iSecurity Screen

User Guide
Version 18.32

www.razlee.com

Contents

About this Manual 4
Chapter 1 Preface 8
Intended Audience 9
Conventions used in this Document 10
Chapter 2 Introduction to Screen 11
Key Features 12
Chapter 3 Starting Screen 13
Modifying Operators' Authorities 14
Activation Procedures 16
De-activate Monitor 17
Manual Activation 18
Auto Enable after Running a Command 19
Enabling Protection for Terminal Screens 20
Verify Monitor Subsystem 21
Working with Screen as a Standalone Product 22
Chapter 4 Additional Activation Features 23
Self-Lock 24
"One Touch" Self-Lock 25
Chapter 5 Controlling Screen Activation 26
Enabling and Disabling Protection Globally 27
Enabling Protection for Terminal Screens 28
Protect This Screen 29
Guard this Job When Needed 30
Guard all Jobs in Group 31
Chapter 6 Definitions 32
Working with Timeout Periods 33
Exceptions 35
Exception by User/Profile Groups 36
Exception by Terminal Screens 37

Forced Signoff Exceptions 38
Password 39
Individual User 39
Groups of Users 39
Password Subsystem 41
Chapter 7 Working with Reports/Queries 42
Chapter 8 System Configuration 43
Screen General Definitions 44
Translation 47
Chapter 9 Implementation 48
Adding the GRINIT Command in the Initial Program 49
Forcing GRINIT to Run for All Jobs 50

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The Screen User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Native IBM i (OS/400) User Interface

Screen is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on the previous page.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRAOD **> 81 > 32**

meaning: Syslog definitions activated by typing ***STRAOD***and selecting option: **81** then option: **32**.

Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. *To* select a menu option, simply type the option number and press **Enter**. The command line is

available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press F10 to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- F1: Help Display context-sensitive help
- F3: Exit End the current task and return to the screen or menu from which the task was initiated
- F4: Prompt Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- F6: Add New Create a new record or data item
- F8: Print Print the current report or data item
- F9: Retrieve Retrieve the previously-entered command
- F12: Cancel Return to the previous screen or menu without updating

Legal Notice

applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

Manual Revised: Monday, June 6, 2022

Contacts

Raz-Lee Security Inc. www.razlee.com
Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)
Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Chapter 1 Preface

The Screen software product is designed for terminal screen security by protecting unattended terminals, including PCs running terminal emulation software, from unauthorized use.

Intended Audience

This User Guide is intended for system administrators and security administrators responsible for the implementation and management of security on System i® systems. However, any user with a basic knowledge of System i® operations is able to make full use of this product after reading this User Guide.

Conventions used in this Document

- Menu options, field names, and function key names are written in **`Courier New Bold`**.
- Links (internal or external) are emphasized with underline and blue color as follows: page 3, Raz-Lee Website.
- References to chapters or sections are written in *Italic* and formatted as a link.
- Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.
- Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.
- Emphasis is written in **Bold**.
- Wherever applicable, Notes are provided within the text to draw attention to some critical issues. These looks like:

> **NOTE:** This icon points out useful information that does not affect the integrity of your system.

- Wherever applicable, Warnings are provided within the text to draw attention to some critical alarms. These looks like:

> **WARNING:** This icon alerts you to a situation that could cause a loss of data if a certain action is performed or avoided.

Chapter 2 Introduction to Screen

Screen is a terminal screen security product that protects unattended terminals, including PCs running terminal emulation software, from unauthorized use. Unattended terminals provide a tempting opportunity, even for honest employees, to “play” with programs and data that they are otherwise prevented from using. Such activity is often considered to be harmless, but in fact, can result in catastrophic damage to critical databases or theft of confidential information.

Unauthorized terminal abuse is very difficult to detect or prevent because the actual transaction source cannot be readily identified.

Screen protects unattended terminals by automatically locking them after a specified period of inactivity. Locked terminal screens are released when the user, his supervisor or the security officer enters a valid password. If a locked terminal is not released within a specified period that terminal session may be automatically ended. Time-out periods may be defined according to variable criteria such as date, time of day or user profile.

Screen provides centralized control over the locking of unattended terminal screens, time-out definition for individual terminals and release passwords. Protection may be individually enabled or disabled for specific users and terminals. Time-out periods can also be individually specified for specific users and terminals.

Screen enables a user to quickly lock his own screen in order to protect confidential data displays from prying eyes.

NOTE: This product works for Interactive jobs (*INT*).

Key Features

- Easy-to-use for non-technical system administrators.
- Centralized screen protection control.
- Adjustable time-outs based on user profile, terminal and time of day.
- Optional forced *SIGNOFF* if a terminal is not released within the designated time.
- Definable exceptions to forced *SIGNOFF* based on active program.
- Protects pass-through sessions – optional use of host or target system password.
- Centralized control over screen release passwords.
- Auto-Dim (screen saver) option for PCs running terminal emulation.
- “Self-Lock” manual locking for quick screen blanking.
- “One Touch” option locks terminal by pressing programmable hot key.
- IBM® Operations Navigator Plugin.

Chapter 3 Starting Screen

A system administrator with **SECADM* special authority must logon in order to globally control terminal screens or to configure the product. Any user may start Screen in order to enable or disable protection for his own terminal screen or to change his screen release password.

To start Screen, type *STRSCN* in the command line. The main menu appears as below.

Modifying Operators' Authorities

The Operators' authority management is now maintained in one place for the entire iSecurity on all its modules.

There are three default groups:

- **AUD#SECAD* – All users with both **AUDIT* and **SECADM* special authorities. By default, this group has full access (Read and Write) to all iSecurity components.
- **AUDIT* – All users with **AUDIT* special authority. By default, this group has only Read authority to Audit.
- **SECADM* – All users with **SECADM* special authority – By default, this group has only Read authority to Firewall.

By default, all three groups use the same password (*QSECOFR*).

You may add more operators, delete them, and give them authorities and passwords according to your own judgment. You even have the option to make the new operators' definitions apply to all your systems; therefore, upon import, they will work on every system.

NOTE: When upgrading for the first time to iSecurity, certain user(s) might not have access according to the new authority method. Therefore, the first step you need to take after upgrading is to edit those authorities.

To modify operator authorities, follow this procedure:

1. Select **89. Base Support** menu from the main menu. The **Base Support** screen appears.
2. Select **11. Work with Operators** from the **Maintenance Menu**. The **Work with Operators** screen appears.
3. Type **1** next to the user to modify it (or Press **F6** to add a new user). The **Modify Operator** screen appears.

Option	Description
Password	**Name** = Password **Same** = Same as previous password when edited **Blank** = No password
1 = *USE	**Read** authority only
9 = *FULL	**Read** and **Write** authority
3 = *QRY	Run **Queries**. For auditor use
5 = *DFN	

4. Set authorities and press **Enter**.

Activation Procedures

The **Start Monitor** loads the global parameters used to periodically scan the terminals and starts the monitoring process. Screen uses a subsystem called *ZGUARD* to continuously monitor terminal screens. When *ZGUARD* is active, all terminal screens are protected.

When using Screen for the first time, perform the following steps in to activate Screen monitoring.

1. Select **41. Activation** from the main screen. The **Activation** menu appears.
2. Select **11. Enable Screen** – **All Screens** from the **Activation** menu and specify the subsystem in which interactive jobs run. This is normally *QINTER* or *QBASE*. If more than one such subsystem is used, repeat this step for each interactive subsystem.
3. All terminal screens will be protected automatically immediately upon sign on.
4. Select **13. Activate at IPL** from the **Global Activation** menu. This step automatically activates Screen after each IPL.
5. Define timetable parameters as described in the Working with Timeout Periods section on page 32.
6. Select **21. Add** to add rules for auto-enable screen protection after running a command.
7. Select **1. Activate Screen** Now from the **Activation** menu. This final step ensures that every terminal screen that was already signed when Step 1 was performed is now protected.

De-activate Monitor

This option stops the *ZGUARD* Subsystem and ends the terminal monitoring by Screen.

NOTE: It is recommended to restart the system once a week (Enable and Disable Screen). This action causes a temporary pause in the activity of the control system. By performing this action, the system is reactivated using the current settings of the System Global Parameters. This is essential if there have been changes made to the parameter file that determine the mode of operation of the control system.

To stop Screen monitoring, perform the following steps.

1. Select **41. Activation** from the main screen. The **Activation** screen appears.
2. Select **12. Disable Screen – All Screens** from the **Activation** menu and specify the subsystem in which interactive jobs run. If more than one such subsystem is used, repeat this step for each interactive subsystem.
3. All terminal screens protection will be disabled.
4. Select **14. Do Not Activate at IPL** from the **Global Activation** menu.
5. Select **22. Remove** to remove rules for auto-enable screen protection after running a command.
6. Select **2. De-activate Screen Now** from the **Activation** menu.

Manual Activation

You can configure the monitor subsystem to start automatically on IPL, or you can manually start and stop it.

- To automatically start the monitor subsystem, select **13. Activate at IPL**.
- To prevent the monitor subsystem from automatically starting, select **14. Do Not Activate at IPL.**
- To manually start the monitor subsystem, select **1. Activate Screen Now**.
- To manually stop the monitor subsystem, select **2. De-activate Screen Now**.

Auto Enable after Running a Command

You can also configure the monitor subsystem to start automatically after a specific command was executed. Use the following options from the Activation menu:

- To start the monitor subsystem, select 21. Add. Type a name and the command that will execute the screen protection.
- To stop the monitor subsystem from automatically starting, select 22. Remove. Type the command name to remove from the automatic screen protection.
- To manually start the monitor subsystem, select 1. Activate Screen Now.
- To manually stop the monitor subsystem, select 2. De-activate Screen Now.

Enabling Protection for Terminal Screens

Users can enable or disable protection for their own terminal screen. This is normally done for test purposes only.

- To manually enable protection for your own terminal screen, select **1. Protect this Screen** from the main menu.
- To disable protection for your own terminal screen, select **2. Do Not Protect this Screen** from the main menu.

The system administrator can globally enable and disable protection for all terminal screens. To globally enable all terminal screens, perform the following procedure:

1. Select **41. Activation** from the main menu.
2. Select **11. Enable Screen – All Screens** from the **Global Activation** menu.
3. Select **1. Activate Screen Now** from the **Activation** menu. This final step ensures that every terminal screen that was already signed when Step 1 was performed is now protected.

Verify Monitor Subsystem

This function allows you to verify whether the ***ZGUARD*** is currently active.

1. Select **41. Activation** from the main menu.
2. Select **5. Work with Active Monitor Jobs**. If the ***ZGUARD*** subsystem is active, the **Work with Subsystem Jobs** screen appears and displays the ***ZGUARD*** subsystem and its status. If the ***ZGUARD*** subsystem is not active, the message "*Subsystem ZGUARD not active*" appears at the bottom of the **Help** menu.

Option	Description
2=Change	Runs the Change Job (***CHGJOB***) command. If no value is specified on the Parameters input field, default parameters are shown when you press the **F4** (prompt) key.
3=Hold	Hold the job. The job's spooled files are not held unless the default for the Hold spooled files (***SPLFILE***) parameter is overridden using the Parameter's input field.
4=End	Runs the End Job (***ENDJOB***) command.
5=Work with	Runs the Work with Job (***WRKJOB***) command, which displays the Work with Job Menu.
6=Release	Runs the Release Job (RLSJOB) command, which releases the job if it is in the held condition. The Release Reader (***RLSRDR***) or Release Writer (***RLSWTR***) command (with ***OPTION(*CURRENT)***) is run if this option is selected for a spooling reader or spooling writer job. 'Rls' is placed in the status field if the command runs successfully.
7=Display message	Displays the message for which the job is waiting.
8=Work with spooled files	Runs the Work with Job (***WRKJOB***) command, which displays the jobs' spooled output files.
13=Disconnect	Use this option to run the Disconnect Job (***DSCJOB***) command. All jobs at the device will be disconnected.

3. Enter your desired options.

This option is for verification purposes only. You should never attempt to modify the subsystem or its associated jobs using this screen.

Working with Screen as a Standalone Product

If you are working with Screen as a standalone product, you should remove the Firewall auto-start job entry. This should be done immediately after the initial installation and after every version upgrade.

On the command line, enter the following command:

RMVAJE SBSD(QSYS/QSYSWRK) JOB(GS#FIREWAL)

Chapter 4 Additional Activation Features

Self-Lock

Very often a terminal user will need to leave the workstation for a short while, and it is inefficient and time-consuming to ask the user to sign off and on for each occasion.

The Self-Lock feature of Screen provides an easy yet comprehensive method for locking the user terminal. When locking the terminal, the user can specify the maximum duration he expects to be away from his machine. Should he be absent longer, the terminal's job automatically ends.

To use the Self-Lock feature, follow these procedures.

1. Select 3. Self-Lock from the Screen main menu (alternately, type *GRLOCK* in the command line). The *GRLOCK* screen appears.
2. Enter the timeout period in minutes or keep the default setting of **NOMAX*.
3. Press Enter to confirm you selection.

Your terminal is now locked. To end the lock state, and restore the original display, enter the password you used to log onto the system.

“One Touch” Self-Lock

Users can lock their terminals by pressing a single key regardless of the application that is running at that time. This function is enabled via the use of the Record/Play keyboard functions, or hot-key macros. Using these macros, it is possible to record a sequence of keystrokes and play them back whenever the play function is used. As the exact method to record and play changes between the various terminal types, you should look in your terminal manual to find the exact way of implementation.

The key sequence to be recorded is *[SYS.REQ] 5 999 SMZTMPA/GRSLFL [ENTER]*

The 999 states that the maximum delay are unlimited; the 999 can be replaced with any number (3 digits) to represent the maximum wait time (in minutes) for a release attempt, before job terminates.

To use the “One Touch” Self-Lock feature, follow these procedures.

1. Select 4. Set “One Touch” Self-Lock from the main menu.
2. Follow the instructions displayed on the screen to record the macro.

Chapter 5 Controlling Screen Activation

Enabling and Disabling Protection Globally

The system administrator can globally enable and disable protection for all terminal screens. To globally enable all terminal screens, perform the following steps in order:

1. Select **41. Activation** from the Screen main menu. The **Activation** menu appears.
2. Select **11. Enable Screen – All Screens** from the **Activation** menu. The **Wide/Guard Initiation-Default (*GRINITDFT*)** screen appears.
3. Select **1. Activate Screen Now** from the **Activation** menu. This second step ensures that every terminal screen that was already signed when Step 1 was performed is now protected.

To globally disable protection for all terminal screens:

1. Select **12. Disable Screen – All Screens** from the **Activation** menu. The **Wide/Guard Initiation-Default (*GRINITDFT*)** screen appears.
2. Select **1. De-activate Screen Now** from the **Activation** menu.

Enabling Protection for Terminal Screens

Users can enable or disable protection for their own terminal screen. This is normally done for test purposes only.

- To manually enable protection for your own terminal screen, select **1. Protect this Screen** from the main menu.
- To disable protection for your own terminal screen, select **2. Do Not Protect this Screen** from the main menu.

The system administrator can globally enable and disable protection for all terminal screens. To globally enable all terminal screens, perform the following procedure:

1. Select **41. Activation** from the main menu.
2. Select **11. Enable Screen – All Screens** from the **Global Activation** menu.
3. Select **1. Activate Screen Now** from the **Activation** menu. This final step ensures that every terminal screen that was already signed when Step 1 was performed is now protected.

Protect This Screen

Selecting this option will initialize the ***GRINIT*** program for this terminal only. Monitoring will be active for this terminal.

1. To use the **Protect this Screen** option, select **1. Protect this Screen** from the Screen main menu. The **iSecurity Initiation** screen appears.
2. Choose the correct parameters.

Guard this Job When Needed

Option	Description
*YES	Guard this job.
*NO	Do not guard this job.
*Same	Same as before.

Guard all Jobs in Group

Group Jobs are groups of up to 16 jobs sharing a single screen. Only one job out of them is active at a time.

JOBS information is available from the **OS/400®** yet, we need to protect a single screen.

To **enable** this operation, the job must be a **Group Job** at the time ***GRINIT*** is entered.

Option	Description
*YES	Protect this screen as if it is a **Group Job**. If the job running is not a **Group Job**, it is converted into a **Group Job**, and protected as such.
*IFACTIVE	If the job running on this screen is a **Group Job**, the screen will be protected as a **Group Job**.
*NO	Regardless if the job running on this screen is a **Group Job** or not, the screen will be protected as if it was a regular job – the active job running at the time that this command is entered.

To **disable** the ***GRINIT*** command from the terminal and stop monitoring, select **2. Do Not Protect This Screen** and select parameters.

Chapter 6 Definitions

This section deals with defining your terminal security. The topics that are addressed are:

- Time Table
- Exceptions
- *ENDJOB* exceptions
- Password

Screen protection is based on global timeout periods, which may then be customized for individual terminal screens, users and specific jobs running in a terminal session. Protection may be disabled for individual screens and users.

To work with terminal screen protection parameters, select 21. Time-Out Definitions from the Screen main menu. The Definitions menu appears.

Working with Timeout Periods

Screen uses a calendar to assign global timeout periods for specific dates. These global timeout periods are for screen locking and password entry.

Since the demands on the security system change according to the type of day (work day, weekend, half day, vacation day, and so on) and according to the time of day (during working hours, after work hours, night hours), you may define different timeout periods based on these parameters.

The system contains an annual diary in which the days can be characterized. Each type of day is defined by one character chosen by the user. This character needs to be entered in the appropriate position in the internal calendar (press **F14** to update this) and in the timetable, by type of day and hour. The hour that is entered is the beginning of the period.

Appropriate characteristics can be defined for each type of day and each time.

The way the security system operates is defined by two main parameters:

- The maximum time a workstation can remain inactive before the security system starts protecting it.
- The maximum time the security system will wait for a password to be entered. After this time has elapsed the security system will terminate the activity of this workstation. A special value 999 will render this option inoperative.

To define global timeout periods, follow these procedures.

1. Select **1. Define Timeout Periods** from the **Definitions** menu. The **Timeout Definitions** screen appears.
2. Define day types in the lower section of the screen as follows:

Option	Description
Day type	1 character code representing the day type (weekday, weekend, holiday, and so on)
Hour – Hour	24 hour clock at which these timeout periods take effect
Lock Timeout	Idle time (in minutes) before screen is locked
Password Timeout	Time allowed (in minutes) to enter password before forced signoff

3. Press **F14** to move the cursor to the calendar in the upper section of the screen.

4. Enter the year in the appropriate field.
5. Enter a day type code for each date in the year. The global timeout periods corresponding to the indicated day type will apply for each date. If no day type is entered for a given date, the ***DEFAULT** day type is automatically applied.

Exceptions

You can customize timeout periods, or disable protection entirely, for individual users, profile groups and individual terminal screens by creating exceptions to the global timeout periods.

The exception tables allow one to change the times that have been defined or to change the way the system should operate in special cases where the general parameters are not suitable.

Exception by User/Profile Groups

At this level of exceptions, one can enter a User name or Group profile and by using the multiplication parameter the reaction time of the system can be increased or decreased for specific Users or Groups. For instance, it is natural that the *QSECOFR* should be protected more than other users, so a multiplication factor of 0.5 could be entered so that the time lapse will be half the default time before that terminal is locked.

Exception by Terminal Screens

At this level we can define exceptions by the name of the Terminal (Workstation). For example, terminals located in areas with many workers may need more protection than others. At the extreme, the room where the computer is situated may be protected against break-in. For terminals located there, we can enter a multiplication factor of 3.0. This means that it will take three times longer than the default time until the security system takes control of the workstation.

To define global timeout period exceptions:

1. Select **11. For Users** or **12. For Screens** from the **Definitions** menu. An **Exception** screen appears. The screens are similar for both user and screen exception types.
2. Enter exception parameters as follows:

Parameter	Description
User Profile	User profile or profile group (User exceptions only)
Screen	IBM i® (OS/400®) terminal name (Screen exceptions only)
Lock Time Factor	Screen locking timeout multiplier (See note below)
Pwd Time Factor	Screen release timeout multiplier (See note below)
Protect Active	Protection enabled for this screen or user **Y** = Enable **Blank** = Disable
Auto Dim	Enable screen saver **Y** = Enable – Screen exceptions only

NOTE: Timeout factors are expressed as multipliers to the global timeout setting value. For example, if the global timeout setting value is 15 minutes and the exception value is 4, the exception timeout will occur after 60 (15 x 4) minutes. Likewise, if the global timeout setting is 15 minutes and the exception value is 0 .5, the exception timeout will occur after 7½ (15 x 0.5) minutes.

Forced Signoff Exceptions

If not released within a specified period of time, a locked terminal's session is automatically terminated. Exceptions may be created to prevent jobs running on a locked terminal from automatically terminating in this manner. Forced signoff exception definitions apply to jobs running on all terminals.

An exception may cause one of the following actions to occur for the specified job:

- Place the job on HOLD without terminating it
- Run a user specified program prior to the forced signoff

To define a forced signoff exception:

1. Select **21. For Active Programs** from the **Security Definitions** menu. The **Forced Signoff Exceptions for Active Programs** screen appears (see above).
2. Enter the program name in the first field or enter ***ALWAYS** to apply the exception to all running jobs.
3. Enter ***NEVER-END** in the second field to place the job on **HOLD** or enter the name of the program to run before the job terminates. If the second field is left blank, the job will terminate.

Password

The system administrator can define screen passwords for individual users from any terminal. Each user is assigned an individual password, and a second password may be assigned for use by the users' supervisor. Either password is accepted to release a locked terminal screen.

Individual User

To set a password for an individual user, perform the following procedures:

1. Select **31.Individual User** from the **Definitions** menu (this is the equivalent to running the command *GRCHGPWD*). The **Change Screen Special Password** screen appears.
2. Enter your information in the fields on the screen.

Parameter or Option	Description
Password to release screen	Specify the internal password assigned to the terminal user.
User profile name or *	Specify a user profile or name that the password will be associated to. The default (*) is set as the current user.
Manager	Specify the name of an existing user profile, which has permission to release a locked terminal of a user using the internal password of the product. ***SAME** – The group user profile does not change ***NONE** – No user or group user profile is associated with this user profile.

Groups of Users

To set a password for multiple users, perform the following procedures:

1. Selecting option **32. Multiple Users** from the **Definitions** menu. The **Work with Multiple Passwords** screen appears.
2. Enter the correct field in **User**.

Option	Description
Name	Specify a user name
*generic	Display user by generic name. (For example, D* will display all users whose name starts with a '*D*'.)
*ALL:	This option is allowed only for the ***QSECOFR*** or to member of his user group. Selecting ****ALL*** (the default) will enable all the users of the system to be shown together with their description, their group user and the date of the last password change. The user's password is not displayed.

NOTE: If "Manager" is changed, the password must be reentered. To remove a manager, enter *****NONE.

Password Subsystem

The password system contains a complete set of passwords. The user can update this set of passwords according to the security policy in the user's unit. The password can be equivalent (or different) to those in the operating system. The passwords are encrypted by a method that does not allow retrieval.

Apart from the password, you can also define for each user the name of another user that can release him from security system locks. As this is usually the head of the group, we will refer to this user as the "Manager".

Chapter 7 Working with Reports/Queries

The system collects activity information in a log file. The information includes all *LOCKS*, *RELEASES*, *JOB-END/HELD AFTER LOCKS*. For each entry, the time stamp and the results are attached. A reporting system enables the user to produce reports about Screen activity.

The available report types can be run in batch or interactive mode. Interactive reports are under the 'Display Log' heading, whereas batch reports are under the 'Print Log' heading. The output is sent to *SMZTMPA/WSPRINT*.

To work with reports and queries, select **31. Display Log** from the main menu. The **Display Screen Activity Log** menu appears.

Menu Option	Description
All Entries	This report contains both Enforced Locks as well as Job-Ends.
Locks Enforced by Monitor	This report contains only Enforced Locks.
Job-Ends after Locks	This report contains only Job-Ends.

Select one of the options and the **Display SCREEN Log (*DSPSCLOG*)** screen appears:

Parameter	Description
*LOCKS	Screen locks made by the terminal
*EOJ	End job after lock
*ALL	All reports, dates, or users (depending on where this parameter is placed)
Name	User/terminal name
Generic	Display user/terminal by generic name. (For example, D* will display all users whose name starts with a '*D*'.)

Chapter 8 System Configuration

This option enables you to determine the different modes that the system can operate in, for example, the amount of time between successive checks, or the number of attempts a user is allowed to correctly enter a password.

To set configuration for all the iSecurity Suite products, select **81. System Configuration** from the Screen main menu.

Screen General Definitions

To configure Screen, select **21.Screen** from the **Global Parameters** menu. The **Screen General Definitions** screen appears.

Parameter or Option	Description
Automatic Dim Screen	**Yes** =Activate this feature **No** = Do not activate this feature If the same information is displayed on a screen for a long period of time, the characters become fixed on the screen and are visible even when the screen is not operated. The data will appear as a dark shadow even when something else is displayed on the screen. Therefore, the auto dimming option is important for workstations that do not have auto dim, such as PCs and older workstations. Workstations with auto dim, but do not use this option can also benefit from it.
Number of minutes between checks	Setting this option will define how many minutes will pass between successive checks. The default value is 3.
Maximum Password retries	Enter the number of retries allowed before the terminal is locked. **0** = The number will be taken automatically from the system value (***QMAXSIGN***) that defines the number of trials for entering the operating system password. **99** =Unlimited number of trials ***(*NOMAX***) In screen lock mode, the one before last invalid sign-on attempt issues the following message: Next not valid sign-on ends the job iSecurity Screen issues the message according to value of ***QMAXSIGN*** and the value of this field.
*NEVER-END limit in hours	**1-9**, **N= No limit** The setting of this parameter is used when defining Signoff exceptions for active programs. See Forced Signoff Exceptions section on page 38.
Check Pass-Through previous pwd.	Pass-Through terminals (Home to Target) are protected by Screen on the Target system. The following choices are available for this setting. **Y=Yes** – The lock state can be ended if the entered password corresponds to the ***SIGNON*** Home System. **N=No** – The lock state can be ended if the entered password corresponds to the ***SIGNON*** Target System **B=both systems** – The lock state can be ended if the entered password corresponds to either the ***SIGNON*** Target System or the ***SIGNON*** Home System.
End job	Select the way you wish to extend the control of terminating a job. **1=ENDJOB** – End all active jobs (this is the default) **2=VARY OFF** – End all jobs then vary off terminal

Parameter or Option	Description
	3=JLDJOB – Hold the active job. **6=SIGNOFF ENDCNN(*NO)** – Sign off and end the connection **7=SIGNOFF ENDCNN(*YES)** – Sign off without ending the connection
Inform about screens in which GRINIT has not been entered.	**M**=Send informative message **N**=No
Internal Password Validation pgm and Library	There are two passwords in Screen – entered by the user and entered from the product. If the user internal security program is enabled, it will replace the user password by its own password (10 characters) and the screen password by a system password called *GSPASSWORD*. If the contents of *GSPASSWORD* are identical to the screen password, the user internal security program is run; otherwise an error will occur before the end of the run. ***NONE***: No user internal security **Name:** The name of the security program ***LIBL (Library)**: Enter the library name
Schedule type	Define how you will set up your schedule **1**=Yearly **2**=Weekly

Translation

All screen sections that the user sees can be translated. To translate a screen, select F13 Customize Messages from the System Configuration menu. An example follows:

All visible “constants” and messages are displayed. Overwrite them with your text, clear the field and press Enter.

To translate the help text, follow these steps:

1. Create a new member in the *GRSOURCE* file in library *SMZ8*.
2. Copy the original help text to it.
3. To translate as required without altering the control records identified by *.PGM*, *.FMT*, and so on, select *F13* from the Screen General Definition menu and enter the name of the new member at the bottom of the translation panel.

Chapter 9 Implementation

In order for a terminal to be monitored by the product, the command GRINIT must be run from that terminal.

Performing one of the following to do this:

- Add the *GRINIT* command to the initial program of the users that you want to protect.
- Force *GRINIT* to run for all jobs (no change in any program).

Each time a terminal needs to be protected, and *GRINIT* has not been run, a message is sent to the *QSYSOPR*.

If you want to separate these messages, create a message queue named *SCREEN* in library *QGPL*, and the messages will be directed to it automatically.

Adding the GRINIT Command in the Initial Program

In the initial program of the users that you want to monitor, add the following commands:

- *GRINIT*
- *MONMSG CPF0000*

These commands should be added so that they will be executed before any screen is displayed.

Forcing GRINIT to Run for All Jobs

When an interactive program terminal signs on, a specific "routing entry" is selected from an interactive sub-system to execute it.

The routing entry specifies which program will have control. That program is almost always *QCMD* from *QSYS*. The following procedure will change the program name to another program that will initiate *GRINIT* and only then will it call *QCMD* from *QSYS*.

To ensure the insertion of *GRINIT* for all users, without having to add the GRINIT in all initial programs, the following procedure (designed to prevent possible problems) should be followed, even if the product is no longer installed on the system.

The source of program is included in file *GRSOURCE*, library *SMZ8* member *GR#44QCMD*.

The procedure is as follows.

1. Duplicate the *GR#QCMD* program into *QGPL -CRTDUPOBJ GR#QCMD SMZ8 *PGM QGPL*.
2. Transfer your job to the controlling subsystem – *TFRJOB QCTL.*
3. Ensure no user is using sub-system *QINTER* – *DSPSBS QINTER.*
4. Terminate the sub-system – *ENDSBS QINTER*
5. Print the *QINTER* sub-system description – *DSPSBSD QINTER OUTPUT(*PRINT)*
6. Look at the note on "routing entries" in the "what is happening" section of the previous page.
7. Repeat the following for each line that contains program *QCMD* library *QSYS* as the program to get control – *QCMID* library *QSYS* as the program to get control – *CHGRTGE SBSD(QINTER) SEQNBR(number) PGM(QGPL/GR#44QCMD)*.
8. Start sub-system *QINTER – STRSBS QINTER*.
9. Repeat this procedure for all other interactive subsystems.

Parameter or Option	Description
Opt	1 = Select this rule for modification 3 = Copy this rule for another user 4 = Delete this rule
F6	Add new rule
F8	Print rules