# iSecurity Authority on Demand

## User Guide
## Version 6.01

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 Authority on Demand 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

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

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

## Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

***STRAOD*** **> 81 > 32**

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

## Menus

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

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

## Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

## Legal Notice

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

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

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

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



## 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)

# IBM i Authority on Demand

## Overview

Emergency access to critical application data and processes is one of the most common security slips which is uncovered in System i (AS/400) audits. Currently, manual approaches to this problem are not only error-prone, but do not comply with regulations and auditors' stringent security requirements.

Authority on Demand (AOD) enforces segregation of duties and enables relevant personnel to obtain access to approved information when needed, thereby saving valuable time and resources. AOD's real time audit of access rights protects sensitive corporate assets and significantly reduces the number of profiles with excessive special authorities.

AOD was developed because of numerous requests from iSecurity customers worldwide. In direct response to the growing security-related concerns of different-sized enterprises, Raz-Lee now offers a solution which allocates special authorities on an "as-needed" basis, while at the same time tightening controls over the allocation of these special authorities using advanced logging and reporting facilities.

# Workflow

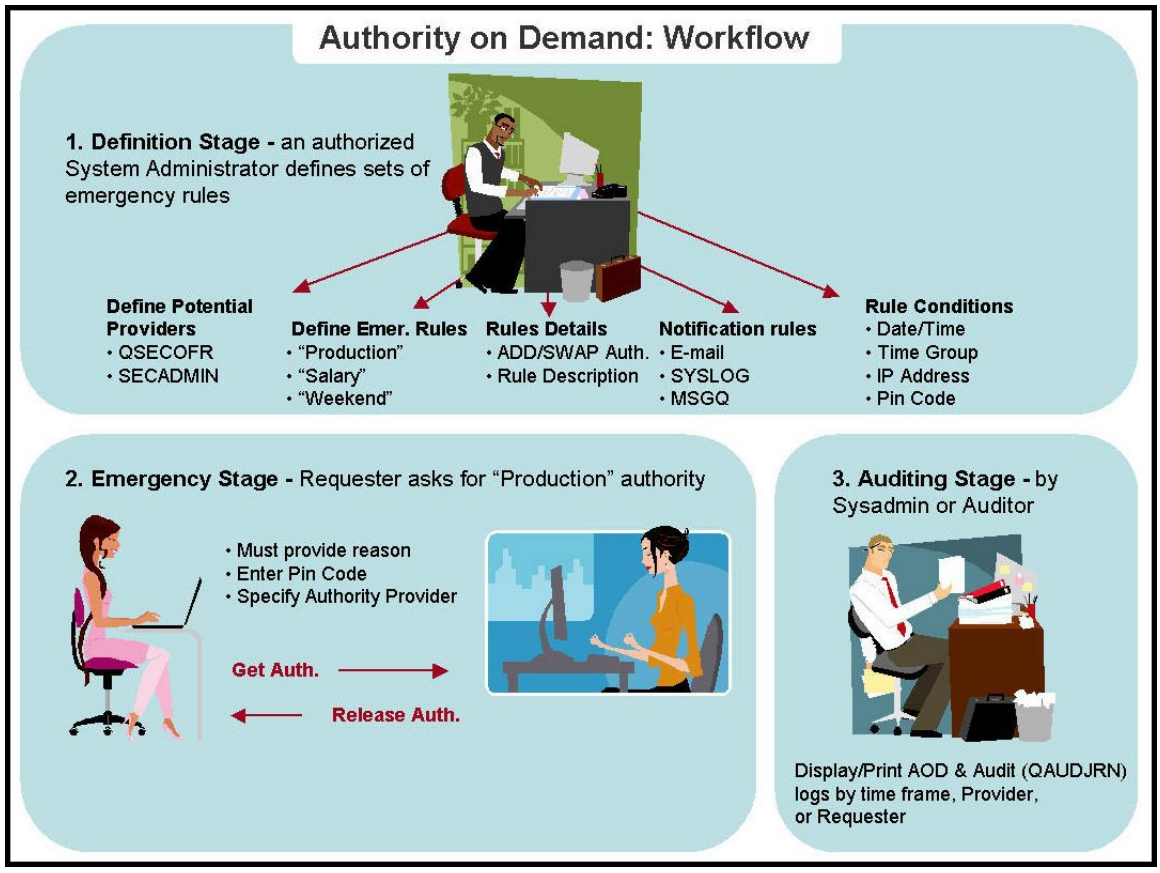



Figure 1: Workflow

# Authority on Demand Features

## Easy-to-Use

AOD simplifies the process of granting special authorities when necessary, and incorporates easy-to-use reporting and monitoring mechanisms to ensure that this extremely sensitive and potentially dangerous capability is not misused.

## Add or Swap Security Levels

AOD can either grant a Requester a totally new security authority level (SWAP) or add additional security rights to a Requester's original security level (ADD) - a feature totally unique to AOD.

## Authority Transfer Rules & Providers

AOD allows for pre-defining special authority "providers" and special authority transfer rules in accordance with specific site security policies.

## Safe Recovery from Emergency Situations

AOD enables you to recover from different types of emergency situations with a minimum risk of human error. For example, AOD can allow Ad Hoc access to critical data; it can enable a programmer to run reports that ended abnormally, and so on.

## Full Monitoring Capabilities

AOD logs and monitors all relevant activities so that managers can receive regular audit reports of AOD activity as well as real time e-mail alerts when employees request higher authority.

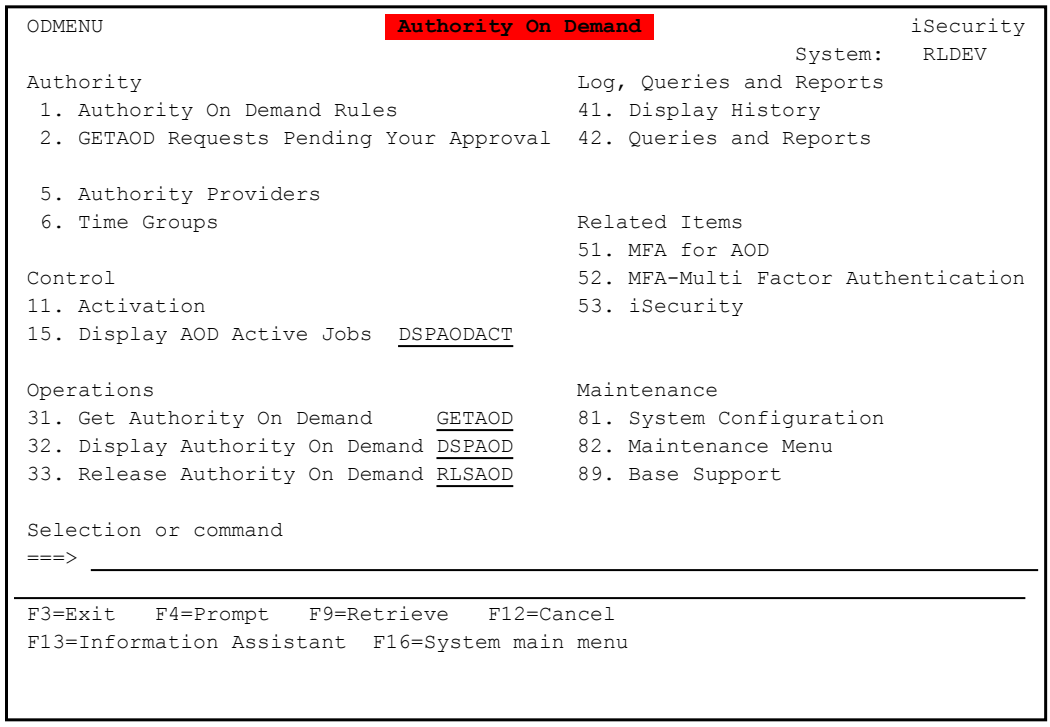
## Full Monitoring Capabilities

AOD logs and monitors all relevant activities so that managers can receive regular audit reports of AOD activity as well as real time e-mail alerts when employees request higher authority.

# Getting Started

This chapter guides you through the steps necessary to begin using **Authority on Demand** for the first time. Also covered in this chapter are the basic procedures for configuring the product for day-to-day use.

To start working with **Authority on Demand**, type ***STRAOD***. The Main menu appears.



# Operators

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

There are three default groups:

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

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.

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

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

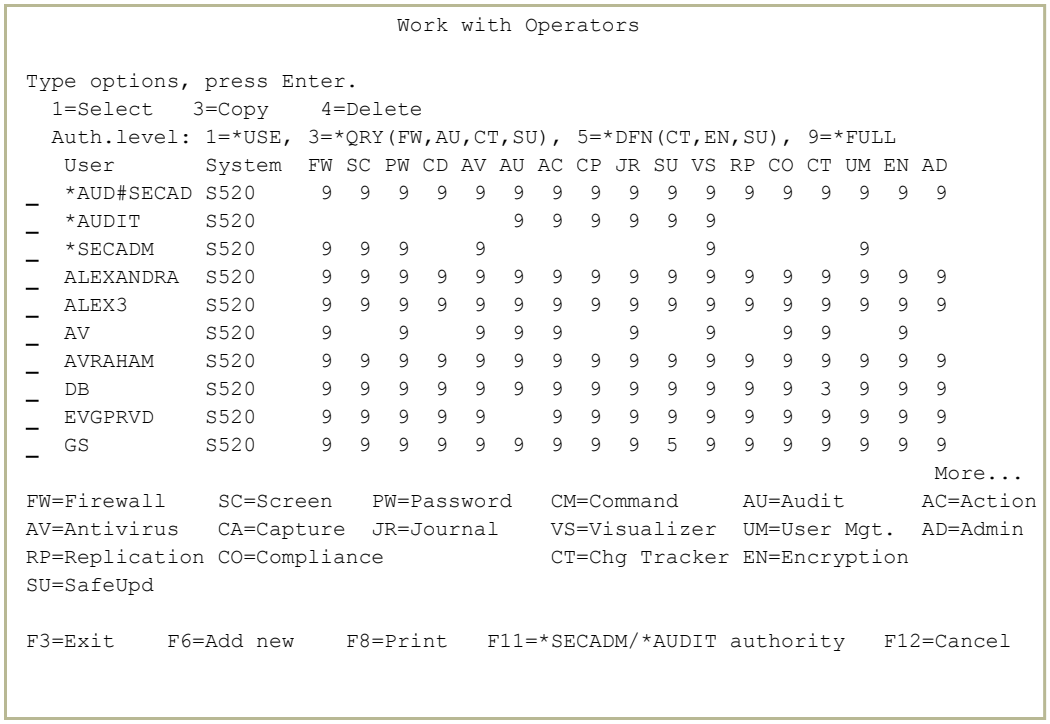
***CRTDTAARA SMZTMPC/DFTPWD *char 10***

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.

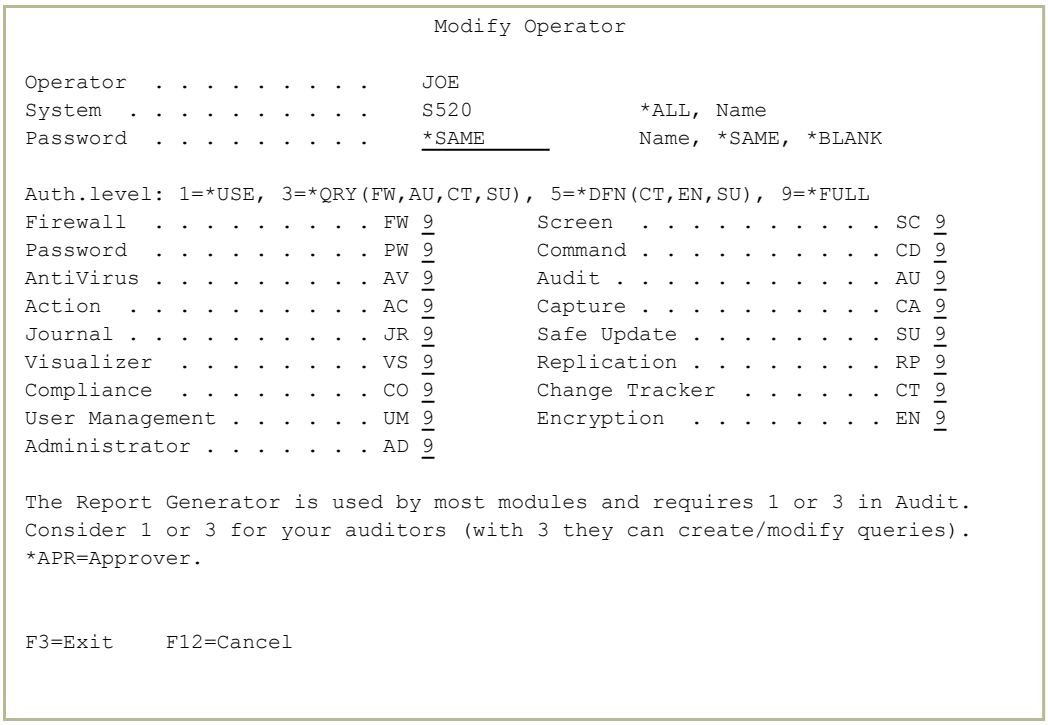
To modify operators' authorities:

1. Select **89. BASE Security** from the **Main Menu**. The **BASE Security** menu appears.
2. Select **11. Work with Operators** from the **BASE Security** menu. 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 UM EN AD
_  *AUD#SECAD S520     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
_  ALEXANDRA  S520     9  9  9  9  9  9  9  9  9  9  9  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
_  AV         S520     9     9     9  9  9     9     9     9  9     9
_  AVRAHAM    S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  DB         S520     9  9  9  9  9  9  9  9  9  9  9  9  9  3  9  9  9
_  EVGPRVD    S520     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
                                                                   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 EN=Encryption
SU=SafeUpd

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

3. 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 the password for the operator. Set it to ***SAME** to make it the same as the password for the previous operator that was set, or to ***BLANK** to have no password.

Set the numeric field for each module to one of these values:

**1 = Use**

Read authority only

**4 = Limited *EMERGENCY**

Can enable or modify emergency rules, but not change PIN codes.

**5 = *EMERGENCY**

Can enable or change emergency rules.

**8 = Limited *FULL**

Read and Write authority, cut cannot change PIN codes.

**9 = *FULL**

Full Read and Write authority

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/modifying queries.

4. Set authorities and press **Enter**. A message is prompted informing that the user being added/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.

***ALL** ***PUBLIC** ***EXCLUDE**

## Work with Operators for Authority on Demand

In addition to the standard iSecurity definition of operators (as shown in the iSecurity Installation & Base Support Manual), Authority on Demand uses specific definitions, primarily related to emergency rules (as shown in "Emergency Rules" on page 77).

To establish these definitions, select **12. Work with AOD, P-R Operators** in the BASE Support menu (*STRAOD*> **89 > 12**). The **Work with Operators** screen appears.

```
                          Work with Operators

Type options, press Enter.
  1=Select   4=Delete
                   Authority level: 1=*USE   9=*FULL
Opt User           System    AOD PR  USP  Adm
 _   *AUD#SECAD    S520        9   9    9    9
 _   ALEX          S520        9   9    5    9
 _   AV            S520        9             9
 _   AVI           S520        9   9    9    9
 _   JAVA2         S520        9   9    9    9
 _   NISSIMM       S520        1   1    1    1
 _   NIV           S520        9   9    9    9
 _   OD            S520        9   9    9    9
 _   OS            *ALL
 _   TEST          S520        9   9    9    9
 _   TZION         S520        9   9    9    9
 _   VICTOR        S520        9   9    9    9
                                                                      More...
AOD=Authority on Demand   PR=Password Reset    USP=User Provisioning
                                               Adm=Administrator
F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

The body of the screen contains lines that show users on specific systems (or ***ALL**) and their authority levels for various programs, including, in the **AOD** column, Authority on Demand.

To **view and modify** these authorities, enter **1** in the **Opt** column of that line. The **Modify Operator** screen appears.

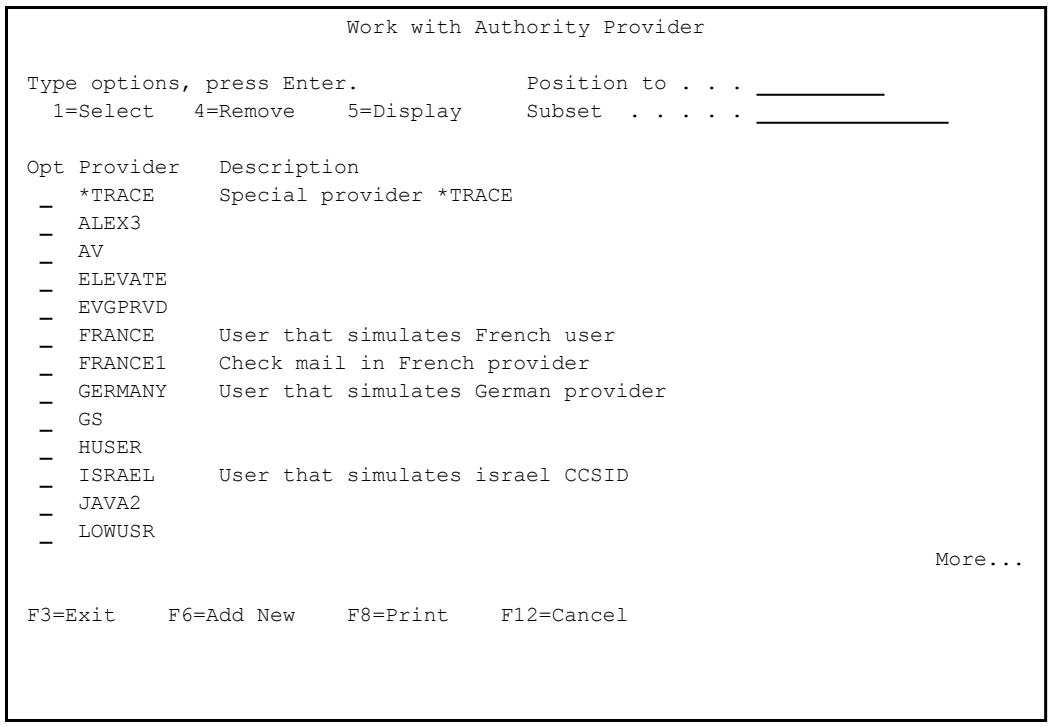
```
                              Modify Operator

Type choices, press Enter.

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

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

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

F3=Exit    F12=Cancel
```

The Authority on Demand field contains a numeric value representing these sets of authorities:

- **1**: ***USE** Can use rules but not change them.
- **4**: **Limited *EMERGENCY** Can modify emergency rules, but cannot change their PIN codes.
- **5**: ***EMERGENCY** Can modify emergency rules, including their PIN codes.
- **8**: **Limited *FULL** Can modify all rules, but cannot change their PIN codes.
- **9**: ***FULL** Can modify all rules, but cannot change their PIN codes.

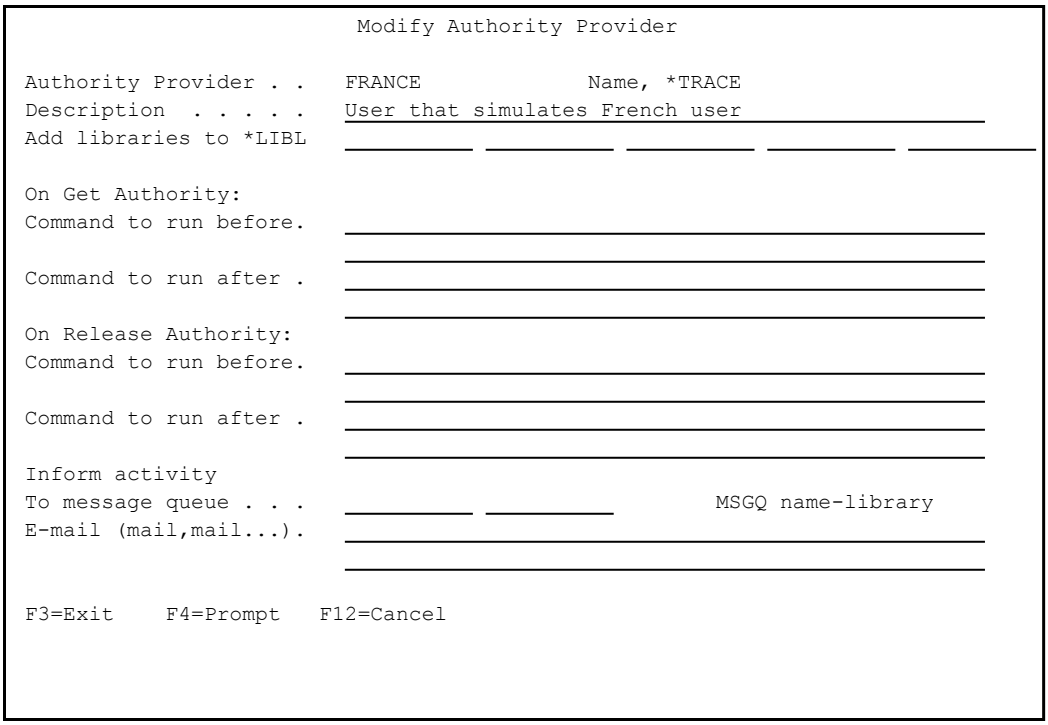
# Authority Provider

1. Select **5. Authority Providers** from the main menu. The **Work with Authority Provider** screen appears. This screen shows a list of user authorization definitions that can be applied on demand to another user profile.



```
                          Work with Authority Provider

Type options, press Enter.              Position to . . . _________
  1=Select   4=Remove    5=Display      Subset  . . . . . _______________

Opt Provider   Description
 _  *TRACE     Special provider *TRACE
 _  ALEX3
 _  AV
 _  ELEVATE
 _  EVGPRVD
 _  FRANCE     User that simulates French user
 _  FRANCE1    Check mail in French provider
 _  GERMANY    User that simulates German provider
 _  GS
 _  HUSER
 _  ISRAEL     User that simulates israel CCSID
 _  JAVA2
 _  LOWUSR
                                                                    More...

F3=Exit    F6=Add New    F8=Print    F12=Cancel
```

2. Type **1** to select an authority Provider for modification, or press **F6** to add a new authority Provider.




The body of the screen includes these fields:

**Authority Provider**

Type an existing user profile as Authority Provider or press F4 to prompt a list of users for selection.

**Description**

A free-form text description.

**Add libraries to *LIBL**

Add additional libraries access authorization to *LIBL. Type in a list of libraries separated by a space. These libraries are added to *LIBL before the Authority on Demand session starts and are removed from *LIBL when the session ends.

**On Get Authority**

**Command to run before**

The name of a program to execute immediately before the new authorization is applied.

**Command to run after**

The name of a program to execute immediately after the new authorization is applied.

**On Release Authority**

**Command to run before**

The name of a program to execute immediately before the new authorization is released.

**Command to run after**

The name of a program to execute immediately after the new authorization is released.

**Inform activity**

**To message queue**

The name and library of a MSGQ to receive notification of when the new authorization takes effect.

**Email**

Email addresses to receive notification of when the new authorization takes effect. Separate the addresses with a comma.

4. Define an informative action that will execute when the new authorization takes effect. Select interactive or batch mode for sending a message, send to a MSGQ and/or an email address.

# Authority Rules

To set Authority on Demand rules, select **1. Authority on Demand Rules** from the main menu. The **Work with Authority Rules** screen appears.

```
AOD-Admin JOE            Work with Authority Rules                  RLDEV

Type options, press Enter.
  1=Select  3=Copy  4=Remove  5=Display    Position to . . . _________
  X=Select for Export                      Subset  . . . . . _______________

Opt Provider   Requester  System   Auth.by
 _  *TRACE     AA100      *ALL     Trace   qwqew
 _  *TRACE     AA200      *ALL     Trace   wrwr
 _  *TRACE     EVGTST     *ALL     Trace   test
 _  *TRACE     VICTOR     *ALL     Trace   self trace test
 _  ALEX3      LOWUSR     *ALL     Swap    aaaaa
 _  ALEX3      TEST       *ALL     GlbSpc  test
 _  AV         QSECOFR    *ALL     Swap    test
 _  EVGPRVD    *ANY       *ALL     Add     WEWRWR
 _  EVGPRVD    EVGTST     *ALL     Swap    Evgeny test
 _  EVGPRVD    LOUSRRX    *ALL     GlbSpc  Low user for 26 min only
 _  FRANCE     *ANY       *ALL     Add     Check mail to French provider
 _  FRANCE     OD         *ALL     Add     asd
                                                                  More...
You can define regular or Emergency rules.
Rules that require Approval displayed in column 'Auth.by' in white.
F3=Exit    F6=Add New    F7=Add Emergency    F8=Print    F12=Cancel
```

The body of the screen contains a line for each existing rule. Each line contains the following fields:

**Provider**

The username providing the expanded authority. For a rule that only traces activity rather than changing authority, set this to ***TRACE**.

**Requester**

The username requesting the expanded authority. To make the rule available to anyone, set this to ***ANY**.

**System**

The system on which this rule can be run. To allow it to run on any system, set this to ***ANY**.

**Auth by**

How authority is provided, as shown in more detail for the Provide Authority by field on the Add Authority Rules screen, shown below. The values shown here correspond to values in that field:

- **Add**: Add authority
- **GlbSpc**: Add *SPCAUT globally
- **Swap**: Swap profile
- **Trace**: Trace activity but do not change authority
- **AddSpc**: Add *SPCAUT by session

**(Unlabeled: Description)**

A free-form description of the rule.

To copy a rule, see "Copying Authority Rules" on page 28.

To export a rule, see "Exporting Authority Rules" on page 31.

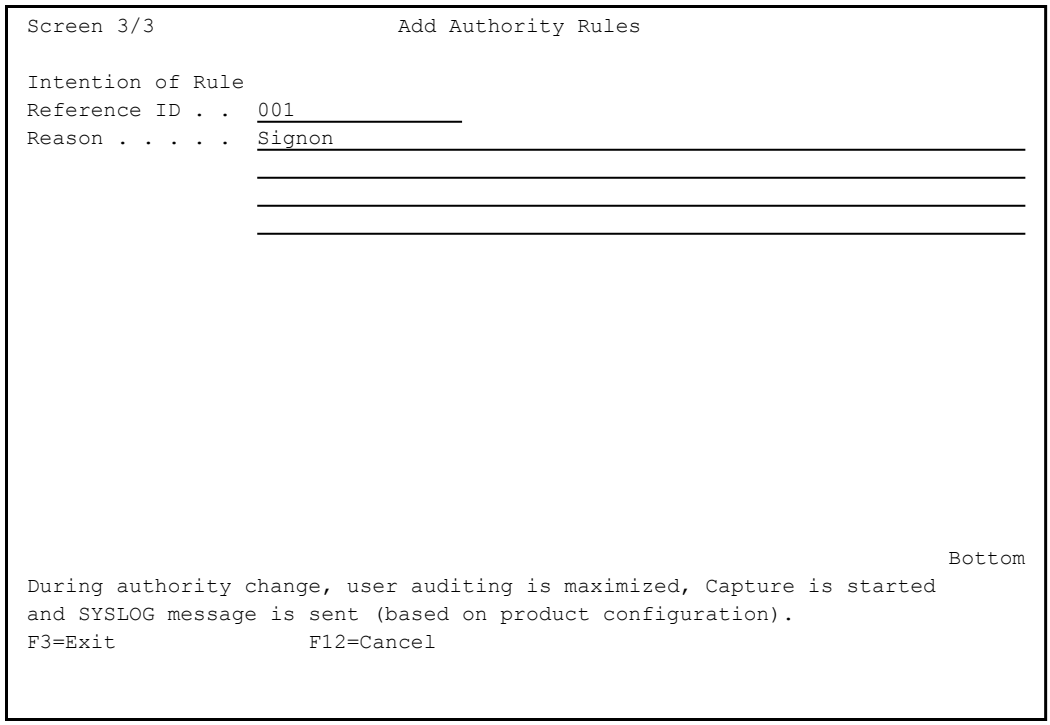
To add a rule, press the F6 key. The Add Authority Rules screen appears.

To add an emergency rule, press the F7 key. The Add Authority Rules screen appears with a red banner saying ***Emergency Use Only***. Only user profiles with emergency operator authority (as shown in "Operators" on page 12) are allowed to change emergency rules.

To modify a rule, enter **1** in the **Opt** field for that rule. The Modify Authority Rules screen appears, which is effectively the same as the Add Authority Rules screen.

```
Screen 1/3                  Add Authority Rules

Requester / *ANY . . .  *ANY          If GrpPrf: Accept for its members Y Y=Yes
Provider / *TRACE  . .  *TRACE
System . . . . . .  *ALL          Name, *ALL
Rule description . . .  Title of Rule                                  
Number of uses left  .  90            0-98, 99=*NOMAX

Real-Time Approval
Request from . . . . .  __________    UsrPrf/GrpPrf, *SECADM, *AOD-ADMIN

Authentication
Authenticate user by .  0             0=No, 1=Pin Code, 2=MFA, 3=Both
            Pin code.  _________
            MFA Type.  _              1=Cell, 2=Email, 3=Both
Perform                               By Session        Globally
Provide authority by .  1             1=Add authority
                                      2=Swap profile
                                      3=Add *SPCAUT     9=Add *SPCAUT
                                      4=Trace
                                                                  More...

F3=Exit   F4=Prompt   F12=Cancel
```

```
Screen 2/3                  Add Authority Rules

Restrictions              N=Not
Time group (week schedule)  _     __________
IP Address . . . . . .  _     ________________ Subnet mask: ________________
Maximum work time  . . . .  _30             Minutes, 0=*NOMAX
Allow next use after . . .  _0              Minutes, 0=Allow consecutive uses

Rule becomes active on . .  _1/01/01_ _0:00_
Usage is permitted until .  31/12/99 23:59

Inform activity
E-mail (mail,mail...)  . .  *PROVIDER                                      
                            ____________________________________________
Message Queue  . . . . . .  *PROVIDER  __________        MSGQ name-library

                                                                  More...
F3=Exit   F4=Prompt   F12=Cancel
```




The body of the screen includes these fields:

## Screen 1/3

### Requester / *ANY

The profile of the user who requested the authorization or ***ANY**. This field is mandatory.

### Provider / *TRACE

Type the name of the authority Provider, or press **F4** to obtain a list of users for selection. For a rule that only traces activity rather than changing authority, set this to ***TRACE**. This field is mandatory.

### System

The name of a specific system for which this rule will be valid. To make the rule valid for all systems in your organization, set this to ***ALL**.

### Rule Description

A meaningful description of the request for this temporary authorization. This field is mandatory.

**Number of uses left**

The number of times that this rule can be used. Valid values are from 0 to 98. Set the field to 99 to indicate that there is no maximum.

**Real-Time Approval**

**Request from**

The user who approved the request. Possible values include the User or Group profile, *SECADM, and *AOD-ADMIN.

**Authentication**

**Authenticate user by**

How to authenticate the user. Possible values include:

- **0** = None
- **1** = PIN Code (as entered below)
- **2** = MFA (as specified below)
- **3** = Both PIN Code and MFA

**PIN Code**

An added security passcode, a minimum of five digits long.

**MFA Type**

How the code is sent for Multi-Factor Authentication. Possible values include:

- **1** = Call
- **2** = Email
- **3** = Both Call and Email

**Perform**

How to add authority

**Provide authority by**

- **1 : Add authority**: Adds the Provider's authorities in addition to the Requester's existing authorities.
  - Current user: Requester
  - Object Authorities: Added
  - *SPCAUT: Added

    - *USRCLS: No change. (Operating system constraints do not allow for changes to *USRCLS.)
    - LMTCPB(): No change. (Operating system constraints do not allow for changes to LMTCPB.)
    - NOTE: Selecting this option gives the Requester the authorities of the Provider in addition to their existing authority. The original Requester user profile is kept and appears in records and logs.
    - NOTE: The Requester cannot be a group profile and the Provider cannot be a member of a group profile.
- **2 : Swap profile**: Replaces the Requester's authorities with the Provider's authorities.
    - Current user: Provider
    - Object Authorities: Provider
    - *SPCAUT: Provider
    - *USRCLS: Provider
    - LMTCPB(): Provider
    - NOTE: Selecting this option also swaps the user name in the records and logs.
- **3 : Add *SPCAUT by session**: Adds the Provider's *SPCAUT authorities only to the Requester's existing authorities. You cannot use this option with SBMJOB.
    - Current user: Requester
    - Object Authorities: No change.
    - *SPCAUT: Added
    - *USRCLS: No change. (Operating system constraints do not allow for changes to *USRCLS.)
    - LMTCPB(): No change. (Operating system constraints do not allow for changes to LMTCPB.)
    - NOTE: The Requester cannot be a group profile and the Provider cannot be a member of a group profile.
- **4 : Trace:** Trace activity without changing authority
- **9 : Add *SPCAUT globally**: Globally adds the Provider's *SPCAUT authorities only to the Requester's existing authorities. You cannot use this option with SBMJOB

- Current user: Requester
- Object Authorities: Added
- *SPCAUT: Added
- *USRCLS: Provider
- LMTCPB(): Provider

**Screen 2/3**

**Restrictions**

These sub-fields restrict the Time Group and IP address range for which the authority rule is valid. If the first, single-character sub-field is set to **N**, the selection is negated: the rule applies to everything except for the specified values.

**Time Group**

A named Time Group (as shown in "Time Groups" on page 39)

**IP Address / Subnet mask**

An IP address range within which the rule is in effect. Press F4 for a list of known IP address ranges.

**Maximum work time**

The maximum number of minutes for which the rule can be used without re-authorization. If set to **0**, there is no maximum.

**Allow next use after**

The number of minutes that must elapse between uses of the rule. If set to **0**, the rule can be used again immediately.

**Rule becomes active on**

A date and time, in **DD/MM/YY** and **HH:MM** format, respectively, at which the rule becomes effective.

**Usage is permitted until**

A date and time, in **DD/MM/YY** and **HH:MM** format, respectively, at which the rule becomes ineffective.

**Inform activity**

Destinations to inform when the rule is used.

**E-mail (mail, mail)**

Email addresses to be notified, separated by commas.

**Message Queue**

The name and library of a MSGQ. The default is the ***PROVIDER** MSGQ.

**Screen 3/3**

**Intention of Rule**

**Reference ID**

A unique, official ID referring to this rule. This field is mandatory.

**Reason**

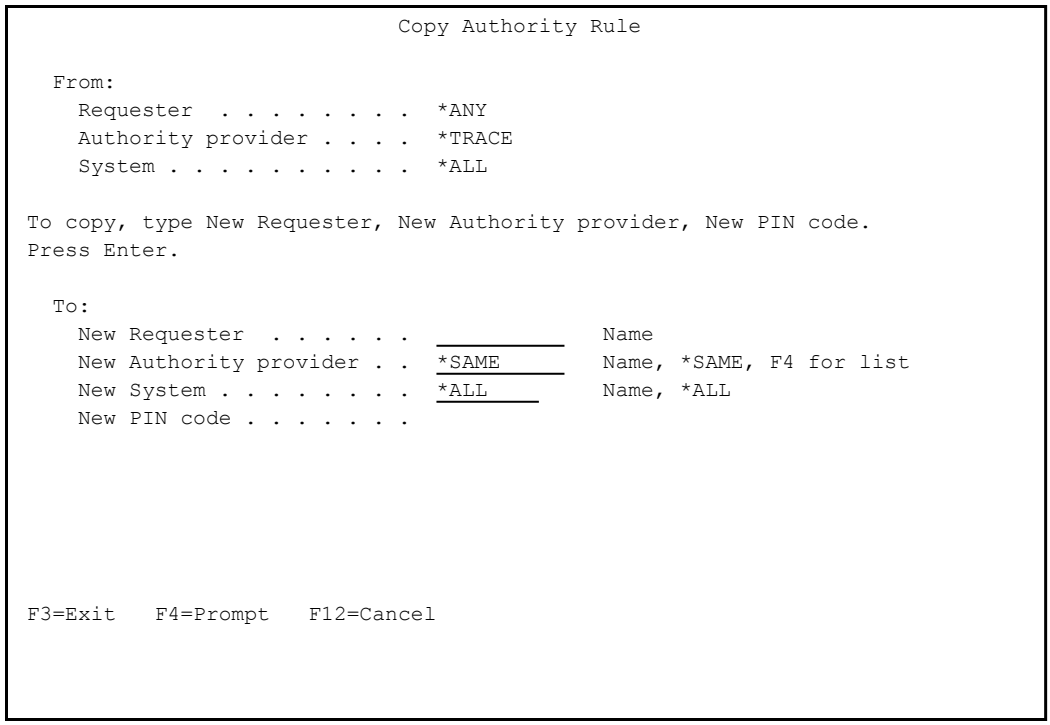
A meaningful description of the rule. This field is mandatory.

# Copying Authority Rules

To **`copy authority rules`**, open the **Work with Authority Rules** screen (*STRAOD* **> 1**) as shown in "Authority Rules" on page 20.

```
AOD-Admin JOE            Work with Authority Rules                  RLDEV

Type options, press Enter.
  1=Select  3=Copy  4=Remove  5=Display    Position to . . . _________
  X=Select for Export                      Subset  . . . . . _______________

Opt Provider   Requester  System   Auth.by
 _  *TRACE     AA100      *ALL     Trace   qwqew
 _  *TRACE     AA200      *ALL     Trace   wrwr
 _  *TRACE     EVGTST     *ALL     Trace   test
 _  *TRACE     VICTOR     *ALL     Trace   self trace test
 _  ALEX3      LOWUSR     *ALL     Swap    aaaaa
 _  ALEX3      TEST       *ALL     GlbSpc  test
 _  AV         QSECOFR    *ALL     Swap    test
 _  EVGPRVD    *ANY       *ALL     Add     WEWRWR
 _  EVGPRVD    EVGTST     *ALL     Swap    Evgeny test
 _  EVGPRVD    LOUSRRX    *ALL     GlbSpc  Low user for 26 min only
 _  FRANCE     *ANY       *ALL     Add     Check mail to French provider
 _  FRANCE     OD         *ALL     Add     asd
                                                                   More...
You can define regular or Emergency rules.
Rules that require Approval displayed in column 'Auth.by' in white.
F3=Exit    F6=Add New    F7=Add Emergency    F8=Print    F12=Cancel
```

Each line on the body of the screen represents an existing rule. To copy a rule, enter **3** in the **Opt** field for its line. The **`Copy Authority Rule`** screen appears.




The body of the screen includes these fields:

**From:**

The lines on the upper part of the screen show values for the rule that is being copied. These values are read-only.

**Requester**

The users who may request the change in authority.

**Authority Provider**

The user providing the authority.

**System**

The systems for which the rule is valid.

**To:**

The values for the new rule.

**New Requester**

The profile of the user who requested the authorization. This field is mandatory.

**New Authority Provider**

The name of the authority Provider, or press F4 to obtain a list of users for selection. This field is mandatory.

**New System**

The systems for which the rule is valid.

**New PIN Code**

An additional security password –minimum of five digits. This field is mandatory.

## Exporting Authority Rules

You can export individual Authority on Demand rules to other systems. You may want to do this when you have created a new rule on one of the computers in your organization and want it to be enforced on all the computers in the organization. You can export more than one rule in the same session. To export all the rules from one system to another system, see "Export Definitions" on page 84 and "Import Definitions" on page 89.

NOTE: You do not need to run an import process on the target computer. The rules are imported automatically.

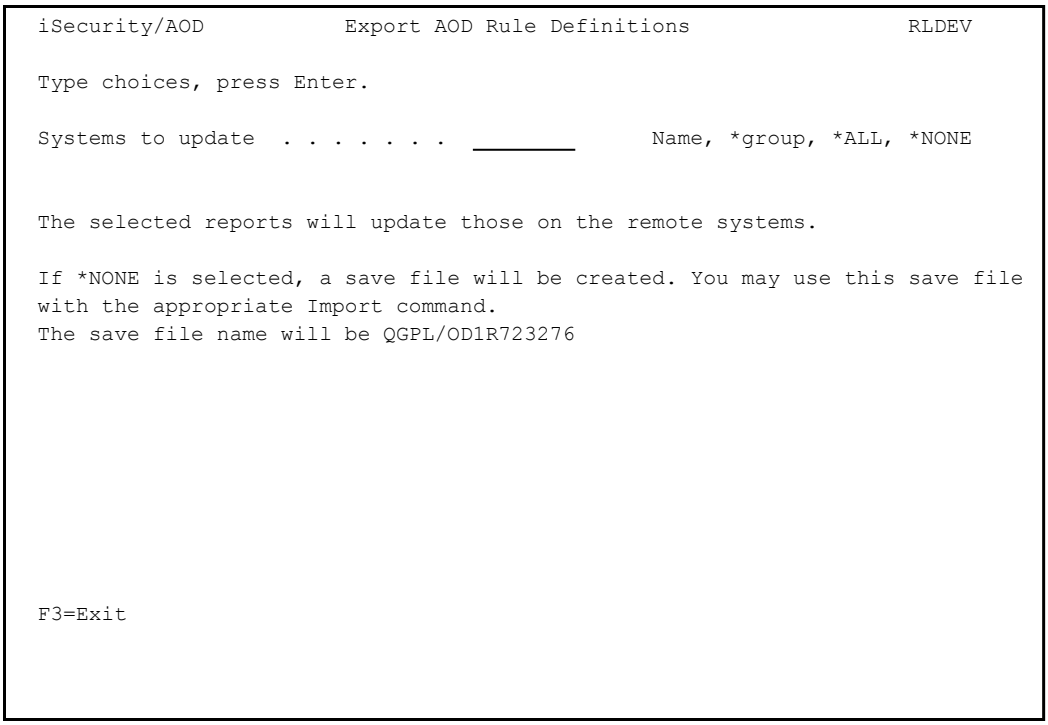
To **`export authority rules`**, open the **Work with Authority Rules** screen (*STRAOD* **> 1**) as shown in "Authority Rules" on page 20.

```
AOD-Admin JOE            Work with Authority Rules                  RLDEV

Type options, press Enter.
  1=Select  3=Copy  4=Remove  5=Display    Position to . . . _________
  X=Select for Export                      Subset  . . . . . _______________

Opt Provider   Requester  System   Auth.by
 _   *TRACE     AA100      *ALL     Trace   qwqew
 _   *TRACE     AA200      *ALL     Trace   wrwr
 _   *TRACE     EVGTST     *ALL     Trace   test
 _   *TRACE     VICTOR     *ALL     Trace   self trace test
 _   ALEX3      LOWUSR     *ALL     Swap    aaaaa
 _   ALEX3      TEST       *ALL     GlbSpc  test
 _   AV         QSECOFR    *ALL     Swap    test
 _   EVGPRVD    *ANY       *ALL     Add     WEWRWR
 _   EVGPRVD    EVGTST     *ALL     Swap    Evgeny test
 _   EVGPRVD    LOUSRRX    *ALL     GlbSpc  Low user for 26 min only
 _   FRANCE     *ANY       *ALL     Add     Check mail to French provider
 _   FRANCE     OD         *ALL     Add     asd
                                                                   More...
You can define regular or Emergency rules.
Rules that require Approval displayed in column 'Auth.by' in white.
F3=Exit    F6=Add New    F7=Add Emergency    F8=Print    F12=Cancel
```

Each line on the body of the screen represents an existing rule.

Enter **`X`** in the Opt field for each rule to be exported. A message appears at the bottom of the screen showing that the rule has been selected for export.

Press **`the F3`** or **`F12 keys`**. The **Export AOD Rules Definitions** screen appears:

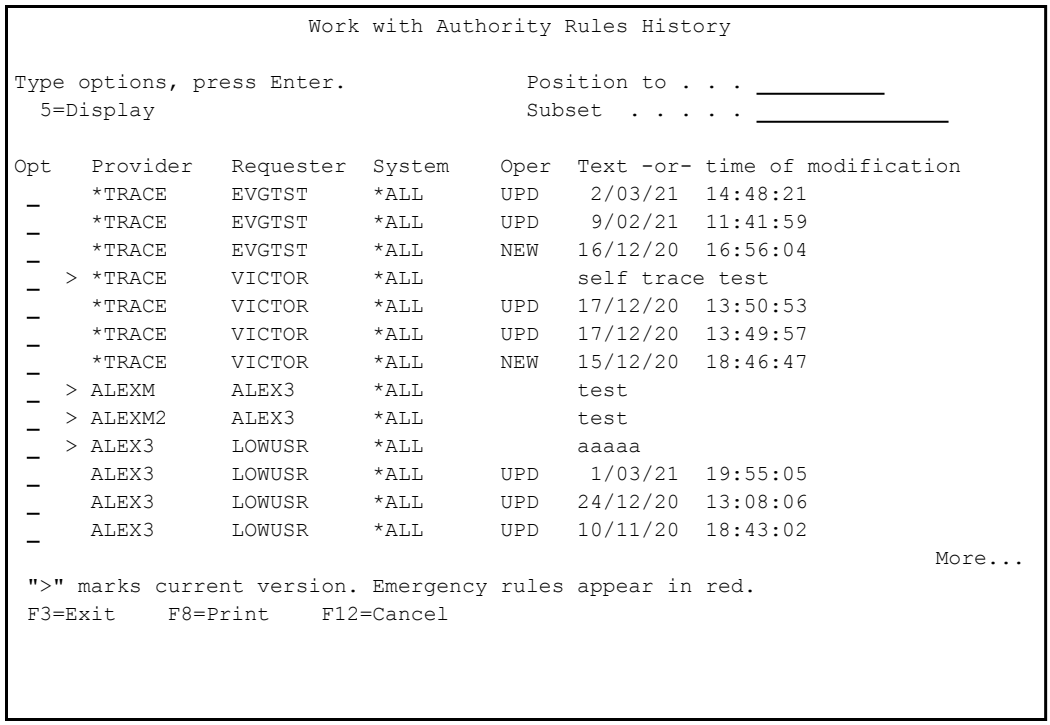



Enter the systems to which you will export the rules in the **Systems to update** field. Possible values include:

- A single system name
- A group containing multiple target systems
- ***ALL** for all systems in the organization
- ***NONE**: to prepare the set to import later (as shown in "Import Definitions" on page 89). A save file is created in **QGPL/OD1R723276** that you can then import into other systems.

## Rules History

To view the history of rules that have been applied, select **6. Display AOD Rules History** from the Maintenance Menu (*STRAOD*> **82 > 6**). The Work with Authority Rules History screen appears.



```
                    Work with Authority Rules History

Type options, press Enter.              Position to . . . _________
  5=Display                             Subset  . . . . . _______________

Opt   Provider   Requester  System    Oper  Text -or- time of modification
 _     *TRACE     EVGTST     *ALL      UPD    2/03/21  14:48:21
 _     *TRACE     EVGTST     *ALL      UPD    9/02/21  11:41:59
 _     *TRACE     EVGTST     *ALL      NEW   16/12/20  16:56:04
 _   > *TRACE     VICTOR     *ALL            self trace test
 _     *TRACE     VICTOR     *ALL      UPD   17/12/20  13:50:53
 _     *TRACE     VICTOR     *ALL      UPD   17/12/20  13:49:57
 _     *TRACE     VICTOR     *ALL      NEW   15/12/20  18:46:47
 _   > ALEXM      ALEX3      *ALL            test
 _   > ALEXM2     ALEX3      *ALL            test
 _   > ALEX3      LOWUSR     *ALL            aaaaa
 _     ALEX3      LOWUSR     *ALL      UPD    1/03/21  19:55:05
 _     ALEX3      LOWUSR     *ALL      UPD   24/12/20  13:08:06
 _     ALEX3      LOWUSR     *ALL      UPD   10/11/20  18:43:02
                                                                  More...
 ">" marks current version. Emergency rules appear in red.
 F3=Exit    F8=Print    F12=Cancel
```

The body of the screen contains a line for each instance of an application of the rules. Each contains the following fields:

**Provider**

The user providing access. For trace requests, this field shows ***TRACE**.

**Requester**

The user requesting access.

**System**

The system for which access was provided.

**Oper**

The most recent operation done with this access. Possible values include:

- **NEW**: New
- **UPD**: Update
- **DLT**: Delete

If the next field contains a text description, this field is left blank.

**Text -or- time of modification**

Either the time that the rule was applied or a text description of what was done.

To display the information about a single instance, enter **5** in the **Opt** field of that line. The first Display Authority Rules History screen appears. To move to the remaining two screens, press Enter.

The screens contain the following fields:

```
Screen 1/3           Display Authority Rules History

Last version

Requesting user  . . . . .  ALEX3        If *GRPPRF, accept for its members . Y
Authority provider . . . .  ALEXM
System . . . . . . . . . .  *ALL
Rule title . . . . . . . .  test

Verify by  . . . . . . . .  0            0=No, 1=PIN Code, 2=MFA, 3=PIN+MFA
PIN Code   . . . . . . . .  *********
Type of MFA (Multi-Factor)               0=No, 1=Cell, 2=Email, 3=Cell+Email

Requires Permission from .               User or Group Profile, *ADMIN

Perform                                  By Session        Globally
Provide authority by . . .  1            1=Add authority   7=Add authority
                                         2=Swap profile
                                         3=Add *SPCAUT     9=Add *SPCAUT
                                         4=Trace


F3=Exit    F8=Print    F12=Cancel    To next screen, press Enter.
```

All three screens begin with these fields:

**Last version**

If this update created the most recent version of the data, this field reads Last version.

Otherwise, it is blank, and a field above the other information fields shows the data and time of the change.

**Requesting user**

The name of the user requesting access. If a *GRPPRF, the access also includes its members.

**Authority provider**

The username providing authority.

**System**

The system for which access was provided.

**Rule title**

The name of the rule.

The rest of the fields differ by screen:

**Screen 1/3**

**Verify by**

How to verify the access. Possible values include:

- **0**: No verification
- **1**: PIN code (as shown in the **PIN Code** field)
- **2**: MFA: Multi-Factor Authentication (as shown in the **TYPE of MFA (Multi-Factor)** field)
- **3**: PIN+MFA: Both the PIN code and Multi-Factor Authentication

**PIN Code**

The PIN Code for verification. Shown masked.

**Type of MFA (Multi-Factor)**

The type of communication used for Multi-Factor Authentication. Possible values include:

- **0**: None
- **1**: SMS to cell phone
- **2**: Email
- **3**: Both SMS to the cell phone and Email

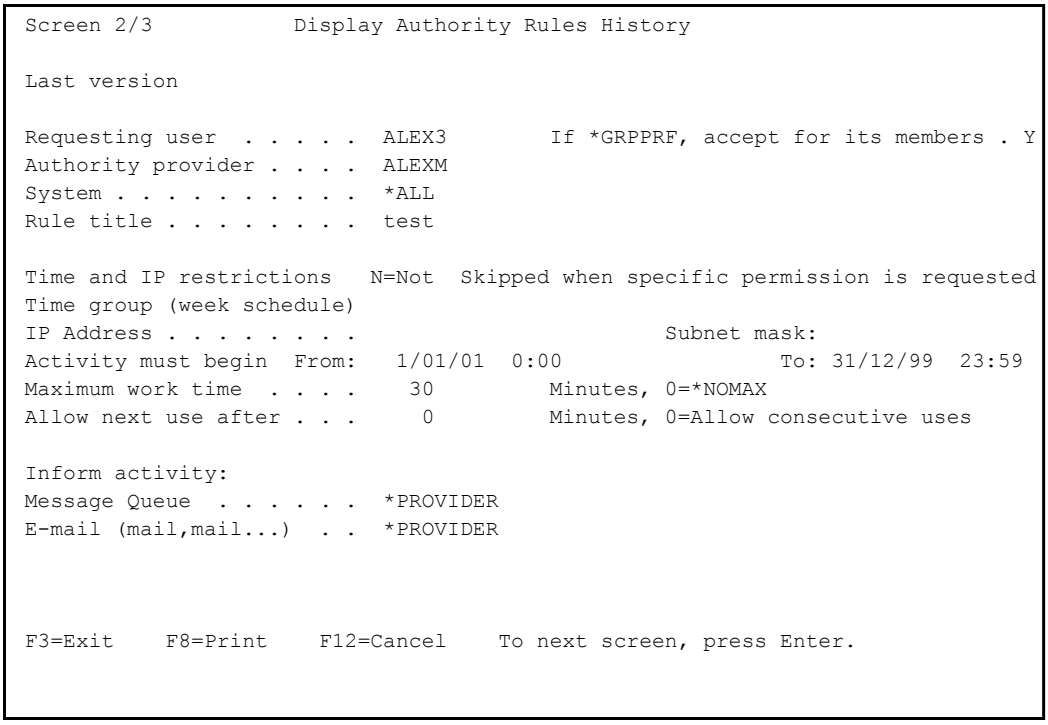
**Request Permission from**

Either a username or group profile, or ***ADMIN**.

### Provide authority by

How authority is provided. Possible values include:

- **1**: Add authority by session
- **2**: Swap profile by session
- **3**: Add ***SPCAUT** by session
- **4**: Trace
- **7**: Add authority globally
- **9**: Add ***SPCAUT** globally




## Screen 2/3

### Time group (week schedule)

The name of a time group (as shown in "Time Groups" on page 39) to which the authority is restricted. If preceded by N, the time group is excluded from the extended authority.

### IP address

The IP address and Subnet mask representing a range of addresses to which the authority is restricted. If preceded by N, the address range is excluded from the extended authority.

**Maximum work time**

The maximum amount of time from the start of the extended authority, after which the authority expires. If set to **0**, the authority never automatilcally expires.

**Allow next use after**

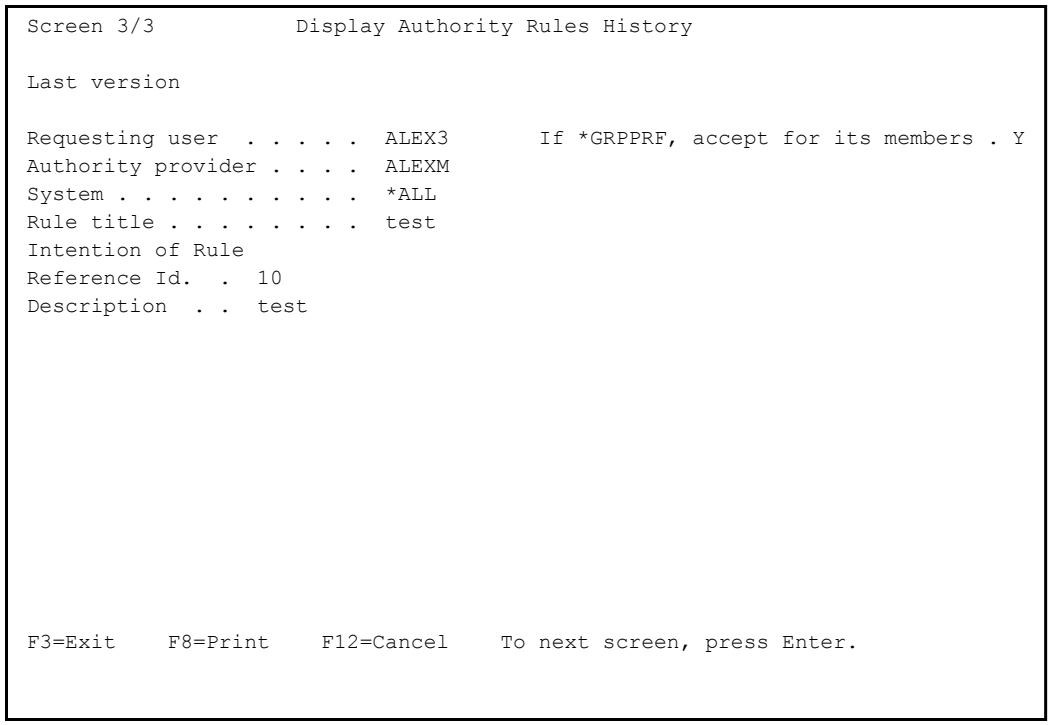
After a session of extended authority expires, the number of minutes that must pass before it can be restarted. If set to **0**, a new session can begin immediately.

**Message Queue**

A message queue to be notified of activity within the session.

**Email (mail, mail...)**

Email addresses, separated by commas, to be notified of activity within the session.




## Screen 3/3

**Reference ID**

A unique, official ID referring to this rule.

**Description**

A meaningful description of the rule.

# Time Groups

Using time groups, you can define both standard and non-standard working hours for your organization. Time groups are sets of time and day parameters that you can use as filter criteria when working with authority rules.

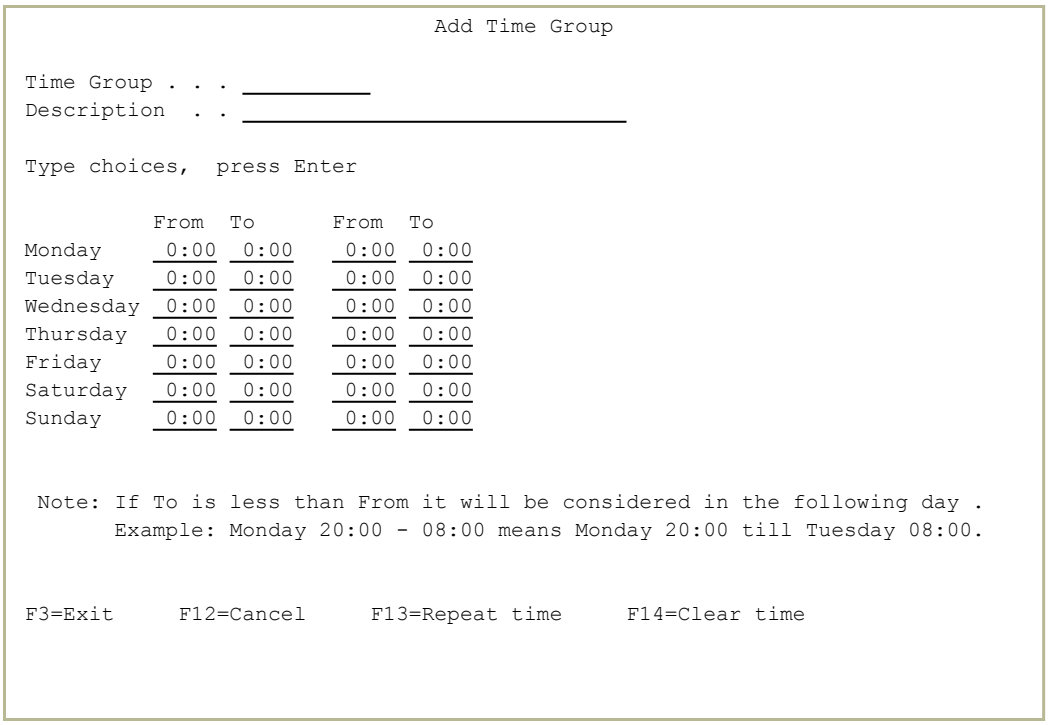
To **create or modify time groups**, select **6. Time Groups** from the main menu. The **Define Time Groups** screen appears.

```
                              Define Time Groups

Type options, press Enter.
  1=Select  3=Copy  4=Delete

Opt Time Group    Description
 _  ALEXANDRA     TEXT FOR ALEXANDRA
 _  ALON          Special group
 _  ALONPP        Special group
 _  ALON88        Special group
 _  CONF1         TEXT FOR CONF1
 _  FRANCEWH      SITE  GROUP
 _  NEW           TEXT FOR NEW
 _  VB123         Special group
 _  WORKHOURS     Regular work hours
 _  WORKHOURS1    Regular work hours + 1
 _  WORKHOURS2    Regular work hours + 2
 _  WORKHOURS3    Regular work hours + 3


                                                                      Bottom
F3=Exit   F6=Add new   F8=Print list   F12=Cancel
```

The body of the screen shows existing time groups, showing the name and a text description for each.

To **add** a time group, press the **F6** key. The **Add Time Group** screen appears.

To **modify** an existing time group, enter **1** in the **Opt** field for that group. The similar **Modify Time Group** screen appears.




The top of the screen includes these fields:

**Time Group**

A meaningful name for the Time Group. This field is mandatory.

**Description**

A meaningful description of the Time Group. This field is mandatory.

The body of the screen has named lines for each day of the week.

Each line has two pairs of fields, with one named **From** and the other named **To**. Each pair specifies a time period during the day. For example, if workers had a shift from 8 AM to 5 PM, with a lunch break from noon to 1 PM, the line for each weekday would show times from **8:00** to **12:00** and from **13:00** to **17:00**.

If the value of the **To** field is less than that of the **From** field, it signifies that the shift continues into the next calendar day. For example, an overnight shift **From 23:00 To 7:00** would run from 11 PM on that day through 7 AM on the next.

To repeat the entered times from the line containing the cursor to those for all other days, press the F13 (Shift+F1) key.

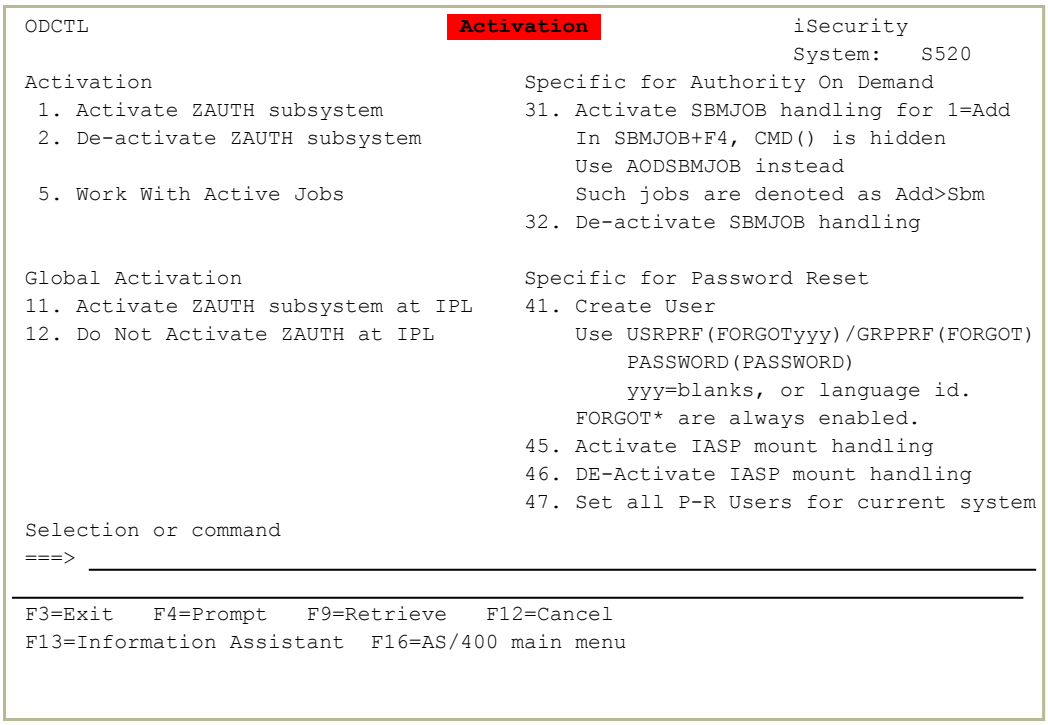
To **clear** the times from all the lines except for the one containing the cursor, press the **F14 (Shift+F2)** key.

# Activation

To **activate** the timer that shows when work periods are over as well as the action feature (see General Definitions), activate the **Authority on Demand** monitor.

**Authority on Demand** should be set to activate automatically each time your IBM i performs an IPL.

To **work with activation**, select **`11. Activation`** from the main menu. The **Activation** screen appears.




## Manual Activation

To **activate the Authority on Demand monitor manually**, select **`1. Activate ZAUTH subsystem`** from the **Activation** menu.

To **de-activate the Authority on Demand monitor manually**, select **`2. De-activate ZAUTH subsystem`** from the **Activation** menu.

## Automatic Activation

To activate Authority on Demand automatically each time an IPL occurs, select **11. Activate ZAUTH subsystem at IPL** from the Activation menu.

To cancel automatic activation, select **12. Do Not Activate ZAUTH subsystem at IPL** from the Activation menu.

## Web Interface Activation

To activate the Authority on Demand web interface, select **21. Start web interface** from the Activation menu.

To de-activate the Authority on Demand web interface, select **22. Stop web interface** from the Activation menu.

## Activating SBMJOB Handling

Rules that use the **1=Add authority** option enable the user to submit jobs that will carry elevated authority, regardless of the state of the submitting Authority on Demand session. This unique capability is subject to retaining the value *USER(*CURRENT)* in the submitted job.

By default, when a user enters the F4=Prompt screen for the command *Submit job (SBMJOB)*, the **Command (*CMD*)** parameter is not displayed and cannot be changed.

To activate SMBJOB handling, select **31. Activate SBMJOB handling for 1=Add** from the Activation menu (*STRAOD* **> 11**). With this set, Activity on Demand uses the *AODSBMJOB* command, which allows changes to the **CMD** parameter and effective use of the F4=Prompt key.

To de-activate Authority on Demand **SBMJOB** handling, select **32. De-activate SBMJOB handling** from the Activation menu.

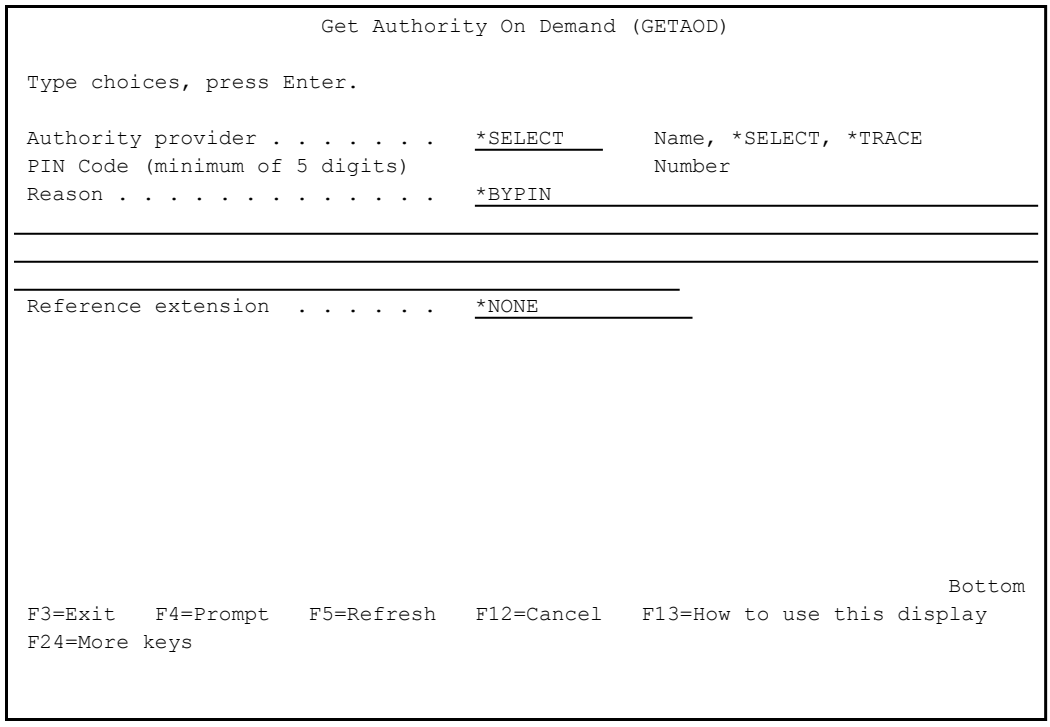
## Verifying that the Authority on Demand Monitor is Active

To view the Authority on Demand monitor subsystem, select **`5. Work With Active Jobs`** from the Activation menu (*STRAOD* **`> 1`**). The **`standard`** Work with Subsystem Jobs screen appears, showing jobs within the ZAUTH subsystem.

# Getting Authority on Demand

To activate Authority on Demand, you must be logged in with the Requester user profile.

To **get Authority on Demand**, select **31. Get Authority On Demand** from the main menu. The **Get Authority On Demand**screen appears.

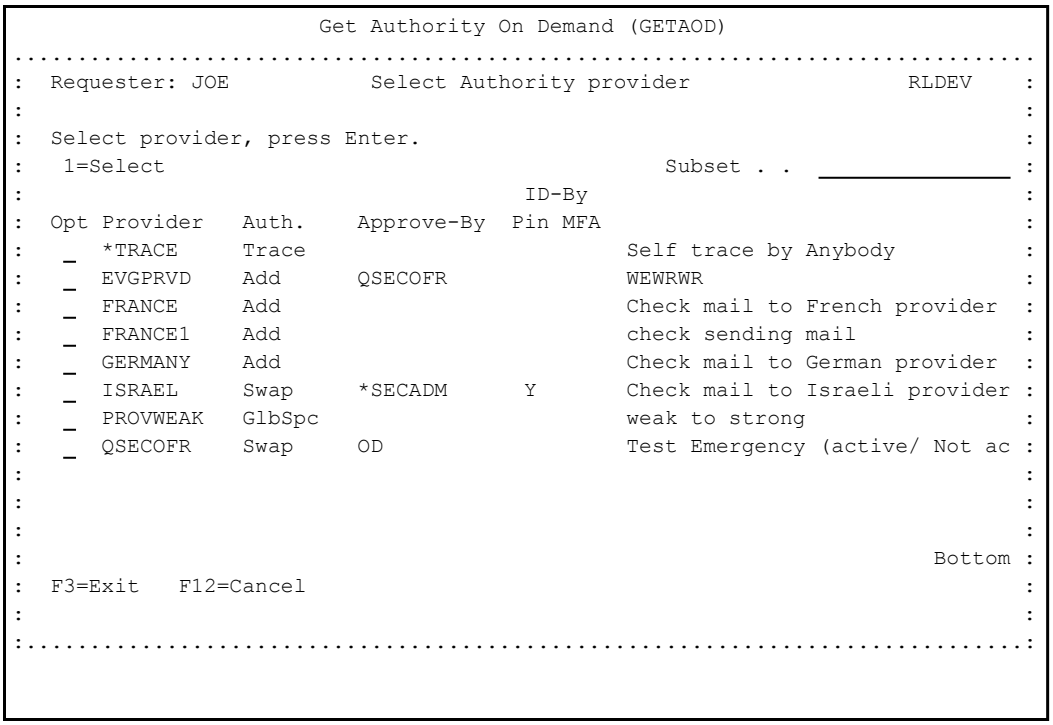



The body of the screen includes these fields:

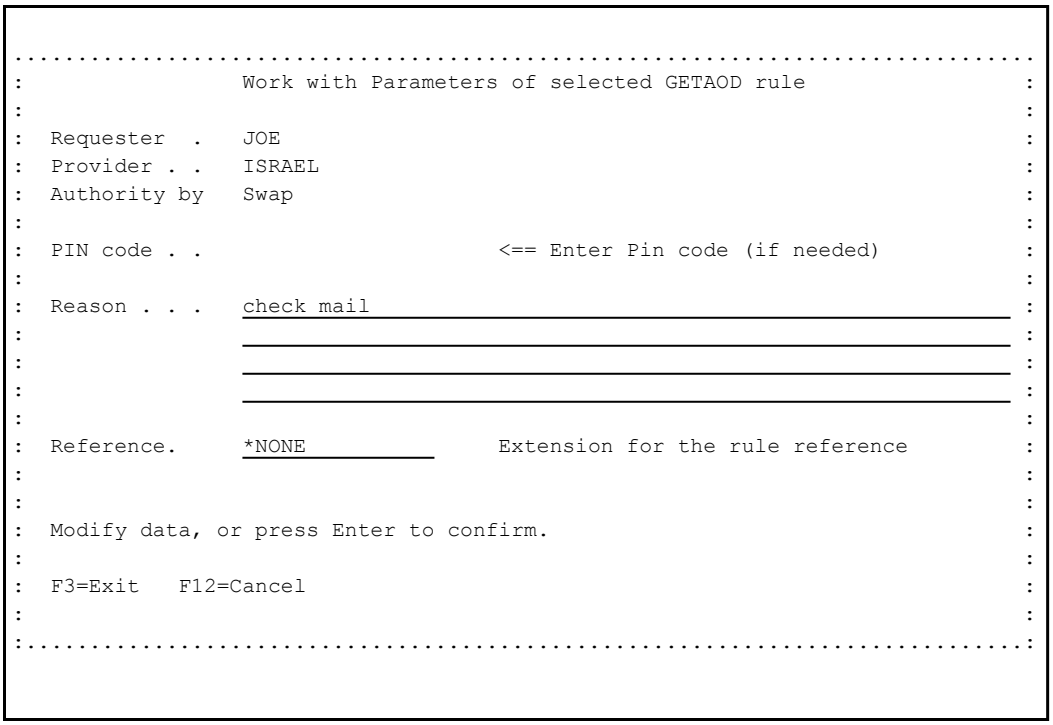
**Authority provider**

The Authority Provider's user profile. Possible values include:

- The provider's user name
- ***SELECT**: If the field is set to ***SELECT**, when you press Enter, the Select Authority Provider window appears, offering a list of authorized providers:




For each provider, the screen shows information on the rule under which the authority is provided. To video and edit further information about the authority provided, enter **1** in the **Opt** field for the provider. The **Work with Parameters of selected GETAOD rule** window appears:



With this screen, you can set a **Reason** for this use of the rule, a **PIN code** for its use, and an **extension to use for references** to the rule.

If the rule requires approval (as shown in the **Approve-by** field of the **Select Authority provider** screen), the **Information about Approval** screen appears once you press **Enter**:

```
                        Information about Approval

You JOE        requested to elevate authority to ISRAEL
in this job 809148/JOE/QPADEV0009

You have to get approval from *SECADM

If he has an active session, he will get a message when you press Enter.
In any case, you are advised to call him and ask for his confirmation.

Once approved, you will be notified. Then, start your AOD session, re-enter
the GETAOD command, with the same provider.

The approval must be obtained within 1 hour, or your request will be deleted.

Now, press Enter to continue with other work.
```

A break message also appears on the screen of every QSECOFR user requesting that they approve the request. The request must be approved within one hour, using the **GETAOD Requests Pending your Approval** screen (*STRAOD*> **2**).

(Continuing with values for the **Authority Provider** field of the **Get Authority on Demand (GETAOD)** screen:)

- ***TRACE**: Create a trace of the activity done within the session without changing authority. At the end, a complete document describing the activity within the sesson is provided.

**PIN code**

The PIN code that was defined when setting up the rule

**Reason**

The reason for requesting the Authority. Free text, up to 240 characters long. If set to ***BYPIN**, the default reason established for authority requests using that PIN.

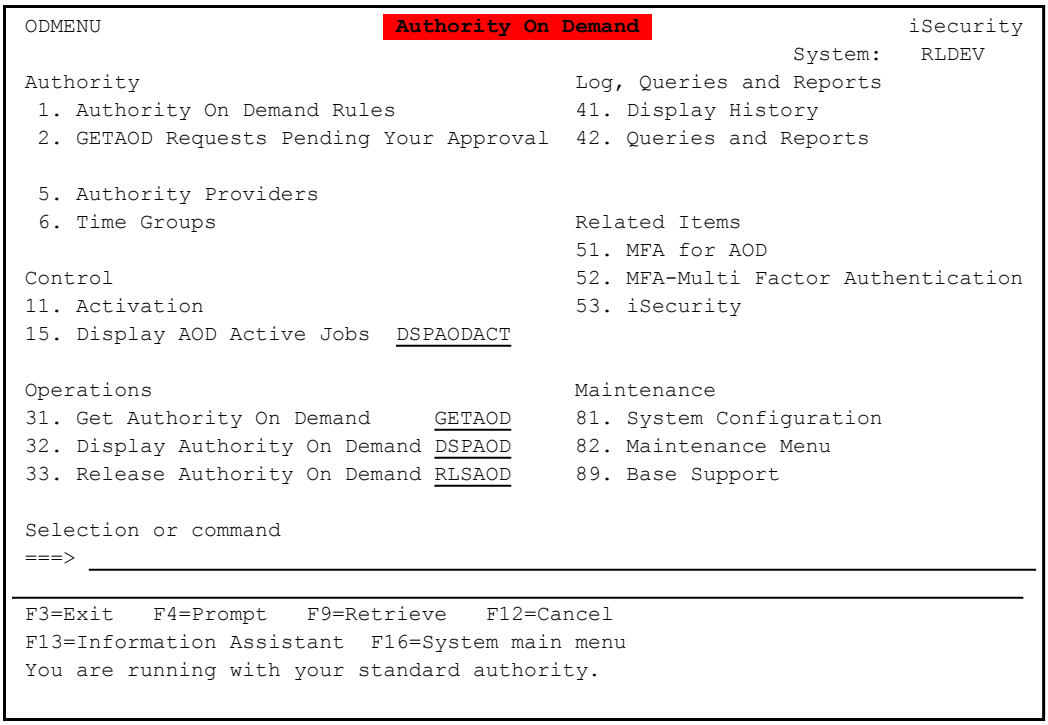
**Reference extension**

An extension attached to references to this authority request.

# Displaying Authority on Demand

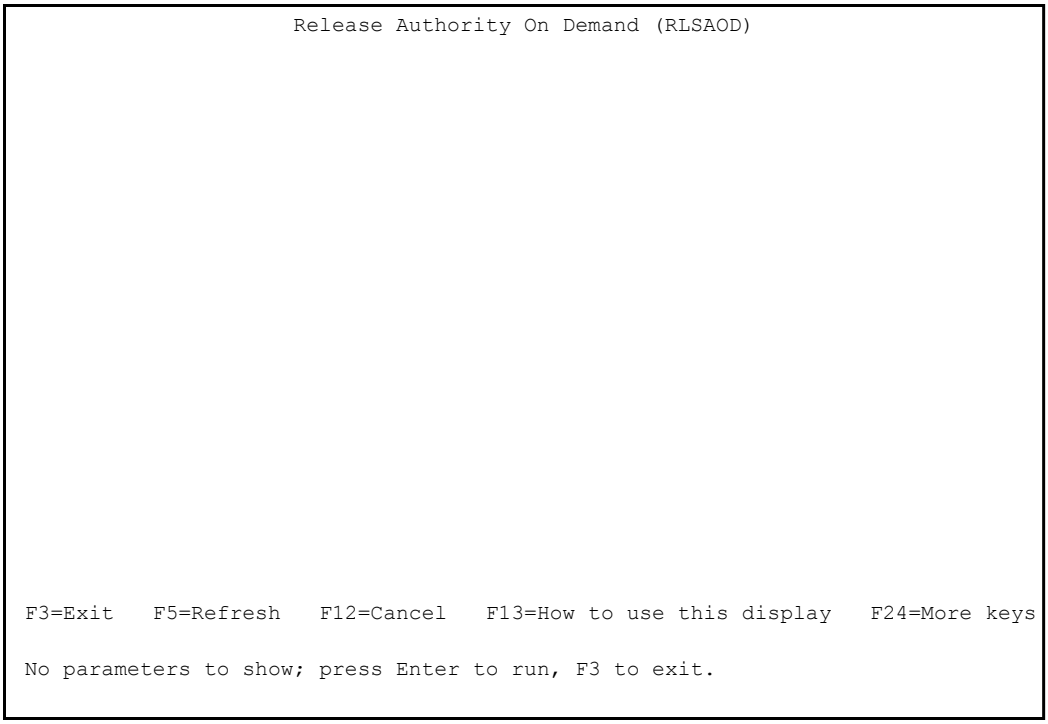
To **display the new authorization currently in use**, select **`32. Display Authority on Demand`** from the main menu.

As shown here, a message appears at the bottom of the screen stating whether you are currently running with standard or extended authority.



# Releasing Authority on Demand

To **release** Authority on Demand and return to working with the standard authorizations, select **33. Release Authority on Demand** from the main menu. The **Release Authority On Demand** screen appears.




To **cancel releasing** the extended authority, press the **F12** key.

Otherwise, press **Enter**. The acquired authority is released.

# Logs

To **view the contents of the history log** in a standard format using basic filter criteria, you can display or print the Authority on Demand activity log.

NOTE: Extended logging capability may depend on other iSecurity modules such as **Capture, Audit, and AP-Journal**, which you may have to install or license separately.

## Displaying the History Log

To **display the Authority on Demand History Log**, select **`41. Display History`** from the main **Authority on Demand** menu. The **Display AOD History (DSPAODHST)** screen appears.

```
                    Display AOD History (DSPAODHST)

Type choices, press Enter.

Display last minutes . . . . . *BYTIME       Number, *BYTIME
Starting date and time:
  Starting date  . . . . . .   *PRVYEARS     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .   000000        Time
Ending date and time:
  Ending date  . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . .   235959        Time
Authority requester  . . . . . *ALL         Name, generic*, *GROUP, *ALL
Authority provider . . . . . .  *ALL         Name, generic*, *ALL
Reference Id (generic*)  . . . *ALL
Reason includes the text . . . .
System to run for  . . . . . .  *CURRENT     Name, generic*, *CURRENT...
Number of records to process . .  *NOMAX      Number, *NOMAX
Output . . . . . . . . . . . .  *            *, *PRINT, *OUTFILE


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

The body of the screen contains these fields, which you can use to select the information from the log to print or display:

**`Display last minutes`**

The number of minutes, counting backward from the current time, for which information should be shown. If set to **`*BYTIME`**, use

the time periods shown in the **Starting data and time** and **Ending date and time fields**.

**Starting date and time**

**Starting date**

The earliest date to be shown. In addition to numerical dates, possible values include:

- ***CURRENT** = Current day
- ***YESTERDAY** = Previous day
- ***WEEKSTR**/***PRVWEEKS** = Current week/Previous week
- ***MONTHSTR**/ ***PRVMONTH** = Current month/Previous month
- ***YEARSTR**/ ***PRVYEARS** = Current year/ Previous year
- ***SUN** -***SAT** = Day of week

**Starting time**

The time on that day to begin, in HHMMSS format

**Ending date and time**

**Ending date**

The latest date to be shown. In addition to numerical dates, possible values include:

- ***CURRENT** = Current day
- ***YESTERDAY** = Previous day
- ***WEEKSTR**/***PRVWEEKS** = Current week/Previous week start
- ***MONTHSTR**/ ***PRVMONTH** = Current month/Previous month
- ***YEARSTR**/ ***PRVYEARS** = Current year/ Previous year start
- ***SUN** -***SAT** = Day of week

**Ending time**

The time on that day to end, in HHMMSS format

**Authority requester**

The user profile that requested the authorization. This can be a single profile, a generic* name, or ***ALL**.

**Authority provider**

The user profile that provided the authorization. This can be a single profile, a generic* name, or ***ALL**.

**Reference ID**

A unique, official string representing the rule.

**Reason includes the text**

Select the record if the free-form text entered appears in the **Reason** field of the request.

**System to run for**

The system for which the authorization was made. This can be a single system name, a generic* name, ***CURRENT**, or ***ALL.**

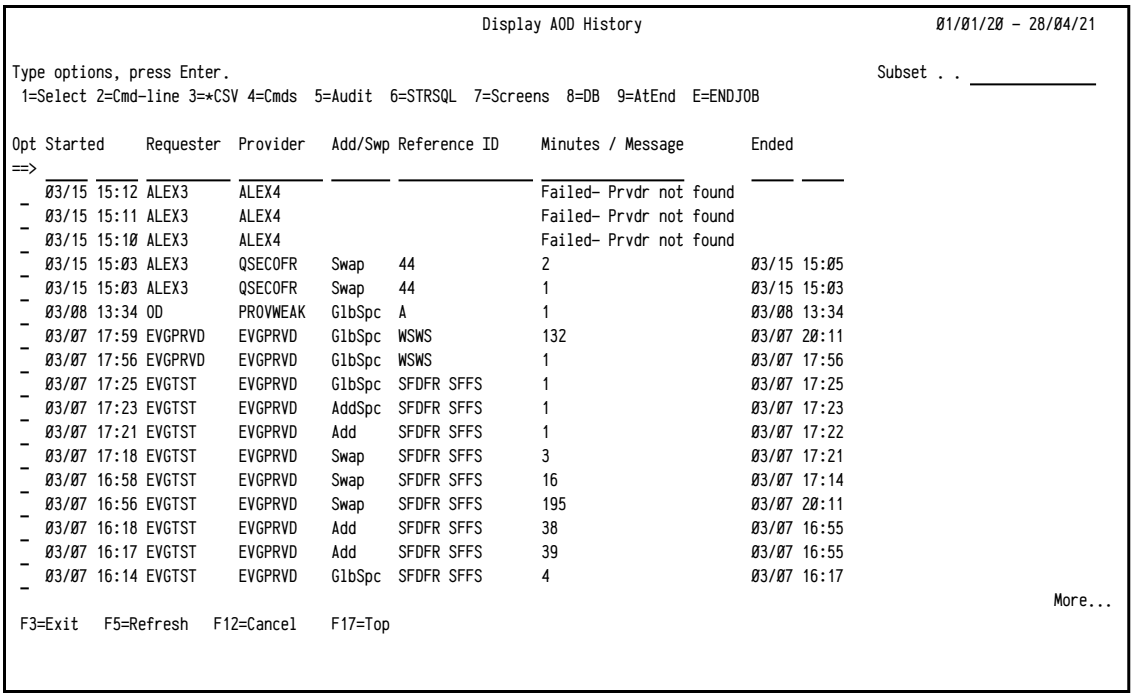
**Number of records to process**

How many records to process. To process all records, set this to ***NOMAX**.

**Output**

Where to send output. Possible values include ***PRINT** and ***OUTFILE**.

When you have entered all the parameters, press Enter. The Display AOD History summary screen appears, showing the collected information.




Each line on the body of the screen refers to a single request for extended authority. The fields on each line include:

**Started**

The date and time that the request was made

**Requester**

The user profile making the request

**Provider**

The user profile asked to authorize the extended authority

**Add/Swp**

How authority would be provided:

- **Add**: Add authority
- **GlbSpc**: Add *SPCAUT globally
- **Swap**: Swap profile
- **Trace**: Trace activity but do not change authority
- **AddSpc**: Add *SPCAUT by session

**Reference ID**

A unique, official string representing the rule

**Minutes/Message**

If the request was successful, the number of minutes for which the extended authority was in effect.

If the request failed, a message explaining the failure.

**Ended**

If the request was successful, the date and time that it ended.

To view detailed information about one of the authorization requests in the list, enter **1** in the **Opt** field on that line. The Display Details screen appears.

```
                              Display Details

Started    . . . . . .  2021-03-15-15.03.25
Ended  . . . . . . . .  2021-03-15-15.05.23
Minutes / Reject-reason  .  2
Requester  . . . . . .  ALEX3
Provider   . . . . . .  QSECOFR
Type . . . . . . . . .  Swap
Description  . . . . .  test

Job  . . . . . . . . .  495952/ALEX3/QPADEV0004
Job type . . . . . . .  Interactive
Current user . . . . .  ALEX3
IP address . . . . . .  1.1.1.199
System     . . . . . .  RLDEV

Reference Id . . . . .  44
Reason . . . . . . . .  sss




F3=Exit               F12=Cancel
```

The screen includes these fields, which are all read-only:

**Started**

The date and time that the request was made, in **YYYY-MM-DD-HH.MM.SS** format

**Ended**

If the request was successful, the date and time that it ended, in **YYYY-MM-DD-HH.MM.SS** format

**Minutes/Message**

If the request was successful, the number of minutes for which the change was in effect.

If the request failed, the message explaining the failure.

**Requester**

The user profile making the request

**Provider**

The user profile asked to authorize the extended authority

**Type**

How authority was provided:

- **Add**: Add authority
- **GlbSpc**: Add *SPCAUT globally
- **Swap**: Swap profile
- **Trace**: Trace activity but do not change authority
- **AddSpc**: Add *SPCAUT by session

**Description**

A free-text description of the Authority on Demand rule that was used

**Job**

The job number of the authorization

**Job Type**

The job type

**Current User**

The user viewing the report

**IP address**

The IP address from which the authorization was requested

**System**

The system for which the authorization was requested

**Reference ID**

A unique, official string representing the rule

**Reason**

The reason for the request

To display **commands entered on the command line** during a session, enter **2=Cmd-line** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen. (This depends on iSecurity/Audit having been active during the session.)

To display **information from the session in Comma Separated Values format**, enter **3=CSV** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen. (This depends on iSecurity/Audit having been active during the session.)

To display all **commands entered** during a session, including those generated by screens, enter **4=Cmds** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen. (This depends on iSecurity/Audit having been active during the session.)

To display an **Audit history** of a session, enter **5=Audit** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen. (This depends on iSecurity/Audit having been active during the session.)

To display all **SQL statements** entered during a session, enter **6=STRSQL** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen.

To display all **screens used** during a session, enter **7=Screen** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen. (This depends on iSecurity/Capture having been active during the session.)

To display all **database activity** during a session, enter **8=DB** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen. (This depends on iSecurity/AP-Journal having been active during the session.)

To display only the **AtEnd report**, enter **9=AtEnd** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen.

To **end a session**, enter **E=ENDJOB** in the **Opt** field for the line representing the session on the **Display AOD History** summary screen.

# Display Log and Entered Commands

To print activity logs with commands entries, select **42. Queries and Reports** from the Activity on Demand main menu, then select **11. Print Log + Entered Commands** from the Queries and Reports menu. The activity log is composed of audit and journal logs.

The Display AOD Log Entries (DSPAODLOG) screen appears.

```
                    Display AOD Log Entries (DSPAODLOG)

Type choices, press Enter.

Display last minutes . . . . . *BYTIME       Number, *BYTIME
Starting date and time:
  Starting date  . . . . . .    *CURRENT     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .    000000       Time
Ending date and time:
  Ending date  . . . . . .      *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . .      235959       Time
Authority requester  . . . . .  *ALL         Name, generic*, *ALL
Authority provider . . . . . .  *ALL         Name, generic*, *ALL
Reference Id (generic*)  . . . . *ALL
Reason includes the text . . . .
System to run for  . . . . . .  *CURRENT     Name, generic*, *CURRENT...
Number of records to process . .  *NOMAX     Number, *NOMAX
Output . . . . . . . . . . . . > *PRINT      *, *PRINT, *OUTFILE
Attach activity log  . . . . . > *CMDENT     *YES, *CMDENT, *CMD, *NO
Attach captured screen . . . . > *NO         *YES, *NO
                                                                  More...
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

The screen includes these fields:

**Display last minutes**

The number of minutes, counting backward from the current time, for which information should be shown. If set to ***BYTIME**, use the time periods shown in the **Starting data and time** and **Ending date and time fields**.

**Starting date and time**

**Starting date**

The earliest date to be shown. In addition to numerical dates, possible values include:

- ***CURRENT** = Current day
- ***YESTERDAY** = Previous day
- ***WEEKSTR**/***PRVWEEKS** = Current week/Previous week
- ***MONTHSTR**/ ***PRVMONTH** = Current month/Previous month
- ***YEARSTR**/ ***PRVYEARS** = Current year/ Previous year
- ***SUN** -***SAT** = Day of week

**Starting time**

The time on that day to begin, in HHMMSS format

**Ending date and time**

**Ending date**

The latest date to be shown. In addition to numerical dates, possible values include:

- ***CURRENT** = Current day
- ***YESTERDAY** = Previous day
- ***WEEKSTR**/***PRVWEEKS** = Current week/Previous week start
- ***MONTHSTR**/ ***PRVMONTH** = Current month/Previous month
- ***YEARSTR**/ ***PRVYEARS** = Current year/ Previous year start
- ***SUN** -***SAT** = Day of week

**Ending time**

The time on that day to end, in HHMMSS format

**Authority requester**

The user profile that requested the authorization. This can be a single profile, a generic* name, or ***ALL**.

**Authority provider**

The user profile that provided the authorization. This can be a single profile, a generic* name, or ***ALL**.

**Reference ID**

A unique, official string representing the rule.

**Reason includes the text**

Select the record if the free-form text entered appears in the **Reason** field of the request.

**System to run for**

The system for which the authorization was made. This can be a single system name, a generic* name, ***CURRENT**, or ***ALL.**

**Number of records to process**

How many records to process. To process all records, set this to ***NOMAX**.

**Output**

Where to send output. Possible values include ***, *PRINT** and ***OUTFILE**.

**Attach activity log**

If the **Output** field is set to ***PRINT**, the printed log includes the included commands. Possible values include:

- ***YES**: Attach full log
- ***CMDENT**: Attach entered commands
- ***CMD**: Attach all commands
- ***NO**: Do not attach commands.

**Attach captured screen**

If the **Output** field is set to ***PRINT**, attach captured screens. The default is ***NO**.

**Attach file record changes**

If the **Output** field is set to ***PRINT**, attach information on record changes. The default is ***NO**. Other options include ***LIST** for a list and ***YES** for more complete information.

**Attach *CSV report for *CMDENT**

If the **Attach activity log** field is set to ***CMDENT**, attach the report of entered commands in ***CSV** (comma-separated values) format.

**Print format**

Whether to print the report in ***SHORT** or ***FULL** format.

To display full transaction details, if the Display Authority on Demand Log is used with parameter **OUTPUT(*)**, you can place the cursor on any log line and press **Enter** to display full transaction details.

## Printing the Log and Attachments

To print a predefined report of the log and attachments, select **`12. Print Log + Attachments`** from the Queries and Reports menu (*STRAOD*`> 42`).

The Display AOD Log Entries (DSPAODLOG) screen appears as shown above, with several fields preset to useful values:

- **`Output`**: **`*PRINT`**
- **`Attach activity log`**: **`*CMDENT`**
- **`Attach captured screens`**: **`*YES`**
- **`Attach file record changes`**: **`*NO`**
- **`Print format`**: **`*FULL`**

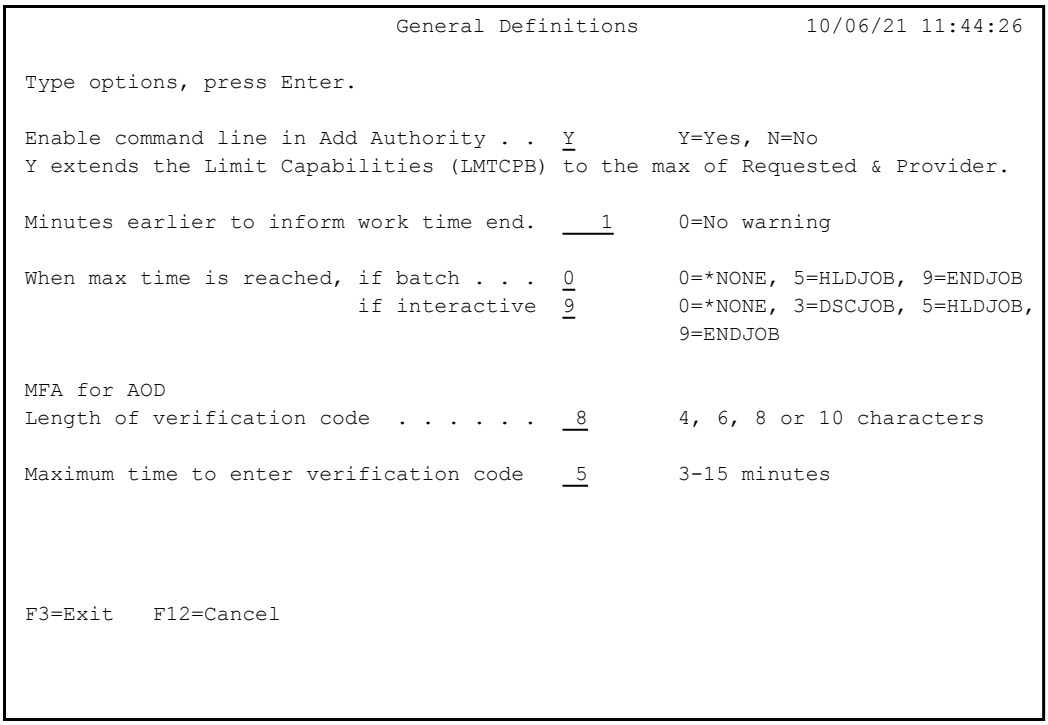
# System Configuration

To **configure general values** for Authority on Demand, select **81. System Configuration** from the main menu. The **Authority On Demand System Configuration** screen appears.

```
ODPARMR                        System Configuration             6/12/21 12:05:39

Authority On Demand                        SIEM Support
 1. Global Parameters                      70. Main Control----->  Active
 3. Session End Activity                   71. SIEM 1:               N
 4. Attachment setup                       72. SIEM 2:               N
 5. Defaults                               73. SIEM 3:               N
 6. Reason Structure                       75. SNMP Definitions
 8. Emergency rules
 9. Log Retention

Person Based Products P-R/MFA/U-P          General
51. P-R  Password-Reset                    91. Language Support
52. MFA  Multi-Factor Authentication       99. Copyright Notice
53. U-P  User-Provisioning
58. Self-Registration Control
59. Customizing web interface


Selection ===>
Release ID . . . . . .  06.04 21-10-19    788C500  41A EP10   2
Authorization code . . . . . .  O02112721700              2   RLDEV
F3=Exit    F22=Enter Authorization Code
```

## General Definitions

To **set global parameters** for Authority on Demand, select **1. Global Parameters** from the **System Configuration** menu. The **General Definitions** screen appears.




The body of the screen includes these fields:

**Enable command line in Add Authority**

Whether the use can enter additional specifications via the command line, to the maximum length allowed for the provider and requester.

**Minutes earlier to inform work time end.**

Authority on Demand can inform the user when the work session us about to end. This field indicated the number of minutes before the end to inform the user. If set to **0**, the user is not warned.

**When max time is reached,**

**if batch**

The action to take if the maximum time is reached when running in batch mode. Possible values include:

- **0**: ***NONE**
- **5**: **HLDJOB**
- **9**: **ENDJOB**

#### if interactive

The action to take if the maximum time is reached when running in interactive mode. Possible values include:

- 0: ***NONE**
- 5: **HLDJOB**
- 3: **DSCJOB**
- 9: **ENDJOB**

### MFA for AOD

#### Length of verification code

If Authority on Demand is set to demand a verification code via Multi-Factor Authentication, the number of characters required for the code. Possible values include **4**,**6**,**8**, or **10**.

#### Maximum time to enter verification code

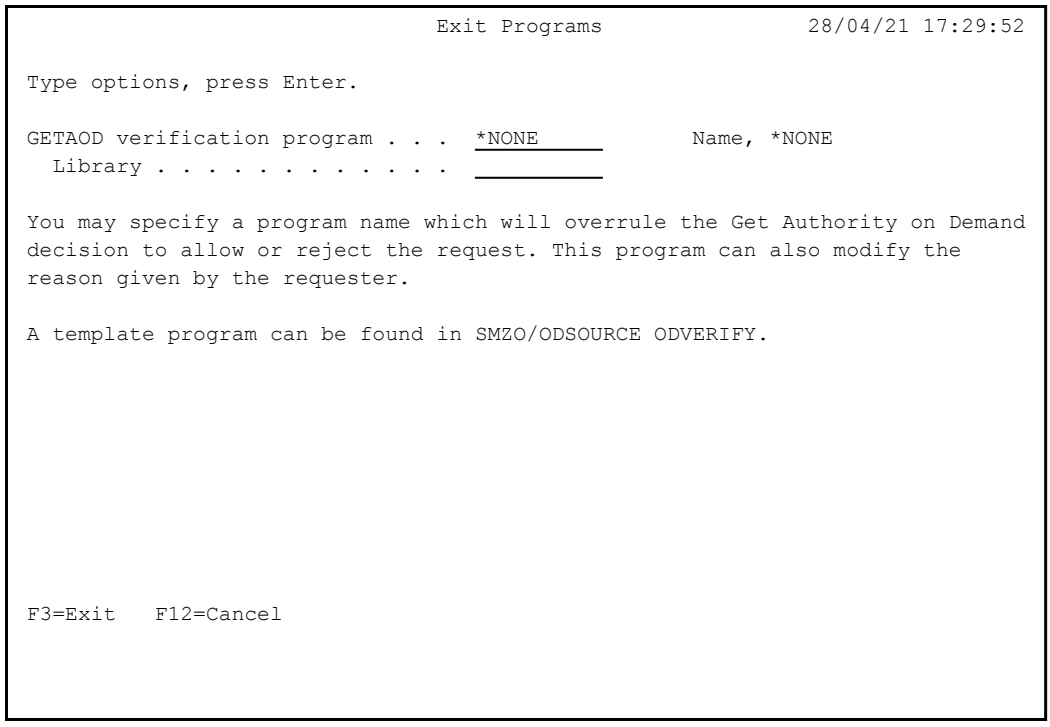
The maximum number of minutes during which the user must enter the verification code. This can be from **3** to **15** minutes.

# Exit Programs

User **exit program**s can specify overrule the **Get Authority on Demand** rule definitions to allow or reject the request. These programs can also modify the reason given by the Requester for the temporary authorization.

You can find a template program in SMZO/ODSOURCE ODVERIFY.

To specify an exit programs, select **2. Exit programs** from the **Authority On Demand** System Configuration menu (*STRAOD* **> 82**). The Exit Programs screen appears.




The body of the screen includes these fields:

**GETAOD verification program**

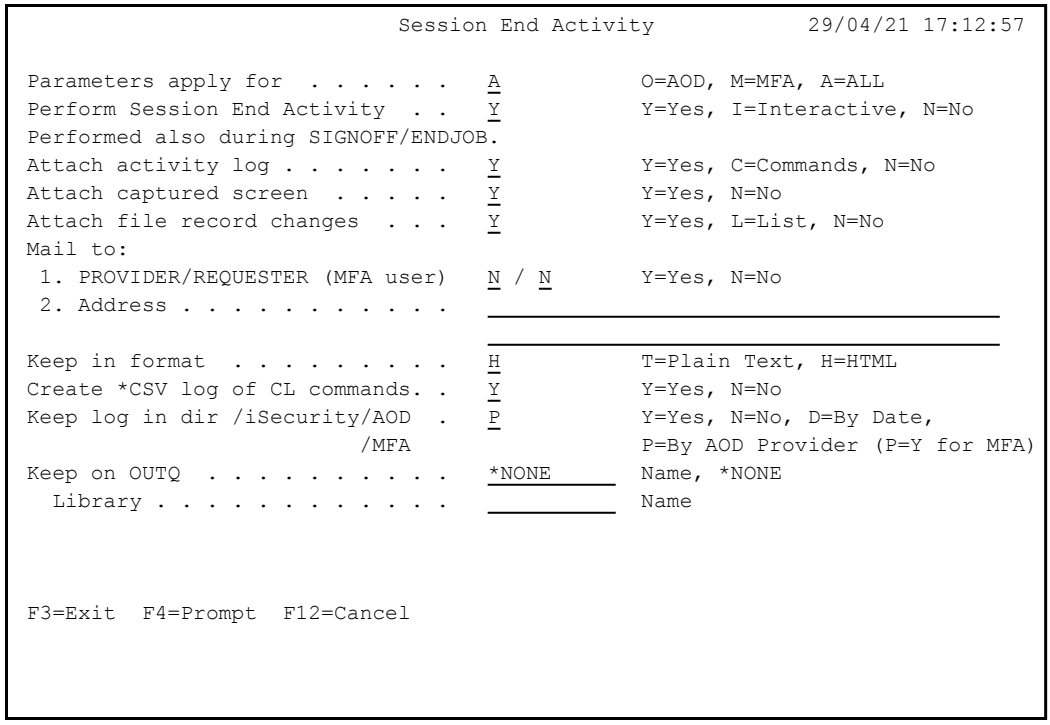
The user program that runs to verify the Get Authority request, or ***NONE**.

**Library**

The library containing the programs.

## Session End Activity

To **define which actions are executed** when the extended authority ends, select **61. Session End Activity** from the **Authority On Demand** System Configuration menu. The **Session End Activity** screen appears.




The body of the screen includes these fields:

**Parameters apply for**

The programs for which these parameters apply. Possible values include:

- **O**: Authority on Demand
- **M**: Multi-Factor Authentication
- **A**: All

**Perform Session End Activity**

Whether and how to perform the activity when the session ends, as well as during SIGNOFF/ENDJOB.

Possible values include:

- **Y**: Yes. Perform Session End Activity in a batch job
- **I**: Interactively. Perform Session End Activity in an interactive job
- **N**: No. Do not perform Session End Activity

**Attach activity log**

Whether to attach the full activity log or a listing of logged commands to the output.

Possible values include:

- **Y**: Yes, attach the full Activity Log
- **C**: Attach logged Commands only
- **N**: No, do not attach the Activity Log

**Attach captured screen**

Whether to attach screens captured during the run to the output.

Possible values include:

- **Y**: Yes, attach the screens
- **N**: No, do not attach the screens

**Attach file record changes**

Whether to attach information on file records changed during the run to the output.

Possible values include:

- **Y**: Yes, attach full information
- **L**: List - attach a list of changes
- **N**: No, do not attach the information

**Mail to:**

Whether to email the report to specified people

**1. PROVIDER/REQUESTER (MFA user)**

A pair of single-character fields (**N / N**) representing the provider and requester.

To send the email to the provider, set the first field to **Y**. Otherwise, set it to **N**.

To send the email to the requester, set the second field to **Y**. Otherwise, set it to **N**.

**2. Address**

Additional email addresses to which the report is to be sent.

**Keep in format**

The format for the report. Possible values include:

- **T**: Plain Text
- **H**: HTML

**Create *CSV log of CL commands**

Whether to create a log in CSV (comma-separated value) format of the commands performed during the session. Possible values are **Y** for Yes or **N** for No.

**Keep log in dir /iSecurity/AOD /MFA**

Whether to keep a log for Authority on Demand in the **/iSecurity/AOD** directory, and for Multi-Factor Authentication in the **/iSecurity/MFA** directory.

Possible values include:

- **Y**: Keep a log in the specified directory
- **N**: Do not keep a log in the directory
- **D**: Keep the log in a subdirectory named for the date.
- **P**: For Authority on Demand, keep the log in a sub-directory named for the provider. For Multi-Factor Authentication, keep the log directly in the specified directory.

**Keep on OUTQ**

The name of an OUTQ in which to keep the log, or ***NONE**

**Library**

The library that contains the named OUTQ.

# Attachment Setup

To **provide attachments for the logs**, you can either use the appropriate iSecurity module or, if available, standard system commands. To indicate which to use, select **`4. Attachment Setup`** from the **`Authority On Demand`** System Configuration menu. The **Attachment Setup** screen appears.

```
                              Attachment Setup              28/04/21 17:39:08

Type options, press Enter.

Use iSecurity/Capture (see Notes) . . . .  Y        Y=Yes, N=No
Use iSecurity/Audit for QAUDJRN . . . . .  N        Y=Yes, N=No
Use iSecurity/Firewall for STRSQL . . . .  Y        Y=Yes, N=No
Use iSecurity/AP-Journal for DB updates .  Y        Y=Yes, N=No

In order to provide the attachment for the logs, the product can either
use the appropriate iSecurity module or attempt to use standard system
commands.
Please specify whether to use iSecurity modules or system commands.

Notes:
1. iSecurity/Capture is the only way to capture user screen activity.
   If Capture is used ONLY for AOD: STRCPT, 81, 1 and set "Minutes between
   checks" to 998=Never check.
2. A maximum of 200 updates are included from each journal that contains DB
   updates made during AOD.

F3=Exit   F12=Cancel
```

The body of the screen contains these fields, along with further explanations:

**`Use iSecurity/Capture`**

iSecurity/Capture is the only way to capture screens for Authority on demand. If this field is set to **`N`**, no screens will be captured. To use Capture, set the field to **`Y`**. iSecurity/**Capture** works for sessions of **Authority On Demand**, even if you have not purchased a license for **Capture**

If you are using Capture only for Authority on Demand, set the **`Minutes between checks`** field on the **Capture General Definitions** screen (*STRCPT***`> 81 > 1`**) to **`998`** (Never check).

**Use iSecurity/Audit for QAUDJRN**

To use iSecurity/Audit for QAUDJRN, set this field to **Y**. Otherwise, set it to **N**.

A maximum of 200 updates are included from each journal that contains DB updates made during Authority on Demand.

**Use iSecurity/Firewall for STRSQL**

To use iSecurity/Firewall for STRSQL, set this field to **Y**. Otherwise, set it to **N**.

**Use iSecurity/Firewall for STRSQL**

To use iSecurity/Firewall for STRSQL, set this field to **Y**. Otherwise, set it to **N**.

A maximum of 200 updates are included from each journal that contains DB updates made during Authority on Demand.

## Defaults

To set a variety of default values for Authority on Demand rules. select **5. Defaults** from the System Configuration screen (*STRAOD* **> 81**). The General Defaults screen appears.

```
                              General Defaults             10/06/21 15:48:36

Type defaults for rules, press Enter.

Maximum work time (minutes)  . . . . . .   30      0=*NOMAX
Remaining uses of PIN code . . . . . .  90        99=*NOMAX
Allow next use after . . . . . . . . . .   0      0=Allow consecutive uses
PIN code valid to current system only  .  Y        Y=Yes, N=No
Apply rules to group profile members . .  Y        Y=Yes, N=No
This is the default for interpreting rules in which the requester is a group
profile. If Y, the rule applies to all the members of the group profile.
During processing, only the first rule found applies.









F3=Exit    F12=Cancel
```

The body of the screen contains these fields:

**Maximum work time (minutes)**

The default number of minutes for which a rule may increase authority. If set to **0**, no limit is set.

**Remaining uses of PIN code**

The default number of times that a PIN code may be used before it must be changed. If set to **99**, no limit is set.

**Allow next use after**

The default number of minutes that must pass after a rule is used before it may be used again. If set to **0**, the rule may be used again immediately.

**PIN code valid to current system only**

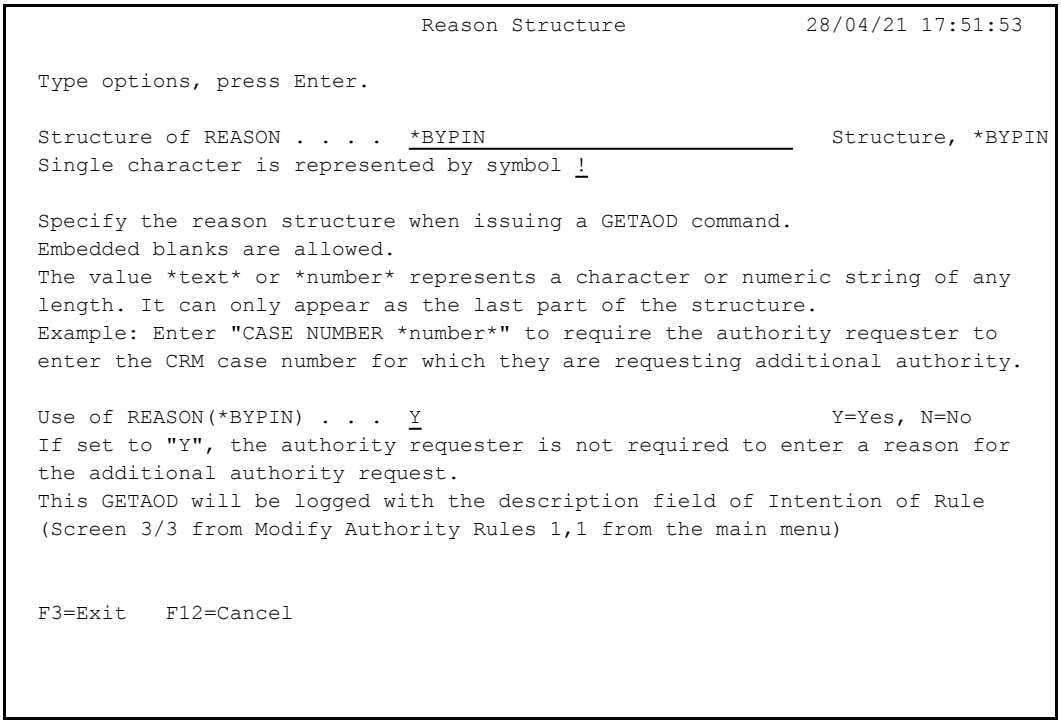
If set to **Y**, a PIN code may only be used on the current system. If set to **N**, it may be used on other systems.

**Apply rules to group profile members**

If set to Y, a rule requested by a user who is a group profile applies to all members of the group. If set to N, it does not. If multiple rules are found, only the first one applies.

## Reason Structure

To predefine the Reason field for the Get Authority On Demand (GETAOD) screen, select **6. Reason Structure** from the **Authority On Demand** System Configuration menu (*STRAOD* **> 81**). The Reason Structure screen appears.




The **Reason** field in authorization listings gives a human-readable reason for the use of a rule. For many rules, you can set the reason with the **Intention of Rule** field from the Modify Authority Rules screen (as seen in "Authority Rules" on page 20). If the **Structure of REASON** field on this screen is set to ***BYPIN** and the **User of REASON (*BYPIN)** field is set to **Y**, Authority on Demand can then find the relevant value based on the PIN code used for the authorization.

If you include the strings ***text*** or ***number*** at the end of the string in the **Structure of REASON** field, the user must enter an appropriate value. Thus, as the screen text says, if you set it to **CASE NUMBER *number***, the user must enter a case number for the authorization.

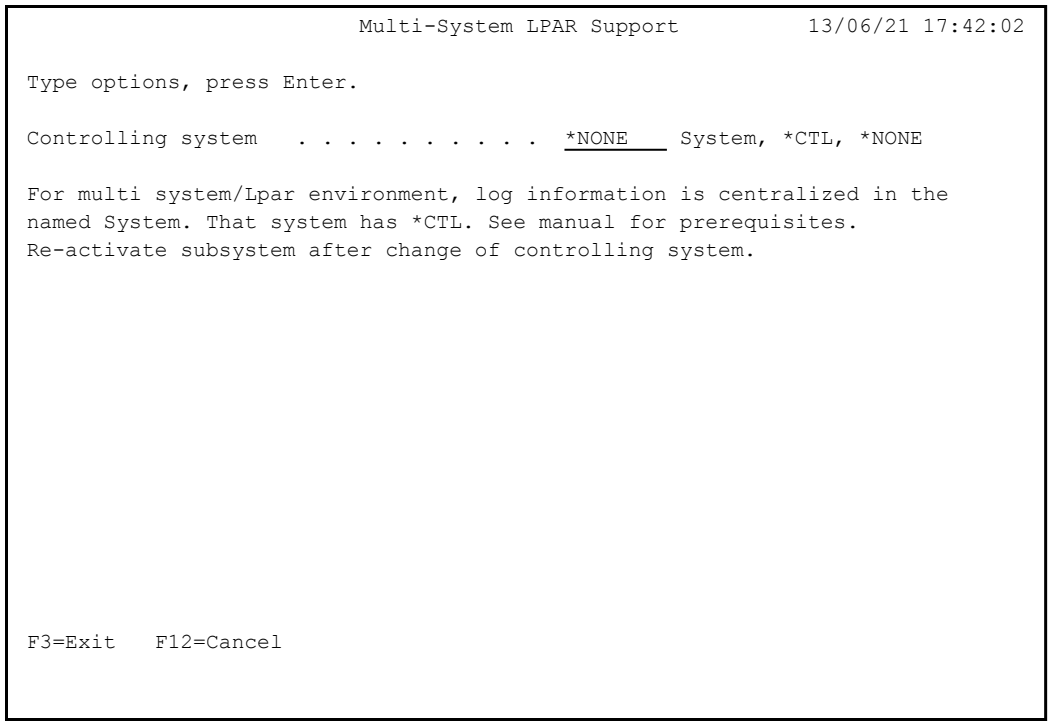
You can also use wildcard characters, set in the **Single character is represented by symbol** field to leave space for a specified number of

characters to be entered by the user. In the example, the character is set as an exclamation point (**!**). Thus, you might set it to **CUSTCODE-!!!!!-AUTH**. The user must then enter a customer code that is exactly five characters long, to be included in the reason.

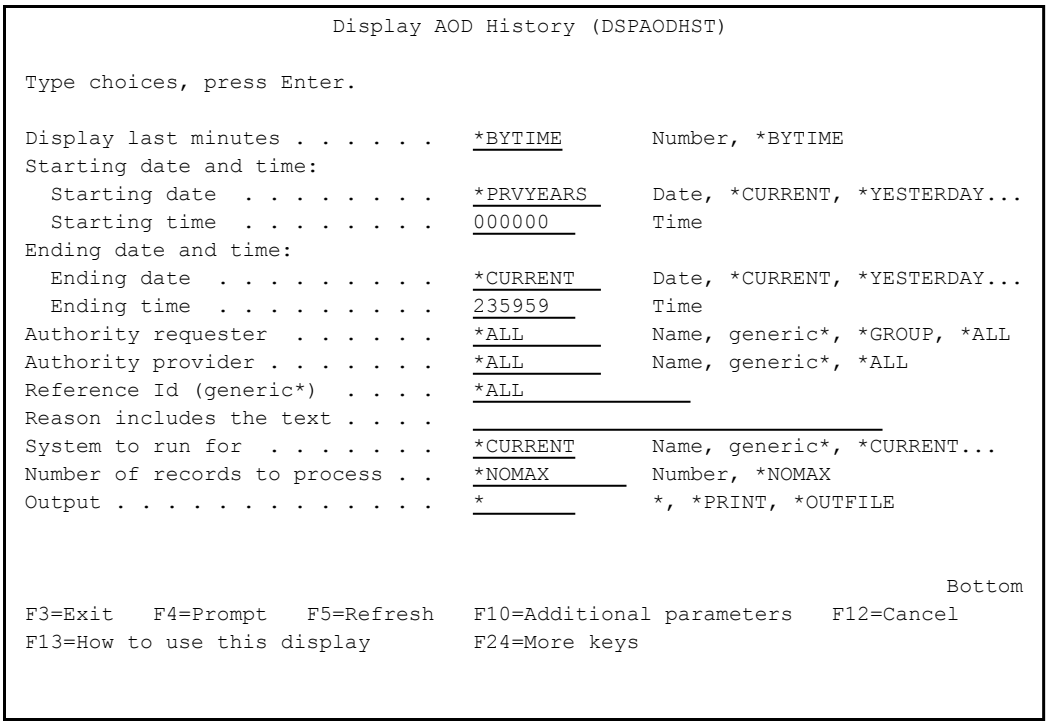
## Multi-System LPAR Support

To set one system to **collect information on Authority on Demand sessions on other systems**, set the **`Controlling System`** field on the **Multi-System LPAR Support** screen (*STRAOD* **`> 81 > 7`**) for that system to **`*LOCAL`**.

To set other systems to **send information on Authority on Demand sessions to that system**, set the **`Controlling System`** field on the **Multi-System LPAR Support** screen (*STRAOD* **`> 81 > 7`**) for those systems to the name of that collecting system. System names are defined through the **Work with Network Systems** screen within **Base Support**, as shown under **Network Support** in the iSecurity Installation and Base Support Manual.




To **`include information on all the systems`** in reports, set the **`System to run for`** field on, for example, the **Display AOD History (DSPAODHST)** screen (*STRAOD* **`> 41`**) to **`*ALL`** on the collecting system.



```
                        Display AOD History (DSPAODHST)

Type choices, press Enter.

Display last minutes . . . . . *BYTIME       Number, *BYTIME
Starting date and time:
  Starting date  . . . . . . . *PRVYEARS     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . . . 000000        Time
Ending date and time:
  Ending date  . . . . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . . . 235959        Time
Authority requester  . . . . . *ALL          Name, generic*, *GROUP, *ALL
Authority provider . . . . . . *ALL          Name, generic*, *ALL
Reference Id (generic*)  . . . *ALL
Reason includes the text . . . _____________________________
System to run for  . . . . . . *CURRENT      Name, generic*, *CURRENT...
Number of records to process . . *NOMAX      Number, *NOMAX
Output . . . . . . . . . . . . . *           *, *PRINT, *OUTFILE


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

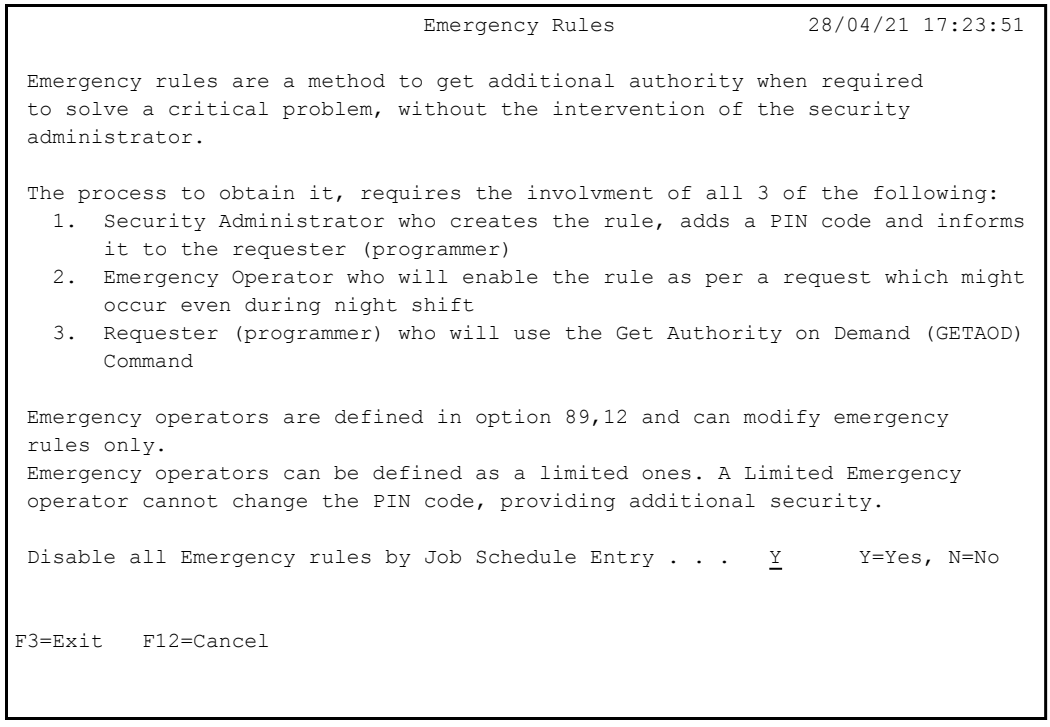
# Emergency Rules

To solve critical problems when a Security Administrator may not be available (such as during midnight shifts), Authority on Demand includes emergency rules.

The authorization to get AOD is split between three entities:

- A Security Administrator who creates the rule
- An Emergency Operator who enables the rule on request
- A Requester (usually a programmer) who uses the Get Authority On Demand (GETAOD) command.

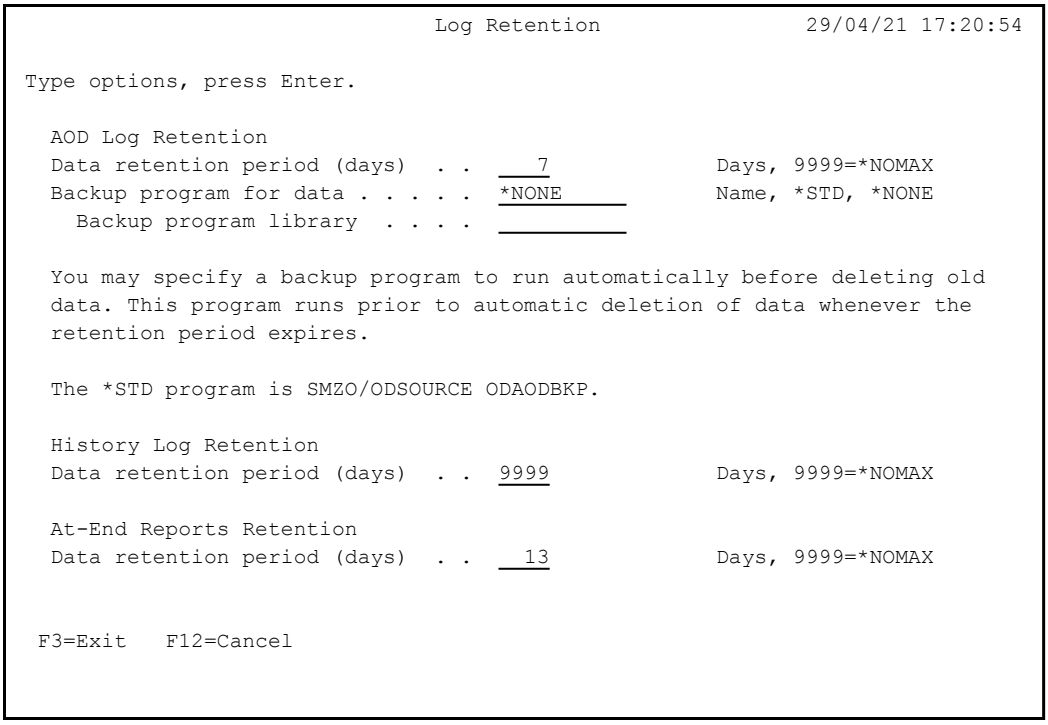
1. Select **11. Work with Operators** in the Maintenance menu to define Emergency Operators. These operators can modify emergency rules only. An Emergency Operator can be defined as a Limited Emergency Operator, with no ability to change PIN codes. This adds an additional layer of security. For more details, see *Operators*.
2. Select **8. Emergency Rules** from the **Authority On Demand System Configuration** menu. The **Emergency Rules** screen appears.



3. Select **Y** to disable all Emergency Rules by Job Schedule Entry or **N** to re-enable them.

## Retention Period

To **define how long to retain** Authority on Demand logs, history logs, and at-end reports, as well as the backup program for data, select **9. Log Retention** from the **Authority On Demand** System Configuration menu (*STRAOD* **> 81**). The **Authority on Demand Log Retention** screen appears.




The body of the screen contains these fields:

**AOD Log Retention**

**Data retention period (days)**

The number of days for which Authority on Demand data is retained. To retain it indefinitely, set this field to **9999**.

**Backup program for data**

The program used to automatically back up the data before it is deleted. To use the standard program, **SMZO/ODSOURCE ODAODBKP**, set this field to ***STD**. To skip running a backup program, set this field to ***NONE**.

**Backup program library**

The library containing the backup program.

**History Log Retention**

**Data retention period (days)**

The number of days for which historical data is retained. To retain it indefinitely, set this field to **9999**.AOD Log Retention

**At-End Reports Retention**

**Data retention period (days)**

The number of days for which at-end reports are retained. To retain them indefinitely, set this field to **9999**.

## Audit reports for Authority On Demand Activity

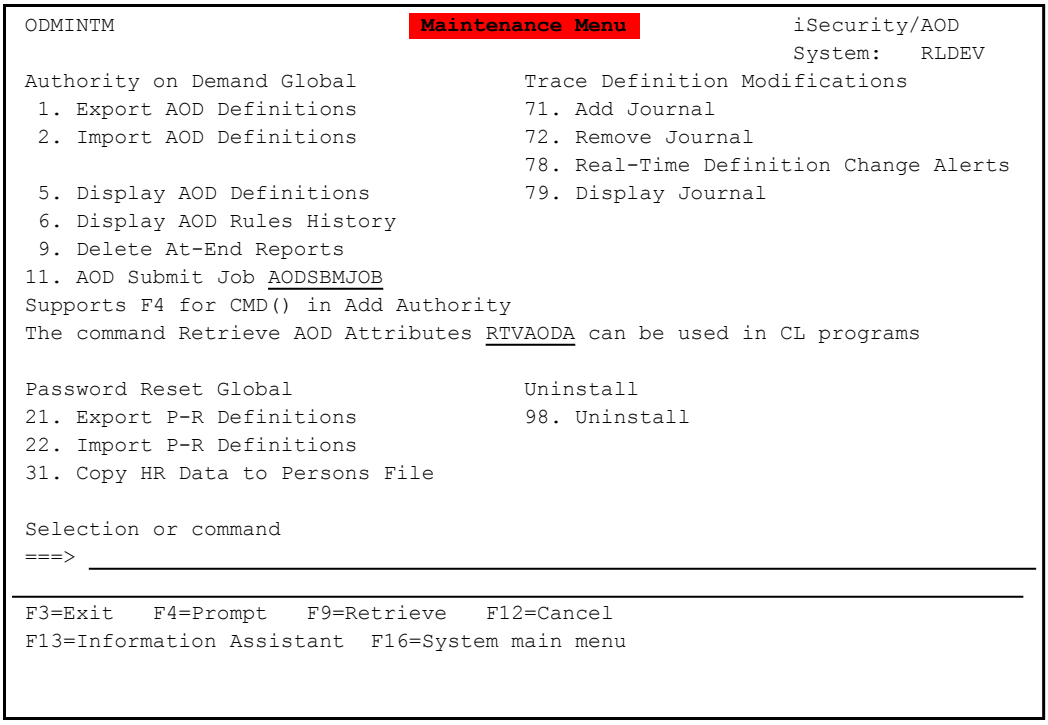
Two configuration parameters define which Audit reports are produced from Authority On Demand at the end of the Authority On Demand job. The two parameters are the **Use iSecurity/Audit for QAUDJRN** in the **Attachment Setup** screen (accessed by **4. Attachment Setup** in the System Configuration menu) and the **Attach Activity Log** in the **Session End Activity** screen (accessed by **8. Session End Activity** in the System Configuration menu). The table below shows the result of each combination of parameters.

In addition, you can use options **51 – 55** to run various Audit reports. For full information on these reports, please see the Audit User Manual.

| Parameter Combination | Result |
| --- | --- |
| • **Use iSecurity/Audit for QAUDJRN** = **Y**<br>• **Attach Activity Log** = **Y** | Runs **Audit** query **ZCD_ALL** for all commands. |
| • **Use iSecurity/Audit for QAUDJRN** = **Y**<br>• **Attach Activity Log** = **Y** | Runs **Audit** query **ZCD_ALL** for all commands initiated by Authority On Demand. |
| • **Use iSecurity/Audit for QAUDJRN** = **Y**<br>• **Attach Activity Log** = **N** | No **Audit** Report |
| • **Use iSecurity/Audit for QAUDJRN** = **N**<br>• **Attach Activity Log** = **Y/C** | Displays the QAUDJRN journal for the current receiving chain for all **CD** type entries for a given job name, user, and number |
| • **Use iSecurity/Audit for QAUDJRN** = **N**<br>• **Attach Activity Log** = **N** | No **Audit** Report |

# Maintenance Menu

The **Maintenance Menu** enables you to set and display global definitions for Authority on Demand. To access the **Maintenance Menu**, select **82. Maintenance Menu** from the main menu.

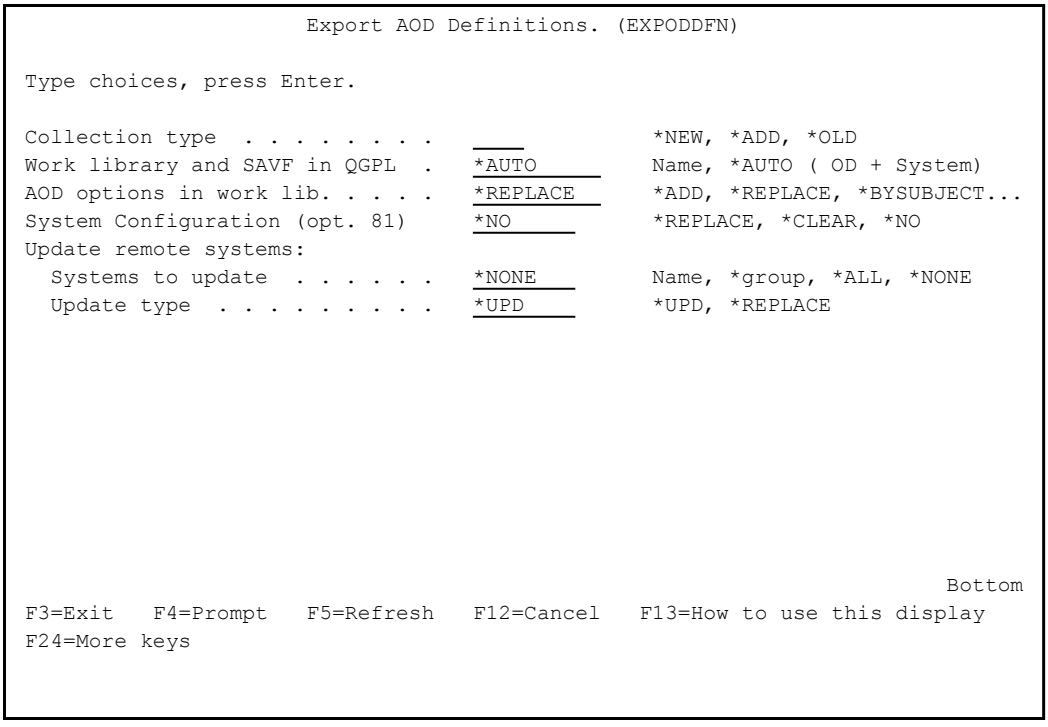


# Export Definitions

Use this option to export the entire set of AOD definitions from one computer to another. Use this option when you initially set up your system or if you add a computer to your organization. You can either send the definitions to target computers where they will be updated automatically, or you can save the definitions and use the Import Definitions to import the definitions to the target computer at a late date.

To export individual rules, see Exporting Authority Rules for details.

1. Select **`1. Export Definitions`** from the **`Authority On Demand System Maintenance`** menu. The **`Export AOD Definitions`** screen appears.




2. Click **`F9`** to see all the parameters, enter the required fields as defined below and press **`Enter`**.

| Parameter | Description |
|---|---|
| **Collection Type** | ***NEW** = designates the first time the Collection is being exported<br>***ADD** = use this to designate that the exported information should be added to an existing collection<br>***OLD** = |
| **Work library and SAVF in QGPL** | **Name** = type a name for the work library and save file.<br>***AUTO** = the system builds the file and library name for you |
| **AOD options in work lib** | ***ADD** = add to a previously exported definition<br>***REPLACE** = replace a previously exported definition<br>***BYSUBJECT** = export definitions by subject (provider and so on) |
| **Update remote systems:**<br>**Systems to update** | When exporting definitions, the user can choose to export and import at once by preparing the definitions in a SAVF and sending it to a remote system or several remote systems, and automatically import them into it.<br>**Name** = the name of a |

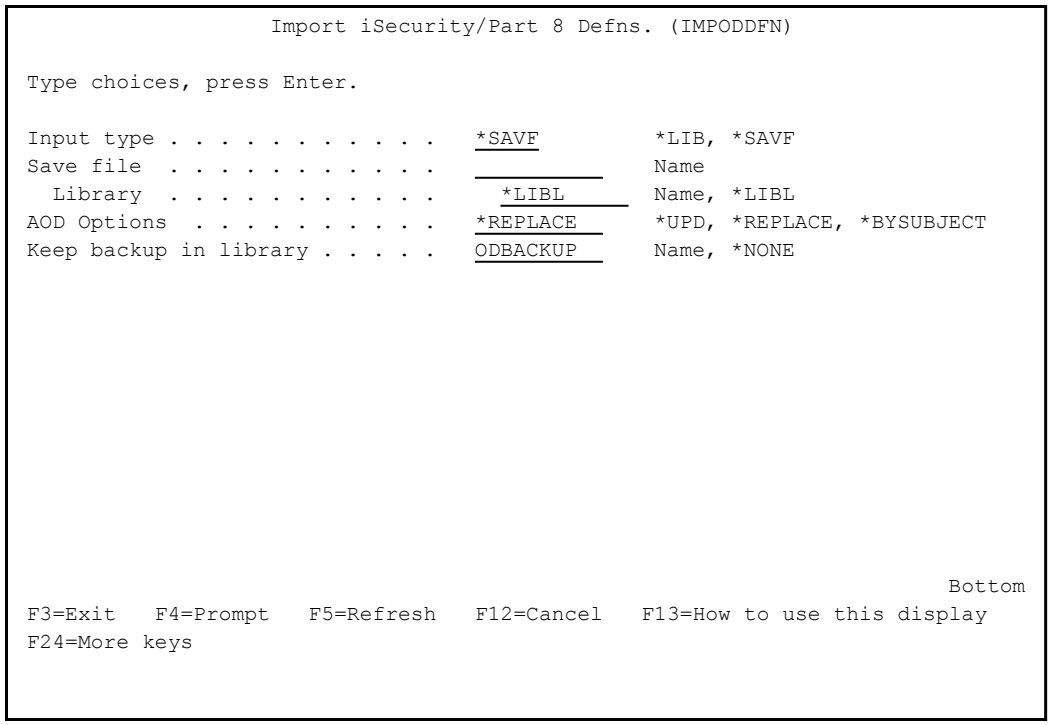
| Parameter | Description |
| --- | --- |
| | specific target system.<br>***group** = a group which contains a number of target systems<br>***ALL** = all systems belonging to the organization<br>***NONE** prepare the definitions for export at a later date |
| **Update remote systems:**<br>**Update type** | ***UPD** = Definitions that only exist on the source system are added to the target system, for definitions that exist on both systems on both systems the target system definition is replaced with the source system definition, and definitions that only exist on the target system are not changed<br>***REPLACE** the complete set of definitions on the source system replaces the complete set of definitions on the target system. At the end of the process, both systems will have an identical set of definitions. |
| **Authority Providers** | ***ADD** = add new definitions to the target system |

| Parameter | Description |
|---|---|
| | ***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing with these definitions |
| **Authority On Demand Rules** | ***ADD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing with these definitions |
| **Time groups** | ***ADD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing with these definitions |

| Parameter | Description |
| --- | --- |
| **Product operators** | ***ADD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing with these definitions |

## Import Definitions

1. Select **2. Import Definitions** from the **Authority On Demand System Maintenance** menu. The **Import AOD Definitions** screen appears.




2. Click **F9** to see all the parameters, enter the required fields as defined below and press **Enter**.

| Parameter | Description |
|---|---|
| **Input Type** | *SAVF<br>*LIB |
| **Save File** | Type the name of the Save File |
| **Library** | Type the name of the library that contains the Save File |
| **AOD Options** | ***UPD** = add to a previously imported definition<br>***REPLACE** = replace a previously imported definition<br>***BYSUBJECT** = import definitions by subject (provider and so on) |
| **Keep backup in library** | The name of the library where the pre-application version of the definitions will be stored. |
| **Authority Providers** | ***UPD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing |

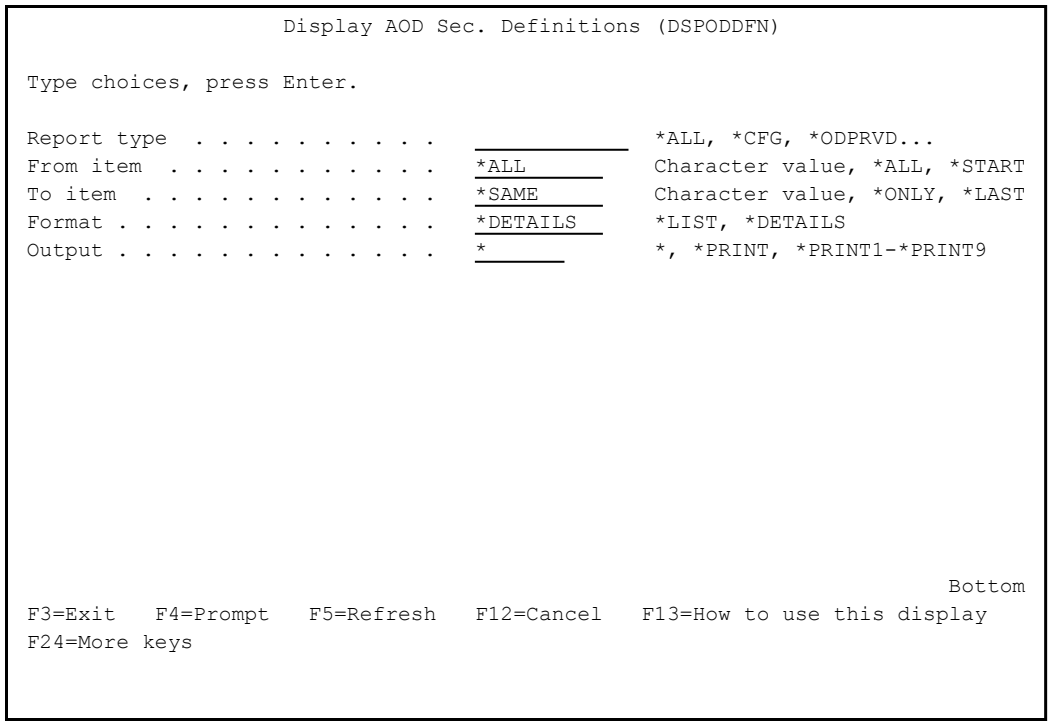
| Parameter | Description |
| --- | --- |
| | with these definitions |
| **Authority On Demand Rules** | ***UPD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing with these definitions |
| **Time groups** | ***UPD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported definitions<br>***CLEAR** = clear the exported definitions from the target system<br>***SAME** = do nothing with these definitions |
| **Product operators** | ***UPD** = add new definitions to the target system<br>***REPLACE** = replace existing definitions in the target system with the exported |

| Parameter | Description |
| --- | --- |
| | definitions<br>***SAME** = do nothing with these definitions |

## Display Definitions

This feature enables the user to display and print iSecurity Part One definitions:

1. Select **5. Display Definitions** from the **Authority On Demand System Maintenance** menu. The **Display AOD Sec. Definitions** screen appears.



| Parameter | Description |
|---|---|
| **Report Type** | Enter the type of report to produce:<br>***ALL** = Report on all definitions<br>***CFG** = Report on configuration definitions<br>***ODPRVD** = List of authority providers<br>***ODRULE** = List of authority rules<br>***ODTIMGRP** = List of time groups |
| **From Item** | Enter the beginning of the range of items to include in the report:<br>**Name** = Start from a specific item<br>***ALL** = Include all items<br>***START** = Start at the first items |
| **To Item** | Enter the end of the range of items to include in the report:<br>**Name** = End at a specific item<br>***SAME** =<br>***ONLY** = Only the item in the **From Item**.<br>***LAST** = End with the last item |

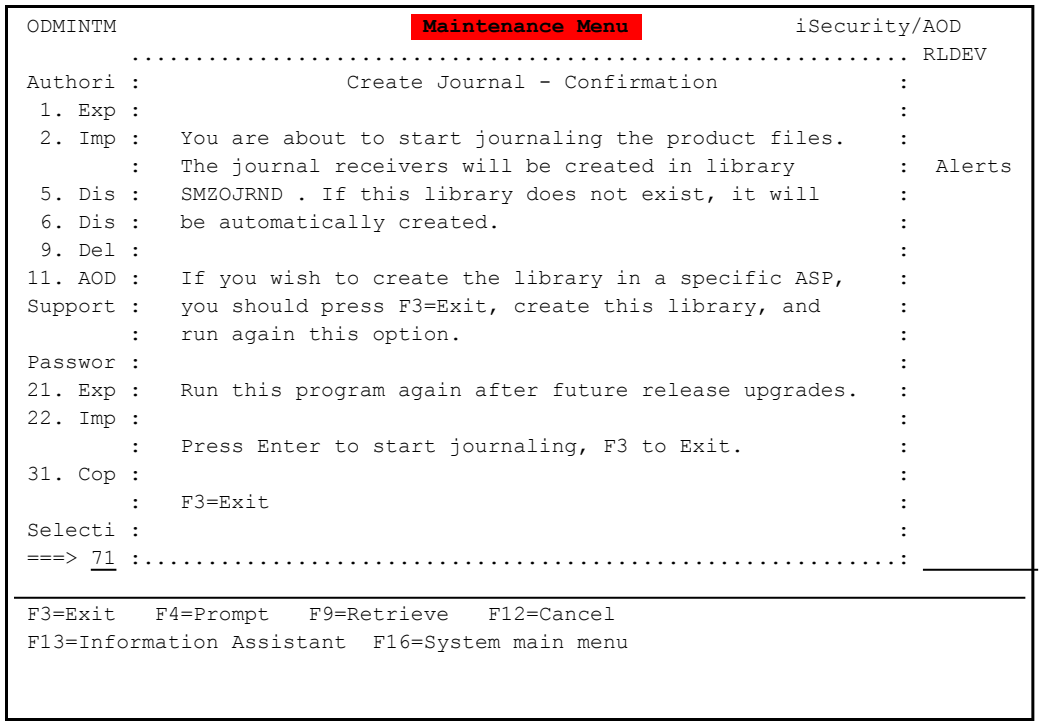
| Parameter | Description |
| --- | --- |
| **Format** | Enter the format to produce the report<br>***LIST** = Only a basic list is produced<br>***DETAILS** = Full details of the requested report |
| **Output** | Define where to send the output:<br>***** = Display the report on the screen<br>***PRINT** = Send the report to the print queue associated with *PRINT<br>***PRINT1** = Send the report to the print queue associated with *PRINT1<br>***PRINT2** = Send the report to the print queue associated with *PRINT2<br>***PRINT3** = Send the report to the print queue associated with *PRINT3<br>***PRINT4** = Send the report to the print queue associated with *PRINT4<br>***PRINT5** = Send the report to the print |

| Parameter | Description |
| --- | --- |
| | queue associated with *PRINT5<br>***PRINT6** = Send the report to the print queue associated with *PRINT6<br>***PRINT7** = Send the report to the print queue associated with *PRINT7<br>***PRINT8** = Send the report to the print queue associated with *PRINT8<br>***PRINT9** = Send the report to the print queue associated with *PRINT9 |

2. Select the desired **Report Type** from the **Display AOD Sec. Definitions** screen. After selecting the **Report Type**, the additional parameters appear. Not all parameters appear for all report types.
3. Select choices and press **Enter**.

## Add Journal

1. Select **71. Add Journal** from the **Authority On Demand System Maintenance** menu. The **Create Journal – Confirmation** screen appears.



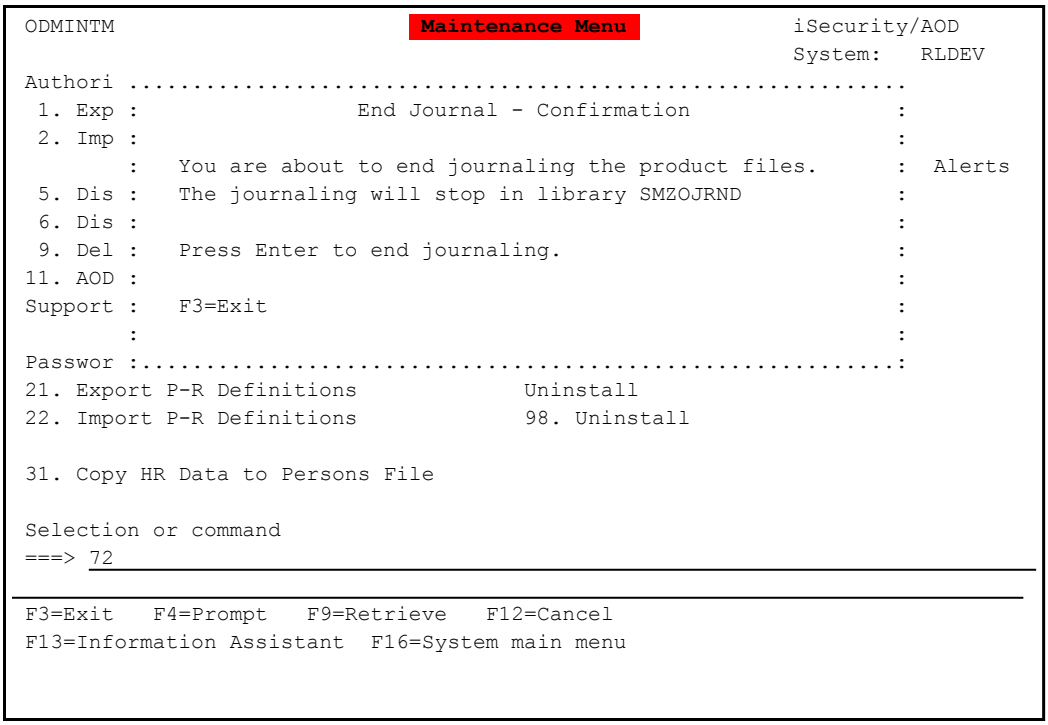

2. Press **Enter** to confirm. The process of journaling the product files begins. The journal receivers will be created in library **SMZ0JRND**. If this library does not exist, it will be automatically created.

Note: If you wish to create the library in a different ASP, press F3=Exit, create the library and run this option again.

You must re-run this option after every release upgrade.

# Remove Journal

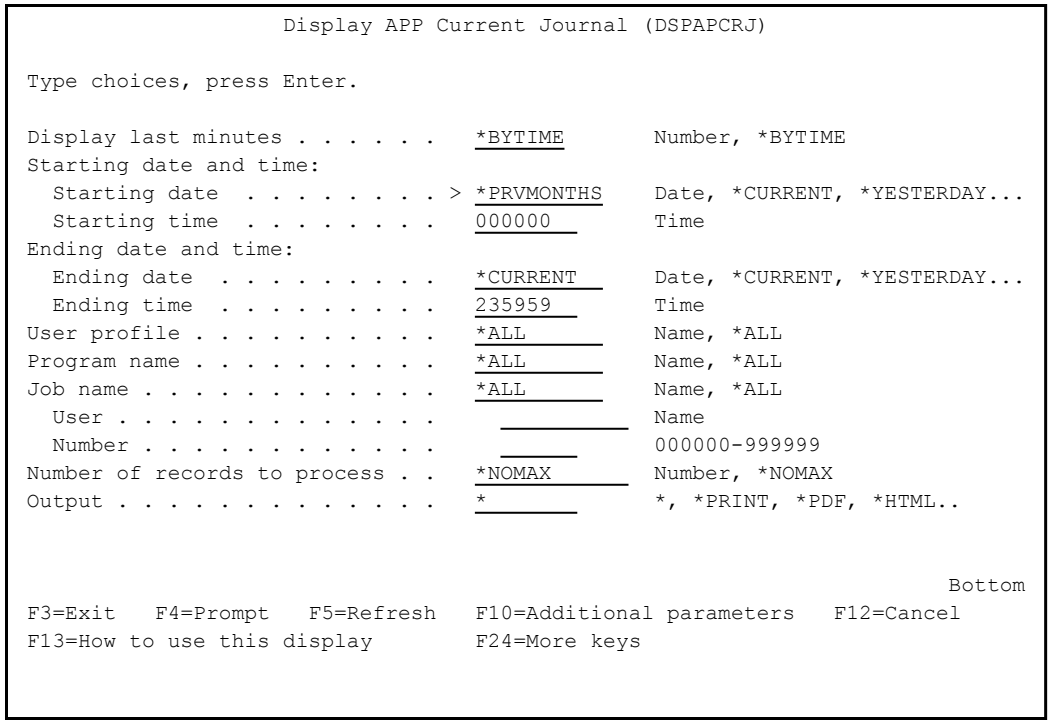
1. Select **72. Remove Journal** from the **Authority On Demand System Maintenance** menu. The **End Journal – Confirmation** screen appears.




2. Press **Enter** to confirm.

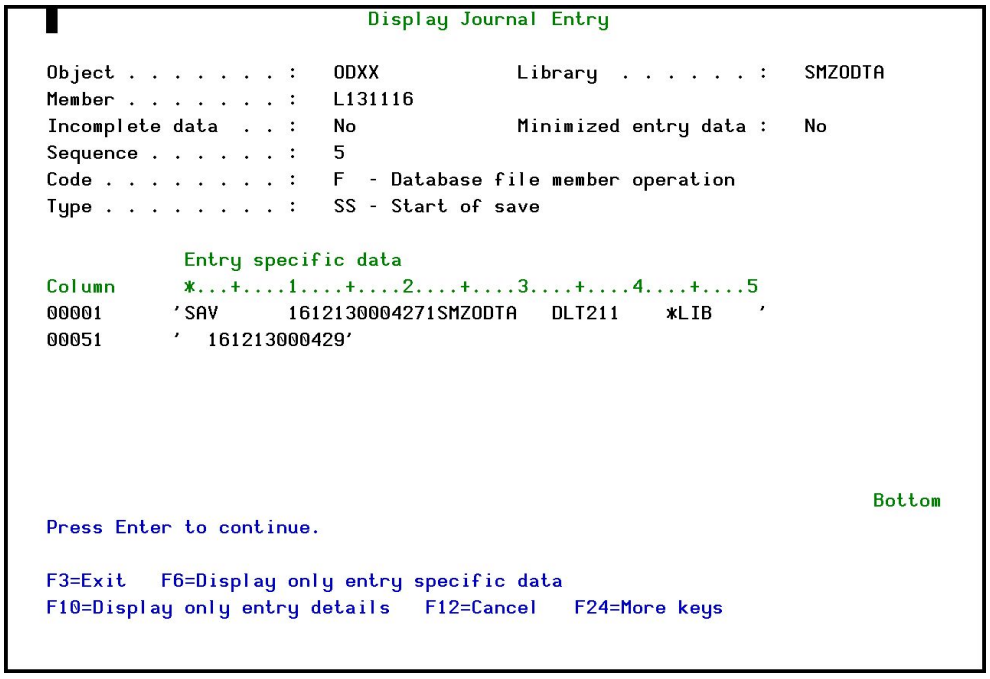
## Display Journal

1. Select **79. Display Journal** from the **Authority On Demand System Maintenance** menu. The **Display Journal (DSPJRN)** screen appears with preset filter parameters entered for you.



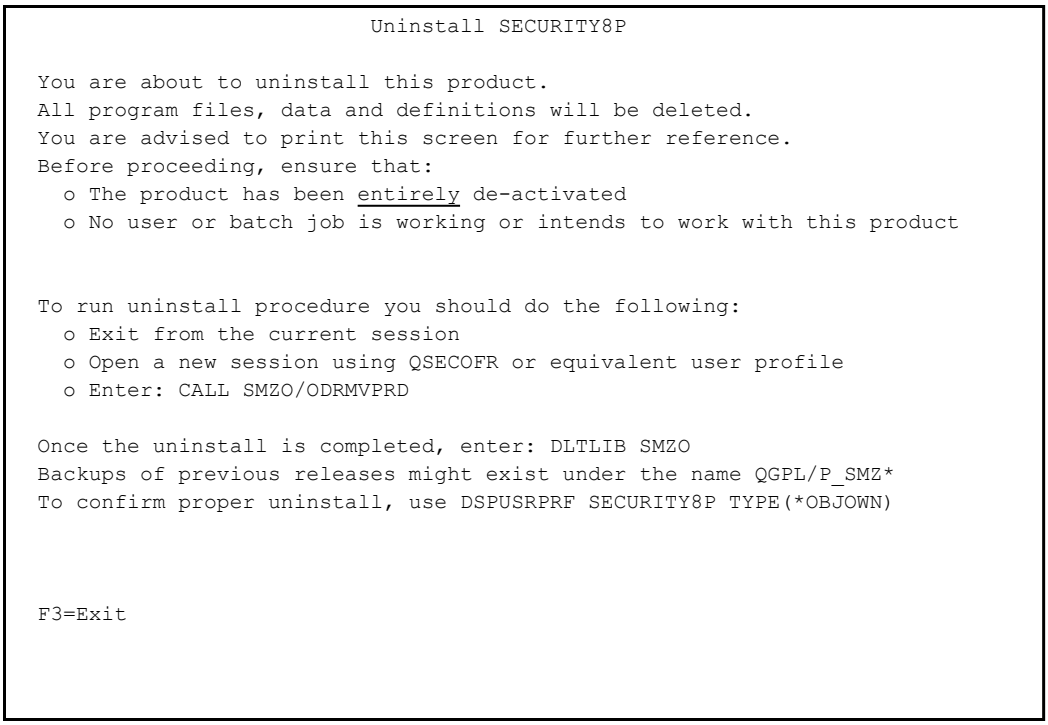
```
                    Display APP Current Journal (DSPAPCRJ)

Type choices, press Enter.

Display last minutes . . . . . *BYTIME       Number, *BYTIME
Starting date and time:
  Starting date  . . . . . . . > *PRVMONTHS   Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .   000000        Time
Ending date and time:
  Ending date  . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . . .   235959        Time
User profile . . . . . . . . .   *ALL          Name, *ALL
Program name . . . . . . . . .   *ALL          Name, *ALL
Job name . . . . . . . . . . .   *ALL          Name, *ALL
  User . . . . . . . . . . . .     __________  Name
  Number . . . . . . . . . . .     ______      000000-999999
Number of records to process . .   *NOMAX        Number, *NOMAX
Output . . . . . . . . . . . .   *             *, *PRINT, *PDF, *HTML..



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

2. Press **Enter**. The **Display Journal Entries** screen appears.
3. To display a specific entry, type **5** by that entry and press **Enter**. The **Display Journal Entry** screen appears.


Display Journal Entry
Object . . . . . : ODXX Library . . . . . : SMZODTA
Member . . . . . : L131116
Incomplete data . . : No Minimized entry data : No
Sequence . . . . . : 5
Code . . . . . : F - Database file member operation
Type . . . . . : SS - Start of save
Entry specific data
Column *...+....1....+....2....+....3....+....4....+....5
00001 'SAV 1612130004271SMZODTA DLT211 *LIB '
00051 ' 161213000429'
Bottom
Press Enter to continue.
F3=Exit F6=Display only entry specific data
F10=Display only entry details F12=Cancel F24=More keys

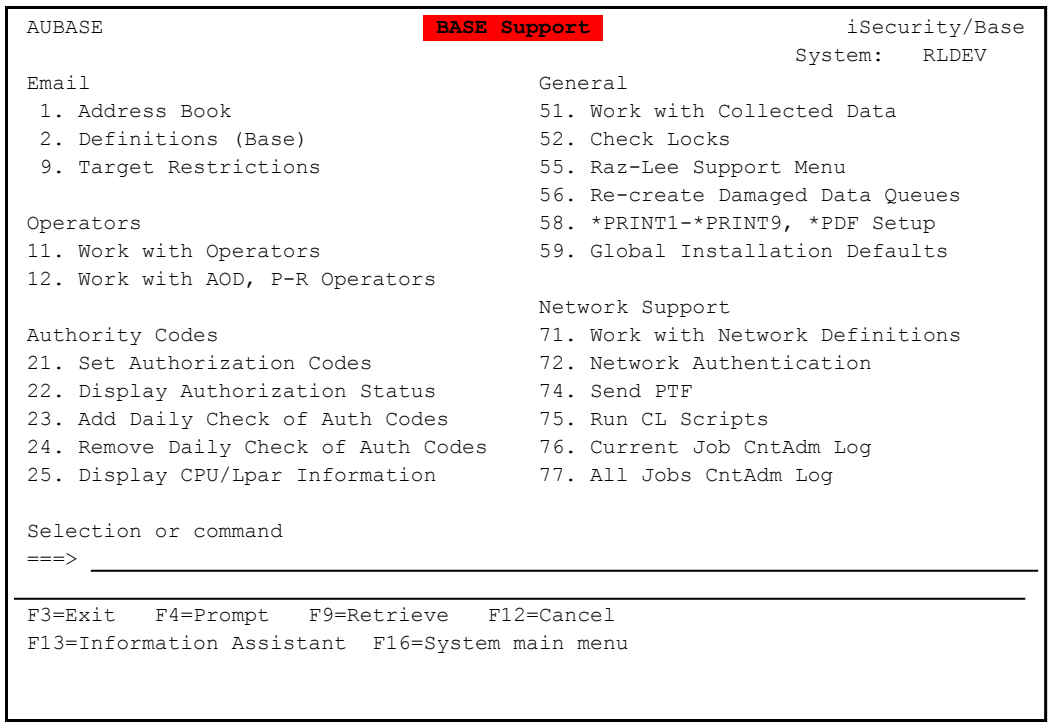
# Uninstall

To uninstall the Authority On Demand product, select **98. Uninstall Product** from the **Authority On Demand System Maintenance** menu, and follow the directions on the screen.



# BASE Support

The **BASE Support** menu enables you to work with various settings that are common for 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** from the Authority on Demand main menu.




The functions in the BASE Support menu are documented in the iSecurity Installation and Base Support manual, available at https://www.razlee.com/manuals/installation-base-support.