is the one with the most characters left of the first generic character.

Resource table

The administrator reviews resource profile contents in the Resource table.

Typically a profile contains an access list that specifies the access to the resources, which users and groups have, covered by the profile. Some general resource classes grant access by a different procedure.

Use the **Find** dialog to locate a list of all resources. You can use * in the class to get profiles of different resource classes in one table. If you leave the class field empty, you can get all resources but without users or groups.

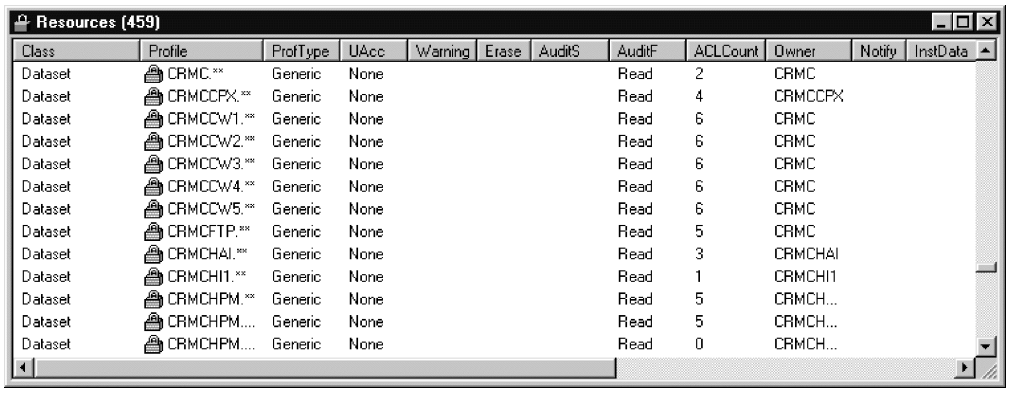


Figure 46. Resources table

The resulting fields in the **Resource** table are:

Complex
The name of the complex where the result was found. This field is displayed only if you are operating in multi-system mode.

Class Class in which the profile resides.

Profile
Name of the profile.

ProfType
Profile type. For general resources, it can be discrete or generic. For data sets, it can be generic, nonvsam, vsam, tapedsn, or model.

UAcc Access granted by the profile to any user whose access cannot be determined from the access list.

Warning
A profile in warning mode always allows access to the resource (!), but if the access is more than ed by the Access List or UACC, an audit log record is written.

Erase Overwrite the dataset on deletion. This flag is only taken into account if the central Erase flag has been set using a SETROPTS ERASE command.

AuditS
Audit level for successes.

AuditF
Audit level for failures.

ACLCount
Number of user IDs and groups on the access list of the profile.

Owner
User ID or group that can change the profile.

Notify User ID that receives a message when an audited violation occurs.

InstData
The contents and means of this field are defined by your organization.

Appldata
This field is only defined for generic resource profiles, which are all resource profiles except profiles in the DATASET class. Its contents and means depend on the class.

Volser For discrete DATASET profiles, it contains the volumes the profile protects.

Created
Date the profile was created.

UserIDcount
For the IDIDMAP profiles, it indicates the number of user ID associated with this profile.

The extra selection fields for resources in the **Find** dialog are:

Installation data
Select only resources that have the specified pattern in their installation data.

Owner
Select only resources whose owner matches the specified filter.

Segment
Select the resources that have the segment you specified. If this option is grayed you cannot view segments or there are none. The option *any* gives you the complete resource list, whether the profiles have segments or not.

Viewing mapping information

The administrator uses the **Mappings** selection to view mapping information for IDIDMAP profiles.

Procedure

For the IDIDMAP profiles, you can view their associated mapping information by following these steps:

1. Select the IDIDMAP profile from the main menu.
2. Select **Navigate > Mappings**. Alternatively, you can right-click the IDIDMAP profile to display the pop-up menu and select **Mappings**.

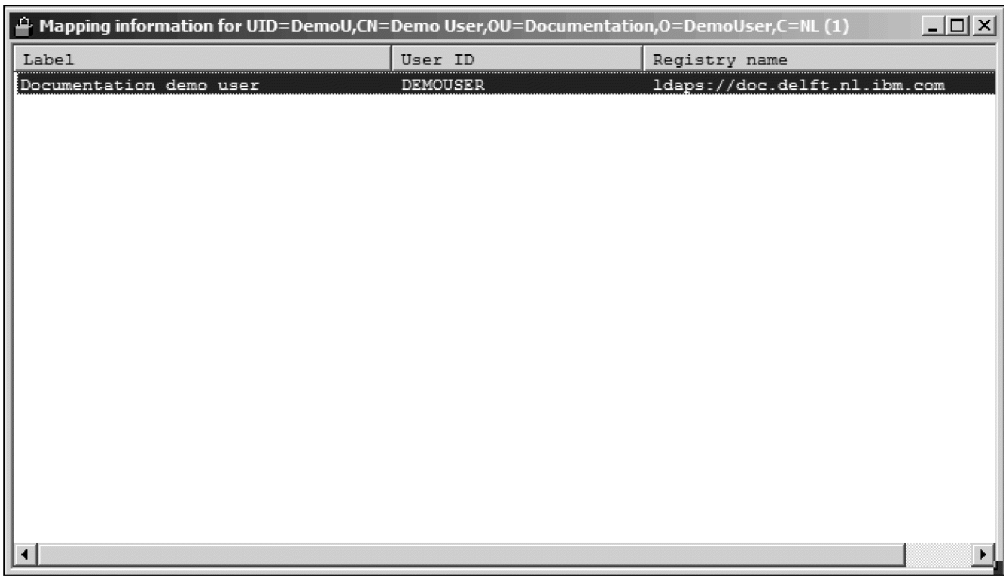


Figure 47. Mapping information of an IDIDMAP profile

On the displayed window, you can view these fields:

Complex
The name of the complex where the result was found. This field is displayed only if you are operating in multi-system mode.

Label The label associated with the identity mapping.

User ID
The user ID associated with the identity mapping.

Registry name
The registry name of the identity mapping.

Note: You cannot duplicate, add, edit, or delete an IDIDMAP profile. For more information, see "Viewing mappings" on page 60.

Adding a resource profile

The administrator uses the **Add resource profile** dialog to create a resource profile from scratch.

About this task

You can create a new resource profile through the resource table.

Note: You can only create generic DATASET profiles, including fully qualified generics.

Procedure

To create a resource profile from scratch, complete these steps:

1. Open a resource table.
2. Select the profile from the resource table and select **Action > Add Resource**.

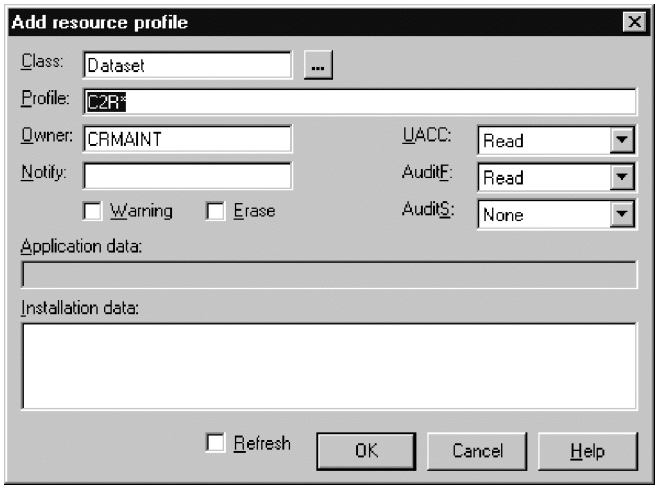


Figure 48. Add resource profile dialog

3. Enter the profile data. The fields and options are described here:

Complex: Node
The complex and node names to which this action applies are displayed in the header of the dialog only if you are operating in multi-system mode.

Class Class in which the profile resides. zSecure Visual uses as default class the class of the profile you have selected. You can change the class.

Profile
Name of the profile.

UACC Access granted by the profile to any user whose access cannot be determined from the access list.

Warning
A profile in warning mode always allows access to the resource (!), but if the access is more than ed by the Access List or UACC, an audit log record is written.

Erase This flag is only valid when class is DATASET. When the flag is set, the dataset is overwritten on deletion, but only if the central Erase flag has been set using a SETROPTS ERASE command.

AuditS
Audit level for successes.

AuditF
Audit level for failures.

Owner
User ID or group that can change the profile.

Notify User ID that can receive a message when an audited violation has occurred.

InstData
The contents and means of this field are defined by your organization.

Appldata
This field is only defined for generic resource profiles, which are all resource profiles except profiles in the DATASET class. Its contents and means depend on the class.

Refresh
Refreshes the class, so the new profile becomes effective immediately, even for users that have cached profiles of the class. If you do not specify **Refresh**, the profile becomes active only for users that do not have cached profiles.

4. If you need the profile changes to take effect immediately for all users, click **Refresh** to refresh the class. If you do not refresh the class, the profile becomes active only for those users that do not have it cached.
5. Click **OK** to create the profile, or click **Cancel** to cancel the new profile.

   If you are operating in single-node mode, **OK** is disabled until you change one or more values.

   If you are operating in multi-system mode, **OK** is enabled so you can create the selected resource profile in a different node.

Duplicating a resource profile

The administrator uses the **Duplicate resource profile** dialog to create a resource profile from an existing profile.

About this task

You can create a profile by duplicating an existing profile. Duplicating a profile copies the access list and member list of the original profile to a new profile. You can customize the new profile and change the data as required.

Note: You cannot copy a resource profile from a DATASET class to a general resource class or vice versa.

Procedure

To duplicate a resource profile, perform these steps:

1. Select the resource profile in a resources table and select **Action > Duplicate** from the main menu.

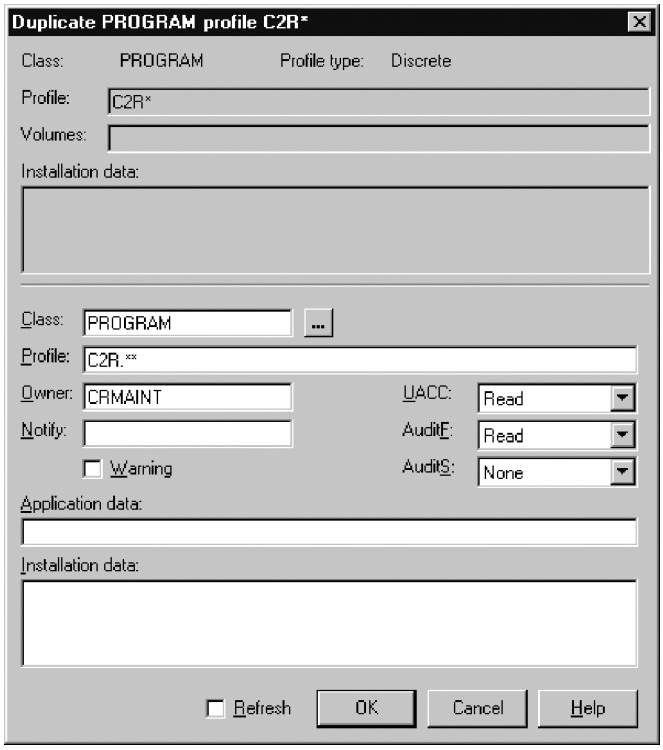


Figure 49. Duplicate resource profile dialog

2. If you are duplicating the profile to create a new profile for a single node, change the data in the fields. For descriptions of the fields, see "Adding a resource profile" on page 89.
3. If you need the new profile to take effect immediately for all users, click **Refresh** to refresh the class. If you do not refresh the class, the profile becomes active only for those users that do not have it cached.
4. Click **OK** to create the profile. If you are duplicating the profile for another node, select the nodes to which the profile applies, then click **OK**.

Editing resource profile properties

The administrator uses the **Properties of resource profile** dialog to change the properties of a resource profile.

Procedure

To change the properties of a resource profile, complete these steps:

1. Select the profile and select **Navigate > Properties** from the main menu.

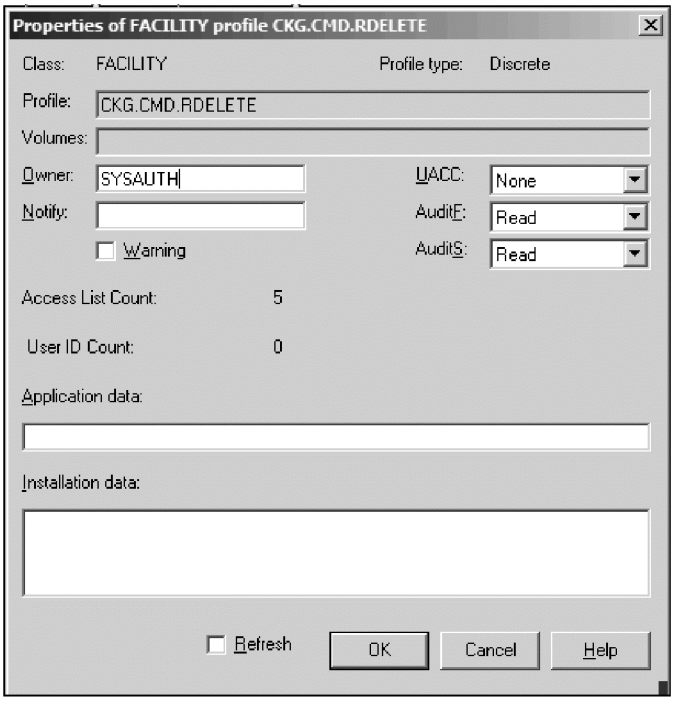


Figure 50. Properties of resource profile dialog

2. Edit the properties as needed.

   Note: You *cannot* edit these properties in this dialog:
   - Class
   - Profile
   - Volumes
   - Access List Count
   - User ID Count

   If you are operating in multi-system mode, the complex and node to which you selection applies is displayed in the header of the dialog.

   The following properties are displayed:

   Class Class in which the profile resides.

   Profile type
   Type of the RACF profile, for example, Generic, VSAM, Non VSAM, Model, Type DSN, and so on.

   Profile
   Name of the profile.

   Volumes
   For discrete DATASET profiles, this field contains the volumes that the profile protects.

   Owner
   User ID or group that can change the profile.

Notify User ID that receives a message when an audited violation occurs.

Warning
A profile in warning mode always allows access to the resource (!), but if the access is more than ed by the Access List or UACC, an audit log record is written.

Erase Overwrite the dataset on deletion. This flag is only taken into account if the central Erase flag has been set using a SETROPTS ERASE command.

ACLCount
Number of user IDs and groups on the access list of the profile. You cannot directly change the number here. However, if you select the profile and select **Navigate > Access List** from the main menu, you can extend or shorten the access list.

Application data
This field is only defined for generic resource profiles, which are all resource profiles except profiles in the DATASET class. Its contents and means depend on the class.

Installation data
The contents and means of this field are defined by your organization.

Profile type
Type of profile.

UACC Access granted by the profile to any user whose access cannot be determined from the access list.

AuditF
Audit level for failures.

AuditS
Audit level for successes.

User ID count
For the IDIDMAP profiles, it indicates the number of user IDs associated with this profile.

3. Click **Refresh** to refresh the class if you need the profile changes to take effect immediately.
4. Click **OK** to apply your changes.
5. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. Note that the local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Deleting a resource profile

The administrator uses the **Delete resource profile** dialog to delete a resource profile.

Procedure

To delete a resource profile, follow these steps:

1. Select the resource profile in a resource table and select **Action > Delete** from the main menu.

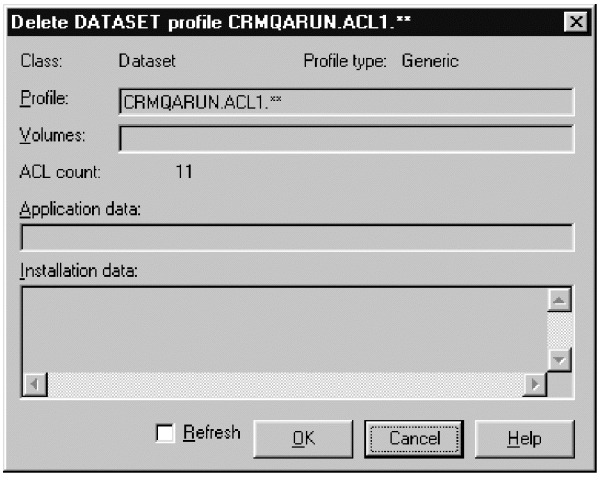


Figure 51. Delete resource profile dialog

2. Select **Refresh** to apply the deletion of the profile immediately.
3. Click **OK** to delete the profile.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. Note that the local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

Modifying an Access List (ACL)

The administrator uses the **Access list** window to view, add, and change entries in the access list of a resource profile.

About this task

The name access list is often abbreviated as ACL. A resource profile typically has an access list, which is a list of user IDs and group IDs, their granted access and, optionally, a condition.

Procedure

1. To view the access list of a resource profile, select the profile and click **Navigate > Access List** in the main menu.

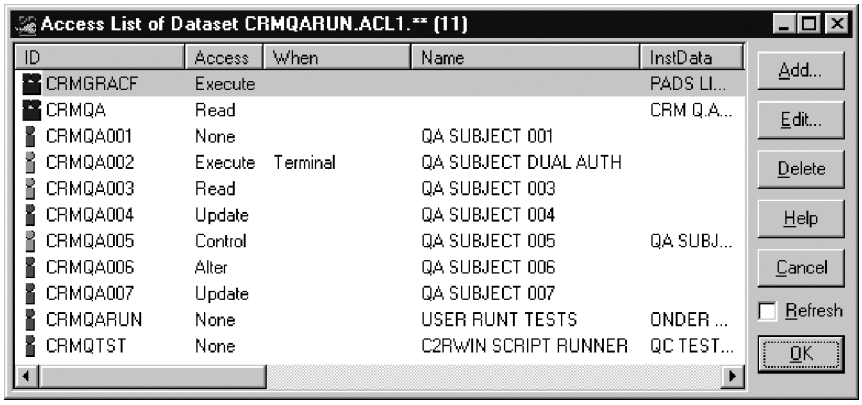


Figure 52. Access list

When a group is placed on the access list, all its users get access, see "Viewing an Effective Access List" on page 37. The user and group columns are described in Chapter 1, "IBM Security zSecure Visual customization and primary tasks," on page 1 and Chapter 3, "User management," on page 39. The following columns are also in the access list table:

Node The name of the node that is associated with the ID.

ID User ID or group.

Access
Granted access. It is always one of these options:

None All means of access is denied for the specified user or group.

Execute
The specified user or group can execute the resource. It is only effective for data sets and programs.

Read The specified user or group can execute and read the resource.

Update
The specified user or group can execute, read, and update or write the resource.

Control
The specified user or group can execute, read, update or write, and create or remove the resource.

Alter The specified user or group can do anything with the resource and change the resource profile, just as the owner.

When A blank field means there is no condition, so the access is granted without restriction. Entries in this field have this form:

```
APPCPort appcport Console console  JESInput class  Program
program SYSID id  Terminal terminal
```

2. Complete these steps to add, delete, or change ID entries in the list and process your changes:
   a. Select a list entry (ID).

b. Click **Add**, **Edit**, or **Delete**, to change the list entry. A dialog for the selected task is displayed:
   - "Adding a user or group to an access list"
   - "Editing an access list entry" on page 97
   - "Deleting an access list entry" on page 98

c. After you make a change, the **OK** and **Cancel** buttons become available in the main Access List window.

3. Click **Refresh** to refresh the class. The new access list becomes effective immediately, even for users that have cached profiles of the class.

   Note: Your changes do not become effective for users whose affected profiles are cached until you refresh the class.

4. Click **OK** to apply your changes to the access list to the mainframe.
5. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the changes applies. You must select at least one node to continue. Note that the local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The IDs of the current node, if selected, are updated with your changes. Your changes to the current node are then replicated to the other selected nodes.

      Note:
      - You must understand the differences in the ID data across your RACF databases; other nodes might not have the same initial access list as the current node.
      - IDs that are different than the current node remain in the other nodes.
      - The client does not verify that the user or group IDs exist in the other nodes. If an ID does not exist in the target database, it is rejected by RACF as an error and ignored.

Adding a user or group to an access list

The administrator uses the **Add to access list** dialog to add a user or group to the access list of a resource profile.

Procedure

To add a user or group to the access list, follow these steps:

1. Display the access list and click **Add** in the table window.

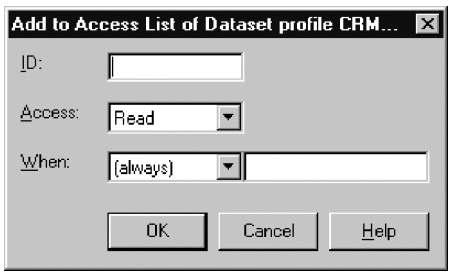


Figure 53. Add to access list dialog

2. Specify this information:

   ID The user ID or group ID.

   Access
   The access ed for ID.

   When The condition for which access is granted.
3. Select **Refresh** to make the new ID immediately active for all users. If you do not refresh, the ID only becomes active for those users that do not have it cached.
4. To add the same ID with different conditions to the access list, click **OK**. If the same ID is added with the same condition but a different access, the new access overrides the previous access.

   Your changes are updated in the Access List main form. The changes are not processed until you click **OK** in the main Access List dialog to process all changes.

Editing an access list entry

The administrator uses the **Edit Access List** dialog to edit the entry of a user or group in the access list of a resource profile.

Procedure

To edit the entry of a user or group in the access list, follow these steps:

1. Select the entry and click **Edit** in the table window.

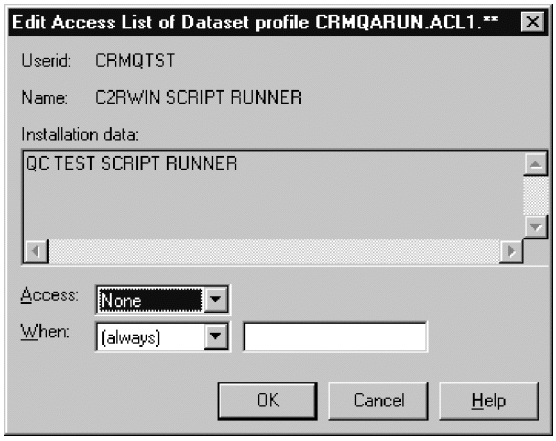


Figure 54. Edit access list dialog

2. Edit these fields as needed:

   ID A user ID or group ID.

   Access
   The access level that is set for the ID.

   When The condition for which access is granted.
3. Click **OK** to apply the changes to the access list.

   Your changes are updated in the Access List main form. The changes are not processed until you click **OK** in the main Access List dialog to process all changes.

Deleting an access list entry

The administrator uses the **Delete** option to remove the entry of a user or group in the access list of a resource profile.

Procedure

Follow these steps to delete an entry:

1. Select the user or group entry in the access list.
2. Click **Delete** in the table window or select **Action > Delete**.
3. Click **OK** to delete the selection.

   Your changes are updated in the Access List main form. The changes are not processed until you click **OK** in the main Access List dialog to process all changes.

Profile members

The administrator uses these guidelines to plan and implement the use of grouping classes.

All resource profiles except DATASET profiles can have a member list. In practice, only some classes have profiles with members. The typical way to use profile members is to access on groups of resources instead of individual resources. You need a member and grouping class.

Member and grouping classes are linked together in the Class Descriptor Table. The member class can contain profiles that accept access the normal way. The grouping class is grant access for groups of resources. A group is represented by a profile in the class. This grouping profile can have a list of members, each of which contains a resource name. Any rights granted on the grouping profile accepts access on all the resources named in the members.

Attention: The design of the group structure is important. For ease of use, a group name must give a good indication of either the contents or the use of the resource group. Avoid this usage:

- Use of both the member and grouping class simultaneously for the same resource.
- Recurrence of the same resource in more than one group, if you plan to grant access on those resource groups to a user or group.

The various issues involved when merging access rights for multiple resources are complex and can result in unexpected and undesired effects. Also, no clear report of the result is available.

Example of grouping class

The administrator uses this sample scenario to plan and implement grouping classes.

The main reason to use grouping is to avoid excessive administration overhead. An example of where this grouping can be useful is the administration of CICS transactions. TCICSTRN, the member class, can be granted access on individual transactions. For every transaction, a profile is needed. However, it quickly becomes cumbersome. To avoid creating large piles of individual transaction profiles, it is possible to organize them in the GCICSTRN grouping class. A useful group division might be by CICS system and job description:

GCICSTRN class

Profile	Members
CICSPROD.OPER	CICSPROD.CEMT CICSPROD.CSOT CICSPROD.CSFR ...
CICSPROD.DEV	CICSPROD.CEMT CICSPROD.CEDA CICSPROD.CAUT ...
CICSTEST.DEV	CICSTEST.CEMT CICSTEST.CAUT ...
...	...

Figure 55. Grouping class example

If you carefully plan and implement your groupings, granting rights on the resource groups is simpler and less error-prone than granting rights on individual transactions.

Exceptions

The administrator must be aware of these exceptional grouping classes, which need special consideration.

In some classes profile members are used in different ways than previously described. Explaining the mechanisms involved is beyond the scope of this manual. Some of the better known exceptions are:

- The Global Access Table (GLOBAL class, DATASET profile)
- NODES class
- PROGRAM class
- RACFVARS class

Viewing and changing a member list

The administrator can use the **Members** window to view and change the member list of a general resource profile.

Procedure

To display the member list of a resource profile and change the list, perform these steps:

1. Select the profile and select **Navigate > Members** from the main menu.

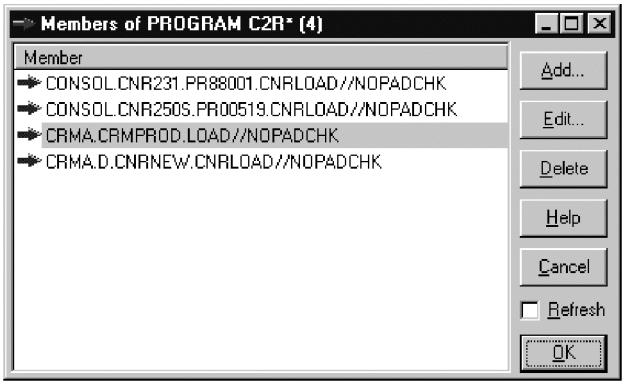


Figure 56. Member list

2. Click **Add**, **Edit**, or **Delete** to change the member list.
3. Click **Refresh** to make the changes effective immediately. For users that have cached profiles of the same class, the changes might not become effective until you refresh the class.
4. Click **OK** to apply the changes to the mainframe.
5. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. Note that the local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The members of the current node, if selected, are updated with your changes. The members lists of the other selected nodes are replaced by the current members list.
   d. Click **Cancel** to return to the previous dialog without selecting any nodes.

Adding a member

The administrator can use the **Add member** dialog to add a new member to a member list of a resource profile.

Procedure

To add a member, perform these steps:

1. Click **Add** in the member table window.

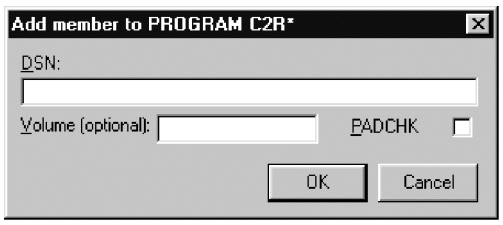


Figure 57. Add member dialog

2. Enter the new member.

   Note: When adding a member to the PROGRAM class, use the **DSN**, **Volume**, and **PADCHK** fields to construct the new member string.
3. Click **OK** to add the new member to the list. The changes do not become effective for users whose affected profiles are cached until you refresh the class in the main member list.

Editing a member

The administrator can use the **Edit member** dialog to change a member of a list.

Procedure

To edit a member, perform these steps:

1. Select the member and click **Edit** in the member table window.

Figure 58. Edit member dialog

2. Change the member and click **OK** to place it in the list.

   Note: When editing a member in the PROGRAM class, use the **DSN**, **Volume**, and **PADCHK** fields to construct the member string.
3. Click **OK** to apply the changes to the member list. The changes do not become effective for users whose affected profiles are cached until you refresh the class in the main member list.

Deleting a member

The administrator uses the **Delete** function to delete a member from a list.

Procedure

To delete a member, perform these steps:

1. Select the member and click **Delete** in the member table window, or select **Action > Delete** from the main menu.

2. Click **Refresh** to make the changes effective immediately. For users that have cached profiles, the changes do not become effective until you refresh the class.
3. Click **OK** to send the deletion to the mainframe.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. Note that the local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The members of the current node, if selected, are updated with your changes. The members lists of the other selected nodes are replaced by the current members list.
   d. Click **Cancel** to return to the previous dialog without selecting any nodes.

Refreshing a class

The administrator uses the **Refresh** function to refresh a class after changing resource profiles in the RACF database.

About this task

After changing resource profiles in the RACF database, a refresh is required to propagate the changes to cached profiles for all users.

Procedure

To refresh a class, perform these steps:

1. Select **Action > Refresh** from the main menu.

Figure 59. Refresh class dialog

2. Enter the class name in the **Class** field.
3. Select the **Refresh GLOBAL** class to refresh the global access table for this class instead of the class itself. If you do not know the class, click the button next to the class field to get the **Select** class dialog. See "Finding classes with the Select class dialog" on page 26 for more information.

Chapter 7. Segment management

The administrator uses the Visual Client to perform zSecure segment management tasks for users, groups, and general resources.

An application segment is part of a profile that contains information about a mainframe application other than RACF, like TSO or OMVS. Users, groups, and general resources all have their own segments. Use the following tasks to manage segments:

"Authorities and settings required to manage segments"
The administrator uses these required settings to view and edit segments in the Visual Client.

"Viewing and editing segment types" on page 104
The administrator uses the **Segmenttypes** table to view and edit segments.

"Viewing the segment list" on page 106
The administrator uses the **Segment list** option to view the segments of a class with a specific segment type.

"Using the Segment Detail window" on page 107
The administrator uses the **Segments** option to view information about the segments of a single profile.

"Adding a segment" on page 108
The administrator uses the **Add segment** option to add a segment directly to a profile.

"Exceptions" on page 109
The administrator uses this list to determine which segments cannot be edited with the segment detail window.

"Segment fields" on page 111
The administrator uses segment field descriptions in to get information on the segment type.

"Consulting IBM books" on page 110
The administrator uses this procedure to look up information on segment fields.

Authorities and settings required to manage segments

The administrator uses these required settings to view and edit segments in the Visual Client.

To view segments you must set the **Interface level** option at administration level *Full*. To select this level, go to **View > Options** on the main menu.

To edit segments, you need this authorization:

- User has `UPDATE` or better on `XFACILIT`[1] resource `CKG.CMD.CMD.EX.ALTUSER`
- User has `UPDATE` or better on `XFACILIT`[1] resource `CKG.CMD.CMD.EX.ALTGROUP`
- User has `UPDATE` or better on `XFACILIT`[1] resource `CKG.CMD.CMD.EX.ALTDSD`
- User has `UPDATE` or better on `XFACILIT`[1] resource `CKG.CMD.CMD.EX.RALTER`
- User has `UPDATE` or better on `FIELD` resource class.segment.field (or System Special)

Viewing and editing segment types

The administrator uses the **Segmenttypes** table to view and edit segments.

About this task

IBM Security zSecure Visual enables you to view and edit segments. The **Segmenttypes** table displays an overview of all segments that zSecure Visual can show.

Procedure

Follow these steps to view and edit segments:

1. Select **Navigate > Segmenttypes** in the main menu.

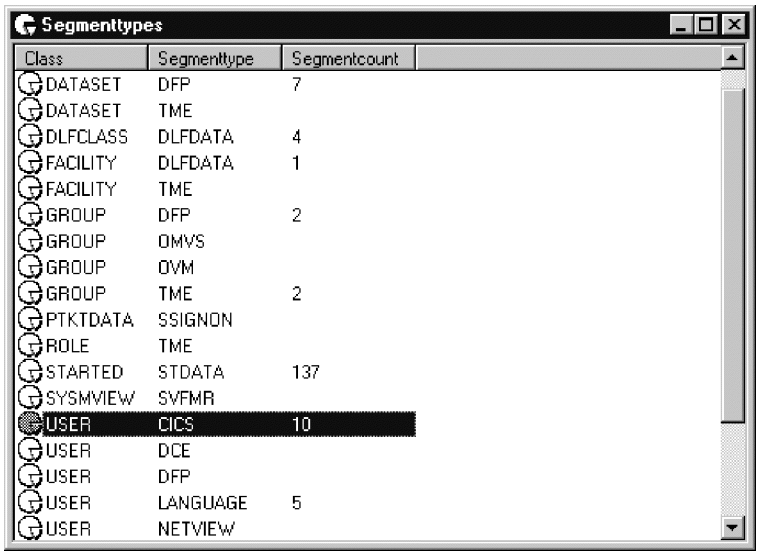


Figure 60. Segment types

The **Segmenttypes** table has these columns:

Complex
The complex to which segment applies. This column is displayed only if you are operating in multi-system mode.

Class The class that the segment belongs to.

Segmenttype
The segment type.

Segmentcount
The number of segments.

Note: This number is not initially specified. Each time you view information about a segment, the relevant number of that segment is updated in the **Segmenttypes** list.

2. To view information about segments, right-click a row and select **Segment List**. See "Viewing the segment list" on page 106.

1. XFACILIT is the default name for the general resource class in the Site Module. If this name is customized during installation, verify that you have the required authorizations for the class configured for the installation.

Application segments

The administrator uses this table to determine which segments are associated with the general resource, group, and user profiles.

The following table lists the segments of general resource profiles in their related classes.

Class	Segment
APPCLU	SESSION
CDT	CDTINFO
CFIELD	CFDEF
CSFKEYS, GCSFKEYS	ICSF
DATASET	DFP
DATASET	TME
DIGTCERT	CERTDATA
DIGTRING	CERTDATA
DLFCLASS	DLFDATA
EJBROLE	TME
FACILITY	DLFDATA
FACILITY	EIM
FACILITY	PROXY
FACILITY	TME
ICSF	CSFKEY, XCSFKEY
LDAPBIND	EIM
LDAPBIND	PROXY
PTKTDATA	SSIGNON
REALM	KERB
PROGRAM	SIGVER
ROLE	TME
STARTED	STDATA
SYSMVIEW	SVFMR
XCSFKEY, GXCSFKEY	ICSF

The segments of group profiles are:

- CSDATA
- DFP
- OMVS
- OVM
- TME

The segments of user profiles are:

- CICS
- CSDATA
- DCE
- DFP
- EIM
- KERB
- LANGUAGE
- LNOTES
- NDS
- NETVIEW

- OMVS
- OPERPARM
- OVM
- PROXY
- TSO
- WORKATTR

Viewing the segment list

The administrator uses the **Segment list** option to view the segments of a class with a specific segment type.

Procedure

To view the segment list, follow these steps:

1. Open the Segment Types window.
2. Select the class-segment type combination and select **Navigate >Segment list** from the main menu, or,
3. Right-click the class-segment type and select **Segment list**.

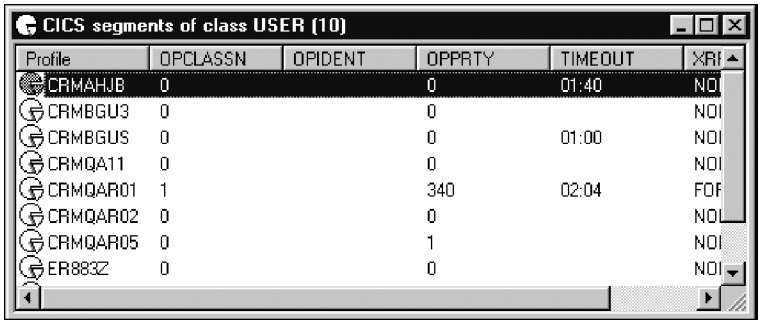


Figure 61. Segment list

The segment list always starts with the name of the profile. The other fields are segment specific. The names are abbreviations. You can find the complete names in the segment detail window. For more information about the segment fields, see "Segment fields" on page 111.

4. If you select a profile in the segment list, you have these possibilities:
   - View the properties of the profile by performing one of these steps:
     - Select **Navigate > Properties** on the main menu and double-click the profile; or,
     - Right-click the profile and select the option **Properties**.
   - View the segment detail window of the profile by performing one of these steps:
     - Select **Navigate > Segments** from the main menu; or,
     - Right-click the profile and select the option **Segments**.
   - Add a segment to a profile. For more information, see "Adding a segment" on page 108.

Using the Segment Detail window

The administrator uses the **Segments** option to view information about the segments of a single profile.

About this task

The segment detail window gives you all the information about the segments of a single profile. From this window, you can also edit the profile. To access the Segment Detail Window, you must be in the segment list or in either the user, group, resource, connected users, or connected groups table.

Procedure

To open the Segment Detail window, follow these steps:

1. Select the specific profile you want to edit or look at.
2. Select **Navigate > Segments** from the main menu, or
3. Right-click the profile and select **Segments** from the pop-up menu.

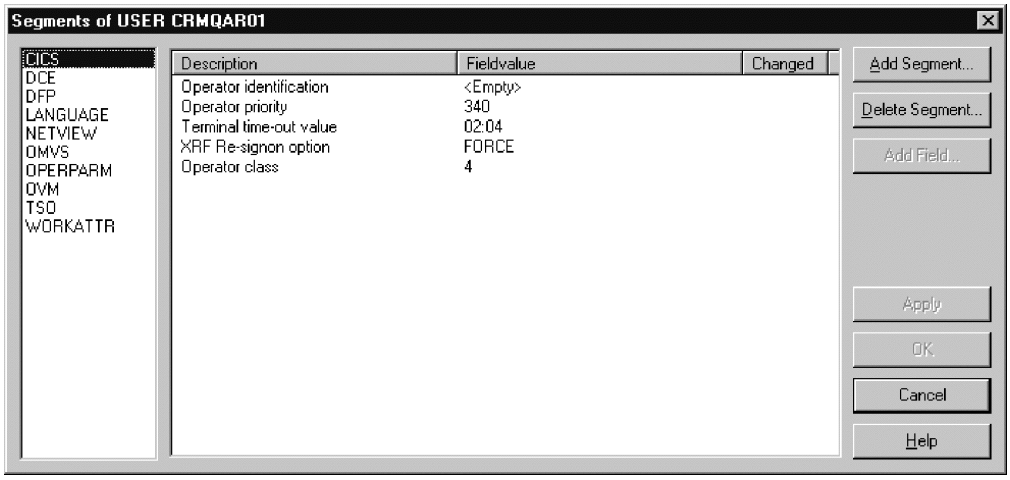


Figure 62. Segment Detail Window

When you open the segment detail window, on the left pane you see all segments of the profile. If you select a segment here, you get the detailed information about the right pane. The right pane has three columns:

Description
A description of the segment.

Fieldvalue
Value of the field. You can edit the value. All empty fields are shown with a blue-colored <Empty> in this column. When a repeating field count is zero, a single <Empty> field is shown here, although it does not exists yet. It enables the user to create the first repeating field by simply entering a value.

Changed
This column tells you whether any changes you made are yet to be applied on the mainframe by clicking **Apply**.

The buttons on the right are the edit options.

4. To edit a field, follow these steps:

a. Select the row you want to change using one of these methods:
   - Click the row you want to change then click the row a second time. After a short pause the **Fieldvalue** field will open for you to start editing.
   - Select the row you want to edit with the tab and arrow keys and press the **Ins** key to open the editing dialog.

b. To cancel editing, use the **Esc** key or select another row.

c. Press **Enter** to save your changes.

The edit options are listed as follows:

Add segment
Clicking this button opens the pop-up menu **Add segment**. You can select the segment you want to add.

Delete segment
Select the segment you want to delete and click the button. You get a warning box with the question if you want to delete the selected segment. Click **Yes** to delete it or **Cancel** to undo the deletion.

Add Field
This option is only possible for repeating fields. To add a new, empty field, select the field you want to add. The **Add Field** button becomes enabled. Click the button to add the field.

Refresh
After changing a field, you check the box to refresh it to propagate the changes to cached profiles for all users. You must have the right authorization to refresh the profiles.

Apply To apply the changes to the mainframe, click **Apply**. All indications in the Changed column disappear while the changes take effect.

Adding a segment

The administrator uses the **Add segment** option to add a segment directly to a profile.

About this task

You can add segments directly to a profile or from the segment detail window. See “Using the Segment Detail window” on page 107 in information on adding segments in the segment detail window.

Procedure

To add a segment directly to a profile, complete these steps:

1. In the table, right-click the profile you want to add a segment to.
2. Select **Action > Add segment** from the main menu, or select **Add segment** from the pop-up menu.

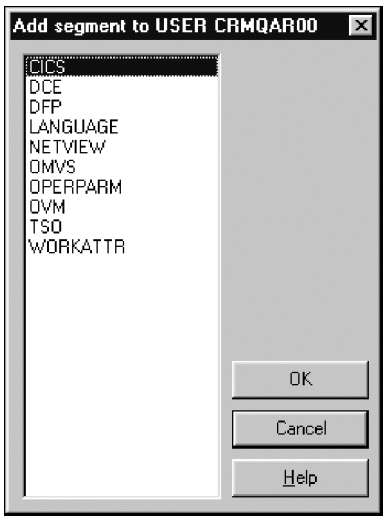


Figure 63. Add Segment dialog

3. Select the segment to add. Then, click **OK**.
4. If you are operating in multi-system mode, the **Select Nodes** dialog displays your preferred list of nodes. If you have performed an action already, the nodes that you selected previously are displayed. Complete these steps if you are using multi-system mode:
   a. Specify the nodes to which the action applies. You must select at least one node to continue. Note that the local node entry is highlighted.
   b. If a node is defined as a zSecure node and an RRSF node, select only one of these node types. If you select an RRSF node, you can use the **AT** or **ONLYAT** options to select from the dropdown list an alternative user ID to run the command.
   c. Click **OK** to verify the selected list of nodes. The action is performed for each selected node.

   Note:
   - To propagate the add-segment action across nodes, the segments need to be very similar.
   - The segment is added to the node *if possible*.
   - The segment is added immediately to the nodes.

Exceptions

The administrator uses this list to determine which segments cannot be edited with the segment detail window.

Most segments exist in the segment list and can be edited with the segment detail window. There are these exceptions:

- `CSDATA` segments are shown in SegmentTypes, SegmentList, and Segment Detail only if present.
- `DIGTCERT-CERTDATA` is displayed but cannot be edited.
- `DIGTCERT-CERTDATA-CERT` is not read from the mainframe, as it causes errors while doing so.
- `DIGTCERT-CERTDATA-*RSV*` is not read from the mainframe, they are reserved fields and must not be shown.

- DIGTCRIT cannot be edited, so it only appears in SegmentTypes and SegmentList, not in Segment Detail.
- DIGTNMAP cannot be edited, so it only appears in SegmentTypes and SegmentList, not in Segment Detail.
- DIGTRING cannot be edited, so it only appears in SegmentTypes and SegmentList, not in Segment Detail.
- FACILITY PROXY-BINDPW and BINDPWKY are read-only fields, so they only exist in SegmentList, not in Segment Detail.
- REALM-KERB-CURKEY, CURKEYV, ENCTYPE, PREVKEY, PREVKEYV, and SALT are read-only fields, so they only exist in SegmentList, not in Segment Detail.
- PTKTDATA-SSIGNON contains an encryption key only, so it only appears in SegmentTypes, not in SegmentList or Segment Detail.
- USER-KERB-CURKEY, CURKEYV, DEFTKTLF, ENCTYPE, MINTKTLF, PREVKEY, PREVKEYV, and SALT are read-only fields, so they only exist in SegmentList, not in Segment Detail.
- USER PROXY-BINDPW and BINDPWKY are read-only fields, so they only exist in SegmentList, not in Segment Detail.
- USER-TSO-TCONS, TOPTION, TPERFORM, TRBA, TUPT are read-only fields, so they only exist in SegmentList, not in Segment Detail.

Consulting IBM books

The administrator uses this procedure to look up information on segment fields.

About this task

You can find information about segments and segment fields in the IBM Bookshelf named EZ239118 under the title V1R13.0 Base Elements, Optional Features. A complete listing of all segments and their fields is in “Segment fields” on page 111. In this example, the IBM names and titles refer to z/OS V1R13.0. In other versions, the names and titles might differ.

Procedure

To find information about a particular field, follow these steps:

1. Open IBM Books.
2. Go to the bookshelf named EZ239118.
3. Select **Search >All Books Listed** from the main menu.
4. Enter the name of the field in the Search Request field of the Search dialog. If the Segment Field section provides a command parameter, use this name instead of the field name.
5. Click **Run Search**.
6. All books that contain the name of the field are displayed In the Search Result dialog.
7. Select a book and click **OK**. Typically, the most useful information is in ICH1A420, the Security Server Command Language Reference. A list of all matches is displayed in the new Search Result dialog.
8. To open a match, select and double-click it.

Segment fields

The administrator uses segment field descriptions in to get information on the segment type.

To view the segment fields for a segment type, click on the segment name. In the segment field table, each column is explained as follows:

Fieldname
The names of the fields as you see them in the segment list.

Repeats
If the fields of the segment display more than once, you find them all in the segment detail window. In the segment list, you find the number of repetitions.

Description
The descriptions of the fields as you see them in the segment detail window.

Command parameter

Lists the parameter that identifies the field in RACF commands that manipulate the field. This column is filled in only when this parameter is different from **Fieldname**.

Segments of general resource profiles

The administrator uses these field descriptions to determine the details of each segment in a general resource profile.

This section lists the segments of general resource profiles:

• "SYSMVIEW - SVFMR" on page 118

APPCLU - SESSION

The administrator uses this table to determine the fields in the APPCLU- SESSION segment type.

Fieldname	Repeats	Description	Command parameter
CONVSEC	No	Conversation security flags	
KEYDATE	No	Session key last change date	
KEYINTVL	No	Session key days to expiry #	INTERVAL
MAXFAIL	No	Failed tries before lockout #	
SENTCNT	No	Session entities in list #	
SENTFLCT	Yes	Failed attempts #	
SENTITY	Yes	Session entity name	
SESSKEY	No	Session key	
SLSFAIL	No	Invalid attempts #	
SLSFLAGS	No	Session flag byte	LOCK

CDT - CDTINFO

The administrator uses this table to determine the fields in the CDT-CDTINFO segment type.

The `CDTINFO` segment is only valid for the `CDT` resource class. It is used to define classes in the dynamic `CDT`.

Fieldname	Repeats	Description	Command parameter
CDTCASE	No	Profile names case sensitive	
CDTDFTRC	No	Default not-found RC	
CDTFIRST	No	Syntax 1st character (raw)	
CDTGEN	No	GENERIC/GENCMD status	
CDTGENL	No	GENLIST status	
CDTGROUP	No	Related grouping class	
CDTKEYQL	No	Generic scan limit (quals)	
CDTMAC	No	MAC checking	
CDTMAXLN	No	Maximum length with ENTITY	
CDTMAXLX	No	Maximum length	
CDTMEMBR	No	Related member class	
CDTOPER	No	OPERATIONS honored	
CDTOTHER	No	Syntax remainder (raw)	
CDTPOSIT	No	POSIT (options set id)	
CDTPRFAL	No	Profile definition ed	
CDTRACL	No	RACLIST status	
CDTSIGL	No	Send ENF signal	
CDTSLREQ	No	SECLABELs required	
CDTUACC	No	Default UACC	

CFIELD - CFDEF

The administrator uses this table to determine the fields in the CFIELD - CFDEF segment type.

The CFDEF (Custom Field DEFinition) segment for CFIELD class profiles defines the characteristics of the field.

Fieldname	Repeats	Description	Command parameter
CFDTYPE	No	Custom field type	
CFFIRST	No	Custom field first char	
CFHELP	No	Custom field help text	
CFLIST	No	Custom field listing header	
CFMIXED	No	Custom field mixed chars	
CFMNVAL	No	Custom field min value	
CFMXLEN	No	Custom field max length	
CFMXVAL	No	Custom field max value	
CFOTHER	No	Custom field other chars	

CSFKEYS, GCSFKEYS, XCSFKEY, GXCSFKEY - ICSF

The administrator uses this table to determine the fields in the ICSF segment type.

The ICSF segment defines Integrated Cryptographic Service Facility storage attributes for the keys that are controlled by general resources profiles in classes CSFKEYS, GCSFKEYS, XCSFKEY, and GXCSFKEY.

Fieldname	Repeats	Description	Command parameter
CSFSEXP	No	Symmetric key export option.	SYMEXPORTABLE
CSFCSPW	No	Symmetric key CPACF wrap option.	SYMCPACFWRAP
CSFSKLCT	No	Count of PKDS labels.	
CSFSKLBS	Yes	PKDS labels which might be export this symmetric key.	SYMEXPORTKEYS
CSFSCLCT	No	Count of certificate labels.	
CSFSCLBS	Yes	Certificate labels which might be export this symmetric key.	SYMEXPORTCERTS
CSFAUSE	No	Asymmetric key usage.	ASYMUSAGE

DATASET - DFP

The administrator uses this table to determine the fields in the DATASET - DFP segment type.

Fieldname	Repeats	Description	Command parameter
RESOWNER	No	DFP - resource owner	

DATASET - TME

The administrator uses this table to determine the fields in the DATASET - TME segment type.

Fieldname	Repeats	Description	Command parameter
ROLEN	No	# TME role access specs	
ROLES	Yes	TME role access specs	

DIGTCERT - CERTDATA

The administrator uses this table to determine the fields in the DIGTCERT - CERTDATA segment type.

Because this segment cannot be edited, it appears only in Segment List and Segment Types.

Fieldname	Repeats	Description	Command parameter
CERT	No	Digital certificate	
CERTCT	No	# Digital certificates	
CERTDFLT	Yes	Default cert for this keyring	
CERTEND	No	Certificate end date	
CERTLABL	Yes	Digital certificate labels	
CERTLSER	No	Certificate lse	
CERTNAME	Yes	Digital certificate names	
CERTPRVK	No	Private Key	
CERTPRVS	No	Private Key Size	
CERTPRVT	No	Private Key Type	
CERTSJDN	Yes	Distinguished name of Subject	
CERTSTRT	No	Certificate start date	
CERTUSAG	Yes	Certificate usage in this keyring	
RINGCT	No	Number of keyrings	
RINGNAME	Yes	Name of the keyring	
RINGSEQN	No	Ring sequence number	

DIGTRING - CERTDATA

The administrator uses this table to determine the fields in the DIGTRING - CERTDATA segment type.

Because this segment cannot be edited, it appears only in Segment List and Segment Types.

Fieldname	Repeats	Description	Command parameter
CERT	No	Digital certificate	
CERTCT	No	# Digital certificates	
CERTDFLT	Yes	Default cert for this keyring	
CERTEND	No	Certificate end date	
CERTLABL	Yes	Digital certificate labels	
CERTLSER	No	Certificate lse	
CERTNAME	Yes	Digital certificate names	
CERTPRVK	No	Private Key	
CERTPRVS	No	Private Key Size	
CERTPRVT	No	Private Key Type	
CERTSJDN	Yes	Distinguished name of Subject	
CERTSTRT	No	Certificate start date	
CERTUSAG	Yes	Cert. usage in this keyring	
RINGCT	No	Number of keyrings	
RINGNAME	Yes	Name of the keyring	
RINGSEQN	No	Ring sequence number	

DLFCLASS - DLFDATA

The administrator uses this table to determine the fields in the DLFCLASS - DLFDATA segment type.

Fieldname	Repeats	Description	Command parameter
JOBNAMES	Yes	Job names	
OBNMCNT	No	Job names #	
RETAIN	No	Retain flag byte	

EJBROLE - TME

The administrator uses this table to determine the fields in the EJBROLE - TME segment type.

Fieldname	Repeats	Description	Command parameter
CHILDN	No	# TME child roles	
CHILDREN	Yes	TME child roles	
GROUPN	No	#TME associated groups	
GROUPS	Yes	TME associated groups	
PARENT	No	TME parent role	
RESN	No	#TME resource access specs	
RESOURCE	Yes	TME resource access specs	
ROLEN	No	# TME role access specs	
ROLEN	Yes	TME role access specs	

FACILITY - DLFDATA

The administrator uses this table to determine the fields in the FACILITY - DLFDATA segment type.

Fieldname	Repeats	Description	Command parameter
JOBNAMES	Yes	Job names	
JOBNMCNT	No	Job names #	
RETAIN	No	Retain flag byte	

FACILITY - EIM

The administrator uses this table to determine the fields in the FACILITY - EIM segment type.

Definition of the Enterprise Identity Mapping (`EIM`) domain.

Fieldname	Repeats	Description	Command parameter
DOMAINDN	No	EIM Domain Distinguished Name	
LOCALREG	No	Local RACF registry for EIM	LOCALREGISTRY
OPTIONS	No	EIM options	

FACILITY - PROXY

The administrator uses this table to determine the fields in the FACILITY - PROXY segment type.

`BINDPW` and `BINDPWKY` are read-only fields, so they only exist in SegmentList, not in Segment Detail.

Fieldname	Repeats	Description	Command parameter
LDAPHOST	No	LDAP Server URL	
BINDDN	No	Bind Distinguished Name	
BINDPW	No	Bind Password	
BINDPWKY	No	Bind Password Mask | Encrypt Key	

FACILITY - TME

The administrator uses this table to determine the fields in the FACILITY - TME segment type.

Fieldname	Repeats	Description	Command parameter
CHILDN	No	# TME child roles	
CHILDREN	Yes	TME child roles	
GROUPN	No	# TME associated groups	
GROUPS	Yes	TME associated groups	
PARENT	No	TME parent role	
2RESN	No	# TME resource access specs	
RESOURCE	Yes	TME resource access specs	
ROLEN	No	# TME role access specs	
ROLES	Yes	TME role access specs	

LDAPBIND - EIM

The administrator uses this table to determine the fields in the LDAPBIND - EIM segment type.

Definition of the Enterprise Identity Mapping (`EIM`) domain.

Fieldname	Repeats	Description	Command parameter
DOMAINDN	No	EIM Domain Distinguished Name	
LOCALREG	No	Local RACF registry for EIM	LOCALREGISTRY
OPTIONS	No	EIM options	

LDAPBIND - PROXY

The administrator uses this table to determine the fields in the LDAPBIND - PROXY segment type.

The `PROXY` segment is used to store LDAP proxy server information.

Fieldname	Repeats	Description	Command parameter
BINDDN	No	Bind information for LDAP server being contacted	
LDAPHOST	No	Host of LDAP server to contact	

PROGRAM - SIGVER

The administrator uses this table to determine the fields in the PROGRAM - SIGVER segment type.

The SIGVER (SIGnature VERification) segment for PROGRAM class profiles contains fields that are verify digital signatures of program modules.

Fieldname	Repeats	Description	Command parameter
SIGREQD	No	Module must have a signature.	SIGREQUIRED
FAILLOAD	No	Loader failure conditions	
SIGAUDIT	No	RACF audit condition	

PTKTDATA - SSIGNON

The administrator uses this table to determine the fields in the PTKTDATA - SSIGNON segment type.

PTKTDATA - SSIGNON contains an encryption key only, so it only appears in SegmentTypes, not in SegmentList or Segment Detail.

Fieldname	Repeats	Description	Command parameter
SSKEY	No	Single Signon key	

REALM - KERB

The administrator uses this table to determine the fields in the REALM - KERB segment type.

REALM - KERB/CURKEY, CURKEYV, ENCTYPE, PREVKEY, PREVKEYV, and SALT are read-only fields, so they only exist in SegmentList, not in Segment Detail.

Fieldname	Repeats	Description	Command parameter
CURKEY	No	Current Kerberos key	
CURKEYV	No	Current Kerb key version	
DEFTKTLF	No	Default ticket life	
ENCTYPE	No	Kerberos encryption type	
ENCRYPT	No	ed encryption types	
KERBNAME	No	Kerberos name	
MAXTKTLF	No	Maximum ticket life	MAXTKTLFE
MINTKTLF	No	Minimum ticket life	MINTKTLFE
PREVKEY	No	Previous Kerberos key	
PREVKEYV	No	Previous Kerb key version	
SALT	No	Seed for Kerberos Randomizer	

ROLE - TME

The administrator uses this table to determine the fields in the ROLE - TME segment type.

Fieldname	Repeats	Description	Command parameter
CHILDN	No	# TME child roles	
CHILDREN	Yes	TME child roles	
GROUPN	No	# TME associated groups	
GROUPS	Yes	TME associated groups	
PARENT	No	TME parent role	
2RESN	No	# TME resource access specs	

Fieldname	Repeats	Description	Command parameter
RESOURCE	Yes	TME resource access specs	
ROLEN	No	# TME role access specs	
ROLES	Yes	TME role access specs	

STARTED - STDATA

The administrator uses this table to determine the fields in the STARTED - STDATA segment type.

Fieldname	Repeats	Description	Command parameter
FLAGPRIV	No	Privileged - any, nolog	PRIVILEGED
FLAGTRAC	No	Trace - issue IRR812I	TRACE
FLAGTRUS	No	Trusted - any, log all	TRUSTED
STGROUP	No	Started task RACF group	GROUP
STUSER	No	Started task RACF user ID	USER

SYSMVIEW - SVFMR

The administrator uses this table to determine the fields in the SYSMVIEW - SVFMR segment type.

Fieldname	Repeats	Description	Command parameter
PARMN	No	SVFMR parameter list	PARMNAME
SCRIPTN	No	Default logon scripts	SCRIPTNAME

Segments of group profiles

The administrator uses these field descriptions to determine the details of each segment in a group profile.

This section describes the fields for the group segment types.

- "GROUP - CSDATA"
- "GROUP - DFP"
- "GROUP - OMVS" on page 119
- "GROUP - OVM" on page 119
- "GROUP - TME" on page 119

GROUP - CSDATA

The administrator uses this table to determine the fields in the GROUP - CSDATA segment type.

The `CSDATA` segment of a `GROUP` profile is where custom fields of that profile are added. You can add fields using the RACF `CFIELD` class to define the new fields to `GROUP` profiles and the labels you want to use for them. The fields of this segment are installation defined.

GROUP - DFP

The administrator uses this table to determine the fields in the GROUP - DFP segment type.

Fieldname	Repeats	Description	Command parameter
DATAAPPL	No	DFP - Data Application	

Fieldname	Repeats	Description	Command parameter
DATACLAS	No	DFP - Data Class	
MGMTCLAS	No	MDFP - Management Class	
STORCLAS	No	DFP - Storage Class	

GROUP - OMVS

The administrator uses this table to determine the fields in the GROUP - OMVS segment type.

The OMVS segment contains logon information for OMVS. OMVS, sometimes also called Open MVS, stands for OS/390 or z/OS UNIX System Services. The OMVS segment provides an OS/390 or z/OS UNIX Security context, which you need to log on to OMVS.

Fieldname	Repeats	Description	Command parameter
GID	No	OpenMVS group (grpid)	GID

GID The OMVS group identifier. To have the system assign an unused value, use "auto." If you want more than one group to share the GID, add "s" at the end of the GID value.

GROUP - OVM

The administrator uses this table to determine the fields in the GROUP - OVM segment type.

The OVM segment is used to store UNIX System Services information.

Fieldname	Repeats	Description	Command parameter
GID	No	UNIX group (gid)	

GROUP - TME

The administrator uses this table to determine the fields in the GROUP - TME segment type.

Fieldname	Repeats	Description	Command parameter
ROLEN	No	# TME role access specs	
ROLES	Yes	TME role access specs	

Segments of user profiles

The administrator uses these field descriptions to determine the details of each segment in a user profile.

This section describes the fields for the user segment types.

- "USER - CICS" on page 120
- "USER - CSDATA" on page 120
- "USER - DCE" on page 120
- "USER - DFP" on page 121
- "USER - EIM" on page 121
- "USER - KERB" on page 121

USER - CICS

The administrator uses this table to determine the fields in the USER - CICS segment type.

The CICS segments show information about CICS, an online transaction processing system. CICS is used to handle large numbers of data transactions from large computer or terminal networks. This topic shows the fields of the segment.

Fieldname	Repeats	Description	Command parameter
OPCLASS	Yes	Operator class	
OPCLASSN	No	Operator class values #	
OPIDENT	No	Operator identification	
OPPRTY	No	Operator priority	
TIMEOUT	No	Terminal time-out value	
XRFSOFF	No	XRF Re-signon option	

USER - CSDATA

The administrator uses this table to determine the fields in the USER - CSDATA segment type.

The CSDATA segment of a USER profile is where custom fields of that profile are added. You can add fields using the RACF CFIELD class to define the new fields to USER profiles and the labels you want to use for them. The fields of this segment are installation defined.

USER - DCE

The administrator uses this table to determine the fields in the USER - DCE segment type.

Fieldname	Repeats	Description	Command parameter
DCEENCRY	No	DCE password encr. key no.	
DCEFLAGS	No	DCE Autologin	AUTOLOGIN
DCENAME	No	DCE username	
DPASSWDS	No	DCE password	
HOMECELL	No	DCE homecell	
HOMEUUID	No	DCE homecell UUID	
UUID	No	DCE UUID	

USER - DFP

The administrator uses this table to determine the fields in the USER - DFP segment type.

Fieldname	Repeats	Description	Command parameter
DATAAPPL	No	DFP - Data Application	
DATACLAS	No	DFP - Data Class	
MGMTCLAS	No	DFP - Management Class	
STORCLAS	No	DFP - Storage Class	

USER - EIM

The administrator uses this table to determine the fields in the USER - EIM segment type.

Segment to store the name of an LDAPBIND class profile. This profile contains the information needed to connect to the EIM domain on the LDAP host it resides on.

Fieldname	Repeats	Description	Command parameter
LDAPPROF	No	LDAP Profile	

USER - KERB

The administrator uses this table to determine the fields in the USER - KERB segment type.

USER - KERB/CURKEY, CURKEYV, DEFTKTLF, ENCTYPE, MINTKTLF, PREVKEY, PREVKEYV, and SALT are read-only fields, so they only display in SegmentList, not in Segment Detail.

Fieldname	Repeats	Description	Command parameter
CURKEY	No	Current® Kerberos key	
CURKEYV	No	Current Kerb key version	
DEFTKTLF	No	Default ticket life	DEFTKTLFE
ENCTYPE	No	Kerberos encryption type ed encryption types	
ENCRYPT	No	Kerberos name	
KERBNAME	No	Maximum ticket life	MAXTKTLFE
MAXTKTLF	No	Minimum ticket life	MINTKTLFE
MINTKTLF	No	Previous Kerberos key	
PREVKEY	No	Previous Kerb key version	
PREVKEYV	No	Seed for Kerberos Randomizer	
SALT	No		

USER - LANGUAGE

The administrator uses this table to determine the fields in the USER - LANGUAGE segment type.

Fieldname	Repeats	Description	Command parameter
USERNL1	No	Primary language of a user	PRIMARY
USERNL2	No	Secondary language of a user	SECONDARY

USER - LNOTES

The administrator uses this table to determine the fields in the USER - LNOTES segment type.

Fieldname	Repeats	Description	Command parameter
SNAME	No	Lotus Notes short username	

USER - NDS

The administrator uses this table to determine the fields in the USER - NDS segment type.

Fieldname	Repeats	Description	Command parameter
UNAME	No	NDS username	

USER - NETVIEW

The administrator uses this table to determine the fields in the USER - NETVIEW segment type.

Fieldname	Repeats	Description	Command parameter
CONSNAME	No	Default console name	
CTL	No	Scope of control	
DOMAINS	Yes	Cross-domain authority	DOMAINS
DOMAINSN	No	# cross-domain authorities	
IC	No	Initial command list	
MSGRECVR	No	Receive undelivered messages	
NETVIEW	No	Admin auth Graphic Mon Fac	NGMFADMN
NGMFVSPN	No	View span opts Graph.Mon.Fac.	
OPCLASS	Yes	Operator class	
OPCLASSN	No	Operator class values #	

USER - OMVS

The administrator uses this table to determine the fields in the USER - OMVS segment type.

The OMVS segment contains logon information for OMVS. OMVS, sometimes also called Open MVS, stands for OS/390 or z/OS UNIX System Services. The OMVS segment provides an OS/390 or z/OS UNIX Security context, which you need to log on to OMVS.

Fieldname	Repeats	Description	Command parameter
ASSIZE	No	Max. address space size	ASSIZEMAX
CPUTIME	No	Maximum CPU time	CPUTIMEMAX
FILEPROC	No	Max. files open per proc	FILEPROCMAX
HOME	No	OpenMVS home path	
MMAPAREA	No	Max. data space for mapping	MMAPAREAMAX
PROCUSER	No	Max. nr. of active procs	PROCUSERMAX
PROGRAM	No	Conditional access program	

Fieldname	Repeats	Description	Command parameter
THREADS	No	Max. nr. of active threads	THREADSMAX
UID	No	OpenMVS user (uid)	

UID OMVS `UID` field with the user identifier. To have the system assign an unused value, fill in "auto." If you want more than one user to share the UID, add "s" at the end of the `UID` value.

USER - OPERPARM

The administrator uses this table to determine the fields in the USER - OPERPARM segment type.

Fieldname	Repeats	Description	Command parameter
OPERALTG	No	Alternate console group	ALTGRP
OPERAUTH	No	Console authority	AUTH
OPERAUTO	No	Receive msgs automated by MPF	AUTO
OPERCMDS	No	System to send commands to	CMDSYS
OPERDOM	No	Delete operator messages type	OM
OPERKEY	No	KEY keyword of D,CONSOLES,KEY	KEY
OPERLEVL	No	LEVEL of msgs to be received	LEVEL
OPERLOGC	No	Command response logging	LOGCMDRESP
OPERMCNT	No	MSCOPE systems #	
OPERMFRM	No	Message format	MFORM
OPERMGID	No	Migration id to be assigned	MIGID
OPERMON	No	Events to be monitored	MONITOR
OPERMSCP	Yes	MSCOPE systems	MSCOPE
OPERROUT	No	ROUTCODEs for msg reception	ROUTCODE
OPERSTOR	No	STORAGE in MB for msg queuing	STORAGE
OPERUD	No	Receive undelivered messages	UD

USER - OVM

The administrator uses this table to determine the fields in the USER - OVM segment type.

Fieldname	Repeats	Description	Command parameter
FSROOT	No	OpenVM file system root	
HOME	No	OpenMVS home path	
ROGRAM	No	Conditional access program	
UID	No	OpenMVS user (uid)	

USER - PROXY

The administrator uses this table to determine the fields in the USER - PROXY segment type.

BINDPW and BINDPWKY are read-only fields, so they only exist in SegmentList, not in Segment Detail.

Fieldname	Repeats	Description	Command parameter
LDAPHOST	No	LDAP Server URL	
BINDDN	No	Bind Distinguished Name	
BINDPW	No	Bind Password	
BINDPWKY	No	Bind Password Mask | Encrypt Key	

USER - TSO

The administrator uses this table to determine the fields in the USER - TSO segment type.

TSO is the abbreviation of Time Sharing Option, a specific way to communicate with MVS by entering line commands, the mainframe equivalent of a DOS prompt. The TSO segment contains information about how to log on to MVS.

USER - TSO/TCONS, TOPTION, TPERFORM, TRBA, and TUPT are read-only fields, so they only exist in SegmentList, not in Segment Detail.

Fieldname	Repeats	Description	Command parameter
TACCNT	No	Default account number	ACCTNUM
TCOMMAND	No	Default command	COMMAND
TCONS	No	Consoles support	
TDEST	No	Destination identifier	DEST
THCLASS	No	Default held sysout class	HOLDCLASS
TJCLASS	No	Default job class	JOBCLASS
TLPROC	No	Default logon procedure	PROC
TLSIZE	No	Default logon region size (KB)	SIZE
TMCLASS	No	Default message class	SGCLASS
TMSIZE	No	Maximum region size	MAXSIZE
TOPTION	No	Mail/Notice/Recon/OID options	
TPERFORM	No	Performance group	
TRBA	No	RBA of user broadcast area	
TSCLASS	No	Default sysout class	SYSOUTCLASS
TSOSLABL	No	Default logon SECLABEL	SECLABEL
TUDATA	No	Site data TSO user (2 byte)	USERDATA
TUNIT	No	Default unit name	UNIT
TUPT	No	UPT control block data	

USER - WORKATTR

The administrator uses this table to determine the fields in the USER - WORKATTR segment type.

Fieldname	Repeats	Description	Command parameter
WAACCNT	No	Account number	
WAADDR1	No	SYSOUT address line 1	
WAADDR2	No	SYSOUT address line 2	
WAADDR3	No	SYSOUT address line 3	
WAADDR4	No	SYSOUT address line 4	

Fieldname	Repeats	Description	Command parameter
WABLDG	No	Building for delivery	
WADEPT	No	Department for delivery	
WANAME	No	User name for SYSOUT	
WAROOM	No	Room for delivery	

Chapter 8. Running REXX scripts

zSecure Visual can be customized to allow running site-defined REXX scripts.

When the Visual Server has been configured to access site-defined REXX scripts, you can use the Visual Client to select and run a REXX script. You can find more information in the following topics.

"Prerequisites for running REXX scripts on the Visual Server"
Before you can run site-defined REXX scripts from a Visual Client, an association file must be created in the Visual Server.

"Running a REXX script in the Visual Client"
You can use the Visual Client interface to run a REXX script that is configured on the Visual Server.

Prerequisites for running REXX scripts on the Visual Server

Before you can run site-defined REXX scripts from a Visual Client, an association file must be created in the Visual Server.

Use the instructions in "Site-defined REXX scripts" in the *Installation and Deployment Guide* to configure an association file for site-specific REXX scripts. You can then use the Visual Client to select and run a REXX script from a location that is remote from the Visual Server.

Scripts will only show when such an association file was defined on the server. If an association file was not defined on the server, the client will not provide a message indicating that no REXX scripts have been defined.

Running a REXX script in the Visual Client

You can use the Visual Client interface to run a REXX script that is configured on the Visual Server.

Before you begin

A REXX script must be defined in the Visual Server before the Visual Client can be used to run the script. Scripts can be associated with user names and group names. See "Prerequisites for running REXX scripts on the Visual Server."

Note: Visual Client shows the configured description for the script, not the actual name of the script.

Procedure

To run a REXX script in Visual Client, use one of these methods:

- Right-click an object that belongs to the class for which you want to run a REXX script. For example, use **Navigate**, **Find**, and **Class:** User. Right-click an object to view the list of the available actions, navigation options, and the description of the REXX scripts that are defined on the Visual Server. Click a description to run the script. This option works for all classes for which REXX scripts have been defined on the Visual Server such as User, Group, and Dataset, or a specific class such as XFACILIT.

- Select **Navigate** in the main client window to view a list of descriptions of the available REXX scripts. Then click the listed description to run the script. This option is available only for scripts that are defined to be run against the class User.

Chapter 9. Maintenance

The administrator uses this information to understand the parameters required for communication between the Visual server and client.

To access the server, a zSecure Visual client needs a local server definition and a corresponding client definition on the server. With these definitions, a safe communication channel is created. To set up a new, previously unused channel, an initial password is needed once. The client definition contains more information than the server definition; otherwise they are similar.

The mainframe provides limited support for managing client definitions. For more information, see the section about configuring zSecure Visual clients in the server in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

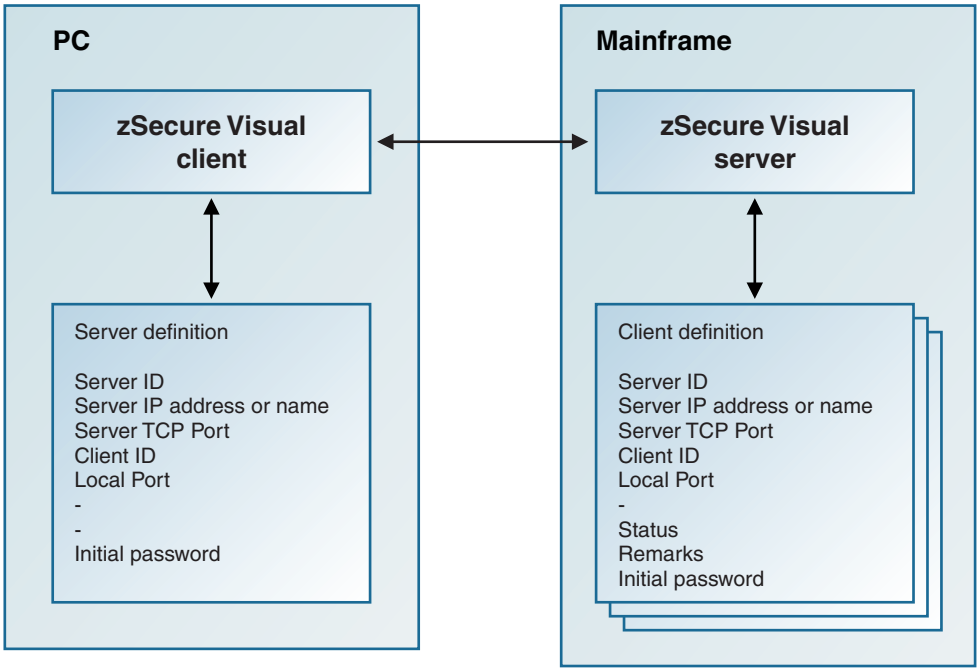


Figure 64. Server and client definitions needed for communication between the server and a client

Maintaining client definitions

The administrator performs these tasks to create, edit, and delete client definitions for zSecure Visual.

About this task

The Maintain Client window enables you to:

- Create client definitions
- Edit or delete existing client definitions
- Generate initial passwords

Procedure

- To open the Maintain Client window, select **Maintenance > Client** from the main menu. The Maintain Client window lists all existing client definitions for an instance of the zSecure Visual server.

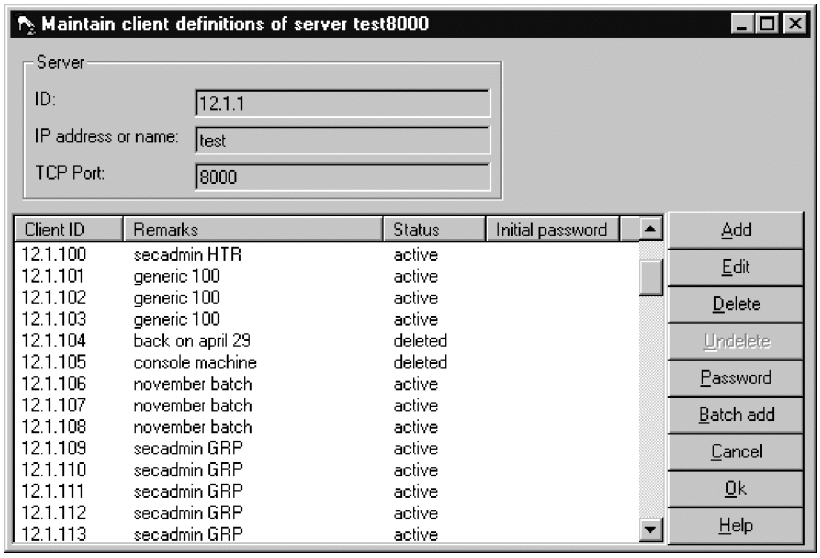


Figure 65. Maintain Client window

The client fields are:

Client ID
Optional. Must be unique to the server. If left empty, the server generates one for you. This field is also known as **Agent id** on the server.

Remarks
Optional. Stores any notes for the client definition.

Status Read only. Shows deleted or active. You cannot use a deleted client definition to log on.

Initial password
Read only. Required to initiate communication for a new client. It is generated by the server. The validity is limited to seven days or the length of the server run, whichever ends first.

Note: The initial password is displayed only after being generated and only as long as the window remains open. Newly created client definitions are automatically assigned an initial password.

The server attributes are shown at the top of the window: **Server ID**, **IP address or name**, and **TCP Port**. For information about server fields and creating server definitions on the client, see "Server definition parameters" on page 140.

- Select the **Add** button to add a single definition.
- Select the **Edit** button to edit a single definition.
- To delete one or more definitions, select the entries and click **Delete**.
- Use the **Undelete** button to activate a deleted definition.
- To generate one or more new passwords, select the definitions and click **Initial password**.

Batch mode to add multiple client definitions

The administrator uses the **Batch add** dialog to create multiple client definitions for zSecure Visual in a batch run.

Use the **Batch Add** dialog to create multiple client definitions using a single action.

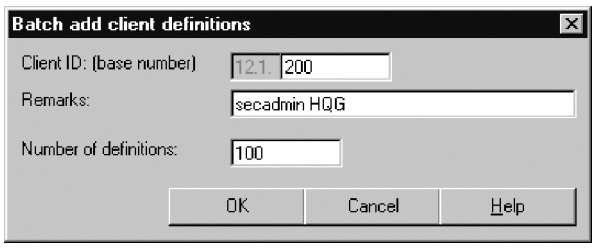


Figure 66. Batch add client definitions dialog

The following fields are displayed:

Client ID base number
Optional. Specifies the value to start with when generating the Client IDs.

Remarks
Optional. Text that identifies the purpose of the batch of IDs.

Number of definitions
Specifies the total number of Client IDs to generate. You can specify a value up to 100.

When the batch run finishes, the **Maintain Client** window is displayed showing the new entries with initial passwords. See Figure 65 on page 130.

Client definition attributes

The administrator specifies these attributes to create the corresponding server definition in zSecure Visual.

After you create a client definition, you must specify these attributes for the client:

- Server IP address or name
- Server TCP port number
- Client ID
- Initial password

These attributes are used to create the corresponding server definition. The client and server definitions enable the client to log on to the server. See "Server definition parameters" on page 140 for more information.

Copying a client definition to the clipboard

The administrator uses this procedure to select and distribute specific Visual client definitions to users.

About this task

From the **Maintain Client** window, you can copy selections of client IDs and initial passwords to the clipboard and mail them to your users.

Procedure

To copy client definitions to the clipboard, complete these steps:

1. Open the **Maintain Client** window.
2. Generate the client definitions and initial passwords needed for distribution.
3. Select the client definitions that you want to distribute.
4. Copy the selected definitions to the clipboard. The server attributes are added at the top as a header. The client information is laid out in tabbed columns. You can paste to a spreadsheet to retain the column spacing, or to an email. The email layout does not retain the equally spaced tabbed alignment.

   Clipboard example:

```
Server
IP address or name:     test
TCP Port:       8000

Client ID       Remarks Status  Initial password
12.1.100        secadmin HTR    active  63F693FF96
12.1.101        generic 100     active  99F239EF6F
12.1.102        generic 100     active  01E671F0A6
```

Chapter 10. Setup and configuration

To use zSecure Visual on a client, you must:

- Install the client software on the system that you are using as the Visual client.
- Define the client on the mainframe where the Visual server is installed.
- Configure the client to connect to and establish a session with the Visual server.

For information on installing zSecure Visual on the server, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*. For information about known problems and limitations, see the *IBM Security zSecure: Release Information* in the information center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.htm.

Installation and configuration are described in the following topics:

Prerequisites for installation

Before you install the zSecure Visual client, ensure that the system meets these hardware and software requirements:

Hardware requirements

- 1 GHz processor or greater
- 512 MB RAM or greater
- Minimum 155 MB disk space
- Minimum S-VGA display
- TCP/IP adapter for connection to the mainframe
- Minimum disk space for .NET Framework Version 4 client:
  - 32-bit: 600 MB
  - 64-bit: 1.5 GB

Software requirements

- Microsoft Windows 7, Windows 8, Windows Server 2008R2, or Windows Server 2012

  You can check the operating system level when you start the workstation.
- To work with the IBM Eclipse Help System, install Microsoft Internet Explorer Version 7.*x*, 8.*x*, 9.*x*, 10.*x* or Firefox up to version 17. To ensure that all the functions of the IBM Eclipse Help System are usable:

  - Enable cookies and JavaScript in the browser.
  - Disable the blocking of pop-up windows in the browser.
- To connect to the zSecure Visual server on the mainframe, you must configure:
  - TCP/IP network that provides a connection to the mainframe.
  - Name of the localhost where the client is installed.

To connect to the zSecure Visual server on the mainframe, install and configure this software on the mainframe:

- Supported release of z/OS, up to V2R1
- RACF Security Server
- TCP/IP
- IBM Security zSecure Visual 2.1.0 server

After installation, you must create a server definition on the client to connect to the mainframe. Determine these settings to prepare for the server definition:

- Server IP address or name
- Server TCP port number
- Client ID
- Initial password

You can obtain this information from your system administrator.

Installing IBM Security zSecure Visual

The administrator uses this task to install the Visual client component.

About this task

You can install the new version of the IBM Security zSecure Visual client *only once* on a workstation. You can upgrade from a previously installed version of the client, for example, version 1.12. See "Upgrading IBM Security zSecure Visual" on page 137 and "Compatibility of IBM Security zSecure Visual and zSecure components" on page 139 for guidelines on upgrading the client.

Although you cannot install the new Visual client multiple times on the same workstation, you can define multiple Visual server definitions in one client and run multiple Visual client instances concurrently. See "Multiple Visual server definitions" on page 142.

The zSecure Visual client software for Windows is available on CD. The CD also contains the zSecure Visual client manual in PDF format.

Note: Information on installing and configuring the zSecure Visual server is in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

You can either install a complete version or a custom version of the zSecure Visual client program.

The Complete version of the installation program installs the Java Run time. If you want to continue using your current version of the Java Run Time, use the Custom version of the installation and specify to bypass installing the Java Run Time.

This section describes how to complete each type of installation.

Procedure

Follow these steps to install the Visual client program:

1. Ensure that the system where you are installing the Visual client meets the hardware and software requirements. Review the requirements in "Prerequisites for installation" on page 133.
2. Take one of the following actions to start the installation:
   - *Install directly from CD.*
     a. Insert the CD in the system where you are installing the Visual client. The installation starts automatically after inserting the CD.
     b. If the automatic installation fails or is canceled, start the installation by running **launchpad.exe** from the root directory.
   - *Install from a LAN directory.*
     a. Specify the network location of the CD image.
     b. If the installation directory contains one or more spaces, you must specify the filepath in quotation marks, for example:

        ```
        "C:\installation dir\visual210\DISK1\setup.exe"
        ```
3. Select the language that displays the contents of the Visual client and click **OK**.
4. Click **Next** in the welcome window.
5. Accept the license agreement and click **Next**.

   Note: You can print the terms of the license agreement by clicking **Print**. The license files are in the `\License` subdirectory. You can view the license in English and the locale language configured on the target system, but other languages might not be viewable.
6. Select one of the following options and click **Next**.

   Complete
   Installs all program files in the default directory. This option is for normal use and uses more disk space.

   Custom
   Provides two options for advanced users.
   - *If you do not want to install the program files in the default directory:*
     a. Click **Change...** to specify a different installation directory than the default directory (`C:\Program Files\IBM\Security zSecure Visual\2.1`).

        Attention: If the Windows system folder is not located on the destination drive, but you know the destination drive has adequate space to receive the files, the following warning could still occur when you click **Next**:

        ```
        There is not enough space to install these option(s).
        Please free some disk space or modify your selections.
        ```

        This warning refers to the drive that contains the Windows system folder. If it occurs, use the Feature description area in the Custom Setup dialog to determine how much space is required by the selected components and ensure that the drive containing the Windows system folder also has adequate space.

b. Browse to the directory where you want to install the files or specify the complete filepath in the **Folder name** field.

   Note: If you are upgrading a previous version of the Visual client, each version must reside in its own folder; ensure that the version number is shown in the folder title so you can distinguish between different versions.

c. Click **OK** to return to the Custom Setup window.

- *If you do not want to install the help files associated with the product* (for example, you might have limited space on your destination drive):

a. Click **Help Files > This feature will not be available** .

   Note:

   – The

   The first two options (beginning with **This Feature**...) perform the same installation. All help files are installed in both cases.

b. Click **Space** to view the storage requirements for the help files.

c. Click **OK** to return to the Custom Setup window.

7. Click **Install** to start the installation.
8. Click **Finish** to exit the installation program or click **Launch zSecure Visual** to start the Visual client and set up the client to connect to a Visual server.

What to do next

Before you can use zSecure Visual, you must configure it. You can manually or automatically configure it. For more information about configuration, see "Configuring IBM Security zSecure Visual" on page 139.

If the installation does not complete without errors, you can examine the log file for information to help troubleshoot the causes. The information is detailed and intended for expert use.

zSecure Visual maintenance

The administrator uses these topics to uninstall, modify, and repair IBM Security zSecure Visual.

You can uninstall, modify, and repair IBM Security zSecure Visual. This section provides the procedures to perform these tasks.

A fix pack is provided as a zip file. Installing it effectively overwrites the existing instance of the Client.

Uninstalling IBM Security zSecure Visual

The administrator uses this task to uninstall IBM Security zSecure Visual.

Procedure

To completely remove IBM Security zSecure Visual and all of its components, perform these steps:

1. Go to the Control Panel.
2. Select **Add/Remove Programs**.

3. Select **IBM Security zSecure Visual 2.1.0**.
4. Click **Add/Remove** to start the setup program.
5. In the Welcome dialog for the maintenance program, select **Remove**. Then, click **Next**.
6. In the Confirm uninstall dialog, click **OK**.
7. When Maintenance detects a shared file, you get a warning message. Click **Yes** to continue. Maintenance starts to remove IBM Security zSecure Visual.

   When Maintenance is complete, the Maintenance Complete window is displayed. Restart your computer.

Modifying IBM Security zSecure Visual

The administrator uses this task to change selected installed components in IBM Security zSecure Visual.

About this task

If you are an advanced user, you can modify your Visual client installation to add new program components or remove currently installed components.

Procedure

Perform these steps to change a Visual client installation:

1. Start Control Panel and select **Add/Remove Programs**.
2. Select **IBM Security zSecure Visual 2.1.0** and click **Add/Remove**.
3. In the Welcome dialog window, select **Modify**. Then, click **Next**.
4. In the Select Components window, select the components to be modified.
5. Click **Next** to modify your installation. The Setup Status dialog is displayed to monitor the setup process. When Maintenance has finished the modifications, it ends with the Maintenance complete screen.
6. Restart your computer.

Repairing IBM Security zSecure Visual

The administrator uses this task to reinstall all program components for IBM Security zSecure Visual.

About this task

If you find damaged files, reinstall all program components. To reinstall all program components, perform these steps:

Procedure

1. Start Control Panel and select **Add/Remove Programs**.
2. Select **IBM Security zSecure Visual 2.1.0** and click **Add/Remove**.
3. In the Welcome dialog window, select **Repair**. Then, click **Next**.
4. After the repair process completes, click **Finish**.

Upgrading IBM Security zSecure Visual

The administrator uses this task to upgrade IBM Security zSecure Visual.

About this task

You can upgrade IBM Security zSecure Visual using the method described in “Installing IBM Security zSecure Visual” on page 134. The new installation does not contain any server definitions. You can copy the server definitions from the previous version, as described in“Copy function for multiple server definitions” on page 143. You can also use the automated process, see “Automate upgrade path examples” on page 148.

After you upgrade the zSecure Visual server, you can upgrade the zSecure Visual client software on the client machines and connect to the new server instance. This procedure creates a new server definition in the new client that uses a copy of the old certificate and points to the new server. Copying the old certificate enables you to perform the upgrade process without having to create a new initial password for the client.

Procedure

Follow these steps to upgrade zSecure Visual client software.

1. Install the new client software.
2. Start the client.
3. Update the configuration to create the server definition:
   a. From the Visual client menu, select **File > Configure > Copy**.
   b. On the Copy configuration panel, update the Visual server **IP address** or **name** and **TCP port** to point to the location of the upgraded server.
   c. Click **Test Connection** to verify the connection.
   d. Click **OK** to save the changes and create the new server.

   Table Table 5 lists available support based on the zSecure Visual server version.

Table 5. zSecure Visual client versions compatibility

zSecure Visual Client	**zSecure Visual Server**				
	Version 2.1	**Version 1.13.*x***	**Version 1.12**	**Version 1.11**	**Version 1.10**
Version 2.1	Supported	No formal support	No formal support	No formal support	No formal support
Version 1.13.1	Compatible	Supported for 1.13.1 server only	No formal support	No formal support	No formal support
Version 1.13	Compatible	Supported	No formal support	No formal support	No formal support
Version 1.12	Compatible	Compatible	Supported	No formal support	No formal support
Version 1.11	No formal support	Compatible	Compatible	Supported	No formal support
Version 1.10	No formal support	No formal support	Compatible	Compatible	Supported

Note: *Compatible* means that new function is not supported in a downlevel client.

Compatibility of IBM Security zSecure Visual and zSecure components

The administrator uses this information to plan for an upgrade of IBM Security zSecure Visual.

To optimize zSecure Visual features, all related components must be the same version. For optimum performance, combine zSecure Visual client 2.1.0 with:

- z/OS V2R1
- CKRCARLA 2.1
- CKGRACF 2.1
- zSecure Visual server 2.1

Upgrading the zSecure Visual client does not require the client to be at the same release level as the zSecure Visual server. However, IBM does not support using previous releases of the Visual client with the current release of the Visual server. See Table 5 on page 138.

First upgrade the server to the latest release, and then begin installing the new client. Multiple instances of the client can exist while you manage the workload of upgrading all the client instances.

Multiple zSecure Visual client versions can coexist on the same workstation. For example, on a single computer you can install version 2.1 of the client without first removing version 1.13.1. In general, multiple client versions can exist concurrently on a single computer *if no port conflicts exist*:

- Configure a different local port number than the default to run multiple versions in parallel.
- Ensure that the port value for each client version corresponds to the port of the Visual server with which it communicates.

Multiple zSecure server instances with different versions are also supported if your configuration prevents port conflicts. For more information, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Configuring IBM Security zSecure Visual

The administrator uses this task to define a Visual server to a Visual client.

About this task

You configure IBM Security zSecure Visual by defining the Visual server to the client and by defining the Visual client to the Visual server. This topic describes how to define the Visual server to the client. See “Maintaining client definitions” on page 129 for information on adding client definitions to the Visual server.

Visual server definitions are stored in the Common application data folder, for example, `C:\Documents and Settings\All Users\Application Data`. This folder contains application data for all users of the system. The Visual server configuration is available for all users who log on to that system. To edit or delete a Visual server definition, a user must have created it or have administrative privileges.

Procedure

1. If no servers have been defined to the client, you enter the configuration part of the program automatically after you start the program. Otherwise you can select **File > Configure** from the main menu.

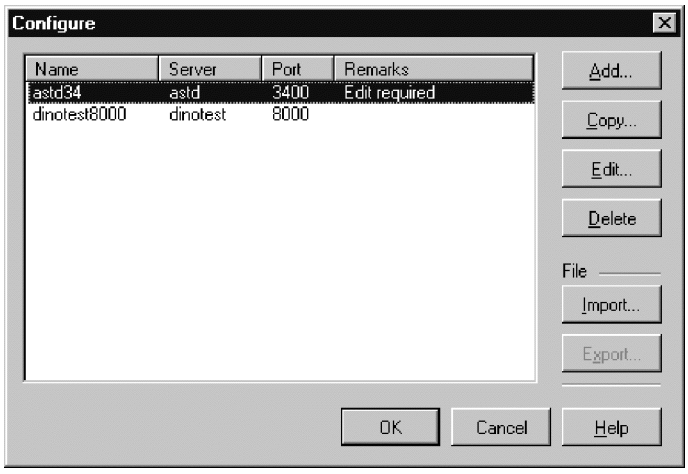


Figure 67. Configure dialog

   The configuration window displays all defined servers and enables you to add, copy, edit, and delete server definitions. When "Edit required" is displayed in the list, you must complete the corresponding server definition before you can use the server.

   With the *Import* function, you can read server definition information from a configuration file prepared for you. With *Export*, you can create configuration files, which enables automatic setup and configuration.

2. After adding, editing or deleting one or multiple server definitions, click **OK** to apply all changes. A status window is displayed, showing the steps performed to configure the program.

Server definition parameters

The administrator uses the **Add system** dialog to create and edit a Visual Server definition in the Visual client.

A server definition contains the parameters listed in this section. After completing the fields, click **OK** to accept them. You can use **Test Connection** to verify if the server is active. You can leave all fields blank except **Name** and complete the definition in another run of IBM Security zSecure Visual.

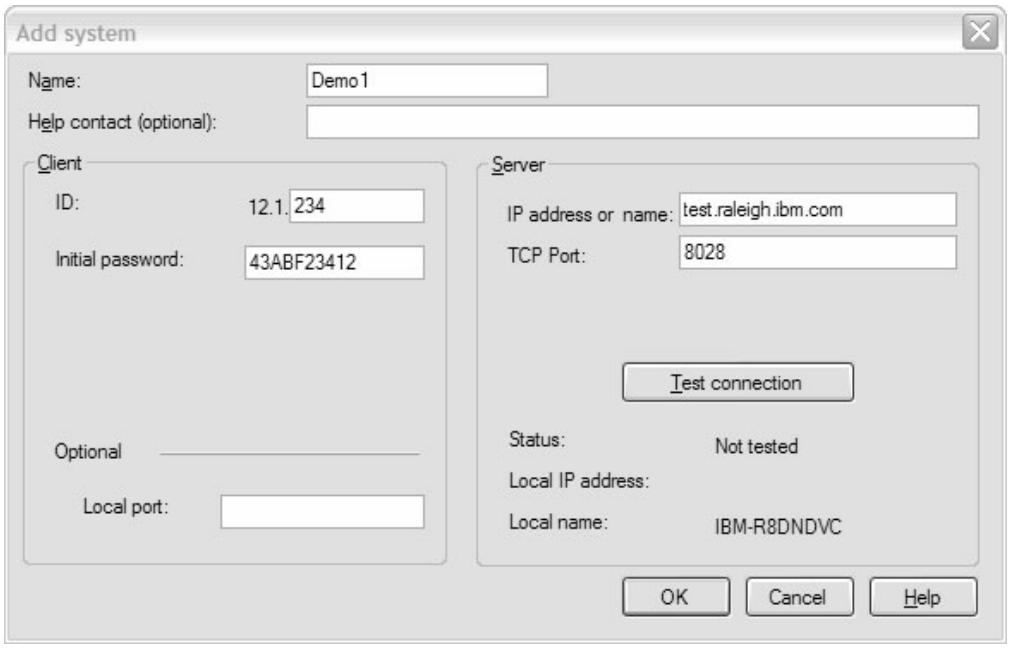


Figure 68. Server definition dialog

To use the server, you need a certificate. When you enter the correct initial password, you get the certificate.

Attention: When you obtain a new certificate, ensure that the clock of your local workstation is synchronized with the mainframe server clock. Out-of-synch clocks can cause errors.

Refer to this list for information about the server definition parameters:

Name This arbitrary name refers to this specific server definition. It is displayed in the **Logon** dialog. The name must be unique on the PC. The name must be a valid filename for Windows, because a subdirectory is created to store files related to the server.

HelpContact (optional)
Enter the name of a person, department name, or anything else that informs the user who to contact in case of trouble. If the field is nonblank it is displayed in error dialogs as follows: Error 3: Time Out. Contact *helpcontact*.

Client ID
This number uniquely identifies the client to its server. It is always 12.1.*n*, where *n* is an integer between 2 - 2,147,483,647. Typically these IDs are defined on the server. Before you can use a client, you must ask for its ID, and enter it here.

Server IP address or name
The IP address or the fully qualified host name of the server.

Server Port
The port that the server agent listens to. A port number is a number 0 - 65535. If you are configuring multiple server definitions to connect to multiple zSecure server instances, see “Multiple Visual server definitions” on page 142 for guidelines on specifying port values.

Local port (optional)
The client agent uses two port numbers to communicate with the server and with the user interface. By default these port numbers are the server port number and the server port number + 1. If there are two servers with equal port numbers, port conflicts occur. With this field, you can override the default local port number. The user interface uses local port number + 1. If you are configuring multiple server definitions to connect to multiple zSecure Server instances, see "Multiple Visual server definitions" for guidelines on specifying port values.

Initial password
A 10 hex digit password required to obtain a new certificate. The certificate is used for encryption. Usually the initial password can be obtained from your mainframe system administrator.

Test connection
To verify if the Server IP address or fully qualified host name and the Server Port are correct, click **Test Connection**. After some time `Connect succeeded` or `Connect failed` is displayed in the status field.

Note: Connection fails if the server parameters are correct but the server is not running.

Multiple Visual server definitions

The administrator uses these guidelines to plan for the implementation of multiple Visual Server definitions.

You *cannot* install the new Visual client multiple times on the same workstation, but you can define multiple Visual server definitions in one client. You can run multiple Visual client instances (sessions) concurrently. You can use each session to administer different RACF databases, based on the server configuration that you select when you log on to a Visual server.

If you configure the zSecure Server to service multiple nodes, the Visual server using that zSecure Server can administer two or more nodes and RACF databases in a single session. You must run the client in multi-system mode to administer multiple nodes (and RACF databases) in a single session. See "Selecting to work locally or in a multisystem environment" on page 2.

To administer multiple Visual servers concurrently, you must ensure that a unique port number is used by each Visual server. For example, if you create two or more Visual server definitions using server TCP 8000, the Visual client tries to use the same local port number (base port+1=8001) for the traffic coming from each server. This will cause port conflict problems and must be avoided. Here are two ways you can configure multiple Visual servers to avoid a port-use conflict:

- Run the Visual servers on different port numbers. For example, if server X uses port 8000, server Y uses port 8010, and server Z uses port 8020, the Visual client automatically uses the local ports 8001, 8011, and 8021, respectively, to communicate with the three servers.
- If the Visual servers are already running using the same port number, for example, port 8000, you can use the **Local port** field in the server definition dialog to separate the traffic coming from the different servers. For example, you can leave the **Local port** field blank in the server definition for server X, which results in that server using port 8001. For server Y, you can specify local port number 8010, and for server Z specify port number 8020.

Copy function for multiple server definitions

The administrator can use the Copy function to create multiple Visual server definitions.

A client needs a definition for each server to access, see “Server definition parameters” on page 140. However, it is not always necessary to enter the whole definition from scratch. You can copy server definitions between different versions of IBM Security zSecure Visual. Avoid port conflicts when doing so. If needed, consult your system administrator.

The Copy function shows you an exact copy of the existing server definition. Some of the fields in the definition are disabled so that you cannot change them.

Automated setup and configuration

The administrator can use automated setup and configuration for an initial installation of the Visual client.

Configuration file

The administrator can use a configuration file to distribute configuration parameters for zSecure Visual.

With the configuration file, you do not have to type the same information again. You write parameters to a file. The target computers read it during their setup and configuration.

Creating a configuration file

The administrator can use zSecure Visual to create a configuration file.

About this task

When you create the configuration file, the changes do not affect your PC. All the server and setup data options you configure are saved to a file.

Procedure

To create a configuration file, perform these steps:

1. Select **File > Configure** from the main menu to enter the configure dialog.
2. Click **Export** to switch to Export mode. The following window displays:

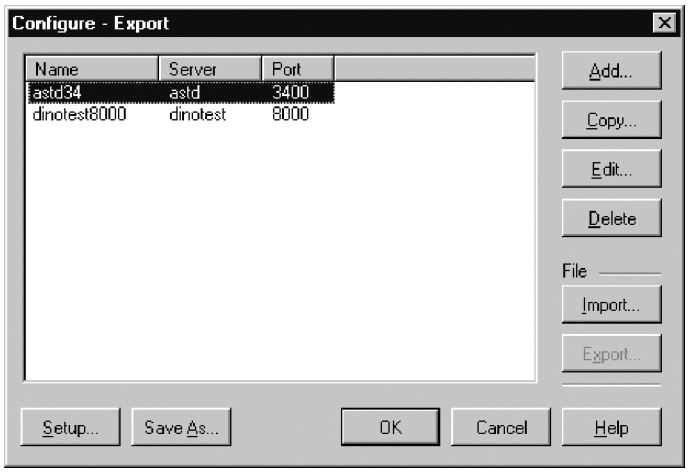


Figure 69. Configuration dialog in export mode

Note: To prevent an accidental switch in or out of Export mode, the **Export** button is disabled after any of these actions: **Add**, **Edit**, **Delete** or **Import**.

From this point, all changes in the configuration do not affect your PC; but the resulting server and setup data can be written to a configuration file by clicking **OK**. You can save an intermediate state by using **Save As**.

3. Specify manual or automated configuration parameters:

   Manual setup

   Use the **Add**, **Copy**, **Edit**, **Delete, and Import** functions to specify the server data.

   In general, you do not save all servers defined on your PC in the file. You can delete all servers that you do not want to include and clear the fields that you do not want to specify, such as Client ID.

4. To save an interim version of the configuration file at any point in the configuration process, click **Save As** and specify the configuration file name.
5. To save the configuration file, click **OK**.

Configuration file layout

The administrator uses these parameter descriptions to add contents to a configuration file.

The settings that define a server are in a Server section. A configuration file can contain more than one Server section.

NAME=server_definition_name
Specifies the server definition name.

CLIENTID=12.1.*n*
Specifies the Client ID, where *n* is an integer between 0 - 4,294,967,295.

SERVERIP=Servername
Specifies the IP address or hostname of the server.

SERVERPORT=8000
Server IP port.

HELPCONTACT=System support
Specifies the help contact, as shown in the error dialogs.

Running a configuration file on the target machine

The administrator can run the **setup** command to configure zSecure Visual on the system.

Procedure

- On the target machine, run setup with the configuration filename as a command-line argument:

  `<full path>\setup /s /v"CMDVISUAL=<full path to configuration file>"`

  Attention:
  - You must specify the `CMDVISUAL` option in uppercase.
  - IBM Security zSecure Visual can find the configuration file only if you specify the full path.
- When installation is finished, setup starts IBM Security zSecure Visual with the configuration file as an input parameter.

Updating server definitions from a configuration file

The administrator can run the **c2racv** command to update Visual server definitions on the system.

Procedure

- On the target machine, run IBM Security zSecure Visual with the configuration filename as a command-line argument:

  `<full path>\c2racv<full path to configuration file>`
- The server definitions are updated according to the parameters found in the configuration file. After this update, the program exits directly.

Configuration limitations

The administrator uses these guidelines to create zSecure Visual configuration files.

Note these configuration limitations:

Storing initial passwords in configuration files
: For security reasons, initial passwords cannot be saved to configuration files.

Renaming a server on the target machine
: You cannot rename a system on the target machine, since the old name cannot be written to the configuration file.

Same version needed for creating and using configuration files
: IBM Security zSecure Visual can only read configuration files that were created using the same version. If the versions differ, no server definitions are copied.

Modifying an existing configuration file

The administrator uses this task to change a zSecure Visual configuration file.

About this task

You can modify an existing configuration file. See “Notes” on page 146 for guidelines on changing or using configuration files.

Procedure

To change an existing configuration file, follow these steps:

1. Switch to **Export** mode.
2. Delete all servers.
3. Import the configuration file to be edited.
4. Edit the data.
5. Save it with the same name.

Notes

The administrator uses these guidelines to create and change zSecure Visual configuration files.

Using a configuration file to copy a certificate
You can copy a certificate using a configuration file. When you prepare the configuration file, perform the copy as if it is on your system. The copying is performed on the target machine when it reads the configuration file. To copy a certificate that is not on the machine where you are making the configuration file, you can enter the server name and version directly.

Blank fields in configuration files
Server parameters that you leave blank are not stored in the configuration file. If a server with the same name exists on the target machine, blank fields are left unchanged.

Client IDs in configuration files
The target computers must have unique Client IDs. You cannot specify a Client ID in a configuration file that is used by multiple target computers. If you specify a dot in the Client ID field after 12.1, the target machine replaces the dot by the Client ID of its other server definitions. This only works if all its other server definitions contain the same Client ID.

Modifying an existing configuration file
See “Modifying an existing configuration file” on page 145 for the steps.

Configuration file sample tasks

The administrator can use these sample tasks to implement configuration files for zSecure Visual.

Procedure

1. Example 1: Prepare automated setup and configuration with one server for multiple clients
   a. Start IBM Security zSecure Visual.
   b. Select **File > Configure** from the main menu.
   c. Select **Export** and confirm you are going to prepare configuration files.
   d. Edit the server definitions using the **Add**, **Edit, and Delete** functions until you have only the server definition you want to configure on the target machines.

      Specify only **Name**, **HelpContact**, **Server IP address** or **name** and **Server Port**. Leave the **Client ID** field blank, because this field needs to be unique for each target machine. In this example, **Local Host** and **Local Port** are also left blank.
   e. Click **OK** and save the configuration file as `setup2.cfg`. Now the configuration file is finished.
   f. On each target machine run this command:

```
c2racv setup2.cfg
```

g. After completing these steps, specify the correct Client ID and Initial Password on the target machine.

2. Example 2: Add a new server to multiple clients
   a. Start IBM Security zSecure Visual.
   b. Select **File > Configure** from the main menu.
   c. Select **Export** and confirm you are going to prepare configuration files.
   d. Edit the server definitions using the **Add**, **Edit, and Delete** functions until you only have the server definition you want to configure on the target machines.

      Specify only **Name**, **HelpContact**, **Server IP address** or **name** and **Server Port**. Leave the **Client ID** field blank, because this field needs to be unique for each target machine. In this example, **Local Host** and **Local Port** are also left blank.
   e. Click **OK** and save the configuration file as `setup2.cfg`. Now the configuration file is finished.
   f. On each target machine run this command:

      ```
      c2racv setup2.cfg
      ```
   g. After completing these steps, specify the correct Initial Password on the target machine to obtain a certificate.

Silent installation

The administrator uses this information to plan a silent installation of zSecure Visual.

A *silent installation* is an installation that is performed without any user interaction.

For the silent installation to succeed, the initial machine and target machines must have similar configurations. Any deviation that can influence the setup procedure, such as the existence or nonexistence of the target folder to install, can cause the installation to fail.

Silent installation assumes that the accepted license agreement recorded from the initial installation applies to all target machines. Therefore, the silent installation copies the license files to the designated directory on the target systems and creates the status file without user interaction.

To help troubleshoot any silent installation problems, you must log the installation process. See “Log file for silent installation”

Log file for silent installation

The administrator can specify the log file location for a silent installation of zSecure Visual.

A log file is created for each silent installation. If you do not specify the location, the log file is created as `setup.log` in the folder that contains `setup.exe`.

To specify the log file location, use this option:

`-f2<`*`full path to log file`*`>`

For diagnostics, you can create a detailed log with this command-line option:

`/g<full path to detail log>`

The detailed log contains the steps of the installation process, including any error messages. This information must provide pointers to solve what went wrong during the installation.

Attention: Take care to avoid any filename conflicts with the setup log!

Examples of silent installation commands

To perform a silent installation, run the setup program with the appropriate command line options. This section provides some examples.

These examples use standard Microsoft command line parameters with the `InstallShield` setup command. Only the `CMDVISUAL` property is specific to the zSecure Visual client application.

Specify command-line options that require a parameter with no space between the option and its parameter. For example, this command is valid:

```
setup.exe /v"INSTALLDIR=c:\MyDirectory"
```

This command is not valid:

```
setup.exe /v "INSTALLDIR=c:\MyDirectory"
```

Put quotation marks around the parameters of an option only if the parameter contains spaces.

If a path in a parameter contains spaces, you might need to use quotation marks in quotation marks, as in this example:

```
setup.exe /v"INSTALLDIR=\"c:\My Directory\""
```

Silent installation with default settings

```
setup.exe /s /v"/qn"
```

Silent installation with a different target directory

```
setup.exe /s /v"/qn INSTALLDIR=<c:\target_directory>"
```

Silent installation with a different target directory and a configuration file

```
setup.exe /s /v"/qn CMDVISUAL=C:\temp\setup1.cfg INSTALLDIR=<c:\
target_directory>"
```

Silent installation with a different target directory and a log file

```
setup.exe /s /v"/l*v c:\test.log "INSTALLDIR=<c:\target_directory> /qb"
```

Silent installation with default settings and no reboot

```
setup.exe /s /v"/qn /norestart "
```

Automate upgrade path examples

The administrator uses these examples to automate the upgrading of zSecure Visual.

After an initial installation, IBM Security zSecure Visual needs some configuration before the user can log on to a server. For an upgrade, it can be automated with the `/COPYSERVERS` setup command-line option. Any server definition already defined on the system is replicated to the newly installed version, so they are ready for use immediately after installation.

Examples:

The following examples:

- Apply only to an interactive installation.
- Require you to specify the COPYSERVERS option in uppercase.
- Copies only the most recent server definitions.

  Note: If the machine contains more than one version of zSecure Visual, the server definitions of the most recent version are copied. Older versions are skipped.

Example 1:

```
setup.exe /s /v"/qn CMDVISUAL=/COPYSERVERS"
```

Example 2:

The following example specifies to uninstall the existing version of the Visual Client before installing the new version.

```
setup.exe /x /s /v"/qn CMDVISUAL=/COPYSERVERS"
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, Acrobat, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

CKG profile
A number of profiles in the XFACILIT class control access to the CKGRACF commands. The profile names start with "CKG." **Note:** If the Site Module general resource class name is customized during the server setup, as described in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*, the class with the specified name controls access to the CKGRACF commands, rather than the XFACILIT class.

Access authority
The authority a user needs to access a protected resource. The higher the authority, the more a user is ed to do.

Class All RACF entities, such as, users and resources, are categorized into classes. The Class Descriptor Table contains a description of all classes except USER, GROUP, and DATASET.

Class Descriptor Table
An assembled RACF table that contains entries for all general resource classes.

CKGRACF
Short mainframe program name for a utility that issues authority-sensitive RACF commands. Component of IBM Security zSecure.

CKRCARLA
Short mainframe program name for the IBM Security zSecure application.

Connect
A profile that connects a user to a group. Depending on the attributes of the connect, a user has different authorizations.

General Resource
Anything that RACF can protect except users, groups, and data sets. For example, by default the CKG profiles reside in the XFACILIT class, which is a general resource class.

Global Access Table (GAT)
A fast way to allow access to all users, except restricted users, to a list of resources. Most RACF authority processing is bypassed. The list is stored in the DATASET profile of the GLOBAL class.

HLQ High Level Qualifier or first qualifier. The left-most part of a data set name; the string of letters before the first period.

ID User ID or group name.

Member
Profile members are used to create a list of entries associated with a profile.

MVS A mainframe operating system.

OS/390
A mainframe operating system that includes MVS, among others. Renamed to z/OS.

Owner
Every profile has an owner. The user or group that owns the profile can view, change, and delete that profile.

Permit
ed access ability of a user or group to specified resources.

Profile
A description of the security-relevant characteristics of one or more users, groups, or resources. A profile is divided into segments.

Proftype
Profile type. For general resources, it can be discrete or generic. For data sets, it can be generic, nonvsam, vsam, tapedsn, or model.

RACF Resource Access Control Facility. A security program that provides access control on an MVS or a VM environment by user identification, access authorization, etc. Renamed to SecureWay Security Server.

Schedule
Schedules enable you to set and run timed commands, such as revoke intervals. For example, the administrator can define a future interval for the period that a user is on vacation. On the specified start date of the vacation, the user is revoked automatically. At the end

of the specified period, the user is resumed by the system.

Segment
Part of a profile that contains a specific part of the identification.

Setropts
A command to set system-wide z/OS options related to resource protection (Set RACF Options).

Setropts erase
RACF command.

Subgroup
A group becomes a subgroup of the group is has as a superior group.

Supgroup
Every group except SYS1 has one superior group. The hierarchy created this way plays an important role in the way access is granted.

Universal Access Authority (UACC)
Part of a data set or resource profile that defines the default access that is granted if a user or group is not granted explicit access (except restricted users, which have no access through UACC). Note that for sensitive resources, the UACC is usually set to NONE.

Userid
User ID, unique identification for a RACF user.

z/OS A mainframe operating system, containing MVS as a component. Formerly known as OS/390.

Index

Special characters

A

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Printed in USA

SC27-5647-00