iSecurity Installation

Installing and Upgrading iSecurity Software

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

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

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

Native IBM i (OS/400) User Interface

Installation 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

COMMAND **> 81 > 32**

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

Menus

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

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

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

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

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

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

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

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)

Contents

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 Products on IASP

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

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

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

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

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

OS400 also requires that object types *JOBQ, *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 on IASP

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

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

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

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

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

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

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

   *CRTDTAARA DTAARA(SMZTMPC/-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      ' IASP33    IASP33                                  '
  50      '                                                   '
 100      '                                                   '
 150      '                                                   '
 200      '                                                   '
 250      '                                                   '
 300      '                                                   '
 350      '                                                   '
 400      '                                                   '
       More...
Press Enter to continue.

F3=Exit   F12=Cancel
```

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

   If this is an upgrade:

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

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

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

Pre-Requisites

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

Preparation

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

The Installation and Upgrade Process

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

```
DSPDTAARA SMZ4/AUREL
```

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

If this command fails, this is a first time installation. Proceed to Installing from a Link.

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

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

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

These commands should display any locks that affect Audit.

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

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

Deactivation of the Product

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

Installing from a Link

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

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

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

You should now enter:

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

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

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

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

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

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

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

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

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

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

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

For additional information, see "iSecurity Environmental Change Considerations" on page 78.

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

iSecurity/*BASE

iSecurity/*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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

iSecurity/*BASE

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

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

1. **WRKOBJLCK SMZ8 *LIB**
2. **WRKOBJLCK SMZ8DTA *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 78.

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) and Password Reset

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

Pre-Requisites

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

iSecurity/*BASE

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

To ensure that iSecurity/*BASE is installed, enter

```
DSPLIB SMZ4
```

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

Preparation

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

The Installation and Upgrade Process

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

```
DSPDTAARA SMZO/ODREL
```

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

If this command fails, this is a first time installation. Proceed to Installing from a Link.

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

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

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

These commands should display any locks that affect AOD.

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

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

Deactivation of the Product

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

Installing from a Link

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

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

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

You should now enter:

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

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

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

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

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

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

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

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

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

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

For additional information, see "iSecurity Environmental Change Considerations" on page 78.

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

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 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/ARI ('*SAVF' 'AR' "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 78.

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/ARI ('*SAVF' 'AR' '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.

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/Capture

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

Pre-Requisites

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

iSecurity/*BASE

iSecurity/*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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

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

Recovering from a Failed Installation

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

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

Once resolved, run the procedure again.

Running the Procedure Again

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

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

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

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

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

Verifying that the new release is now installed.

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

Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

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

Activating the product

If this was a product upgrade, activate the product.

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

Optional Software

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

Installing and Upgrading iSecurity/Change Tracker

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

Pre-Requisites

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

iSecurity/*BASE

iSecurity/*BASE (also known as "Audit") is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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

iSecurity/*BASE

iSecurity/*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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

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

Recovering from a Failed Installation

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

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

Once resolved, run the procedure again.

Running the Procedure Again

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

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

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

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

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

Verifying that the new release is now installed

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

Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

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

Activating the product

If this was a product upgrade, activate the product.

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

Optional Software

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

Installing and Upgrading iSecurity/DB-Gate

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

Pre-Requisites

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

iSecurity/*BASE

iSecurity/*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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

iSecurity/*BASE

iSecurity/*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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

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

Recovering from a Failed Installation

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

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

Once resolved, run the procedure again.

Running the Procedure Again

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

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

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

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

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

Verifying that the new release is now installed

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

Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRFS** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the F22 (Shift-F10) key.

4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the FileScope main menu.

Activating the product

If this was a product upgrade, activate the product.

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

Optional Software

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

Installing and Upgrading iSecurity/CodeScope

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

Pre-Requisites

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

iSecurity/*BASE

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

To ensure that iSecurity/*BASE is installed, enter

```
DSPLIB SMZ4
```

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

Preparation

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

The Installation and Upgrade Process

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

```
DSPDTAARA SMZ6/CSREL
```

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

If this command fails, this is a first time installation. Proceed to Installing from a Link.

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

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

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

These commands should display any locks that affect CodeScope.

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

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

Deactivation of the Product

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

Installing from a Link

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

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

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

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

You should now enter:

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

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

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

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

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

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

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

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

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

For additional information, see "iSecurity Environmental Change Considerations" on page 78.

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

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

Recovering from a Failed Installation

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

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

Once resolved, run the procedure again.

Running the Procedure Again

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

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

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

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

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

Verifying that the new release is now installed

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

Authorization codes

The email may contain new authorization codes and a command.

Use the command to insert the codes.

Alternatively, manually enter them interactively:

1. Enter the **STRCS** command on the IBM i.
2. Select option **81. System Configuration**
3. Press the F22 (Shift-F10) key.

4. The cursor is moved to two fields that are now opened for entry. The authorization code is composed of one or two parts. Enter them from left to right. Each part is left justified.
5. Press **Enter** several times to return to the CodeScope main menu.

Activating the product

If this was a product upgrade, activate the product.

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

Optional Software

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

Installing and Upgrading iSecurity/WideScope

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

Pre-Requisites

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

iSecurity/*BASE

iSecurity/*BASE (also known as “Audit”) is a software product that must be installed to provide the foundation layer for iSecurity products. It does not have to 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 78.

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 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,	CT#MNT	SECURITYTP

			SMZ4, 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