



# iSecurity Installation and Base Support

## User Guide

[www.razlee.com](http://www.razlee.com)

# Contents

---

Contents .....	2
About this Manual .....	6
Intended Audience .....	6
Native IBM i (OS/400) User Interface .....	7
Conventions Used in the Document .....	7
Menus .....	8
Data Entry Screens .....	8
Legal Notice .....	9
Contacts .....	9
Installing and Upgrading iSecurity Products .....	9
Installing Products on IASP .....	11
Installing and Upgrading iSecurity/Audit, Action, Compliance, Native Object Security and Replication .....	15
Deactivation of the Product .....	18
Installing from a Link .....	18
Recovering from a Failed Installation .....	20
Running the Procedure Again .....	20
Installing and Upgrading iSecurity/AP-Journal and Safe Update .....	25
iSecurity/*BASE .....	26
Deactivation of the Product .....	28
Installing from a Link .....	28
Recovering from a Failed Installation .....	30
Running the Procedure Again .....	30
Installing and Upgrading iSecurity/Firewall, Screen, Password and Command .....	34
iSecurity/*BASE .....	35
Disabling Super Speed before Upgrading .....	37
Working with Object Locks .....	37
Deactivation of the Product .....	38
Installing from a Link .....	38
Recovering from a Failed Installation .....	39
Running the Procedure Again .....	39

---

Installing and Upgrading iSecurity/Authority on Demand (AOD), Multi-Factor Authentication (MFA) and Password Reset .....	44
iSecurity/*BASE .....	45
Deactivation of the Product .....	47
Installing from a Link .....	47
Recovering from a Failed Installation .....	49
Running the Procedure Again .....	49
Installing and Upgrading iSecurity/Advanced Threat Protection (ATP), Antivirus, Anti-Ransomware and Object Integrity Control .....	54
iSecurity/*BASE .....	55
Deactivation of the Product .....	57
Installing from a Link .....	57
Recovering from a Failed Installation .....	59
Running the Procedure Again .....	59
Installing and Upgrading iSecurity/Capture .....	66
iSecurity/*BASE .....	67
Deactivation of the Product .....	69
Recovering from a Failed Installation .....	71
Running the Procedure Again .....	71
Authorization codes .....	72
Installing and Upgrading iSecurity/Change Tracker .....	75
Deactivation of the Product .....	79
Installing from a Link .....	79
Recovering from a Failed Installation .....	81
Running the Procedure Again .....	81
Installing and Upgrading iSecurity/Field Encryption and PGP Encryption .....	86
iSecurity/*BASE .....	87
Deactivation of the Product .....	89
Installing from a Link .....	89
Running the Procedure Again .....	91
Installing and Upgrading iSecurity/DB-Gate .....	96
iSecurity/*BASE .....	97

---

---

Preparation .....	97
Deactivation of the Product .....	98
Installing from a Link .....	98
Recovering from a Failed Installation .....	100
Running the Procedure Again .....	100
Installing and Upgrading iSecurity/FileScope Premium and FileScope Tools .....	105
iSecurity/*BASE .....	106
Deactivation of the Product .....	108
Installing from a Link .....	108
Recovering from a Failed Installation .....	109
Running the Procedure Again .....	110
Installing and Upgrading iSecurity/CodeScope .....	115
iSecurity/*BASE .....	116
Preparation .....	116
Deactivation of the Product .....	117
Installing from a Link .....	117
Recovering from a Failed Installation .....	118
Running the Procedure Again .....	119
Activating the product .....	121
Installing and Upgrading iSecurity/WideScope .....	123
iSecurity/*BASE .....	124
Deactivation of the Product .....	126
Installing from a Link .....	126
Recovering from a Failed Installation .....	127
Running the Procedure Again .....	128
BASE Support .....	132
Email .....	133
Email Address Book .....	133
Working with Operators' Authorities .....	137
Working with Collected Data .....	145
Purging all AUDIT data .....	146
Setting up the *PRINT1-*PRINT9 Printers and *PDF Output ..	147
*PDF Setup .....	149
Network Support .....	151

---

---

Work with network definitions .....	151
Displaying Communication Logs .....	160
Global Installation Defaults .....	161
Installation .....	162
Run Time Attributes .....	164
Output and Logo .....	165
Placing Your Organization's Logo on Reports .....	166
Syslog (SIEM) Support .....	166
Product Behavior .....	167
E-Mail Definitions and Java Path .....	169
Character Set for Person Names .....	170
Post Installation Changes .....	171
iSecurity Environmental Change Considerations .....	171
System values .....	172
iSecurity User Profile Settings .....	179

## 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 Installation and Base Support 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

Installation and Base Support 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

***STRxx > 81 > 32***

meaning: Syslog definitions activated by typing ***STRxx*** 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

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all 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.

2023 © Copyright Raz-Lee Security Inc. All rights reserved.

Manual Revised: Monday, May 22, 2023

## Contacts

Raz-Lee Security Inc. [www.razlee.com](http://www.razlee.com)

Marketing: [marketing@razlee.com](mailto:marketing@razlee.com) 1-888-RAZLEE-4 (1-888-7295334)

Support: [support@razlee.com](mailto:support@razlee.com) 1-888-RAZLEE-2 (1-888-7295332)

## Installing and Upgrading iSecurity Products

To install iSecurity products, select the library that contains the product. Some also require other products as prerequisites, as shown in their

documentation.

Products that are packaged within a single library are installed together.

- "Installing and Upgrading iSecurity/Audit, Action, Compliance, Native Object Security and Replication" on page 15
- "Installing and Upgrading iSecurity/AP-Journal and Safe Update" on page 25
- "Installing and Upgrading iSecurity/Firewall, Screen, Password and Command" on page 34
- "Installing and Upgrading iSecurity/Authority on Demand (AOD), Multi-Factor Authentication (MFA) and Password Reset" on page 44
- "Installing and Upgrading iSecurity/Advanced Threat Protection (ATP), Antivirus, Anti-Ransomware and Object Integrity Control" on page 54
- "Installing and Upgrading iSecurity/Capture" on page 66
- "Installing and Upgrading iSecurity/Change Tracker" on page 75
- "Installing and Upgrading iSecurity/Field Encryption and PGP Encryption" on page 86
- "Installing and Upgrading iSecurity/DB-Gate" on page 96
- "Installing and Upgrading iSecurity/FileScope Premium and FileScope Tools" on page 105
- "Installing and Upgrading iSecurity/CodeScope" on page 115
- "Installing and Upgrading iSecurity/WideScope" on page 123

## Installing Products on IASP

Several iSecurity products support aspects of Independent Auxiliary Storage Pools (IASPs).

The IASP can be varied on to more than one system, especially with the use of PowerHA. This makes the systems easy to use. Consumers can be confident that their systems will survive.

Raz-Lee had always tried to provide the simplest possible installation and upgrade.

Currently, iSecurity products **SMZO** (including Authority on Demand and Password Reset) and **SMZJ** (containing AP-Journal) can be installed either on IASP or on \*SYSBAS, but not on both.

Due to OS400 restrictions, other iSecurity products can only be installed on \*SYSBAS.

OS400 also requires that object types \*JOBQ, \*JOB, \*CLS and \*SBSD cannot be installed on IASP. These objects and some \*DTAARA objects connected to the products, shown in the following table, must be kept in \*SYSBAS. They are now installed in the SMZTMPC library. If you migrate an existing installation of SMZO or SMZJ to IASP, these objects will be moved automatically.

Object	Type	Text
ZAUTH	*JOBQ	Authority on Demand job queue
ZJOURNAL	*JOBQ	Journal job queue
JOBDSMZO	*JOBQ	AOD &P-R Default
JR#MNT	*JOBQ	
JR#STRRTJR	*JOBQ	Journal Auto activation of Real Time
JRSYSLOG	*JOBQ	Journal-Syslog by TCP server
OD#MNT	*JOBQ	
OD#STRRTOD	*JOBQ	Authority on Demand Auto activation
ODSYSLOG	*JOBQ	OD-Syslog by TCP server
PRURMTSND	*JOBQ	Send response by DtaQ
ZAUTH	*JOBQ	Authority on Demand Monitor
ZCTLU	*JOBQ	Authority on Demand *CTL point update
ZPRESET	*JOBQ	Password Reset Monitor
ZAUTH	*CLS	Authority on Demand monitor class
ZJOURNAL	*CLS	Journal monitor class
ZAUTH	*SBSD	Authority on Demand subsystem
ZJOURNAL	*SBSD	Journal subsystem
SMZJ	*DTAARA	IASP definitions to Install SMZJ in
SMZO	*DTAARA	IASP definitions to Install SMZO in

## Installing and Upgrading Products on IASP

To install or relocate a product to IASP follow these steps:

1. Ensure that the library SMZTMPC exists. The library must be on \*SYSBAS.

If it does not exist, create it with the commands:

```
CRTLIB LIB(SMZTMPC) TYPE(*TEST) TEXT('iSecurity Generic data library')  
AUT(*USE) CRTAUT(*USE) ASP(1)
```

```
CHGOBJOWN OBJ(SMZTMPC) OBJTYPE(*LIB) NEWOWN(QSECOFR)
```

2. Add information to specify the IASP you wish to use for the product:

If the \*DTAARA does not yet exist, use the command:

```
CRTDTAARA DTAARA(SMZTMPC/-prdlb-) TYPE(*CHAR) LEN(2000) VALUE  
( 'ASPDEV ASPGRP ' )
```

If it exists, use the command:

```
CHGDTAARA DTAARA(SMZTMPC/-prdlb- (1 20)) VALUE('ASPDEV  
ASPGRP ' )
```

The value entered is ASPDEV followed by ASPGRP. Each one occupies exactly ten positions.

The following shows how it may look:

```
Display Data Area                                     System:  RLDEV  
  
Data area . . . . . : SMZO  
Library . . . . . : SMZTMPC  
Type . . . . . : *CHAR  
Length . . . . . : 2000  
Text . . . . . :  
  
Value  
Offset *...+...1...+...2...+...3...+...4...+...5  
  0      ' IASP33   IASP33      '  
  50     '                                     '  
 100     '                                     '  
 150     '                                     '  
 200     '                                     '  
 250     '                                     '  
 300     '                                     '  
 350     '                                     '  
 400     '                                     '  
  
More...  
Press Enter to continue.  
  
F3=Exit  F12=Cancel
```

3. If this is a first time installation, proceed with the normal installation.

If this is an upgrade:

- a. Take a backup of the SMZx and SMZxDTA (where x stands for the product letter)
- b. Delete these libraries from the ASP
- c. Restore both libraries to the IASP
- d. Then run the installation.

## Installing and Upgrading iSecurity/Audit, Action, Compliance, Native Object Security and Replication

Installing the SMZ4 library installs iSecurity Audit, Action, Compliance, Native Object Security and Replication. For simplicity, this document refers to the product as Audit.

## Pre-Requisites

- Operating system 7.1 or higher
- 300MB of disk space for initial installation



## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether Audit has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZ4/AUREL
```

If Audit has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZ4 \*LIB**
2. **WRKOBJLCK SMZ4DTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZ4) TYPE(\*DSPF)**

These commands should display any locks that affect Audit.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZ4 and SMZ4DTA libraries.

## Deactivation of the Product

Audit will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing Audit is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL RZLnnnn/AUI ('*SAVF' 'AU' "RZLnnnn' 'SMZ4')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITY2P is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within Audit are run, so users who do not have these authorities can run Audit properly.

**NOTE:** If you use Multi-System in a Multi-LPAR environment, setting up Audit creates a password for the user profile. It is not intended to be used to sign on.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/AUI ('*SAVE' 'AU' 'RZLnnnn'  
'SMZ4')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZ4/AUREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

Enter the **STRAUD** command on the IBM i. Select option **81. System Configuration**. Press the **F22 (Shift-F10)** key. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified. Press **Enter** several times to return to the Audit main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.



## Installing and Upgrading iSecurity/AP-Journal and Safe Update

Installing the SMZJ library installs iSecurity AP-Journal and Safe Update. For simplicity, this document refers to the product as AP-Journal.

## Pre-Requisites

- Operating system 7.1 or higher
- 70MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether AP-Journal has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZJ/JRREL
```

If AP-Journal has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information.

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZJ \*LIB**
2. **WRKOBJLCK SMZJDTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZJ) TYPE(\*DSPF)**

These commands should display any locks that affect AP-Journal.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZJ and SMZJDTA libraries.

## Deactivation of the Product

AP-Journal will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing AP-Journal is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn

you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnnnn/JRI ('*SAVF' 'JR' "RZLnnnn'  
      'SMZJ')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITY4P is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within AP-Journal are run, so users who do not have these authorities can run AP-Journal properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL RZLnnnn/JRI ('*SAVE' 'JR' 'RZLnnnn'  
'SMZJ')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZJ/JRREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRJR** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the AP-Journal main menu.



## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Installing and Upgrading iSecurity/Firewall, Screen, Password and Command

Installing the SMZ8 library installs iSecurity Firewall, Screen, Password and Command. For simplicity, this document refers to the product as Firewall.

## Pre-Requisites

- Operating system 7.1 or higher
- 140MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether Firewall has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZ8/GSREL
```

If Firewall has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

## Disabling Super Speed before Upgrading

Well before upgrading, set the **Enable Super Speed Processing** field on the **Firewall General Definitions** screen (*STRFW > 81 > 1*) to **N**.

This causes a new transaction to appear in the same exit point as files that are closed.

If enough time does not elapse after **Enable Super Speed Processing** is set to **N**, the files may remain open, causing file locks to be detected and preventing the upgrade. If this happens, you need to end the jobs that use the files to remove the locks.

## Working with Object Locks

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZ8 \*LIB**
2. **WRKOBJLCK SMZTMPA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZ8) TYPE(\*DSPF)**

These commands should display any locks that affect Firewall.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZ8 and SMZ8DTA libraries.

## Deactivation of the Product

Firewall will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing Firewall is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnxxx/GSI ('*SAVE' 'GS' "RZLnxxx"  
'SMZ8')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITY1P is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within Firewall are run, so users who do not have these authorities can run Firewall properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL RZLnnnn/GSI ('*SAVF' 'GS' 'RZLnnnn'  
'SMZ8')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZ8/GSREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.



## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRFW** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the Firewall main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/Authority on Demand (AOD), Multi-Factor Authentication (MFA) and Password Reset

Installing the SMZO library installs iSecurity Multi-Factor Authentication, Authority on Demand (AOD) and Password Reset. For simplicity, this document refers to the product as AOD.

## Pre-Requisites

- Operating system 7.1 or higher
- 100MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether AOD has already been installed on your IBM i, enter the command:

**DSPDTAARA SMZO/ODREL**

If AOD has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZO \*LIB**
2. **WRKOBJLCK SMZODTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZO) TYPE(\*DSPF)**

These commands should display any locks that affect AOD.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZO and SMZODTA libraries.

## Deactivation of the Product

AOD will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing AOD is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL RZLnnnn/ODI ('*SAVF' 'OD' "RZLnnnn' 'SMZO')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITY8P is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within AOD are run, so users who do not have these authorities can run AOD properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.



## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/ODI ('*SAVE' 'OD' 'RZLnnnn'  
'SMZO')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZO/ODREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRAOD** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the AOD main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/Advanced Threat Protection (ATP), Antivirus, Anti-Ransomware and Object Integrity Control

Installing the SMZV library installs iSecurity Advanced Threat Protection (ATP), Antivirus, Anti-Ransomware and Object Integrity Control. For simplicity, this document refers to the product as ATP.

## Pre-Requisites

- Operating system 7.2 or higher
- 410MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.



## The Installation and Upgrade Process

To determine whether ATP has already been installed on your IBM i, enter the command:

**DSPDTAARA SMZV/ARREL**

If ATP has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. WRKOBJLCK SMZV \*LIB
2. WRKOBJLCK SMZVDTA \*LIB
3. SMZ4/CHKSECLCK PART(SMZV) TYPE(\*DSPF)

These commands should display any locks that affect ATP.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT (\*LIB)** to backup the SMZV and SMZVDTA libraries.

## Deactivation of the Product

ATP will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing ATP is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnnnn/AVI ('*SAVF' 'AV' "RZLnnnn'  
      'SMZV' )
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITY5P is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within ATP are run, so users who do not have these authorities can run ATP properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/AVI ('*SAVE' 'AV' 'RZLnnnn'  
'SMZV')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZV/ARREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRAV** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the ATP main menu.

## Configuring Antivirus after Installation

After entering the authorization code, follow these steps:

1. Set these parameters, as shown in the [iSecurity Antivirus manual](#):
  - A. [Setting General Definitions](#)
  - B. [Setting Definitions for Real-Time Access](#)
  - C. [Scheduling Virus Scans](#)
2. If you will update your virus definitions from Raz-Lee (as shown in [Updating Virus Definitions](#)), open the IP address 212.227.30.66 on your firewall. If you are using iSecurity Firewall, see [Setting Firewall Rules for Outgoing Activity by IP Address](#) in the Firewall manual.
3. Refresh virus definitions via the **UPDAVDFN** command (**STRAV > 21 > 41**)
4. If you are ready to use Antivirus in real-time, activate real time protection as shown in [Activating and De-Activating Real-Time Virus Detection](#) in the Antivirus manual. On the **Antivirus & AntiRansomware (ATP) Configuration** screen (**STRAV > 81**), the red text next to the label **Antivirus** changes to **Loading** and then to **Active**.

## Configuring Antivirus after Upgrading

If you are upgrading to version 7.66 or greater from a version older than 7.66 and you update your virus definition from Raz-Lee (as shown in [Updating Virus Definitions](#)), open the IP address 212.227.30.66 on your firewall. If you are using iSecurity Firewall, see [Setting Firewall Rules for Outgoing Activity by IP Address](#) in the Firewall manual.

**NOTE:** This is **only** needed if you are upgrading to version 7.66 or greater from a version older than 7.66.

## Configuring Anti-Ransomware after Installation

After entering the authorization code, follow these steps:

1. Set these parameters, as shown in the [iSecurity Anti-Ransomware manual](#):
  - a. [Setting Real Time Activities and Internal Logging](#)
  - b. [Examining and Recovering Files in the Recycle Bin](#)
  - c. Schedule updates, as shown in [Updating Anti-Ransomware Definitions](#)
  - d. [Setting Thresholds for Ransomware Detection](#). Some or all of the fields in the **React Y/N** section must be set to **Y**.
  - e. [Setting Reactions to Ransomware Attacks](#)
2. If you have set the **Refresh source** field on the **Update ATP Definitions (UPDATPDFN)** screen (*STRAR > 52 > 1*) to **\*WEB**, open IP addresses within your firewall for refreshing threat information. If you are using iSecurity Firewall, see [Setting Firewall Rules for Outgoing Activity by IP Address](#) in the Firewall manual.
  - If you have set the **If \*WEB: \*RAZLEE, \*BACKUP, url** field to **\*RAZLEE**, open the firewall to the IP address **74.208.236.138**.
  - If you have set the **If \*WEB: \*RAZLEE, \*BACKUP, url** field to **\*BACKUP**, open the firewall to the IP address **104.21.6.198**
3. Refresh the definitions, as shown in [Updating Anti-Ransomware Definitions](#).
4. Once the definitions have refreshed, the screen prompts "**Restart servers now?**" Type **Y** to restart the server.
5. On the **Antivirus & AntiRansomware (ATP) Configuration** screen (*STRAR > 81*), the red text next to the label **Anti-Ransomware** changes to **Loading** and then to **Active**.



## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/Capture

Installing the SMZC library installs iSecurity Capture. For simplicity, this document refers to the product as Capture.

## Pre-Requisites

- Operating system 7.1 or higher
- 100MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

Plan the procedure for off-peak hours, as it may display some messages on end user screens that are being captured.

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether Capture has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZC/CAREL
```

If Capture has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZC \*LIB**
2. **WRKOBJLCK SMZCDTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZC) TYPE(\*DSPF)**

These commands should display any locks that affect Capture.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZC and SMZCDTA libraries.

## Deactivation of the Product

Capture will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing Capture is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL RZLnxxx/CAI ('*SAVF' 'CA' "RZLnxxx"  
'SMZC')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile [[User]] is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within Capture are run, so users who do not have these authorities can run Capture properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/CAI ('*SAVF' 'CA' 'RZLnnnn'  
'SMZC')
```

where **nnnn** is the number completing the library name in the original statement

## Verifying that the new release is now installed.

To verify that the product release has changed, enter the **DSPDTAARA SMZC/CAREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRCPT** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the Capture main menu.



## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definition changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/Change Tracker

Installing the SMZT library installs iSecurity Change Tracker. For simplicity, this document refers to the product as Change Tracker.

## Pre-Requisites

- Operating system 7.1 or higher
- 120MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether Change Tracker has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZT/CTREL
```

If Change Tracker has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZT \*LIB**
2. **WRKOBJLCK SMZTDTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZT) TYPE(\*DSPF)**

These commands should display any locks that affect Change Tracker.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZT and SMZTDTA libraries.

## Deactivation of the Product

Change Tracker will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing Change Tracker is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn

you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnnnn/CTI ('*SAVF' 'CT' "RZLnnnn'  
      ' SMZT' )
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITYTP is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within Change Tracker are run, so users who do not have these authorities can run Change Tracker properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.



## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC. Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/CTI ('*SAVE' 'CT' 'RZLnnnn'  
'SMZT')
```

where **nnnn** is the number completing the library name in the original statement

## Verifying that the new release is now installed.

To verify that the product release has changed, enter the **DSPDTAARA SMZT/CTREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRCT** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key. The cursor is moved to two fields that are now opened for entry.
4. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the Change Tracker main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/Field Encryption and PGP Encryption

Installing the SMZE library installs iSecurity Field Encryption and PGP Encryption. For simplicity, this document refers to the product as Encryption.

## Pre-Requisites

- Operating system 7.1 or higher
- 85MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.



## The Installation and Upgrade Process

To determine whether Encryption has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZE/ENREL
```

If Encryption has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZE \*LIB**
2. **WRKOBJLCK SMZEDTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZE) TYPE(\*DSPF)**

These commands should display any locks that affect Encryption.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZE and SMZEDTA libraries.

## Deactivation of the Product

Encryption will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing Encryption is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn

you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL RZLnnnn/ENI ('*SAVF' 'EN' "RZLnnnn"  
'SMZE')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITYEP is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within Encryption are run, so users who do not have these authorities can run Encryption properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL RZLnnnn/ENI ('*SAVF' 'EN' 'RZLnnnn'  
'SMZE')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZE/ENREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRENC** command on the IBM i.
2. Select option **81. System Configuration**. Press the **F22 (Shift-F10)** key.
3. The cursor is moved to two fields that are now opened for entry.
4. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the Encryption main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/DB-Gate

Installing the SMZB library installs iSecurity DB-Gate. For simplicity, this document refers to the product as DB-Gate.



## Pre-Requisites

- Operating system 7.1 or higher
- 120MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether DB-Gate has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZB/DBREL
```

If DB-Gate has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZB \*LIB**
2. **WRKOBJLCK SMZBDTA \*LIB**
3. **SMZ4/CHKSECLCK PART (SMZB) TYPE (\*DSPF)**

These commands should display any locks that affect DB-Gate.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT (\*LIB)** to backup the SMZB and SMZBDTA libraries.

## Deactivation of the Product

DB-Gate will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing DB-Gate is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnnnn/DBI ( '*SAVF' 'DB' "RZLnnnn'  
      ' SMZB' )
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

If this is a first-time installation, the user profile SECURITYBP is created. This user profile has no password, and no one can sign on with it. This user profile owns the objects of the product and has special authorities that are adopted when programs within DB-Gate are run, so users who do not have these authorities can run DB-Gate properly.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/DBI ( '*SAVE' 'DB' 'RZLnnnn'  
' SMZB' )
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZB/DBREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRDB** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the DB-Gate main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.



## Installing and Upgrading iSecurity/FileScope Premium and FileScope Tools

Installing the SMZ1 library installs iSecurity FileScope Premium and FileScope Tools. For simplicity, this document refers to the product as FileScope.

## Pre-Requisites

- Operating system 7.1 or higher
- 200MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether FileScope has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZ1/FSREL
```

If FileScope has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZ1 \*LIB**
2. **WRKOBJLCK SMZ1DTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZ1) TYPE(\*DSPF)**

These commands should display any locks that affect FileScope.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZ1 and SMZ1DTA libraries.

## Deactivation of the Product

FileScope will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing FileScope is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnnnn/FSI ('*SAVF' 'FS' "RZLnnnn'  
      'SMZ1')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/FSI ('*SAVF' 'FS' 'RZLnnnn'  
'SMZ1')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZ1/FSREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRFS** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the FileScope main menu.



## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/CodeScope

Installing the SMZ6 library installs iSecurity CodeScope. For simplicity, this document refers to the product as CodeScope.

## Pre-Requisites

- Operating system 7.1 or higher
- 14MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether CodeScope has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZ6/CSREL
```

If CodeScope has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. WRKOBJLCK SMZ6 \*LIB
2. WRKOBJLCK SMZ6DTA \*LIB
3. SMZ4/CHKSECLCK PART(SMZ6) TYPE(\*DSPF)

These commands should display any locks that affect CodeScope.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT (\*LIB)** to backup the SMZ6 and SMZ6DTA libraries.

## Deactivation of the Product

CodeScope will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing CodeScope is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn

you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL RZLnxxx/CSI ('*SAVF' 'CS' "RZLnxxx"  
'SMZ6')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/CSI ('*SAVF' 'CS' 'RZLnnnn'  
    'SMZ6')
```

where **nnnn** is the number completing the library name in the original statement.

## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZ6/CSREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.



## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRCS** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the CodeScope main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## Installing and Upgrading iSecurity/WideScope

Installing the SMZ7 library installs iSecurity WideScope. For simplicity, this document refers to the product as WideScope.

## Pre-Requisites

- Operating system 7.1 or higher
- 18MB of disk space for initial installation
- iSecurity/\*BASE

## iSecurity/\*BASE

iSecurity/\*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to be licensed for this purpose.

To ensure that iSecurity/\*BASE is installed, enter

**DSPLIB SMZ4**

If this command fails to show objects of the library, you must first install iSecurity/\*BASE.

## Preparation

In some cases, a high availability (HA) product may interfere with the installation. If this is the case in your organization, you should temporarily suspend the HA solution from replication libraries starting with SMZ\* and RZL\*.

## The Installation and Upgrade Process

To determine whether WideScope has already been installed on your IBM i, enter the command:

```
DSPDTAARA SMZ7/WSREL
```

If WideScope has already been installed, the **Display Data Area** screen appears, providing its version and build date. Make a note of this information..

If this command fails, this is a first time installation. Proceed to [Installing from a Link](#).

The product may not be in use during the upgrade procedure.

From the **OS/400 Main Menu** or Command Entry or PDM screens, enter the commands:

1. **WRKOBJLCK SMZ7 \*LIB**
2. **WRKOBJLCK SMZ7DTA \*LIB**
3. **SMZ4/CHKSECLCK PART(SMZ7) TYPE(\*DSPF)**

These commands should display any locks that affect WideScope.

If locks are found, handle the situation and re-enter the command until the **No locks found** message appears.

As a precaution, use **SAVLIB SAVACT(\*LIB)** to backup the SMZ7 and SMZ7DTA libraries.

## Deactivation of the Product

WideScope will be deactivated automatically as part of the installation procedure. Some messages may appear on end user screens that are being captured.

## Installing from a Link

Click on the link of the product. A ZIP file containing WideScope is downloaded onto the PC.

The ZIP file contains an executable **.exe** file. Double-click that file to begin the installation. Windows Defender or other protection software may warn

you that an unauthorized program is running. If it does, click 'More info' and 'Run anyway'.

The program briefly displays a screen that enables you to proceed automatically or manually. Wait a few seconds and the automatic installation proceeds.

You should now enter:

- The IBM i system name or IP address
- QSECOFR (or equivalent) username and password

To avoid mistakes, the program repeats the name of the product you are about to install and your system name.

The installation program connects to the IBM i via FTP, creates a temporary library, copies a save file to that library, restores the installation program to that library, and runs it.

The program displays the commands that it uses to perform the installation.

The last line of this step is a CALL command similar to:

```
CALL    RZLnnnn/WSI ('*SAVE' 'WS' "RZLnnnn"  
    'SMZ7')
```

where **nnnn** is a number completing the name of the temporary library.

Copy that line. It might be useful if you need to repeat the installation manually.

If the product is active, it will be automatically deactivated.

For additional information, see "iSecurity Environmental Change Considerations" on page 171.

If the installation succeeds, a message saying that it succeeded appears in the window on the PC.

If the email contains links to ZIP files containing PTF patches, download and install them in the same manner.

## Recovering from a Failed Installation

If the procedure ends abnormally, it generates a log file, which opens a window on the PC screen.

To understand the reason for the failure, search backward from the end of the log. In most cases it is a lock that appeared during the installation. Alternatively, contact Technical Support.

Once resolved, run the procedure again.

## Running the Procedure Again

You may run the same automatic installation procedure again from the PC.

Alternatively, you may run it manually from a green screen, which is preferable. This is because when doing so, you will be able to resolve situations while the installation program waits to resume upon your confirmation.

To run it so, enter the command you copied earlier from the initial installation screen.

```
CALL    RZLnnnn/WSI ('*SAVF' 'WS' 'RZLnnnn'  
'SMZ7')
```

where **nnnn** is the number completing the library name in the original statement.



## Verifying that the new release is now installed

To verify that the product release has changed, enter the **DSPDTAARA SMZ7/WSREL** command. The **Display Data Area** screen appears. The release number and build date should differ from the original values prior to the installation.

## Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRWS** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the **F22 (Shift-F10)** key.
4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the WideScope main menu.

## Activating the product

If this was a product upgrade, activate the product.

If this is a first-time installation, see the user guide.

## Optional Software

We recommend installing iSecurity/AP-Journal. AP-Journal tracks definitions changes, highlighting the changed fields. It also sends alerts for specified changes by email or system messages as well as SIEM messages. AP-Journal is free of charge and requires no authorization when used to trace iSecurity definition changes.

## BASE Support

Using the **BASE Support** menu, you can view and modify settings that are common to all modules of iSecurity. This menu, with all its options, is in all iSecurity major modules.

To access the **BASE Support** menu, select **89. BASE Support** in the product's main menu (*STRxx> 89*).

```
AUBASE                                BASE Support                                iSecurity/Base
                                        System:  RLDEV

Email                                  General
  1. Address Book                      51. Work with Collected Data
  2. Email Definitions                 52. Check Locks
  9. Target Restrictions               53. Security Assessment
                                        55. Raz-Lee Support Menu
Operators                              56. Re-create Damaged Data Queues
 11. Work with Operators              58. *PRINT1-*PRINT9, *PDF Setup
 12. Work with AOD, P-R Operators     59. Global Installation Defaults

Authority Codes                        Network Support
 21. Set Authorization Codes          71. Work with Network Definitions
 22. Display Authorization Status     72. Network Authentication
 23. Add Daily Check of Auth Codes   74. Send PTF
 24. Remove Daily Check of Auth Codes 75. Run CL Scripts
 25. Display CPU/Lpar Information     76. Current Job CntAdm Log
                                        77. All Jobs CntAdm Log

Selection or command
===> _____

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=System main menu
```

# Email

## Email Address Book

You can define the email address to be used for each user profile. You can also use this option to define an email group, with multiple addresses.

1. Select **1. Address Book** in the **BASE Support** menu (**STRxx> 89 > 1**). The **Work with Email Address Book** screen appears.

```
Work with Email Address Book

Type options, press Enter.
  1=Modify   3=Copy   4=Remove

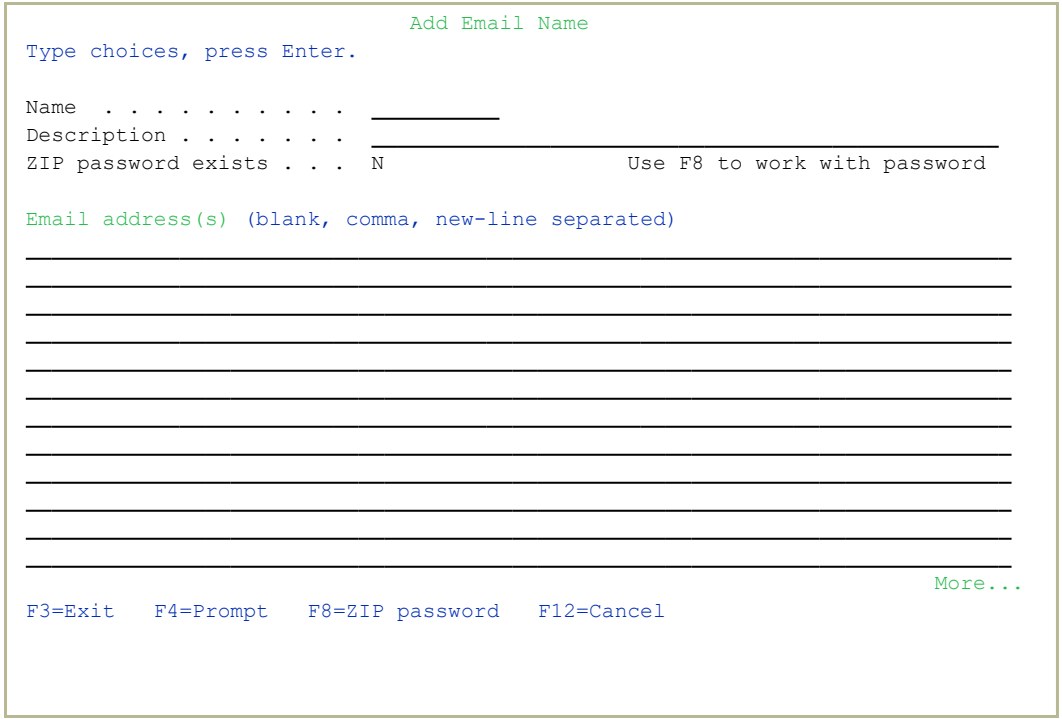
Position to . _____
Subset . . . _____

Opt  Name      Entries      Pwd.
-   AAA@BBB    1 test chkisa      *NO
-   ABRAHAM    1 Abraham Notik    *NO
-   ALEX       2 ALEX              *NO
-   JHJHJH    1 Yuri's Email      *NO
-   NOREPLY    1 Do Not Reply      *NO
-   SUPPORT    1 Support mail box  *NO
-   TZION      1 Tzion's email     *NO
-   VV         1 Victor             *NO
-   YOEL       1 Yoel's email      *NO
-   YURIW      1 Yuri work email   *NO
-   ZAILER     1 Shmuel's email    *NO

F3=Exit   F6=Add new   F12=Cancel

Bottom
```

2. Press **F6** to add a new address entry (or type **1** next to a name to modify it). The **Add Email Name** screen appears.



The screen contains the following fields:

**Name**

The name to identify the email addresses. Use this name when requesting reports that you send by email.

**Description**

A meaningful description

**ZIP Password exists**

You can specify a password to attach to any zip file sent to the addresses in this group. Without the password, the recipients will not be able to open the zip file. To add a password, press F8.

**Email addresses**

The email addresses of the group. Separate the addresses by a comma, or start each email address on a new line.

3. Enter the required parameters and press **Enter**.

## Email Definitions

iSecurity products can send out automatic emails according to settings in **Global Installation Defaults (STRxx> 89 > 59)**.

Select **2. Email Definitions** in the **BASE Support** menu (**STRxx> 89 > 2**). The **E-mail Definitions** screen appears.

```
E-mail Definitions                                23-07-19 11:41:22

Type options, press Enter.

E-mail Method . . . . . 3          1=Advanced, 2=Native, 3=Secured, 9=None
Advanced or Secured mode is recommended for simplicity and performance.

Advanced/Secured E-mail Support
Mail (SMTP) server name . . smtp.land.com
_____ Mail server, *LOCALHOST
Port . . . . . 25          SSL Secured  N   Y=Yes, N=No
Use the Mail Server as defined for outgoing mail in MS Outlook.
Reply to mail address . . . VICTOR@RAZLEE.COM
_____
If Secured, E-mail user . . ALEXM@RAZLEE.COM
_____
Password . *****

Native E-mail
E-mail User ID and Address. _____ User Profile.  _
Users must be defined as E-mail users prior to using this screen.
The required parameters may be found by using the WRKDIRE command.
This option does not support attached files.

F3=Exit  F10=Verify E-mail configuration  F12=Cancel
```

The screen contains these fields:

### E-mail Method

Advanced or Secured mode is recommended for simplicity and performance. Possible values are:

- **1**=Advanced
- **2**=Native
- **3**=Secured
- **0**=None

**Note:** If using **2=Native**, Users must be defined as E-mail users prior to using this screen. The required parameters may be found by using the **WRKDIRE** command. This option does not support attached files.

**Mail (SMTP) server name**

The name of the SMTP server or **\*LOCALHOST**. You can find or enter this information at your system's **Work with TCP/IP Host Table Entries** screen (*CGFTCP > 10*).

**Reply to mail address**

The e-mail address to receive replies.

**If secured, E-mail user and Password**

If you chose **1**=Advanced or **3**=Secured for the E-mail method, enter the email user that will be used to send the emails and the password of that user

**E-mail User ID and Address**

If you chose **2**=Native for the E-mail method, enter the user ID and address that will be used to send the emails.

**User Profile**

If you chose **2**=Native for the E-mail method, enter the user profile that will be used to send the emails.

To **confirm the change** to email definitions and send a confirmation email to the Reply-to mail address, press the **F10** key. A dialog opens in which you can confirm these settings. Check that you have received the confirmation email. If it is not received, there is a problem with your email definitions.



## Working with Operators' Authorities

Operators' authority management for all iSecurity modules is now maintained in a single place.

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.

iSecurity related objects are secured automatically by product authorization lists (named **security1P**). This strengthens the internal security of the product. It is essential that you use **Work with Operators** to define all users who have **\*SECADM**, **\*AUDIT** or **\*AUD#SECAD** privileges, but do not have all object authority. The **Work with Operators** screen has **Usr** (user management) and **Adm** for all activities related to starting, stopping subsystems, jobs, import/export and so on. iSecurity automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

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

Use **Password = \*BLANK** for the default entries. Use **DSPPGM GSIPWDR** to verify. The default for other users can be controlled as well.

If your organization wants the default to be **\*BLANK**, then the following command must be used:

```
CRTDTAARA SMZTMPC/DFTPWD *char 10
```

This command creates a data area called **DFTPWD** in library **SMZTMPC**. The data area is 10 bytes long and is blank.

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

To modify operators' authorities:

1. Select **11. Work with Operators** in the **Base Support** menu (**STRxx > 89 > 11**). The **Work with Operators** screen appears.

```

Work with Operators

Type options, press Enter.
 1=Select      3=Copy      4=Delete
Auth.level: 1=*USE, 3=*QRY (FW,AU,CT,SU), 5=*DFN (CT,EN,SU), 9=*FULL
  User        System  FW SC PW CD AV AU AC CP JR SU VS RP CO CT PR UM EN AD
- *AUD#SECAD  S520    9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
- *AUDIT      S520          9 9 9 9 9 9
- *SECADM     S520    9 9 9      9          9          9
- ALEX3       S520    9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
- AV          S520    9      9      9 9 9      9      9 9 9 9
- AVRAHAM     S520    9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
- DB          S520    9 9 9 9 9 9 9 9 9 9 9 9 3 9 9 9 9 9
- EVGPRVD    S520    9 9 9 9 9      9 9 9 9 9 9 9 9 9 9 9 9
- GS          S520    9 9 9 9 9 9 9 9 9 5 9 9 9 9 9 9 9 9
- JAVA        S520          3          5
More...

FW=Firewall   SC=Screen   PW=Password  CM=Command   AU=Audit     AC=Action
AV=Antivirus  CA=Capture  JR=Journal   VS=Visualizer UM=User Mgt. AD=Admin
RP=Replication CO=Compliance CT=Chg Tracker PR=Pwd Reset
EN=Encryption SU=SafeUpd

F3=Exit      F6=Add new   F8=Print     F11=*SECADM/*AUDIT authority  F12=Cancel

```

2. Type **1** next to the user to modify his authorities (or press **F6** to add a new user). The **Modify Operator** screen appears.

```

                                Modify Operator
Operator . . . . . ALEX3
System . . . . . S520          *ALL, Name
Password . . . . . *SAME      Name, *SAME, *BLANK

Auth.level: 1=*USE, 3=*QRY (FW,AU,CT,SU), 5=*DFN (CT,EN,SU), 9=*FULL
Firewall . . . . . FW 9      Screen . . . . . SC 9
Password . . . . . PW 9      Command . . . . . CD 9
AntiVirus . . . . . AV 9     Audit . . . . . AU 9
Action . . . . . AC 9        Capture . . . . . CA 9
Journal . . . . . JR 9       Safe Update . . . . . SU 9
Visualizer . . . . . VS 9    Replication . . . . . RP 9
Compliance . . . . . CO 9    Change Tracker . . . . . CT 9
Password Reset . . . . . PR 9 User Management . . . . . UM 9
Encryption . . . . . EN 9    Administrator . . . . . AD 9

The Report Generator is used by most modules and requires 1 or 3 in Audit.
Consider 1 or 3 for your auditors (with 3 they can create/modify queries).
*APR=Approver.

F3=Exit   F12=Cancel

```

Set the **Password** field to a valid password, to **\*SAME** to keep it the same as the previous password when edited, or to **\*BLANK** to have no password.

The **AuthLevel** field for each item can have the values:

- **1 = \*USE:** Read authority only
- **9 = \*FULL:** Read and Write authority
- **3 = \*QRY:** Run Queries. For auditor use.
- **5 = \*DFN:** For Change Tracker use

Most modules use the Report Generator, which requires access to the Audit module. For all users who will use the Report Generator, you should define their access to the Audit module as either **1** or **3**. Option **1** should be used for users who will only be running queries. Use option **3** for all users who will also be creating or modifying queries.

3. Set authorities and press **Enter**. A message appears stating that the user being added or modified was added to the Authority list that secures the product's objects; the user carries Authority **\*CHANGE** and will be granted Object operational authority. The Authority list is created in the installation or release upgrade process. The **SECURITY\_P** user profile is granted Authority **\*ALL** while the **\*PUBLIC** is granted Authority **\*EXCLUDE**. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

## Work with Operators for Authority on Demand and Password Reset

iSecurity related objects are secured automatically by product authorization lists (named **security1P**). This strengthens the internal security of the product. It is essential that you use **Work with Operators** to define all users who have **\*SECADM**, **\*AUDIT** or **\*AUD#SECAD** privileges, but do not have all object authority. The **Work with Operators** screen has **Usr** (user management) and **Adm** for all activities related to tasks such as starting, stopping subsystems, jobs, and import/export. iSecurity automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

1. Select **12. Work with AOD, P-R Operators** in the **BASE Support** menu (**STRxx> 89 > 12**). The **Work with Operators** screen appears.

```

Work with Operators

Type options, press Enter.
  1=Select  4=Delete

Authority level: 1=*USE  9=*FULL

Opt User      System  AOD PR  USP  Adm
-  *AUD#SECAD  S520    9  9  9  9
-  ALEX        S520    9  9  5  9
-  AV          S520    9      9
-  AVI         S520    9  9  9  9
-  JAVA2       S520    9  9  9  9
-  NISSIMM     S520    1  1  1  1
-  NIV         S520    9  9  9  9
-  OD          S520    9  9  9  9
-  OS          *ALL
-  TEST        S520    9  9  9  9
-  TZION       S520    9  9  9  9
-  VICTOR      S520    9  9  9  9

More...

AOD=Authority on Demand  PR=Password Reset  USP=User Provisioning
                        Adm=Administrator

F3=Exit  F6=Add new  F8=Print  F11=*SECADM/*AUDIT authority  F12=Cancel

```

2. Type **1** next to the user to modify his authorities (or press **F6** to add a new user). The **Modify Operator** screen appears.

```

Modify Operator

Type choices, press Enter.

Operator . . . . . VICTOR
System . . . . . S520      *ALL, Name
Password . . . . . *SAME    Name, *SAME, *BLANK

Authorities by subject:
Authority on Demand . . . . . 9      1=*USE, 4=Limited *EMERGENCY
                                           5=*EMERGENCY, 8=Limited *FULL
                                           9=*FULL
Password Reset . . . . . 9      1=*USE, 9=*FULL
User Provisioning . . . . . 9      1=*USE, 5=*ENTRY, 9=*FULL
Product Administrator . . . . . 9      1=*USE, 9=*FULL

Note: Emergency operator can enable or modify emergency rules. This allows
      solving of critical problems without the intervention of the security
      administrator.
      The term Limited denotes that the user cannot change PIN codes.

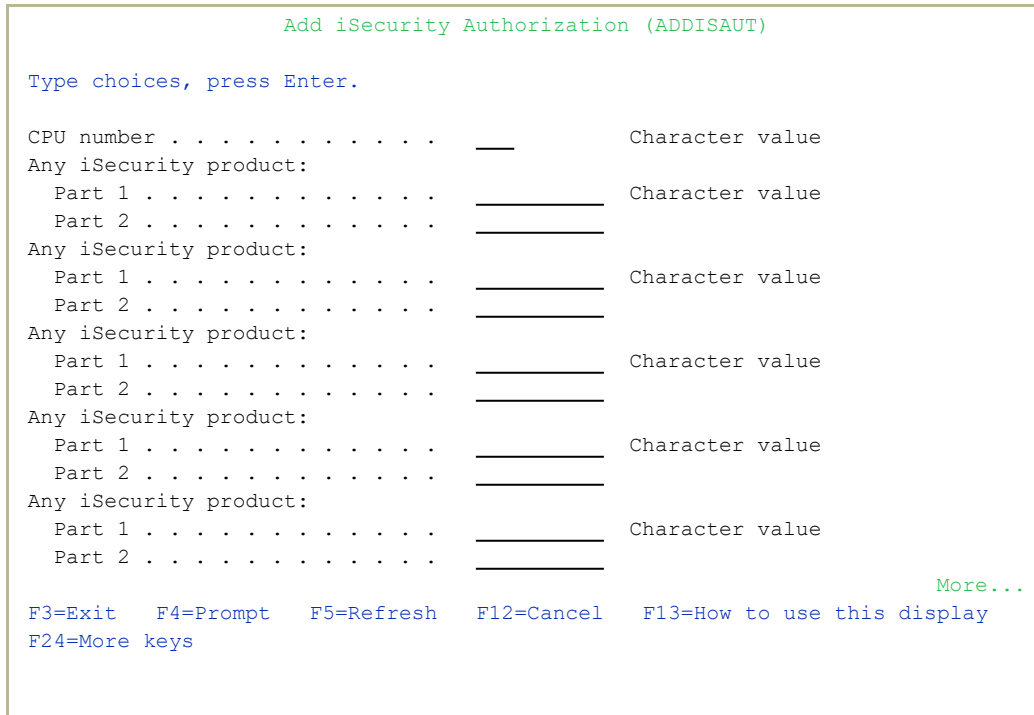
F3=Exit  F12=Cancel

```

## Work with Authorization

You can insert license keys for multiple products on the computer using one screen.

1. Select **21. Add Authorization Codes** from the **BASE Support** screen (*STRxx> 89 > 31*). The **Add iSecurity Authorization (ADDISAUT)** screen appears.



2. Enter the required parameters and press **Enter**.

Set the **Password** field to a valid password, to **\*SAME** to keep it the same as the previous password when edited, or to **\*BLANK** to have no password.

The **AuthLevel** field for each item can have the values:

- **1 = \*USE:** Read authority only
- **9 = \*FULL:** Read and Write authority
- **3 = \*QRY:** Run Queries. For auditor use.
- **5 = \*DFN:** For Change Tracker use

3. Set authorities and press **Enter**. A message appears to inform that the user being added or modified was added to the Authority list that secures the product's objects; the user carries Authority **\*CHANGE** and will be granted Object operational authority. The Authority list is created in the installation/release upgrade process. The **SECURITY\_P** user profile is granted Authority **\*ALL** whilst the **\*PUBLIC** is granted Authority **\*EXCLUDE**. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

## Display Authorization Status

You can display the current authorization status of all installed iSecurity products on the local system.

1. Select **22. Display Authorization Status** from the **BASE Support** menu (**STRxx > 89 > 22**). The **Status of iSecurity Authorization** screen appears.

```
44DE466 520 7459  Status of iSecurity Authorization  LPAR Id 1 S520
Type choices, press Enter.  Subset by . . . . .
1=Select  Warning days before expiration . 14

Opt Lib.  Status  Release ID  Product
- SMZ4-A Demo 19-08 14.04 19-06-27 *BASE, Audit, Action, SIEM, MSys, CmpEvl
  Auth code: 499999999999 1 Valid until 2019-08-31
- SMZ4-B Demo 19-08 14.04 19-06-27 Compliance (User,Native,IFS), Replicate
  Auth code: 499999999999 1 Valid until 2019-08-31
- SMZ8 Demo 19-08 18.06 19-07-14 Firewall, Screen, Command, Password
  Auth code: 899999999999 1 Valid until 2019-08-31
- SMZJ Demo 19-08 09.05 19-07-16 AP-Journal, Update-Control
  Auth code: J99999999999 1 Valid until 2019-08-31
- SMZO Demo 19-08 05.09 19-05-21 Authority on Demand,Pwd-Reset
  Auth code: O99999999999 1 Valid until 2019-08-31
- SMZC Demo 19-08 05.00 18-10-08 Capture, w^BI
  Auth code: C99999999999 123 Valid until 2019-08-31
- SMZT Demo 19-08 01.35 19-07-10 Change Tracker
  Auth code: T99999999999 *ALL Valid until 2019-08-31
- SMZV Demo 19-08 06.98 18-03-20 Antivirus, Anti-Ransomware, ICAP
  Auth code: V99999999999 1 Valid until 2019-08-31

F3=Exit  F10=Authority Code  More...
```

2. Select a specific line and type **1** in the **Opt** field to see the authority details of one specific product.

**NOTE:** Codes that will expire in less than 14 days appear in pink. Permanent codes have deliberately been hidden in this screenshot.



## Working with Collected Data

Administrators can view summaries of Audit, Firewall, and Action journal contents by day, showing the number of entries for each day together with the amount of disk space occupied. Administrators can optionally delete individual days to conserve disk space.

1. Select **51. Work with Collected Data** from the **BASE Support** screen (*STRxx> 89 > 51*). The **Work with Collected Data** screen appears.

```
Work with Collected Data                               S520

Type options, press Enter.

Module . . . . . -                                     1=Firewall
                                                         2=Audit
                                                         3=Action
                                                         4=Capture
                                                         5=Journal
                                                         6=Change Tracker
                                                         7=Authority On Demand

F3=Exit
```

2. Enter **2 (Audit)** and press Enter. The **Work with Collected Data –**

**Audit** screen appears.

```
Work with Collected Data - Audit                                     S520
Type options, press Enter.                                         Total Size (MB):      502.8
  4=Delete

Opt Collected Date      Records  Size (MB)  Save Date  Save Time
- 16/07/19                19,907    90.2      22/07/19   23:51:37
- 17/07/19                28,430   111.2     22/07/19   23:51:37
- 18/07/19                10,619    45.1      22/07/19   23:51:37
- 19/07/19                 7,412    27.6      22/07/19   23:51:37
- 20/07/19                11,225    54.1      22/07/19   23:51:37
- 21/07/19                14,066    69.3      22/07/19   23:51:37
- 22/07/19                15,479    78.2      22/07/19   23:51:37
- 23/07/19                 5,950    27.1

F3=Exit  F5=Refresh  F12=Cancel

Bottom
```

3. Select **4** to delete data from specific date(s) and press Enter.

### Purging all AUDIT data

You can purge all AUDIT data.

**WARNING:** Before you run these commands, back up the Audit data to offline storage.

To purge all Audit data, run these commands:

- *RMVM SMZ4DTA/AUXX \*ALL*
- *CLRPFM SMZ4DTA/AUSTTSP*

## Setting up the \*PRINT1-\*PRINT9 Printers and \*PDF Output

You can define up to nine specific printers to which you can send printed output. These may be local or remote printers. **\*PRINT1-\*PRINT9** are special values that you can enter in the OUTPUT parameter of any commands or options that support printed output.

Output to one of the nine remote printers is directed to a special output queue specified on the **\*PRINT1-\*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the **CHGOUTQ** command to specify the IP address of the designated remote location and the name of the remote output queue.

By default, two remote printers are predefined. **\*PRINT1** is set to print at a remote location (such as the home office). **\*PRINT2** is set to print at a remote location in addition to the local printer. In addition:

- **\*PRINT3** creates an excel file.
- **\*PRINT3-9** are user modifiable

To define remote printers:

1. Select **58. \*PRINT1 - \*PRINT9, PDF Setup** from the **BASE Support** menu (**STRxx> 89 > 58**). The **Printer Files Setup** screen appears.

```
Printer Files Setup

Select one of the following:

1. *PRINT1-*PRINT9 Setup
2. *PDF Setup

Selection ===>  _

F3=Exit
```

- Enter **1** and press **Enter**. The **\*PRINT1 - \*PRINT9 Setup** screen appears.

```

                                *PRINT1-*PRINT9 Setup

Type options, press Enter.
Using OUTPUT(*PRINTn) where n=1-9, provides extra control over prints.
Use this screen to specify parameters for this feature. This functionality can
be modified. For details see the original source SMZ8/GRSOURCE GSSPCPRT.

Press F14 for setup instructions

```

*PRINT	OutQ Name	OutQ Library	Save Hold	Description
1	CONTROL	SMZ4DTA	- -	OUTQ to print on the remote
2	CONTROL	SMZ4DTA	- -	Local+OUTQ that print on the remote
3			- -	
4			- -	
5			- -	
6			- -	
7			- -	
8			- -	
9			- -	

```

                                Bottom

F3=Exit      F8=Print      F12=Cancel      F14=Setup instructions

```

- Enter the name of the local output queue and library as shown in the above example. You can optionally enter a description. Possible values are:

- **OUTQ ( )** : Name of the local output queue
- **RMTprtQ ( )** : Name of the remote print queue
- **INTNETADR ( )** : IP address of the remote system

If the desired output queue has not yet been defined, use the **CRTOUTQ** command to create it. The command parameters remain the same.

For example, for **\*PRINT1** in the above screen, the following command would send output to the output queue '**MYOUTQ**' on a remote system with the IP address '**1.1.1.100**' as follows:

- **CHGOUTQ OUTQ(CONTROL/SMZTMPA) RMTSYS(\*INTNETADR)  
+ RMTprtQ(MYOUTQ) AUTOSTRWTR(1) CNNTYPE(\*IP)  
TRANSFORM(\*NO)  
+ INTNETADR(1.1.1.100)**

## \*PDF Setup

The operating system, from release 6.1, directly produces \*PDF prints. In the absence of such support a standard \*PDF is printed by other means.

To define PDF printers:

1. Select **58. \*PRINT1 - \*PRINT9, PDF Setup** from the **BASE Support** menu (*STRxx* > **89** > **58**). The **Printer Files Setup** screen appears..

```
Printer Files Setup

Select one of the following:

1. *PRINT1-*PRINT9 Setup
2. *PDF Setup

Selection ==>  _

F3=Exit
```

2. Enter **2** and press Enter. The **\*PDF Setup** screen appears.

```
*PDF Setup

The operating system, from release 6.1, directly produces *PDF prints.
In the absence of such support a standard *PDF is printed by other means.

When the operating system *PDF capability exists, it is used, and the
Query Generator uses the printer file SMZ4/AUQRYPDF to print the *PDF.

This file is shipped with the following parameters:

  CHGPRTF FILE(SMZ4/AUQRYPDF) LPI(8) CPI(15) PAGRTT(*COR)

You may wish to change the attributes of this printer file to suit your
needs.

Such changes must be re-applied after each iSecurity/Base (SMZ4) upgrade.

Press Enter to continue...
```

3. Follow the instructions on the screen.

**NOTE:** You must repeat this task after every upgrade of the Base System.

# Network Support

## Work with network definitions

To get current information from existing report or query, adjust system parameters, or to collect information from all the groups in the system into output files that can be sent via email, open the **Work with Network Systems** screen by selecting **71. Work with network definitions** from the **BASE Support** menu (*STRxx> 89 > 71*).

**NOTE:** Whenever you create or modify a network definition, you must re-enter the password in the **Network Authentication** screen, as shown in Network Authentication.

```
System type: AS400          Work with Network Systems          System: RLDEV
                               Position to . . . _____
Type options, press Enter.
  1=Select  4=Remove  7=Export dfn.  8=Test DDM  9=Ping

Opt  System  Group
-    RLDEMO  *TT      Demo system Audit release 14.16
-    RLDEV   *NONE    Razlee Develop
-    RLG     *TT      RL Germany
-    RLMED   *TT      RLEMD
-    RLPRV   *TT      Razlee Production
-    RL74A   *VVVV    Demo system
-    RL74B   *NONE    Test Yoel
-    VERDE   *NONE    verde

F3=Exit    F6=Add New    F7=Export dfn cmd    F12=Cancel

Bottom
```

To define a new network system, press the **F6** key. The **Add Network Systems** screen appears:

```

System type: AS400          Add Network System          System: S520

System . . . . . _____
Description . . . . . _____
Group where included . . . *NONE _____ *Name

Communication Details
IP or remote name . . . . . _____
_____

Type . . . . . *IP _____ *SNA, *IP
Entry of *LOCAL on System . _____ Use WRKRDBDIRE to verify
Auto filled for this system. Required for Multi-LPAR of AOD, P-R, Replication.

Copy of QAUDJRN on a different system
Where is QAUDJRN analyzed . *SYSTEM _____ Name, *SYSTEM
Extension Id on remote . . . _____

Note: After adding a system, run again "Network Authentication".

F3=Exit  F12=Cancel
Modify data, or press Enter to confirm.

```

## System

The name of the system

## Description

A meaningful description of the system

## Group where included

Enter the name of the group to which the IBM is assigned

## Where is QAUDJRN analyzed

Give the name of the System where QAUDJRN is analyzed. Enter **\*IBM** if it is analyzed locally.

## Default extension Id

Enter the extension ID for local copy details

## Type

The type of communication this system uses, Valid values are **\*SNA** and **\*IP**.

## IP or Remote Name

Enter the IP address or SNA Name, depending on the Type of communication you defined.



Enter your required definitions and press **Enter** to confirm.

To **modify a network definition**, enter **1** in the **Opt** field for the definition that you want to modify in the **Work with Network Systems** screen. The **Modify Network System** screen appears, which contains the same fields as the **Add Network System** screen.

## Network Authentication

DDM Data Queues are rebuilt automatically. This program also handles the TCP/IP Host Table Entry and performs *ADDTCPHTE* or *CHGTCPHTE* to apply the definition automatically.

To perform the activity on remote systems, you must define the user **SECURITY2P** with the same password on all systems and LPARS with the same password.

1. Select **72. Network Authentication** in the **BASE Support** menu (*STRxx> 89 > 72*). The **Network Authentication** screen appears.

```

                                Network Authentication

Type choices, press Enter.

User for remote work . . . SECURITY2P      Name
Password . . . . .
Confirm password . . . . .

In order to perform activity on remote systems, the user SECURITY2P must be
defined on all systems and LPARS with the same password.
Product options which require this are:
- referencing a log or a query with the parameter SYSTEM()
- replication of user profiles, passwords, system values
- populating definitions, log collection, etc.

Values entered in this screen are NOT preserved in any iSecurity file.
They are only used to set the user profile password and to set server
authentication entries. Ensure that SysVal QRETSVRSEC is set to 1.

F3=Exit                                F12=Cancel
```

2. Enter the **SECURITY2P** user password twice and press **Enter**.

## Send PTF

This option allows you to run a set of commands that will send objects as a PTF. This option is restricted to iSecurity products only. If you need to send PTFs for other products, please contact [RazLee Support](#).

Before you can use this option, you must

- define the entire network, as described in Network Definitions, and
- define user SECURITY2P on all nodes, using the same password, as described in Network Authentication.

Select **74. Send PTF** from the **BASE Support Menu (STRxx> 89 > 74)**. The **iSecurity Send PTF (RLSNDPTF)** screen appears.

```

iSecurity Send PTF (RLSNDPTF)

Type choices, press Enter.

System to run for . . . . . _____ Name, *CURRENT, *group, *ALL..
Objects . . . . . _____ Name, generic*, *ALL, *NONE
      + for more values _____
Library . . . . . _____ Name, ISECSETUP
Object types . . . . . *ALL _____ *ALL, *ALRTBL, *BNDDIR...
      + for more values _____
Save file . . . . . *LIB _____ Name, *LIB
  In library . . . . . QGPL _____ Name
Send SAVF to remote library . . *AUTO _____ Name, *AUTO (RL+job number)
On remote, backup LIB to SAVF . *NONE _____ Name, *NONE, *LIB
  In library . . . . . _____ Name
Restore the objects . . . . . *NONE _____ Name, generic*, *NONE, *ALL
  Into library . . . . . _____ Name, *LIB, *SAVF, ISECSETUP
Call the installation pgm . . . *NONE _____ Name, *NONE
  Library . . . . . _____ Name, *LIBL, *RSTLIB

More...

F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display   F24=More keys
  
```

### System to run for

- **Name** = The specific name of the system>
- **\*CURRENT** = The current system
- **\*group** = All systems in the group>
- **\*ALL** = All systems on the network

## Objects

- **Name** = A specific object
- **generic\*** = A group of objects with the same prefix
- **\*ALL**= All the objects
- **\*NONE** = No objects need to be extracted, the SAVF has already been prepared

## Library

The name of the library that contains the objects

## Object types

The object types to be sent

## Save file / Library

The name and library of the SAVF to contain the objects.

If you enter **\*LIB** for the file name, the name of the library containing the objects will be used.

If you enter **\*AUTO** as a name for the library, a library will be created with the name of RL<jobnumber>

## Remote library for SAVF

The name of the remote library to receive the SAVF to contain the objects. If you enter **\*AUTO** as a name for the library, a library will be created with the name of RL<jobnumber>

## Restore objects

The objects to be restored

- **Name** = A specific object
- **generic\*** = A group of objects with the same prefix
- **\*ALL**= Restore all objects
- **\*NONE**= Do not restore any objects

## Restore to library

The name of the library to receive the restored objects

- **Name** = A specific library
- **\*LIB** = the name of the original library containing the objects will be used.
- **\*SAVF**= the same name as the SAVF

### **Program to run / Library**

The name and library of a program to run after the objects have been restored.

### **Parameters**

The parameters for the program that runs after the restore.

Select the correct options and press **Enter**.

## Run CL Scripts

With the iSecurity Remote Command screen, you can run a set of commands either from a file or by entering specific commands as parameters. Each command must be preceded by a label:

- **LCL**: Run the following command on the local system
- **RMT**: Run the following command on the remote system
- **SNDF**: Send the save file (format: library/file) to RLxxxxxxx/file (xxxxxxx is the local system name)

Before you can use this option, you must

- define the entire network, as described in Definitions, and
- define user SECURITY2P on all nodes, using the same password, as described in "Network Authentication" on page 154.

Select **75. Run CL Scripts** from the **BASE Support** menu (**STRxx > 89 > 75**). The **iSecurity Remote Command (RLRMTCMD)** screen appears.

```
iSecurity Remote Command (RLRMTCMD)

Type choices, press Enter.

System to run for . . . . . _____ Name, *CURRENT, *group, *ALL..
Starting system . . . . . *START Name, *START
Ending system . . . . . *END Name, *END
Run on *CURRENT if in *group . . *NO *NO, *YES
Source file for commands . . . . *CMDS Name, *CMDS
  Library . . . . . _____ Name, *LIBL
Source member . . . . . _____ Name
Cmnds-LCL:cmd RMT:cmd SNDF:savf _____

+ for more values _____

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
```

### System to run for

- **Name**: The specific name of the system>
- **\*CURRENT**: The current system

- **\*group**: All systems in the group>
- **\*ALL**: All systems on the network

### Starting system

Use to define the start of a subset within \*group or \*ALL

This is useful if you want to rerun a command that previously failed

### Ending system

Use to define the end of a subset within \*group or \*ALL

This is useful if you want to rerun a command that previously failed

### Allow run on local system

**\*YES**: The remote command can run on the local system

**\*NO**: The remote command cannot run on the local system

### Source file for commands

**Name**: The file where the commands to run are stored.

**\*CMDS**: Use the commands entered below

### Library

**Name**: The library that contains the commands source file

**\*LIBL**: The library list

### Source member

**Name**: The member that contains the commands

### Cmds –LCL:cmd RMT:cmd SNDF:savf

The commands that can be run (if the Source file for commands parameter is **\*CMDS**).

**LCL : cmd** : A command that will be run on the local computer

**RMT : cmd** : A command that will be run on a remote computer

**SNDF : savf**: A save file

Select the correct options and press **Enter**.

## Displaying Communication Logs

To display the **current job log**, select **76. Current Job CntAdm Messages** from the **BASE Support** menu (*STRxx> 89 > 76*).

To display the **job log for all jobs**, select **77. All Jobs CntAdm Messages** from the **BASE Support** menu (*STRxx> 89 > 77*).



## Global Installation Defaults

Global installation configuration now includes access to the Raz-Lee Support Menu. Customers should not use it without guidance. It includes:

- Adding a system to enter field help and possible values for all fields in Query Generator and Logs in all products
- Setting of Default Report Summaries

You can set the parameters that iSecurity uses to control the Installation and upgrade processes. The option includes a Product-Admin Email and SYSTEM was added to the query mail subject line.

**NOTE:** Consult Raz-Lee support staff at support@razlee.com before changing any of the values on this form.

Select **59. Global Installation Defaults** from the **BASE Support** menu (**STRxx > 89 > 59**). The **Global Site Defaults - Menu** screen appears.

```
Global Site Defaults - Menu                                iSecurity

1. Installation
2. Run Time Attributes
3. Output and Logo
4. Syslog (SIEM) Support
5. Product Behavior
6. E-Mail definitions and Java Path
7. Character Set for Person Names

9. Post Installation Changes

Select option ==> _

F3=Exit   F12=Cancel                                     More...
```

The items in the menu lead to seven further screens. You can also use the **PgUp** and **PgDn** keys to move among them:

- 1. "Installation" below
- 2. "Run Time Attributes" on page 164
- 3. "Output and Logo" on page 165
- 4. "Syslog (SIEM) Support" on page 166
- 5. "Product Behavior" on page 167
- 6. "E-Mail Definitions and Java Path" on page 169
- 7. "Character Set for Person Names" on page 170
- 9. "Post Installation Changes" on page 171

## Installation

```

Global Site Defaults - Installation                                iSecurity
General purpose cmd library . . . QGPL_____
ASP for data libraries . . . . . 01
Wait for STROBJCVN to end . . . . Y           Y=Yes
Auto journal definition files . . N           Y=Yes
SBS to start iSec after IPL . . . QSYSWRK *LIBL_____
Allow group access to IFS . . . . Y           Y=Yes
Refresh Z* report definitions . . N           Y=Yes, A=Add new
Z* reports are provided with the products. User should use other names.

First day of work week . . . . . _           1=Monday, 2=Sunday, 3=Saturday
For backward compatibility, blank is considered Sunday.

More...

F3=Exit  F12=Cancel

```

The **Installation** page includes these fields:

### **General purpose cmd library**

An alternative library to QGPL from which all **STR\***, **RUN\***, and **\*INIT** commands will be run.

### **ASP for data libraries**

Products which are installed for the first time will be installed to this ASP. This refers to the product library and data library (for

example, SMZ4, SMZ4DTA)

In some products such as APJournal, other libraries are created. For example, in the AP-Journal a library is created per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number.

Change the current ASP of the library. All future upgrades will use this ASP.

All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.

#### **Wait for STROBJCVN to end**

**Y:** Yes

**N:** No

When installing the product on an OS400 version which is not the one that it was created for, objects require conversion and this is normally done in a batch job sent to work in parallel to the installation. If you want the conversion to run inline, (wait until it ends), this field should be set to **Y**.

The default value, which Raz-Lee recommends, is **N**.

#### **Auto journal definition files**

**Y:** Yes

**N:** No

#### **SBS to start iSec after IPL**

The Subsystem name and library to use for the Autostart Job.

#### **Allow group access to IFS**

Allow access to IFS from group profiles.

**Y:** Yes

**N:** No

#### **Refresh Z\* report definitions**

**Y:** Yes

**A:** Replace all

## First day of work week

The day on which the work week begins. If left blank, this defaults to Sunday.

### Run Time Attributes

```
Global Site Defaults - Run Time Attributes          iSecurity
Product-Admin Email . . . . . victor@razlee.com
Days before to warn Code-Expires. 15
Special Customer Id. . . . .          Raz-Lee Support Restricted Usage

F3=Exit  F12=Cancel                               More...
```

The **Run Time Attributes** page includes these fields:

#### **Product-Admin Email**

The email of the product admin to send automated messages to.

#### **Days before to warn Code-Expires**

All products whose authorization expires in less than this number of days are reported as an exception.

Enter a number between 01 and 99. The default is 14 days.

#### **Special Customer ID**

To be used only by Raz-Lee Support.

## Output and Logo

Global Site Defaults - Output		iSecurity
Append date to report gen files .	<u>_</u>	Y=Yes, S=Subject, B=Both
Add SYSTEM to query mail subject.	<u>Y</u>	Y=Yes. D=For AOD, B=Body
Use old PDF generation . . . . .	<u>N</u>	Y=Yes
Excel extension . . . . .	<u>.xml</u>	.xls, .xml
Set SPLF attribute to query name.	<u>U</u>	U=USRDTA, N=No
Attach empty reports . . . . .	<u>Y</u>	Y=Yes
Use group text as ZIP file name .	<u>N</u>	Y=Yes, N=Use group name
Setting your Logo for PDF reports Rename /iSecurity/LOGO/LOGO.JPG to LOGO-RAZLEE.JPG and place yours instead. File should be no more than 110 x 50 pixels, 120 DPI.		
F3=Exit F12=Cancel		More...

The **Output** page includes these fields:

### **Append date to report gen files**

**Y:** Yes

**N:** No

**B:**Both

### **Add SYSTEM to query mail subject**

**Y:** Yes

**D:** For Authority on Demand

**B:** Body

### **Use old PDF generation**

Whether to use the older method of generating PDFs, rather than the current method.

**Y:** Yes

**N:** No

### **Excel extension**

The extension to be used when creating Excel files

## Set SPLF attribute to query name

Whether to set the SPLF attribute in a query to USRDTA

### *Placing Your Organization's Logo on Reports*

The screen also describes how to place your own logo on reports. In the product, as shipped, the file **/iSecurity/LOGO/LOGO.JPG** contains the Raz-Lee logo. Rename this file to **LOGO-RAZLEE.JPG**. Place your own logo in the **LOGO.JPG** file. It must be no more than 110 pixels wide by 60 pixels tall, at 120 DPI.

## Syslog (SIEM) Support

Global Site Defaults - Syslog (SIEM) Support		iSecurity
Leave blank for defaults		
Syslog source	Port/IP 1 .	_____
	Port/IP 2 .	_____
	Port/IP 3 .	_____
TLS DCM Applic. ID	SIEM 1	SUMO
	SIEM 2	SUMO
	SIEM 3	1.1.1.192
Std CEF Ext. fld. names	. <u>Y</u>	Y=Yes
Include QAUDJRN Seq. Num.	. <u>N</u>	Y=Yes
Helps identify the original message.		
*AUTO Level of message	. <u>1</u>	1=1st-*AUTO1, 2=2nd-*AUTO2
The meaning of *AUTO when specified: 1st/2nd level of message.		
F3=Exit F12=Cancel		More...

The Syslog (SIEM) Support page includes these fields:

### **Syslog source Port/IP 1, 2, 3**

Syslog port source IP for each of the three Syslog sources

### **TLS DCM Applic. ID SIEM 1, 2, 3**

TLS ID for SIEM application for each of the three Syslog sources

### **Std CEF Ext. fld. names**

Whether to use standard external Common Event Field names, which include the company and product names.

**Y:** Yes

**N:** No

**Include QAUDJRN Seq. Num.**

Whether to include QUADJRN sequence numbers. These might be useful in tracking back to the source of Syslog messages.

**Y:** Yes

**N:** No

**\*AUTO Level of message**

Whether \*AUTO, when specified, means the first or second level of message.

**1**=1st-\*AUTO1

**2**=2nd-\*AUTO2

**Product Behavior**

Global Site Defaults - Product Behavior		iSecurity
GUI must run in SSL . . .	<u>N</u>	Y=Yes
Use IBM std auto disable. <u>Y</u> On change, set ANZPRFACT accordingly.		Y=Yes (IBM), E=Extended (iSec, generic*)
Mask User name & text . .	<u>?--%-----</u>	?=Display, %=Display, random if blank
Masks sensitive info in the report of user profiles that have default passwords		
AP-Journal shares Groups. <u>_</u>		Y=Yes, share Audit groups
Reference to General Groups in AP-Journal is to the groups in Audit.		
Firewall shares Groups . <u>I</u>		Y=Yes, share Audit groups, I=Items only
Reference to General Groups in Firewall is to the groups in Audit. As soon as you change this, use STRFW, 82, 99, 5. to merge the values.		
F3=Exit F12=Cancel		More...

The **Product Behavior** page includes these fields:

**GUI must run in SSL**

Whether the GUI must run in SSL mode.

**Y:** Yes

**N:** No

### **Use IBM std auto disable**

How ANZPRFACT is set on changes.

**Y**=Yes (IBM)

**E**=Extended (iSec, generic\*)

### **Mask User name & text**

How to mask sensitive info in the report of user profiles that have default passwords.

**?**: Display

**%**: Display

**Blank**: Random character

### **AP-Journal shares Groups**

Whether references to General Groups in AP-Journal are to the groups in Audit.

**Y**: Yes, share Audit groups

### **Firewall shares Groups**

Whether references to General Groups in AP-Journal are to the groups in Audit.

**Y**: Yes, share Audit groups

**I**: Items only

As soon as you change this, use **STRFW > 82 > 99 > 5** to merge the values.



## E-Mail Definitions and Java Path

```
Global Site Defaults - E-Mail definitions and Java Path  iSecurity

Email type .  J          A=Auto, J=Java, I=IBM-API

When setting I=IBM-API, a directory entry is created in the system directory,
where USRID is RLSNDM, the address is system name and the user is SECURITY2P.
SECURITY2P is also defined as a SMTP user.
For other requirements, see
https://www.ibm.com/support/knowledgecenter/ssw\_ibm\_i\_74/cl/sndsmtpemm.htm

Java path . .  /qopensys/QIBM/ProdData/JavaVM/jdk80/64bit/bin/java
Leave empty if the Java system default corresponds the email needs. Otherwise,
use the format /qopensys/QIBM/ProdData/JavaVM/jdk80/64bit/bin/java

More...

F3=Exit  F12=Cancel
```

The **E-Mail Definitions and Java Path** page includes the following fields:

### **Email type**

**A:** Auto

**J:** Java

**I:** IBM-API

When setting I=IBM-API, a directory entry is created in the system directory, where USRID is RLSNDM, the address is system name and the user is SECURITY2P. SECURITY2P is also defined as a SMTP user. For other requirements, see

[https://www.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i\\_74/cl/sndsmtpemm.htm](https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/cl/sndsmtpemm.htm)

### **Java path**

The path to the Java executable on your system. In many cases, the default value is accurate. If it is not, change it to refer to the actual location on your system.

## Character Set for Person Names

```
Global Site Defaults - Character Set for Person Names      iSecurity
Character set for names . . . . . 2      1=No check
                                           2=Is compatible with CCSID 273
                                           5=CCSID 640 + #@
                                           6=CCSID 640 + #@$^~[\]\{\}!\`
CCSID 640 represents all English alphanumeric in upper and lower case. These
characters have the same hex code in all single byte CCSID, except CCSID 290.
i.e. ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz-%&()* ,./:;?_'"<=>
We recommend using options 5 or 6 in a multi-language environment.

F3=Exit   F12=Cancel

More...
```

To define the character set for Person names, enter the value corresponding to the set in the Character set for name field:

- **1**: Do not check the character set
- **2**: CCSID 273 (used in Austria and Germany)
- **5**: CCSID 640, which incorporates all uppercase and lowercase English letters, plus the characters **#** and **@**.
- **6**: CCSID 640, plus the following characters: **#@\$^~[\]\{\}!\`**

## Post Installation Changes

Global Site Defaults - Post Installation Changes

Place Site modifications in program datalib/xxUPGRADE e.g. SMZ4DTA/AUUPGRADE  
When such a program exists, it is called automatically after products upgrades.

Bottom

F3=Exit    F12=Cancel

To make changes after installation, follow the instructions on the **Post-Installation Changes** page.

## iSecurity Environmental Change Considerations

## System values

- QFRCCVNRST – intermediate change, original value is auto-restored
- QALWOBJRST – not changed. Make sure it is set to \*ALL for the installation duration
- QSCANFSCTL and QSCANFS change at AntiVirus activation
- QRMTSIGN and QPWDVLDPGM change at Firewall activation

## iSecurity Jobs and Subsystems

Many of iSecurity products run part of their activity in dedicated subsystems. Raz-Lee's subsystems starts with the letter "Z".

iSecurity auto-start jobs perform one-time initialization or repetitive work that is associated with a particular subsystem.

See the table for QSYSWRK changes.

## Job Routing Entries

To enable activation of a controlled function at job entry (For products like Screen, Capture and WideScope), some Routing Entries are modified in the subsystems (specified by the user) to enable the product proper function.

The program RL#QCMD is added

If exists, do not delete it before running the command xxINITDFT SET (\*NONE) for all subsystems specified by the user(xx varies).

## User Profiles

During installation, a user profile with special authorities is built to own the product objects.

The special authorities of this user are used to allow proper run of the product.

This is done by programs that adopt the authority of their owner, or by user profile swap.

Those user profiles have no password and cannot sign on. A table of those users is listed below.

**Note:** Some general activities such as interconnection between different LPARs or the organization require a user with a password. This is true for SECURITY2P the owner of SMZ4 (Audit) objects. For this user profile the password in all the LPARs of the company must be identical, but there is never a need to actually sign on with this user profile.

## Libraries, Special Users and more

For each product installed, specific product libraries are installed as well as special user profiles, authorization lists, and Job Schedule Entries are created.

These product libraries, special users and job schedule entries are:



Product Name	Commands in QGPL	QSYSWRK Auto start Job Entries	Libraries	Job Schedule Entries	User
Audit / SIEM (AUD) Action Compliance Native Object Security Replication	STRAUD STRACT STRCMP STRRPL	AU#STRRTA U AU#STRRTM G	SMZ4, SMZ4DTA, SMZTMPA, SMZTMPB, SMZTMPC  /iSecurity  /smz4  /snmp	AU#MNT AU@DAILY AU@DAILYG U AU@DAILYH T	SECURITY2 P
Firewall / SIEM (FW) Screen Password Command	STRFW STRSCN STRPWD STRCMD	GS#FIREWAL	SMZ8, SMZTMPA, SMZTMPB, SMZTMPC	GS#MNT GS@DAILY GS@DAILYG U GS@DAILYH T	SECURITY1 P
AP-Journal / SIEM Safe Update (SU)	STRJR STRSU	JR#STRRTJR	SMZJ, SMZJDTA (SMZTMPC)	JR#MNT JR@DAILY	SECURITY4 P
Authority On Demand / SIEM (AOD) Password Reset (PR)	STRAOD STRPWDRS T		SMZO, SMZODTA (SMZTMPC)	OD#MNT OD@RMVE M	SECURITY8 P FORGOT
Capture	STRCPT		SMZC, SMZCDTA, SMZTMPA, SMZTMPB	CP#MNT	SECURITY7 P
Change Tracker	STRCT		SMZT, SMZTDTA, SMZ4,	CT#MNT	SECURITYT P

			SMZ4DTA SMZTyymmd d		
Advanced Threat Protection Antivirus Anti- Ransomwar e Object Integrity Control	STRATP STRAV STRAR STROBJITG		SMZV, SMZVDTA /smzvdta /snmp	AV\$UPDDFN AV#MNT AV@NTV	SECURITY5 P
Encryption (FIELD)  (FILE)	STRENC STRPGP		SMZE, SMZEDTA	EN#MNT EN#WATCH	SECURITYE P
DB-Gate	STRDB		SMZB, SMZBDTA	DB#MNT	SECURITYB P

## iSecurity User Profile Settings

User Profile	Usage	In Network	STATUS	PASSWORD	Remember it
SECURITYAP	Imperva Agent		*DISABLED	*NONE	
SECURITYBP	DB-Gate		*ENABLED	Must exist	No need to remember it
SECURITYEP	Encryption	Multi-system	*DISABLED	*NONE	
SECURITYEP	Encryption	Single-System	*DISABLED	*NONE	
SECURITYTP	Change Tracker		*DISABLED	*NONE	
SECURITY1P	Firewall, Command, Screen	*DISABLED	*NONE		
SECURITY2P	*BASE, Audit, Action	Multi-system	*ENABLED	Must exist	STRSEC, 89, 71-72
SECURITY2P	*BASE, Audit, Action	Single-System	*DISABLED	*NONE	
SECURITY4P	AP-Journal		*DISABLED	*NONE	
SECURITY5P	Antivirus, Anti-Ransomware	*DISABLED	*NONE		
SECURITY7P	Capture		*DISABLED	*NONE	
SECURITY8P	AOD, MFA, Password-Reset	Multi-system	*DISABLED	*NONE	
SECURITY8P	AOD, MFA, Password-Reset	Single-System	*DISABLED	*NONE	

