iSecurity Installation and Base Support

User Guide

www.razlee.com

Contents

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 SupportUser 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

Manual Revised: Wednesday, May 14, 2025

Contacts

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

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

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 7.2 or higher
- 300MB of disk space for initial installation
- user with the QSECOFR (or equivalent) profile

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 109.

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 ('*SAVF' '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 7.2 or higher
- 70MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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 109.

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 ('*SAVF' '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 7.2 or higher
- 140MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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   RZLnnnn/GSI ('*SAVF' 'GS' "RZLnnnn'
'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 109.

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 7.2 or higher
- 100MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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.

To deactivate AOD manually, select **2. Deactivate ZAUTH subsystem** from the **Activation** screen (*STRAOD > 11. Activation*).

To disable subsystems in MFA, select **12. Disable** from the **MFA Setup** screen (*STRMFA > 25*) and disable all enabled subsystems.

To remove TCP Enablement in MFA, select **61. Remove Option 21**, **62. Remove Option 22**, **63. Remove Option 23** from the **MFA Setup** screen (*STRMFA > 25*).

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 109.

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 ('*SAVF' '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
- user with the QSECOFR (or equivalent) profile

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 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*.

Preparation for an Anti-Ransomware Upgrade

Before upgrading the Anti-Ransomware components in the iSecurity/ ATP suite, you must clean the **`Recycle Bin`**.

To clean the **`Recycle Bin`** using the Work with Recycle Bin menu:

1. From the main Anti-Ransomware screen (**STRAR**), select option **12. Work with ReCycle Bin**.
2. Enter **4** in the Opt field, press **F13 (Shift-F1)** to repeat the entered option for all lines and press the **Enter** key. The **Confirm Delete Recycle bin files** screen appears. Press the **Enter** key to confirm and complete the deletion.
3. Verify the **Recycle Bin** is clean.

To clean the **Recycle Bin** using the **System Configuration** menu

1. From the **Antivirus & AntiRansomware (ATP) Configuration** screen (**STRAR> 81**), select option **25. Recycle Bin**.
2. Enter **1** in the **Keep data in Recycle bin for__Days** field and press the **Enter** key three times to confirm the configuration and exit the menu. The main Anti-Ransomware screen appears.
3. Type **WRKJOBSCDE AV#MNT** on the command line and press the **Enter** key.
4. Enter **10** in the Opt to submit immediately the **AV#MNT** job and press the **Enter** key.
5. Verify the **Recycle Bin** is clean.

Once you have confirmed that the **Recycle Bin** is clean, you can proceed with the upgrade of the Antivirus or Anti-Ransomware components.

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 109.

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 ('*SAVF' '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 7.2 or higher
- 100MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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   RZLnnnn/CAI ('*SAVF' 'CA' "RZLnnnn'
'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 109.

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 7.2 or higher
- 120MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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 109.

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 ('*SAVF' '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 7.2 or higher
- 85MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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 109.

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 7.2 or higher
- 120MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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 109.

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 ('*SAVF' '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 7.2 or higher
- 200MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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 109.

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/WideScope

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

Pre-Requisites

- Operating system 7.2 or higher
- 18MB of disk space for initial installation
- iSecurity/*BASE
- user with the QSECOFR (or equivalent) profile

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 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 ('*SAVF' '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 109.

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.

iSecurity in 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, *JOBD, *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 exiting 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	*JOBD	AOD &P-R Default
JR#MNT	*JOBD	
JR#STRRTJR	*JOBD	Journal Auto activation of Real Time
JRSYSLOG	*JOBD	Journal-Syslog by TCP server
OD#MNT	*JOBD	
OD#STRRTOD	*JOBD	Authority on Demand Auto activation
ODSYSLOG	*JOBD	OD-Syslog by TCP server
PRURMTSND	*JOBD	Send response by DtaQ
ZAUTH	*JOBD	Authority on Demand Monitor
ZCTLU	*JOBD	Authority on Demand *CTL point update
ZPRESET	*JOBD	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 in 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/-prdlib-) TYPE(*CHAR) LEN(2000) VALUE ('ASPDEV ASPGRP ')*

If it exists, use the command:

CHGDTAARA DTAARA(SMZTMPC/-prdlib- (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      'ASPDEV     ASPGRP                                '
   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.

iSecurity in HA Environments

Administrators of HA (High Availability) environments must take particular steps when installing or updating iSecurity products.

HA environments combine two or more systems through either Hot or Cold backup:

- In **Hot Backup** environments,

  Production and Active systems are active at the same time.

  Each system uses a software-based replication product such as Mimix, iTera, Quick EDD, or BUS for i.

  All systems have active iSecurity modules that produce logs and statistical information. Each has a valid active license code.

- In **Cold Backup** environments,

  The Production system is attached to mirrored or unmirrored storage.

  The Backup system only becomes active when the Production CPU is down.

  The system uses products such as IBM Power HA.

The environments can use either full or data replication.

In **full replication**, both objects and data, with exceptions, are synchronized between production and backup.

In **data replication**, only data with exceptions is synchronized between production and backup.

We recommend using **data replication** for iSecurity modules. This means that we install iSecurity initially or during updates on both production and backup systems, and only data **with exceptions** is synchronized between production and backup.

The names of all iSecurity libraries begin with the three-character string “SMZ”. Except for temporary libraries, whose names begin with “SMZTMP”, the fourth character in the library name indicates the products that use it. All products require the Base system in SMZ4.

Library	Product
SMZ4, SMZ4DTA, SMZ41	Base/Audit/Compliance Evaluator/IFS Object/Compliance/Native Object Compliance/Replication/Central Admin/User Compliance
SMZ8/SMZTMPA, SMZTMPB, SMZTMPC	Firewall/Password/Screen/Command
SMZB, SMZBDTA	DB-Gate
SMZC, SMZCDTA	Capture
SMZE, SMZEDTA	Encryption
SMZJ, SMZJDTA	AP-Journal
SMZO, SMZODTA	Authority on Demand/Password Reset/User Provisioning/MFA
SMZT, SMZTDTA	Change Tracker
SMZV, SMZVDTA	Antivirus
SMZ1, SMZ1DTA	Filescope
SMZ6, SMZ6DTA	CodeScope
SMZ7, SMZ7DTA	WideScope

Replication

In case of Full Replication, all SMZ* libraries should be replicated.

Libraries to exclude

Exclude libraries SMZ* and RZL* from object replication.

IFS objects to exclude

The following IFS directories (and the sub-directories below them) should be replicated in case of Full Replication:

/isecurity

/smzvdta (Antivirus-Anti Ransomware)

/atptest (Anti Ransomware simulator)

/SMZ*

Files to replicate

Replicate all files in SMZ* libraries except the following exclusions.

Files to exclude

Exclude the following files in case of Full and Data Replication:

Product	Dis-tributed by Library	Object to exclude	Type	Usage
All Products	SMZ*		DTAQ	Intermediate data
Base/Audit/Compliance Evaluator/IFS Object/Com-pliance/Native Object Com-pliance/Replication/Central Admin./User Compliance	QGPL	RL#QCMD	*PGM	
	QGPL	ISECCMDLIB	*DTAA-RA	89>59
	SMZ4	SMZ4DTA/AUP-ARM	*FILE	License key file
		SMZ4DTA/AUX-X	*FILE	Log file
		SMZ4DTA/AUC-C	*FILE	Log file
		SMZ4DTA/AUS-TTSP	*FILE	Statistical log file
		SMZ4DTA/AUI-NFSP	*FILE	Audit Journal Receiver info
Fire-wall/Pass-word/Screen/Command	SMZ8	SMZTMPA/GRP-ARM	*FILE	License key file
		SMZTMPA/GRL-OGP	*FILE	
		SMZTMPA/GSC-ALP	*FILE	Log file
		SMZTMPA/GSI-LOGP	*FILE	
		SMZTMPA/GSS-TTSP	*FILE	Statistical log file
DB-Gate	SMZB	SMZBDTA/DBP-ARM	*FILE	License key file
Encryption	SMZE	SMZEDTA/ENP-	*FILE	License key

Product	Distributed by Library	Object to exclude	Type	Usage
		ARM		file
	QSYS	SMZESYS	*LIB	Library
Capture	SMZC	SMZCDTA/CAP-ARM	*FILE	License key file
		SMZCDTA/AUS-C	*FILE	Log file
		SMZCDTA/AUC-HDR	*FILE	Log file
AP-Journal	SMZJ	SMZJDTA/JRPA-RM	*FILE	License key file
		SMZJDTA/JRST-TSP	*FILE	Statistical log file
		SMZJxxxxx/*AL-L	*FILE	(xxxxx-x=Application name)
Authority on Demand Password Reset User Provisioning MFA	SMZO	SMZODTA/ODP-ARM	*FILE	License key file
		SMZODTA/ODX-X	*FILE	Log file
Change Tracker	SMZT	SMZTDTA/CTP-ARM	*FILE	License key file
		CTLOGIG CTMODLP CTLIBIP CTAPLDP CTPRJDP CTTSKIP CTEXPTP CTLOGIG CTMODLP	*FILE	Files representing the transition in production libraries of the same system

Product	Dis-tributed by Library	Object to exclude	Type	Usage
		CTLIBIP CTAPLDP CTPRJDP CTTSKIP CTEXPTP		
Antivirus	SMZV	SMZV/AVPARM	*FILE	License key file
		/SMZVDTA/LO-G/*	*IFS	Log file
Filescope	SMZ1	SMZ1DTA/FSP-ARM	*FILE	License key file
CodeScope	SMZ6	SMZ6DTA/CSP-ARM	*FILE	License key file
WideScope	SMZ7	SMZ7DTA/WSP-ARM	*FILE	License key file

DTAARAs to exclude

Omit data area in case of Full Replication:

SMZ4DTA/AUDAUDIT *DTAARA

DTAQs to exclude

Omit all DTAQ from all SMZ* in case of Full Replication

Report files to exclude:

SMZRyymmdd

SMZTyymmdd

Where **yymmdd** is the date of the reports.

Cross-mirroring of log and statistical files

We recommend performing cross-mirroring for hot backup systems, as described above, with active backup systems and active iSecurity products.

For example, replicate from production system file SMZTMPA/GSCALP to backup system in file SMZTMPA/GSCALP_P and from backup system file SMZTMPA/GSCALP to production system in file SMZTMPA/GSCALP_B.

Using this method, in a disaster recovery of the production system scenario, you are able to activate the backup system for production while copying the SMZTMP/GSCALP_P to SMZTMPA/GSCALP and to continue on the backup system with production working, having the logs of the production system continuously available.

Special handling on production systems

Select **`11. Work with Operators`** from the BASE Support screen (*STRAUD > 89*). The Work with Operators screen appears. Press 3=Copy to copy all the users and fill in the new system name, and press ENTER twice, or use *ALL as system.

Select **`12. Work with AOD, P-R Operators`** from the BASE Support screen (*STRAUD > 89*). The Work with Operators screen appears. Press F6=Add new to create all the existing users for the new system, or use *ALL as the system.

Installation

Installation on a hot backup environment

Consider creating a mirror group for all the iSecurity files described above. This allows you to end in case of installations/updates only the iSecurity group.

End your HA solution or mirror group before installation. If you have configured a mirror group for all new libraries, end this mirror group before installation (we create new libraries during installation – e.g., SMZ8NEW for iSecurity Firewall. This library will be deleted after installation, and the installation will fail if the HA solution is working on mirroring this library to the backup system.

Install the iSecurity products as described in this user guide. Install first in a backup system, then in the production system.

Configure the exclusions/cross mirroring as described above.

Start your HA solution or mirror group.

Add the license code to the production system.

Add the license code on the backup system.

Installation on a cold backup environment

Install the iSecurity modules on the production system as described in this user guide.

Add the command SMZ4/SETISAUT with the proper license codes for iSecurity products on the backup CPU in your switchover procedure to assign the proper license code when doing the switch from production to backup CPU.

Updating

Updating in Hot Backup Environments

Consider creating a mirror group for all the iSecurity objects described above. If you do so, you can stop only the iSecurity group from doing updates.

End your HA solution or mirror group before the update. If you have configured a mirror group for all new libraries, end this mirror group before the update (we create new libraries during the update – e.g., SMZ8NEW for iSecurity Firewall. This library will be deleted after the update, and the update will fail if the HA solution is working on mirroring this library to the backup system.

Disable the iSecurity modules that you plan to update on all production and backup systems.

For Firewall: Suspend the firewall, including restarting the servers, before updating all production and backup systems.

Update the iSecurity modules, first on backup systems and then on production systems, as described in the installation manual.

Restart your HA solution or mirror group and wait for a successful synchronization state.

Enable the iSecurity products that you updated on all production and backup systems.

For Firewall: Resume the firewall, including restarting the servers, after you have completed updating all production and backup systems.

Updating in Cold Backup Environments

Disable the iSecurity products that you plan to update on the production system.

Update the iSecurity products on the production system as described in the installation manual.

For Firewall: Suspend the firewall, including restarting the servers, before updating the production system.

Enable the iSecurity products that you updated on a production system.

For Firewall: Resume the firewall, including restarting the servers after the update on a production system.

Firewall special considerations

No need to replicate libraries SMZ8, SMZTMPB.

Need to exclude the following files:

Product	Distributed by Library	Object to exclude	Type
Firewall	SMZ8	GSREL	*DTAARA
	SMZTMPA	GRPARM	*FILE
		GRLOGP	*FILE
		GSCALP	*FILE
		GSILOGP	*FILE
		GSSTTSP	*FILE
		FWRESUME	*DTAARA
		FWSGN	*DTAARA
		FWSSH	*DTAARA
		GSDBMON	*DTAARA
		GSMSGOPR	*DTAARA
		GSSTTSP	*DTAARA
		GSTIMSO	*DTAARA
		DQGSCALP	*DTAQ
		GR#MONITOR	*DTAQ
		GRRESULT	*DTAQ
		GSACTION	*DTAQ
		GSDBMON	*DTAQ
		GSJAVA	*DTAQ
		GSSYSLOG1	*DTAQ
		GSSYSLOG2	*DTAQ
		GSSYSLOG3	*DTAQ
	QGPL	ISECCMDLIB	*DTAARA
		RL#QCMD	*PGM

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**).

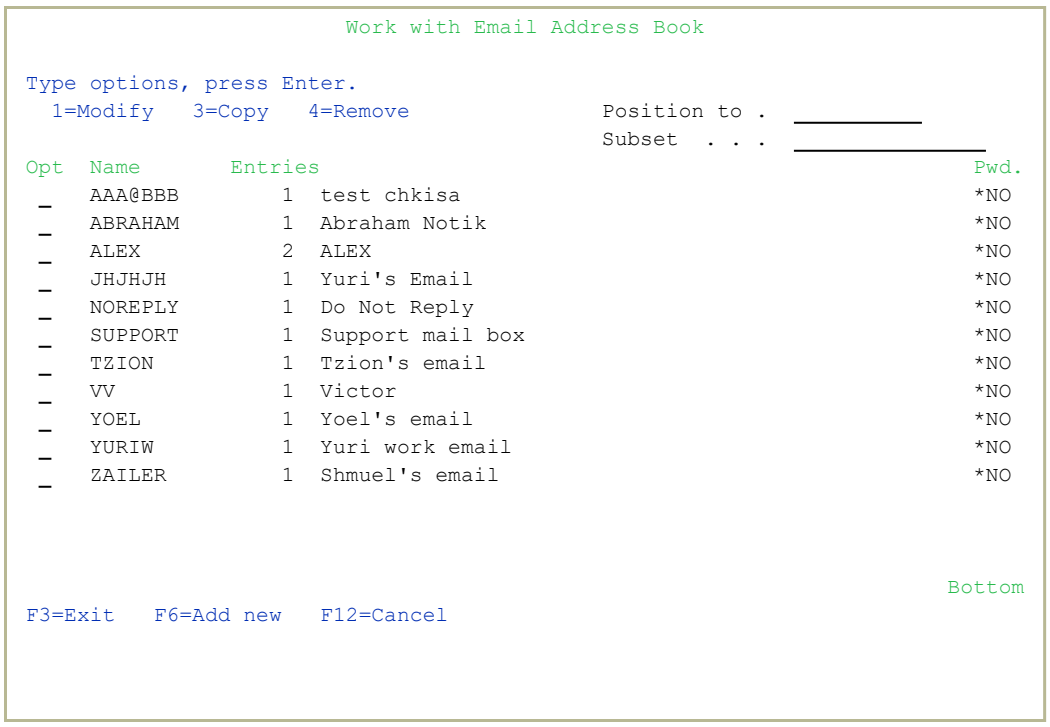
```
AUBASE                          BASE Support                  iSecurity/Base
                                                          System:   RLDEV
Email                                   General
 1. Address Book                        51. Work with Collected Data
 2. Email Definitions                   52. Check Locks
 9. Target Restrictions                 53. Security Assessment
                                        54. Watchdog
Operators                               55. Raz-Lee Support Menu
11. Work with Operators                 56. Re-create Damaged Data Queues
12. Work with AOD, P-R Operators        58. *PRINT1-*PRINT9 Setup
                                        59. Global Installation Defaults
Authorization Codes
21. Set Authorization Codes             Network Support
22. Display/Check Authorization Status  71. Work with Network Definitions
                                        72. Network Authentication
25. Display CPU/Lpar Information        79. Operation on Remote Systems


Selection or command
===> _____________________________________________________________________

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

Email

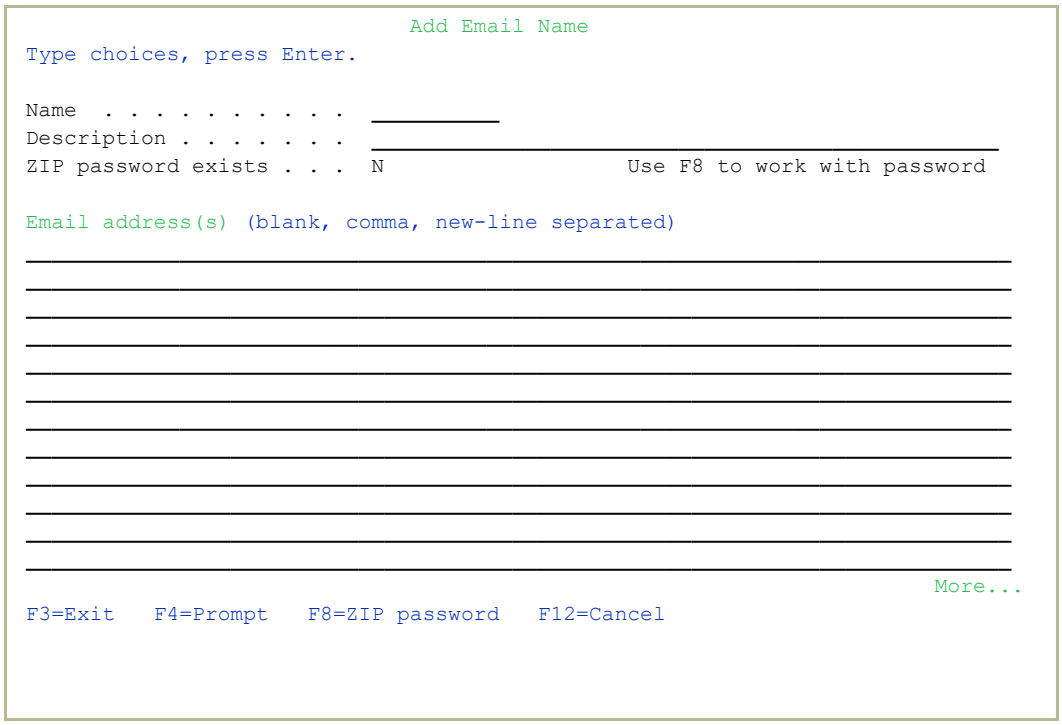
Email Address Book

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.



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            23/10/24 10:17:08

Type options, press Enter.

E-mail Method . . . . . .  3       1=Not secured, 3=Secured, 9=None

Reply to mail address . . .  NOREPLY                                        
Use an existing address. Some SMTP servers check this.

For Secured E-mail Support
Mail (SMTP) server name . .  smtp.ionos.com                                 
  Mail server, *LOCALHOST    ____________________________________________
Use the Mail Server as defined for outgoing mail.

Port  . . . . . .  587              SSL Secured    Y   Y=Yes, N=No

If Secured, E-mail user . .  avdb@razleesecurity.com                        
                Password .  **********                                      



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**=Not secured
- **3**=Secured
- **9**=None

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**).

If secured, E-mail user and Password

If you chose 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

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.

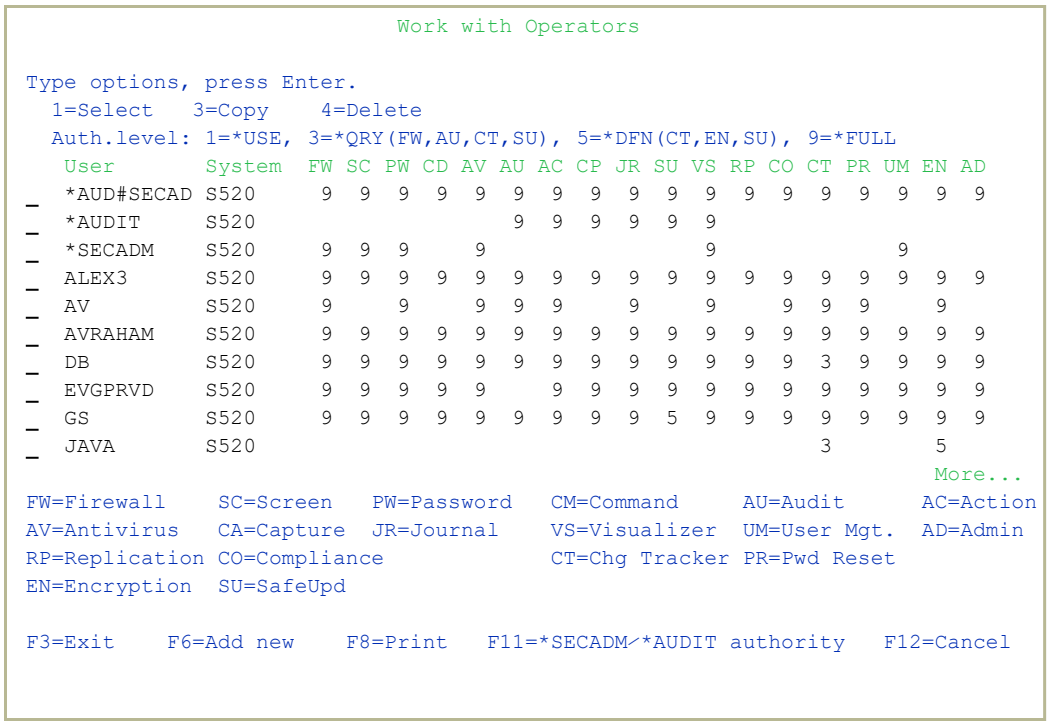
If your organization wants the default to be *BLANK, then the following command must be used:
*CRTDTAARA SMZTMPC/DFTPWD *char 10*

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.

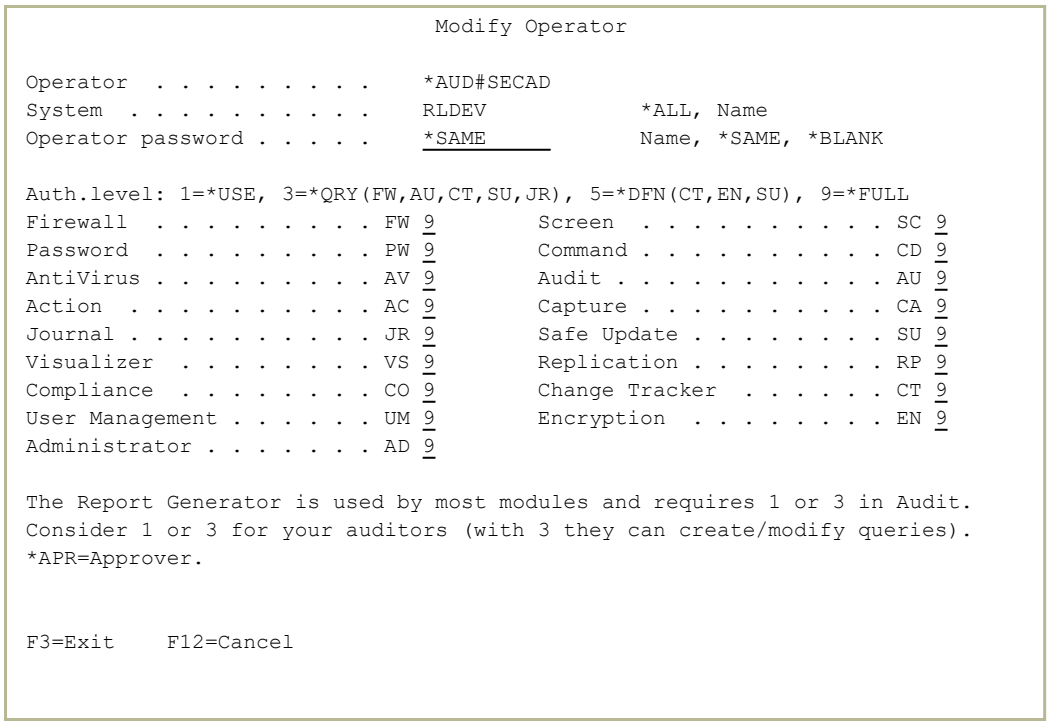
To modify operators' authorities:

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  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  9  3  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.



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.

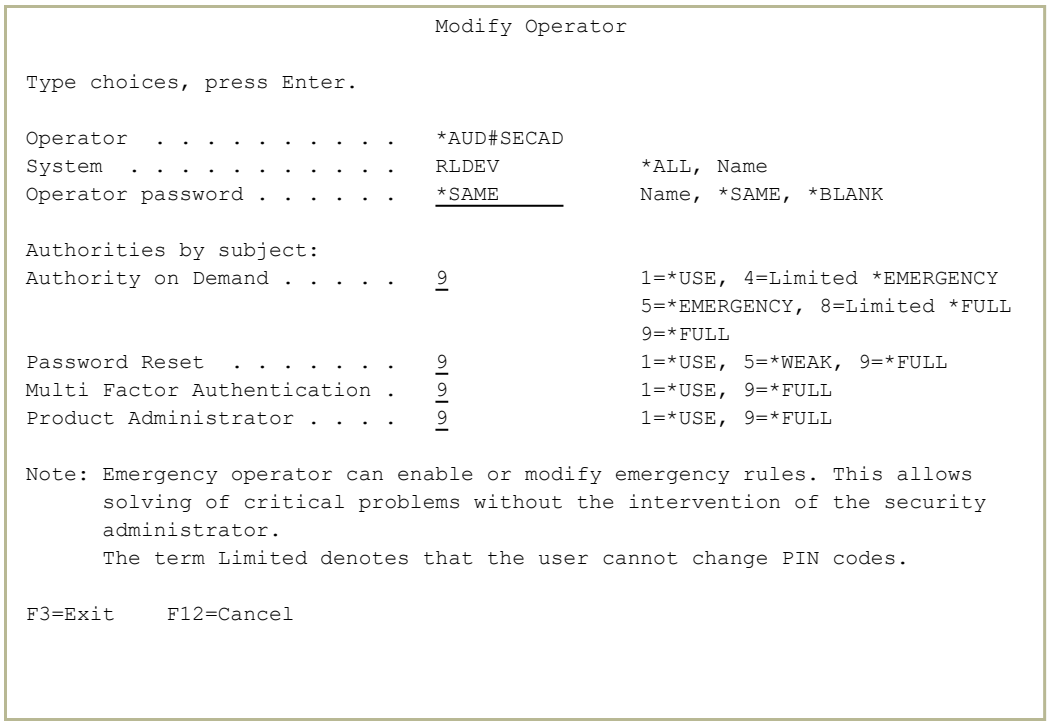
Work with Operators for Authority on Demand and Password Reset

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** (administrator) 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  P-R  MFA  Adm
 _  *AUD#SECAD    RLDEV       9    9    9    9
 _  ADAM          RLDEV       4                9
 _  AMNON         RLDEV       9    9    9    9
 _  CS            RLDEV       9    9    9    9
 _  OD            RLDEV       9    5    9    9
 _  QSECOFR       RLDEV       9    9    9    9
 _  TEST          RLDEV       9    9
 _  TEVG          RLDEV       9    9    9    9
 _  VV1           RLDEV       9    9    9    9




                                                                      Bottom
AOD=Authority on Demand   PR=Password Reset    MFA=Multi Factor Authentication
                                               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  . . . . . .  . . .   *AUD#SECAD
System  . . . . . . . . . . .  RLDEV           *ALL, Name
Operator 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, 5=*WEAK, 9=*FULL
Multi Factor Authentication .  9               1=*USE, 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. Set Authorization Codes** from the BASE Support screen (*STRxx*> **89 > 21**). The Set iSecurity Authorization (SETISAUT) screen appears.

```
                    Set iSecurity Authorization (SETISAUT)

Type choices, press Enter.

CPU serial number  . . . . . .   *CURRENT      Character value, *CURRENT
Any iSecurity product:
  Part 1 . . . . . . . . . . .   ____________   Character value
  Part 2 . . . . . . . . . . .   ____________
Any iSecurity product:
  Part 1 . . . . . . . . . . .   ____________   Character value
  Part 2 . . . . . . . . . . .   ____________
Any iSecurity product:
  Part 1 . . . . . . . . . . .   ____________   Character value
  Part 2 . . . . . . . . . . .   ____________
Any iSecurity product:
  Part 1 . . . . . . . . . . .   ____________   Character value
  Part 2 . . . . . . . . . . .   ____________
Any iSecurity product:
  Part 1 . . . . . . . . . . .   ____________   Character value
  Part 2 . . . . . . . . . . .   ____________
                                                                More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

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:

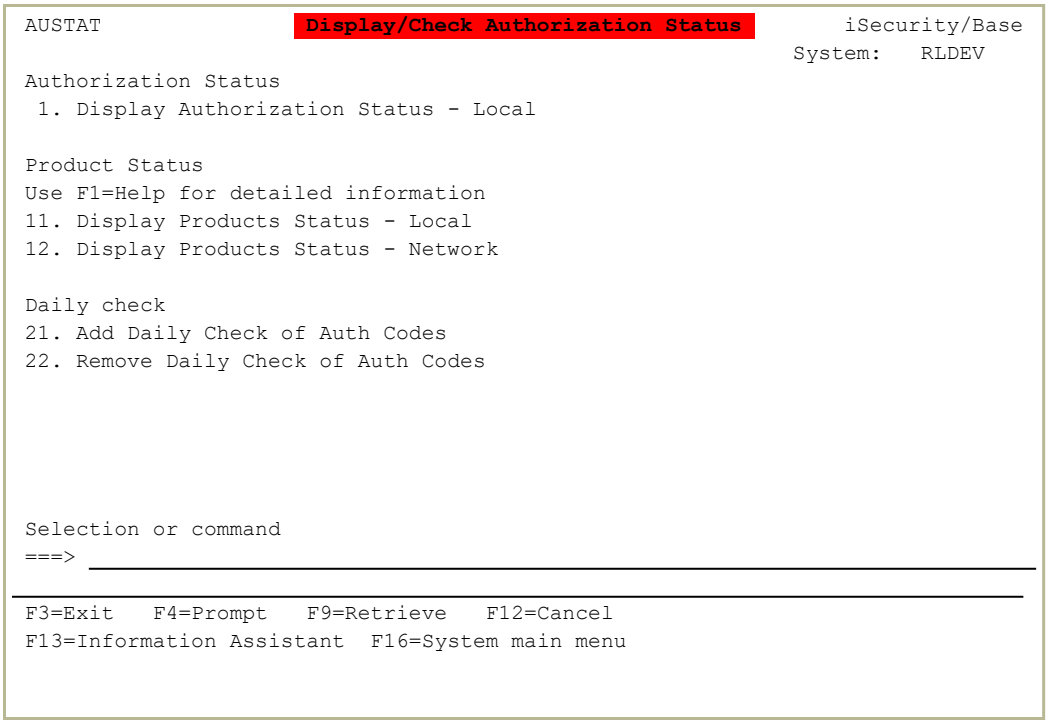
   - **1** = ***USE**: Read authority only
   - **9** = ***FULL**: Read and Write authority
   - **3** = ***QRY**: Run Queries. For auditor use.
   - **5** = ***DFN**: For Change Tracker use

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/Check Authorization Status

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

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



Select **1. Display Authorization Status - Local** to display status of iSecurity authorization. The **Status of iSecurity Authorization** screen appears. Type **1=Select** to display status of iSecurity authority code. Type **X=Explain** to display the brief explanation without code validation.

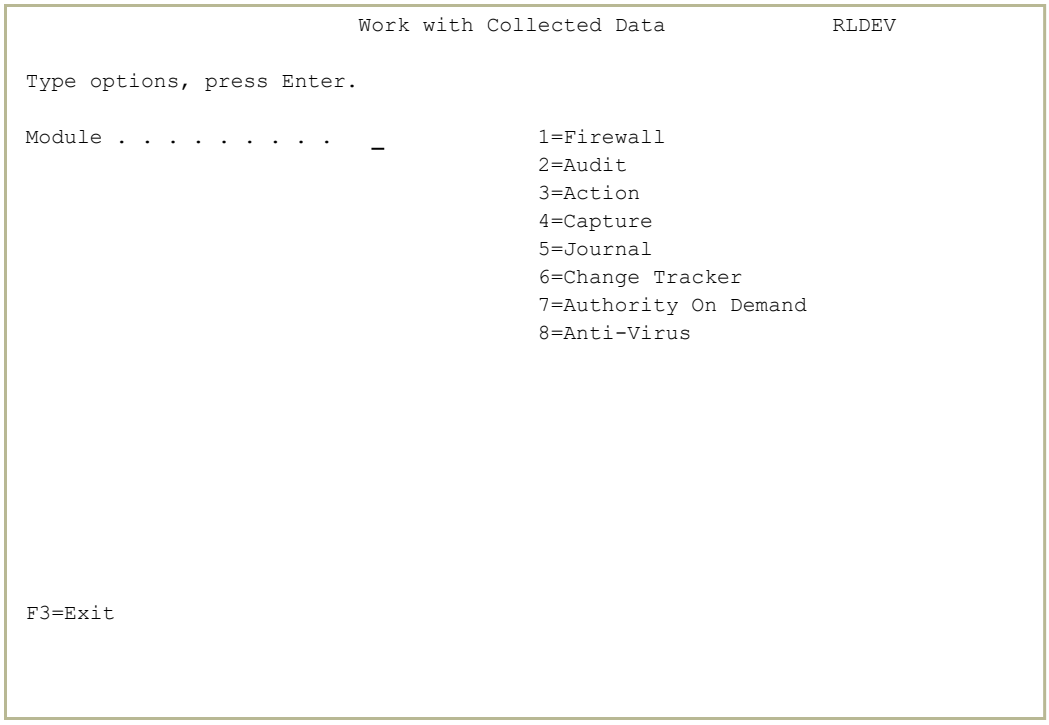
Select **11. Display Products Status - Local** or **12. Display Products Status - Network** to display products status. The **Check Raz-Lee Authorization (CHKISA)** screen appears. Type choices, press **Enter**. The **Display Report** screen appears.

Select **21. Add Daily Check of Auth Codes** or **22. Remove Daily Check of Auth Codes** to set or remove check of iSecurity authorization. The **Change Job Schedule Entry (CHGJOBSCDE)** or **Remove Job Schedule Entry (RMVJOBSCDE)** screen appears. Type choices, press **Enter**.

Working with Collected Data

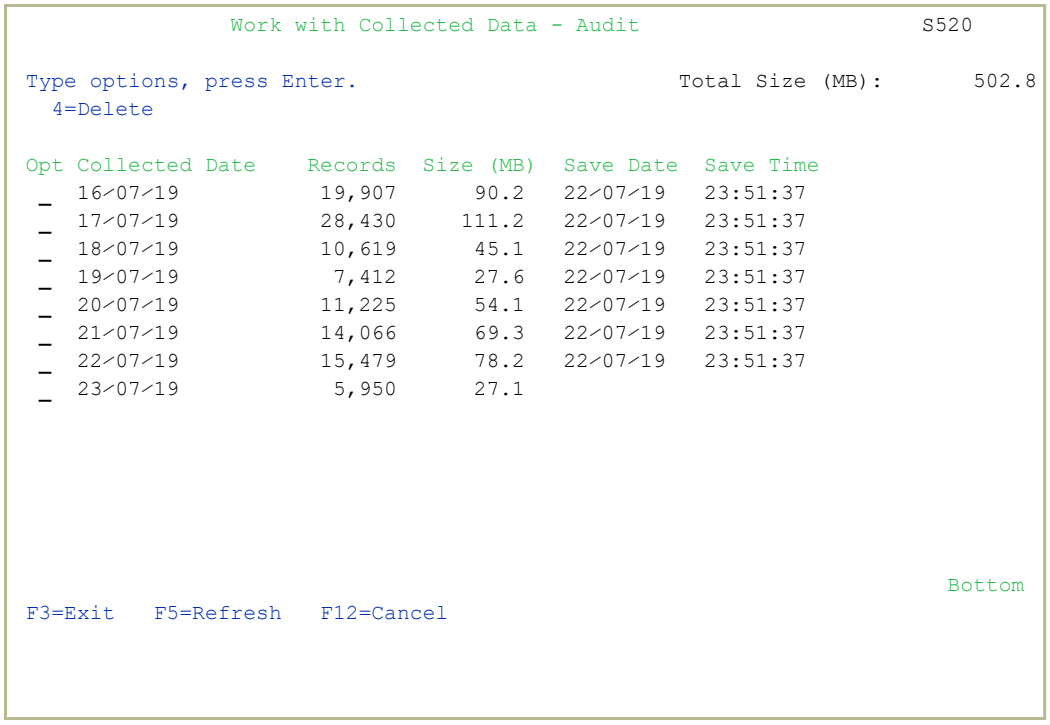
Administrators can view summaries of Audit, Firewall, and Action journal contents by day, showing the number of entries for each day together with the amount of disk space occupied. Administrators can optionally delete individual days to conserve disk space.

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



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

Audit screen appears.



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*

*PRINT1-*PRINT9 Setup

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.

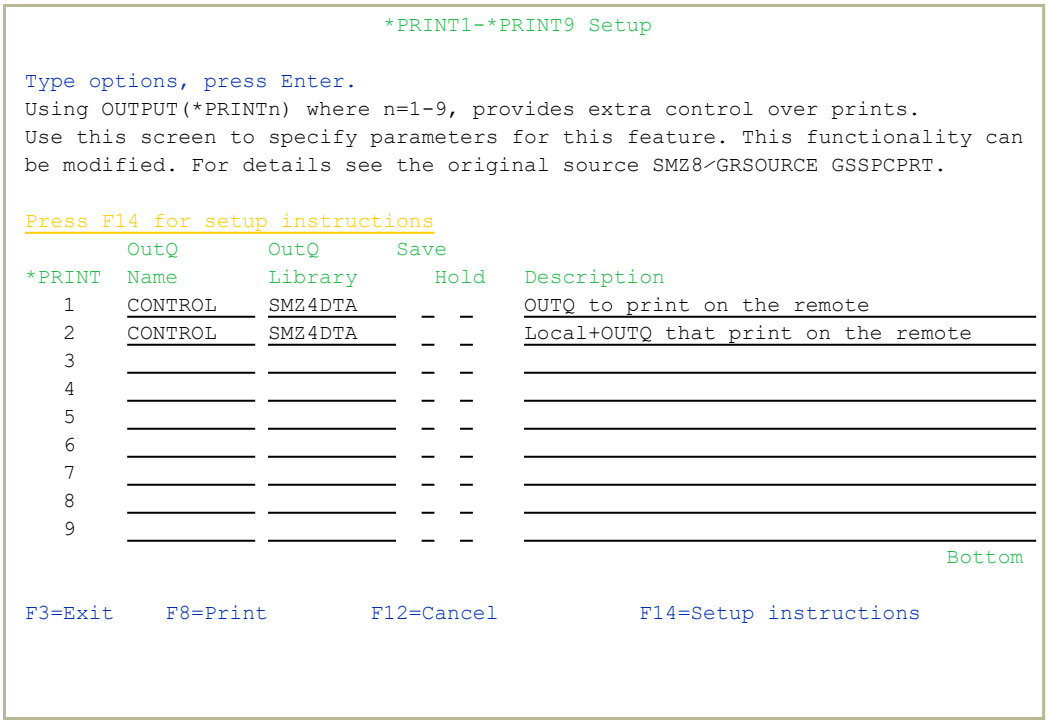
By default, two remote printers are predefined. ***PRINT1** is set to print at a remote location (such as the home office). ***PRINT2** is set to print at a remote location in addition to the local printer. In addition:

- ***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.

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



3. 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)*

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

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

To **define a new netwok 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.
SECURITY2P usually should be *DISABLED & LMTCPB(*YES).

Product options which require this are:
- referencing a log or a query with the parameter SYSTEM()
- populating definitions, log collection, etc.
- replication of user profiles, passwords   Requires *ENABLED & LMTCPB(*NO)

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**.

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.

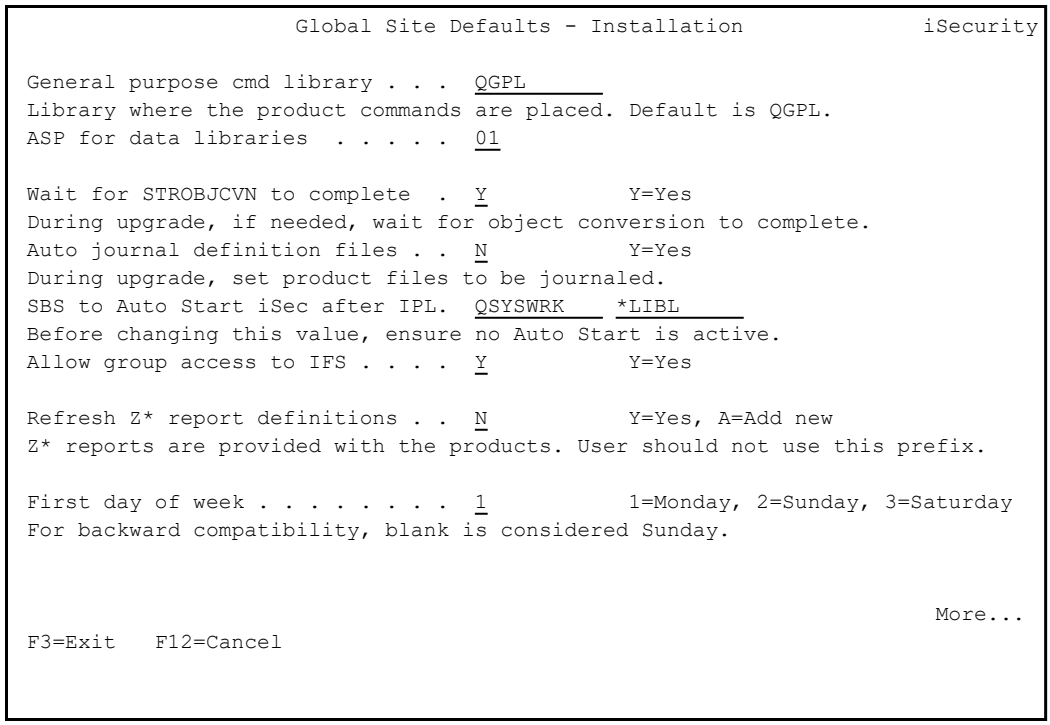
Select **59. Global Installation Defaults** from the **BASE Support** menu (*STRxx* **> 89 > 59**). The **Global Site Defaults - Menu** screen appears.

```
                        Global Site Defaults - Menu                 iSecurity

Select one of the following:

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

 9. Post Installation Changes









Selection ===>  _
Definition made here are stored in QGPL/ISECCMDLIB *DTAARA
                                                                      More...
F3=Exit    F12=Cancel
```

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

- **1.** "Global Installation Defaults" on the previous page
- **2.** "Global Installation Defaults" on the previous page
- **3.** "Global Installation Defaults" on the previous page
- **4.** "Global Installation Defaults" on the previous page
- **5.** "Global Installation Defaults" on the previous page
- **6.** "Global Installation Defaults" on the previous page
- **7.** "Global Installation Defaults" on the previous page
- **9.** "Global Installation Defaults" on the previous page

Installation



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 complete

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 Auto 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

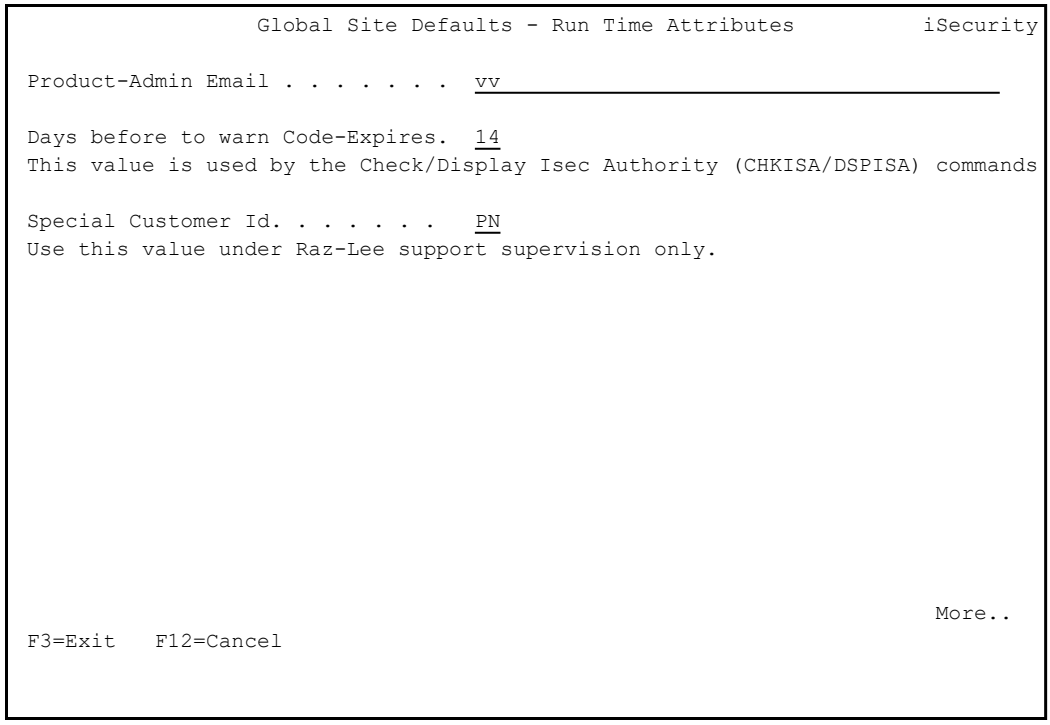
Y: Yes

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



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

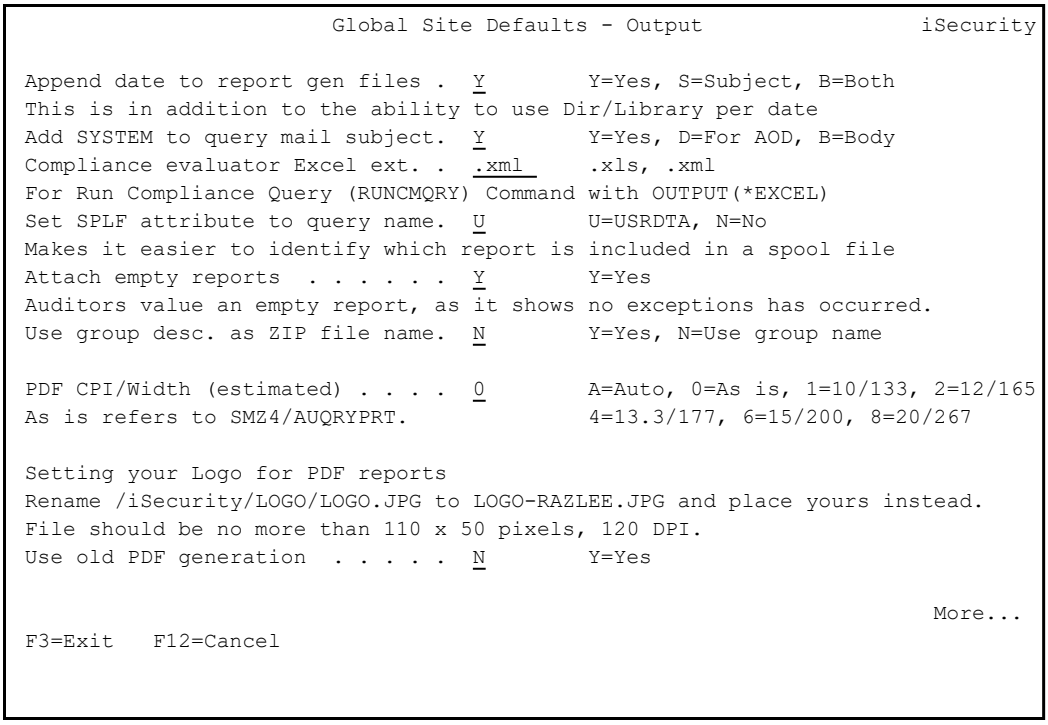
All products whose authorization expires in less than this number of days are reported as an exception.

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

Special Customer ID

To be used only by Raz-Lee Support.

Output Attributes and Logo Settings



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

Compliance evaluator Excel ext

.xml: the output can be created as an XML file

.xls: the output can be created as an Excel file

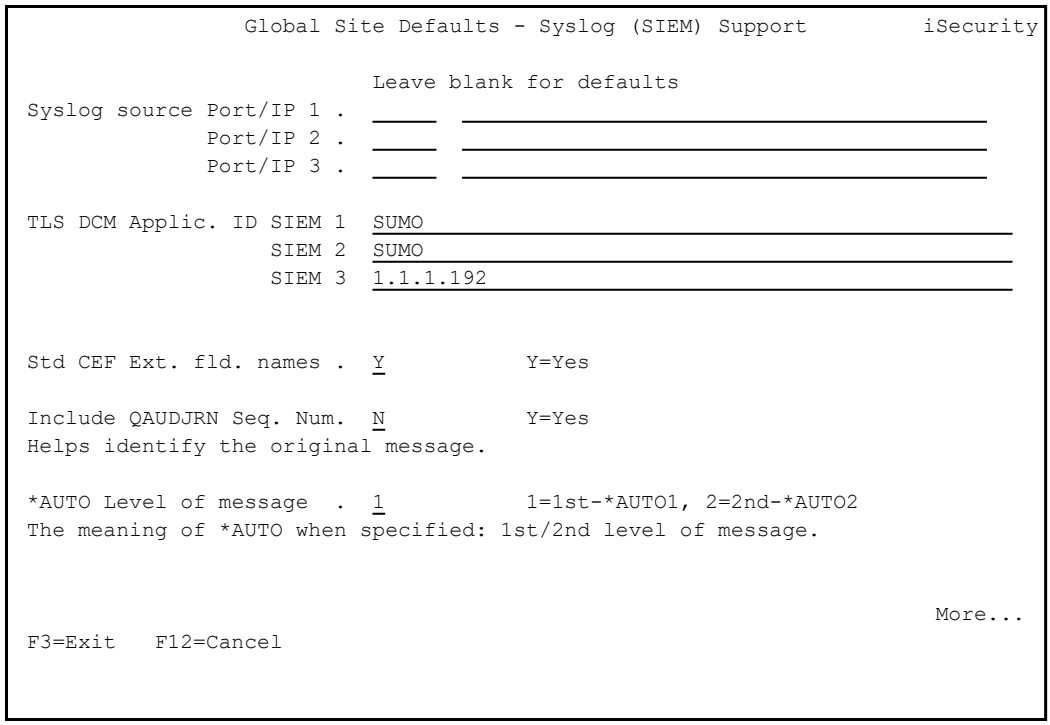
Set SPLF attribute to query name

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 50 pixels tall, at 120 DPI.

Syslog (SIEM) Support



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

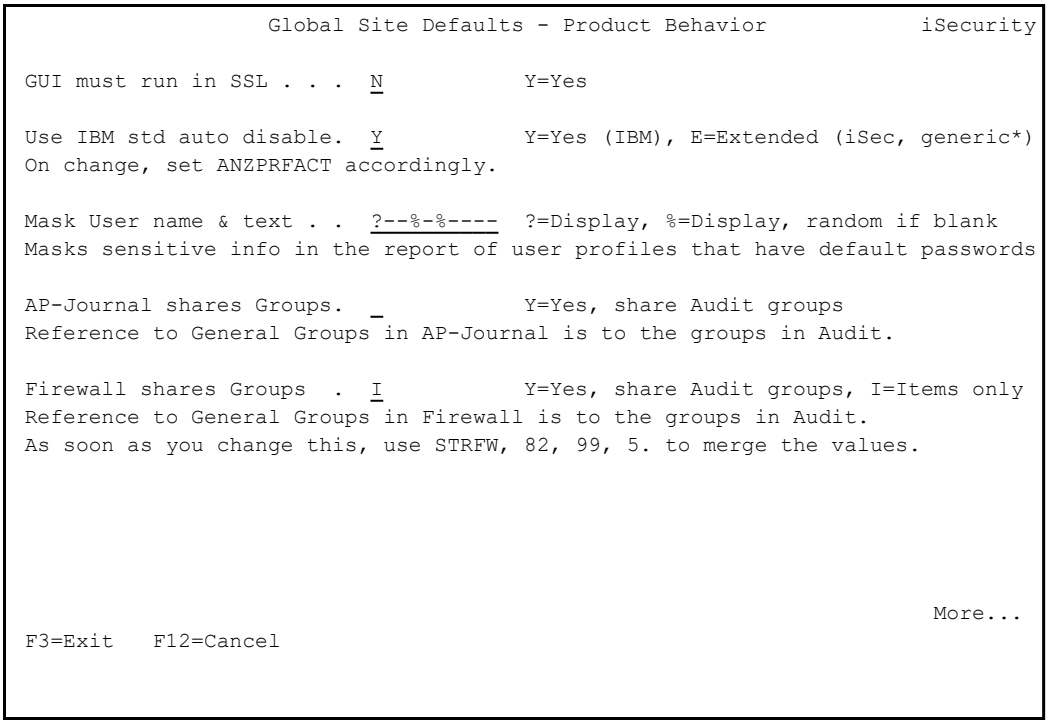
***AUTO Level of message**

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

1=1st-*AUTO1

2=2nd-*AUTO2

Product Behavior



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

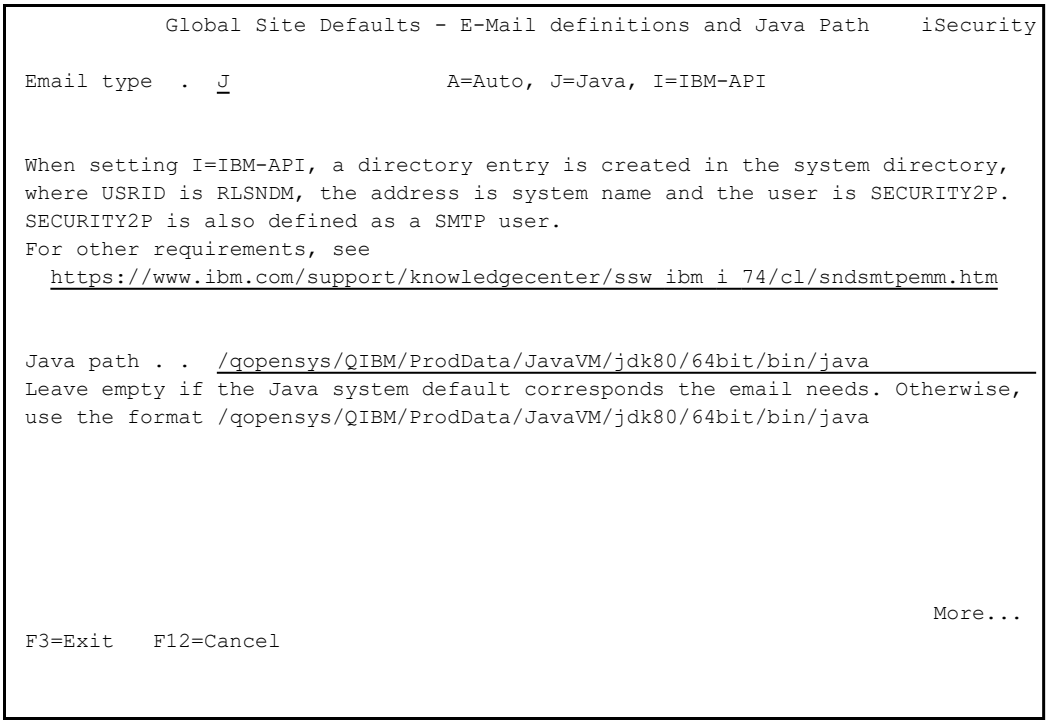
Whether references to General Groups in AP-Journal are to the groups in Audit.

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



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

Email type

A: Auto

J: Java

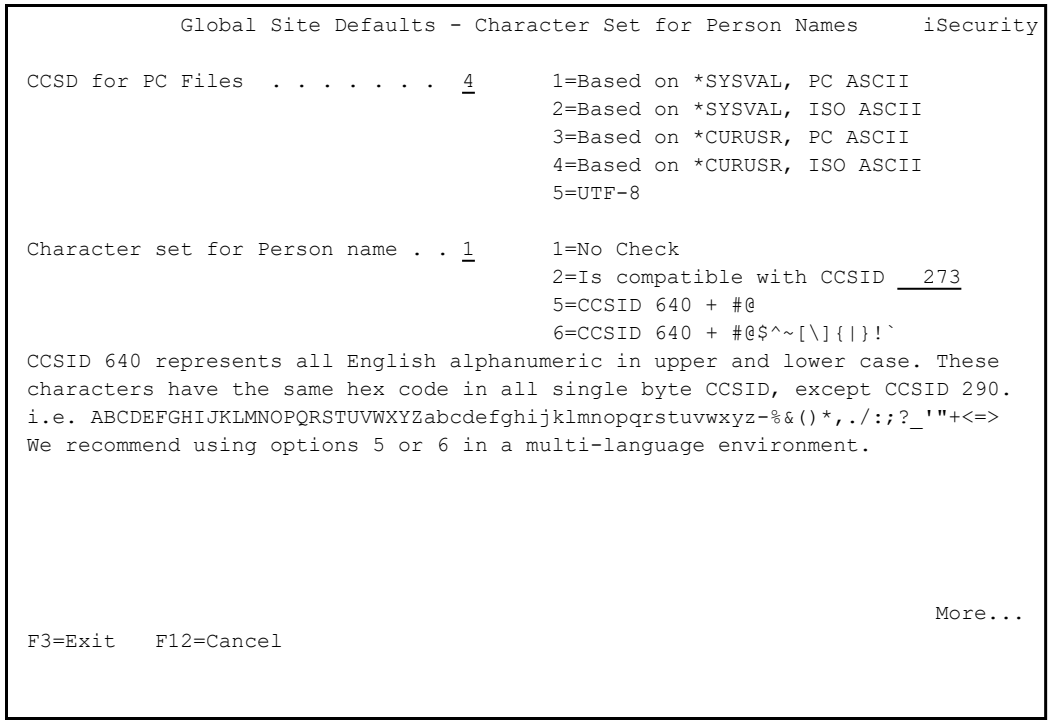
I: IBM-API

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

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 CCSID



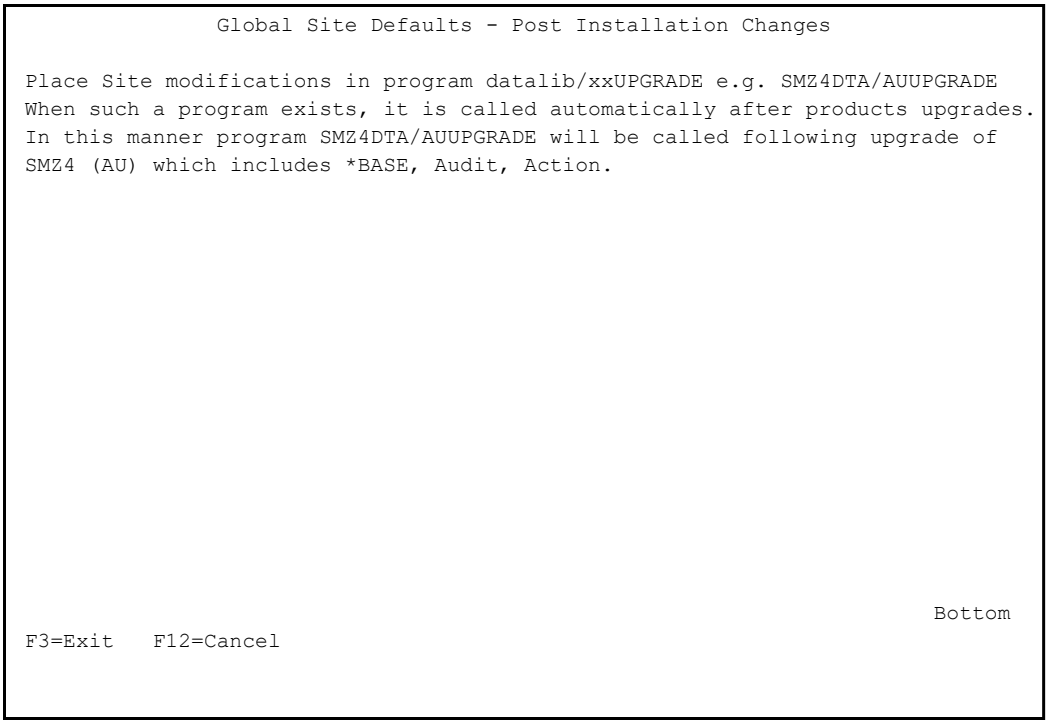
To define the character set for PC Files, enter the value corresponding to the set in the **CCSD for PC Files** field:

- **1**: SYSVAL, PC ASCII
- **2**: SYSVAL, ISO ASCII
- **3**: CURUSR, PC ASCII
- **4**: CURUSR, ISO ASCII
- **5**: UTF-8

To define the character set for Person names, enter the value corresponding to the set in the **Character set for Person 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



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#STRRTAU AU#STRRTMG	SMZ4, SMZ4DTA, SMZTMPA, SMZTMPB, SMZTMPC /iSecurity /smz4 /snmp	AU#MNT AU@DAILY AU@DAILYGU AU@DAILYHT	SECURITY2P
Firewall / SIEM (FW) Screen Password Command	STRFW STRSCN STRPWD STRCMD	GS#FIREWAL	SMZ8, SMZTMPA, SMZTMPB, SMZTMPC	GS#MNT GS@DAILY GS@DAILYGU GS@DAILYHT	SECURITY1P
AP-Journal / SIEM Safe Update (SU)	STRJR STRSU	JR#STRRTJR	SMZJ, SMZJDTA (SMZTMPC)	JR#MNT JR@DAILY	SECURITY4P
Authority On Demand / SIEM (AOD) Password Reset (PR)	STRAOD STRPWDRST		SMZO, SMZODTA (SMZTMPC)	OD#MNT OD@RMVEM	SECURITY8P FORGOT
Capture	STRCPT		SMZC, SMZCDTA, SMZTMPA, SMZTMPB	CP#MNT	SECURITY7P
Change Tracker	STRCT		SMZT, SMZTDTA, SMZ4,	CT#MNT	SECURITYTP

			SMZ4DTA SMZTyymmdd		
Advanced Threat Protection Antivirus Anti-Ransomware Object Integrity Control	STRATP STRAV STRAR STROBJITG		SMZV, SMZVDTA /smzvdta /snmp	AV$UPDDFN AV#MNT AV@NTV	SECURITY5P
Encryption (FIELD) (FILE)	STRENC STRPGP		SMZE, SMZEDTA	EN#MNT EN#WATCH	SECURITYEP
DB-Gate	STRDB		SMZB, SMZBDTA	DB#MNT	SECURITYBP

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	

Restricted State and iSecurity Products

Performing a full system backup or maintenance tasks, such as installing/upgrading IBM i software, requires the system to enter a restricted state. In this mode, all subsystems are ended, and only essential operations are allowed.

Most iSecurity products, including Antivirus, Anti-Ransomware, Audit, Firewall, Capture, Authority-On-Demand, Password Reset, Multi-Factor Authentication, etc., rely on active subsystems to function. These products cannot operate correctly once the system enters a restricted state.

To prevent issues during system saves or upgrades:

before moving to a restricted state, **deactivate the iSecurity product**.

after exiting a restricted state, **activate the iSecurity product**.

NOTE: For detailed instructions on how to properly activate or deactivate iSecurity products, refer to the product-specific user guides available on the

https://razlee.com/documentation-manuals/.

More About IBM i Restricted State

For more information about a restricted state in IBM i, refer to the official IBM documentation:

- IBM i Restricted State - Concept Overview

  https://www.ibm.com/docs/en/i/7.6.0?topic=concepts-i-restricted-state
- Putting Your IBM i System into Restricted State

  https://www.ibm.com/docs/en/i/7.6.0?topic=system-putting-your-in-restricted-state
- Placing IBM i in Restricted State via Subsystems
  https://www.ibm.com/docs/en/i/7.6.0?topic=subsystems-placing-system-in-restricted-state