Authority on Demand™

The Authorization Security Component of

iSecurity

User Manual

Version 3

RAZ-LEE™

The iSeries Security Experts

Updated: 07/09/09

Copyright Notice

Visit our website at http://www.razlee.com .

Record your Product Authorization Code Here:

Computer Model:	
Serial Number:	
Authorization Code	

About This Manual

Who Should Read This Book

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

Product Documentation Overview

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

Printed Materials

This user guide is the only printed documentation necessary for understanding **Authority on Demand**. It is available in user-friendly PDF format and may be displayed or printed using Adobe Acrobat Reader version 4.0 or higher. Acrobat Reader is included on the product CD-ROM.

Authority on Demand includes a single user guide that covers the following topics:

- Introduction
- Installation
- Start-up and Initial Configuration
- Using **Authority on Demand**

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

Online Help

System i context sensitive help is available at any time by pressing the **F1** key. A help window appears containing explanatory text that relates to the function or option currently in use. Online help will shortly be available in Windows help format for viewing on a PC with terminal emulation.

Typography Conventions

- Menu options, field names, and function key names are written in **Sans-Serif Bold**.
- References to chapters or sections are written in *Italic*.
- OS/400 commands and system messages are written in ***Bold Italic***.
- Key combinations are separated by a dash, for example: **Shift-Tab**.
- Emphasis is written in **Times New Roman bold**.

TOC

Table of Contents

Chapter 1: System i Authority on Demand

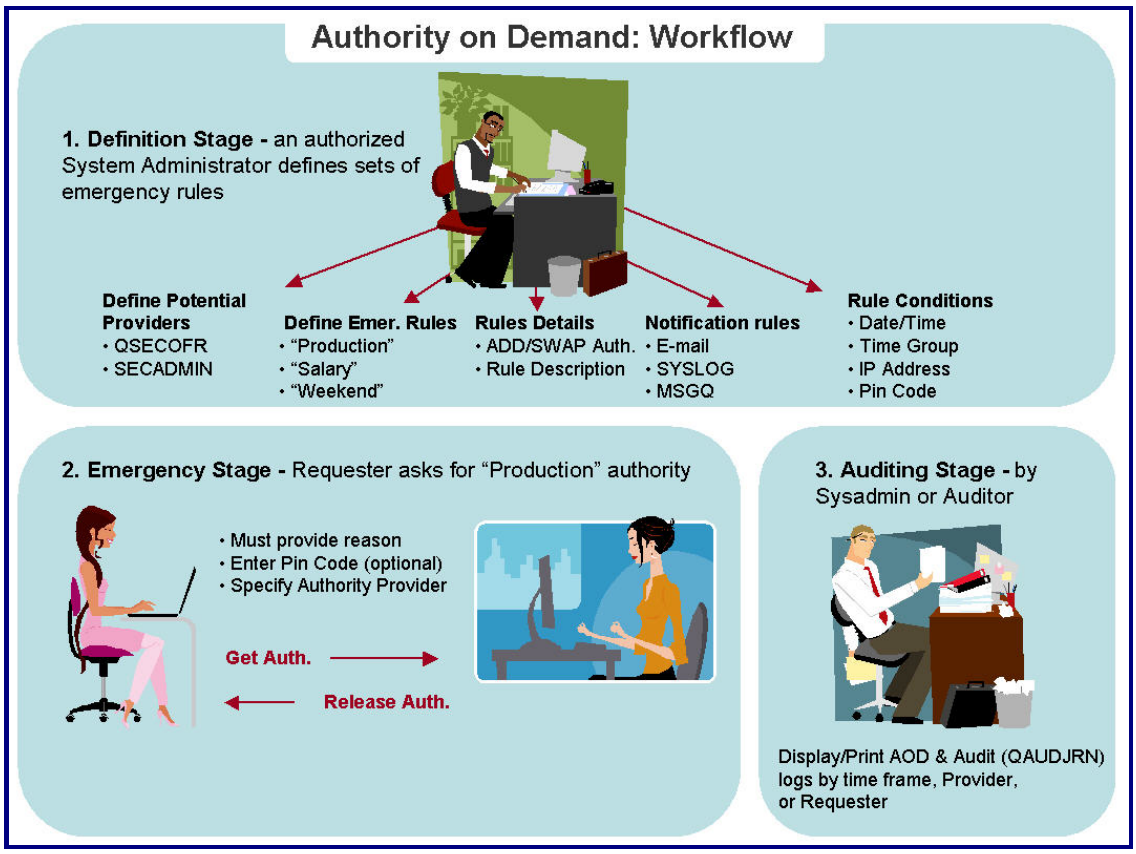
Overview

Emergency access to critical application data and processes is one of the most common security slips which are 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 as a result 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



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 requestor a totally new security authority level (SWAP) or add additional security rights to a requestor'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 recovering from different types of emergency situations with minimum risk of human error. For example, AOD can allow Ad Hoc access to critical data, can enable a programmer to run reports which abended, etc.

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.

Part of a Comprehensive Solution

AOD constitutes a major addition to iSecurity, and solidifies iSecurity's position as the most comprehensive security suite of products on the market for System i security and compliance solutions.

Version 3.0 – New Features:

1. New internal system allows **Emergency Operator** (**option 82 ->11**) limited access to rules definition.
2. Three levels of operator authorization can be defined from **option 82 -> 11:**

   1=*USE: For auditors only who will run reports on AOD user activities

   5=*EMERGENCY: User can edit emergency rules and give emergency rights to pre-defined users

   9=*FULL: Full product authorization capabilities

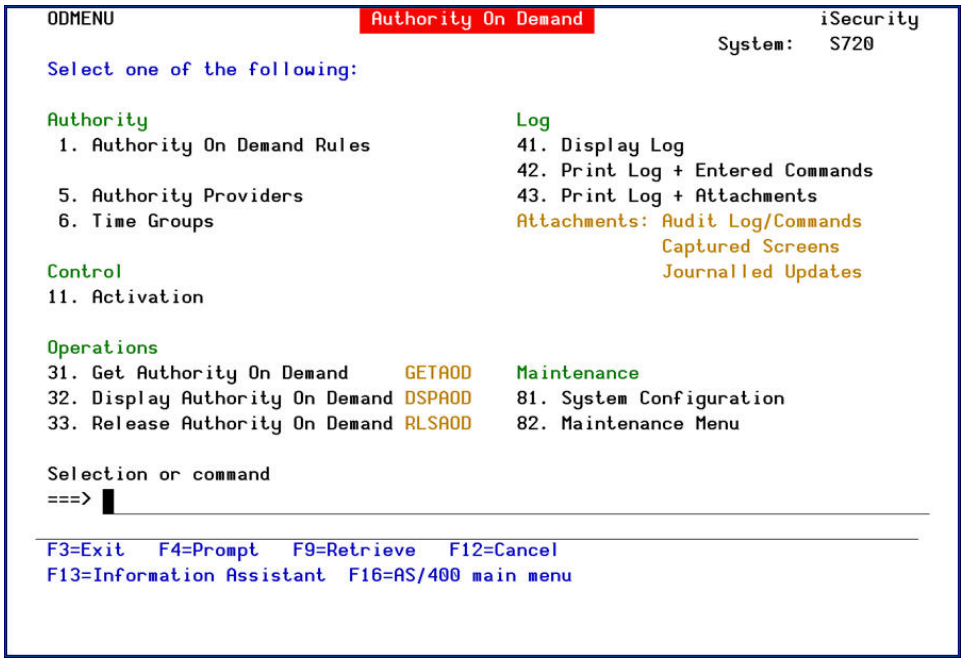
3. In the ***GETAOD*** command (**option 31**), the Reason field defaults to *BYPIN. This value is acceptable only if the PIN number was specified. The value *BYPIN is replaced by the rule explanation given by either the **Emergency Operator** or the product administrator respective to the type of rule and the existence of explanation (up to 240 chars).
4. A new option was added to the main menu, **option 11. Activation which activates the Authority on Demand monitor. This is needed i**n order to activate the feature that reports when the time period for extended authorities has ended, and to activate the Action feature.
5. **Logs**: using **Option 42** a user can print the activity log for command entries which is composed of **Audit** and **Journal** logs. Using O**ption 43** a user can print and attach activity logs, captured screens and journaled updates.
6. Define general time limit for session (**option 81->1**) or specific time limit per rule (**option 1 from the main menu**).
7. New **option 81-> 3** added to the menu with the ability to enter a user **Exit Program**.

   With **Exit Program** a user may specify a program name which will overrule the **Get Authority on Demand** decision to allow or reject the request. This program can also modify the reason given by the requester. A template program can be found in SMZO/ODSOURCE ODVERIFY.
8. New **option 81-> 21. Syslog Definitions** added to the menu. With this option a user can define whether to send a Syslog message, to what IP address, from which facility, in what range of severity and the message format.

Chapter 2: First Steps

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 starting working with **Authority on Demand**, type ***STRAOD***. The main menu appears



Authority on Demand main menu

Operators

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 for **Audit**.
- ***SECADM** - All users with ***SECADM** special authority- By default, this group has only Read authority for **Firewall**.

iSecurity product objects are secured automatically using product authorization lists (named security1P). This strengthens the internal security of the products. The product authorization lists are accessed in all products via option 81→,,, from the main product menu.

It is essential that **Work with Operators** be used to define all users who have ***SECADM, *AUDIT** or ***AUD#SECAD** privileges, but don't have all object authority. The AOD **Work with Operators** screen lists Usr (user management) and Adm authorities for all activities related to starting and stopping subsystems and jobs, import/export of definitions and so on.

iSecurity automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

Users may add more operators (i.e. user profiles), delete operators and give them authorities and passwords according to their own judgment. Users can even make the new operator's 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 users can be controlled as well.

If the system administrator wishes to set the default to *BLANK they should enter:

CRTDTAARA SMZTMPC/DFTPWD *char 10

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

To modify operator's authorities, follow this procedure.

1. Select **82. Maintenance Menu** from the main menu. The **Maintenance Menu** appears.
2. Select **11. Work with Operators** from the **Maintenance Menu**. The **Work with Operators** screen appears.
3. Press **F6** to add new user

4. Select the user level of authority:

   1=*USE: For auditors only who will run reports on AOD user activities

   5=*EMERGENCY: User can edit emergency rules and give emergency rights to pre-defined users

   9=*FULL: Full product authorization capabilities

   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.

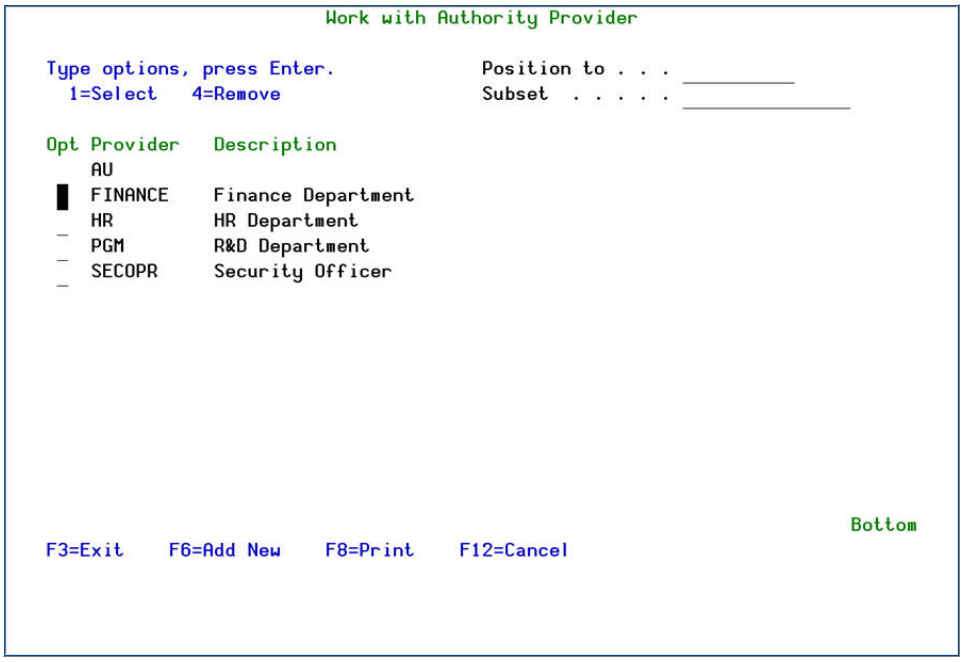
   The Authority list is created in the installation/release upgrade process.

   The SECURITY_P user profile is granted Authority *ALL whilst the *PUBLIC is granted Authority *EXCLUDE.

   All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

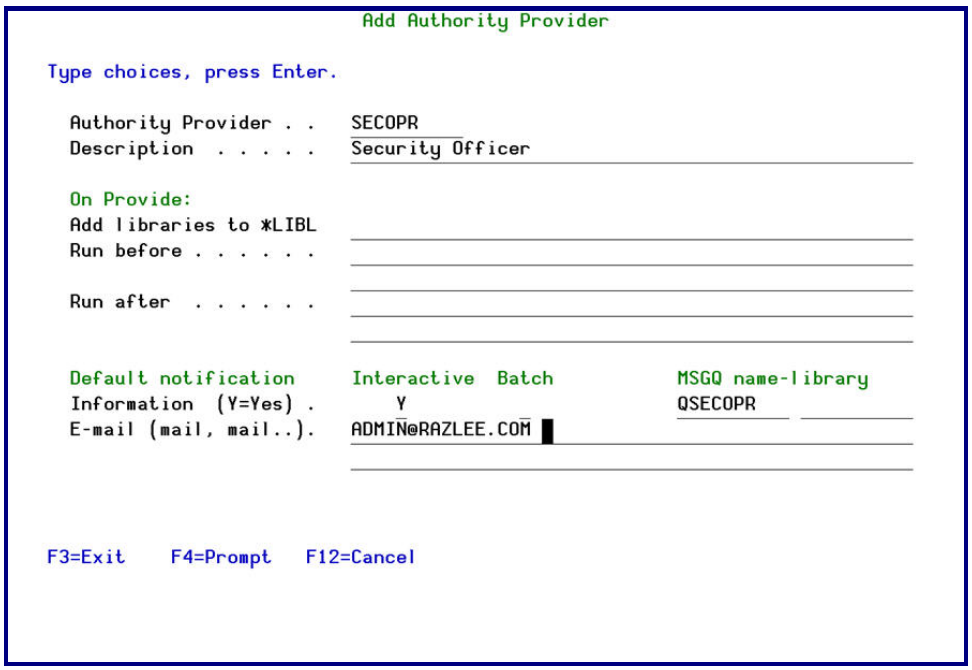
Authority Provider

1. Select option **5. Authority Providers.** 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

2. Press **F6** to add a new authority provider



Add Authority Provider

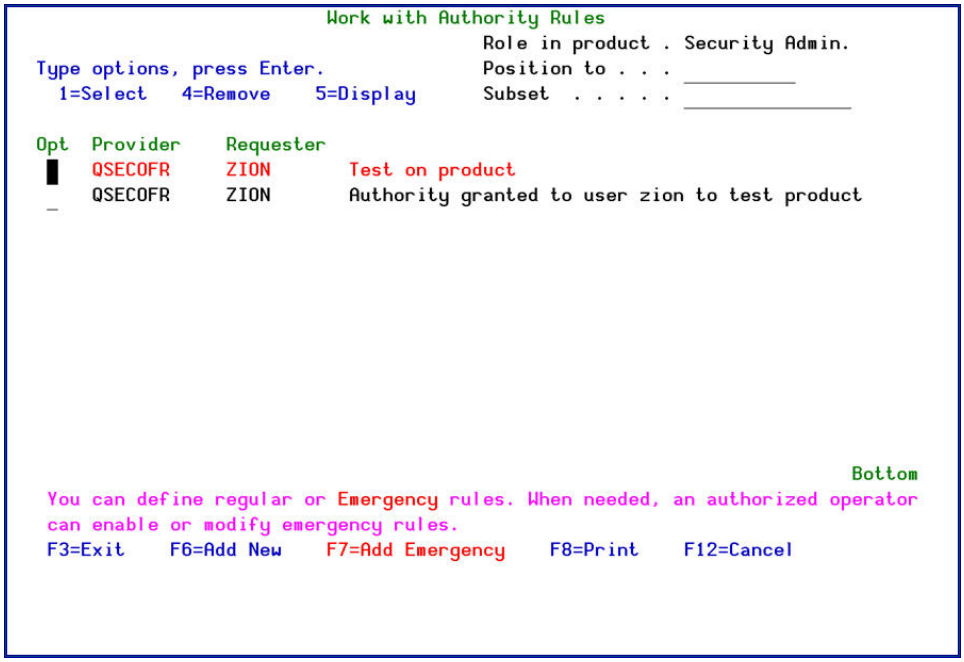
3. Type an existing user profile or press **F4** to prompt a list of users for selection.
4. Type a descriptive text.

Option	Description
Add libraries to *LIBL	Add additional libraries access authorization to *LIBL. Type in a list of libraries separated by a space.
Run before	Type the name of a program you want to execute immediately before the new authorization is applied.
Run after	Type the name of a program you want to execute immediately after the new authorization is applied.

5. 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.

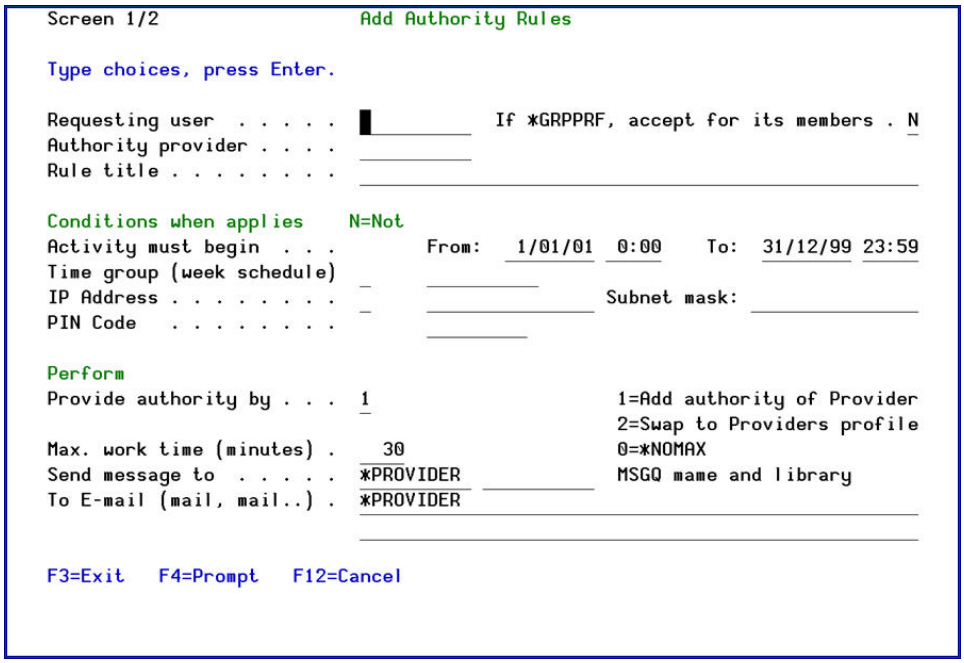
Authority Rules

1. Select option **1. Authority on Demand Rules** from the main menu



Work with Authority Rules

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



Add Authority Rules

3. In the **Requesting user** field, enter the profile of the user that requested the authorization, or press **F4** to obtain a list of users for selection.
4. Type the name of the authority provider in the **Authority Provider** field.
5. Type a description of the request for this temporary authorization in the **Rule title** field
6. Add conditions to determine when the rule should apply and when the authority should be provided (optional):

Parameter	Description
Time Set	Blank=Yes, N=Not this "Time Set" Define when the rule applies and the user can request the temporary authorization. Press F4 to select or create a time group.
PIN Code	Add additional security password. Not a mandatory field
IP Address	Blank=Yes, N=Not this "IP Address/Subnet mask" Define IP address and subnet mask. Press F4 to select from a list of possible subnet masks.

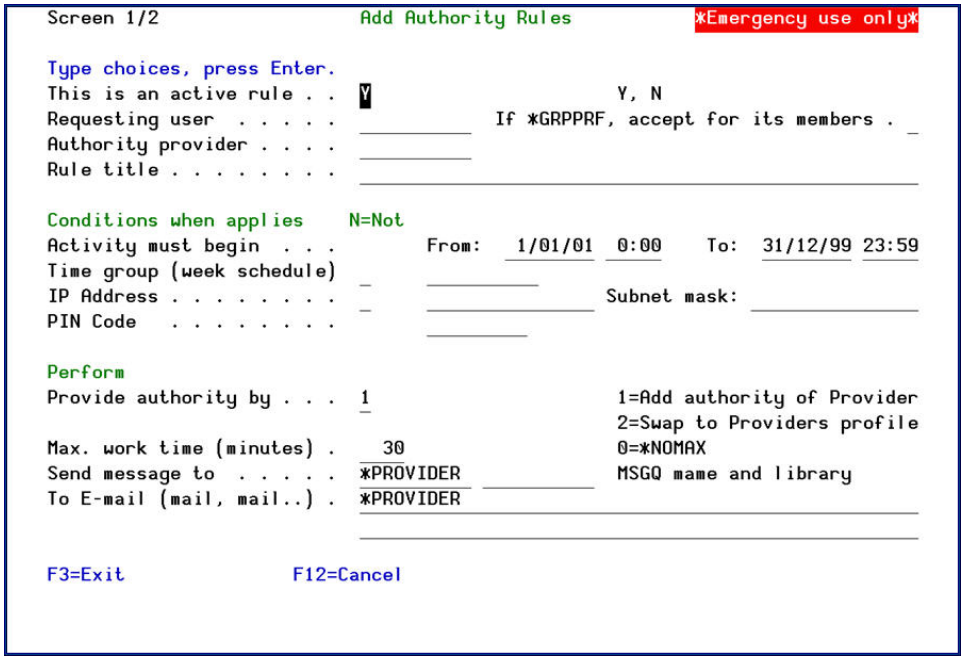
7. Select the type of the authority requested; add or swap authorizations.

NOTE: *Selecting option **2** "Swap" will also swap the user name in the records and logs. Using option **1** "Add" will give the Requester the authorities of the Provider in addition to the existing authorities. In this case the original requester user profile will be kept and will appear in the records and logs.*

8. Limit the work time in minutes. Type **0** for unlimited amount of minutes.
9. Define an action to execute when the new authorization takes effect. Sending the message to a MSGQ and/or an email address.

Emergency Rule

1. Press **F7** to add emergency rule

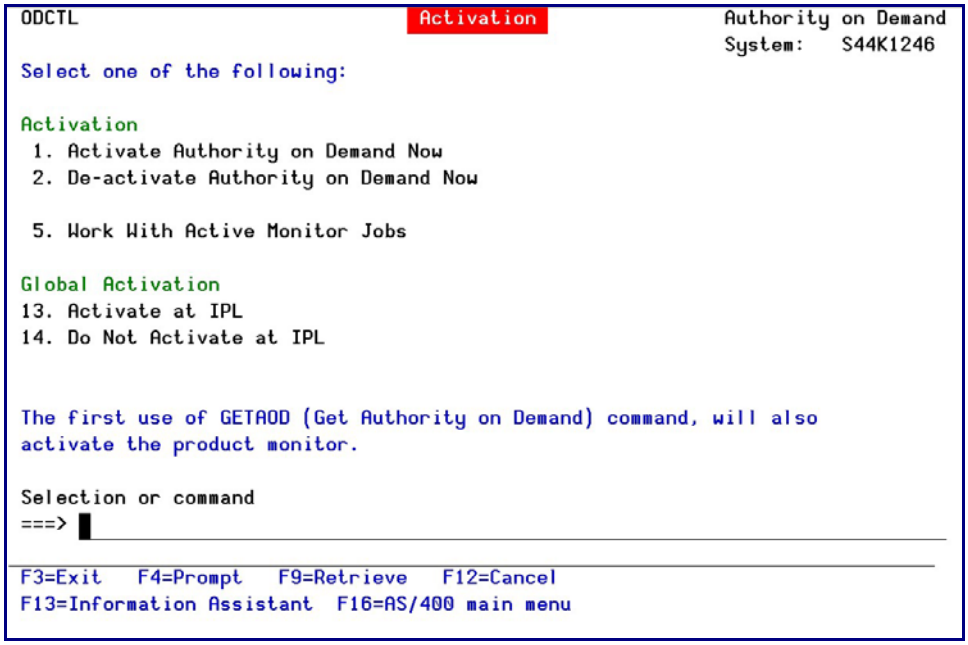


Emergency Rules

In **Emergency Rules** the PIN field is mandatory and only a user profile with emergency operator authority (see ***chapter 2: First Steps - Operators***) allowed to change this rule.

Activation

Activate the **Authority on Demand** monitor in order to activate the message that stipulates that work time is over and to activate the action feature (***see chapter 3: System configuration, General Definitions***).



Activation

It is strongly recommended that you configure **Authority on Demand** to activate automatically each time an IPL occurs on your System i.

To work with activation, select **11. Activation** from the main menu.

Manual Activation

- To manually activate the **Authority on Demand** monitor, select **1. Activate Capture Now** from the **Activation** menu.
- To manually de-activate the **Authority on Demand** monitor, select **2. De-activate Capture Now** from the **Activation** menu.

Automatic Activation

- To activate **Authority on Demand** automatically each time an IPL occurs, select **13. Activate at IPL** from the **Activation** menu.
- To cancel automatic activation, select **14. Do Not Activate at IPL** from the **Activation** menu.

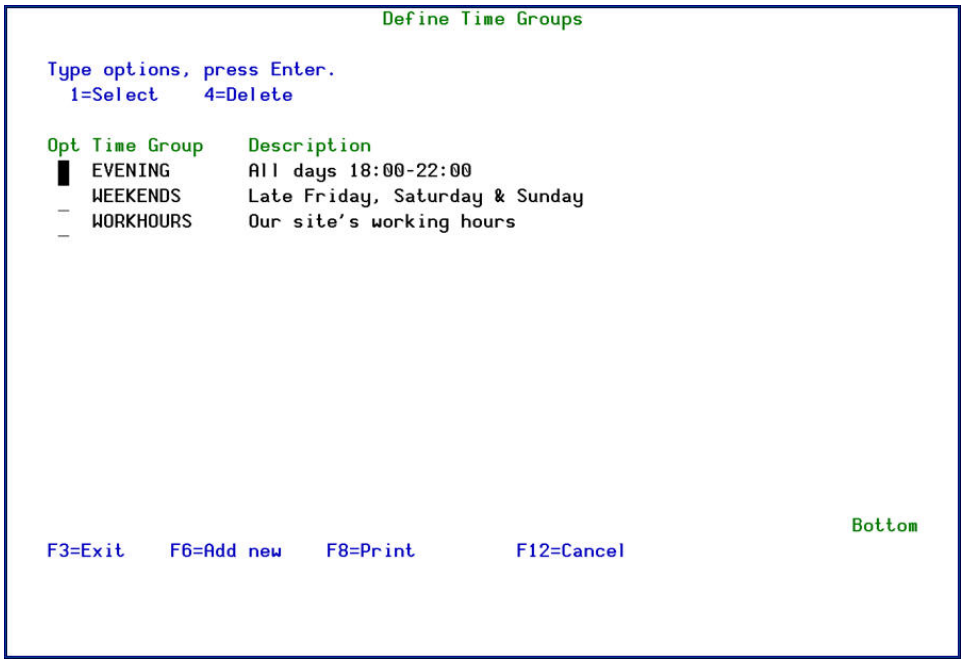
Verifying that the Authority on Demand Monitor is Active

Select **5. Work With Active Monitor Jobs** from the **Activation** menu to view the **Authority on Demand** monitor subsystem. The **Work with Subsystem Jobs** screen appears. It should display several lines similar to those on the screenshot below.

Time Groups

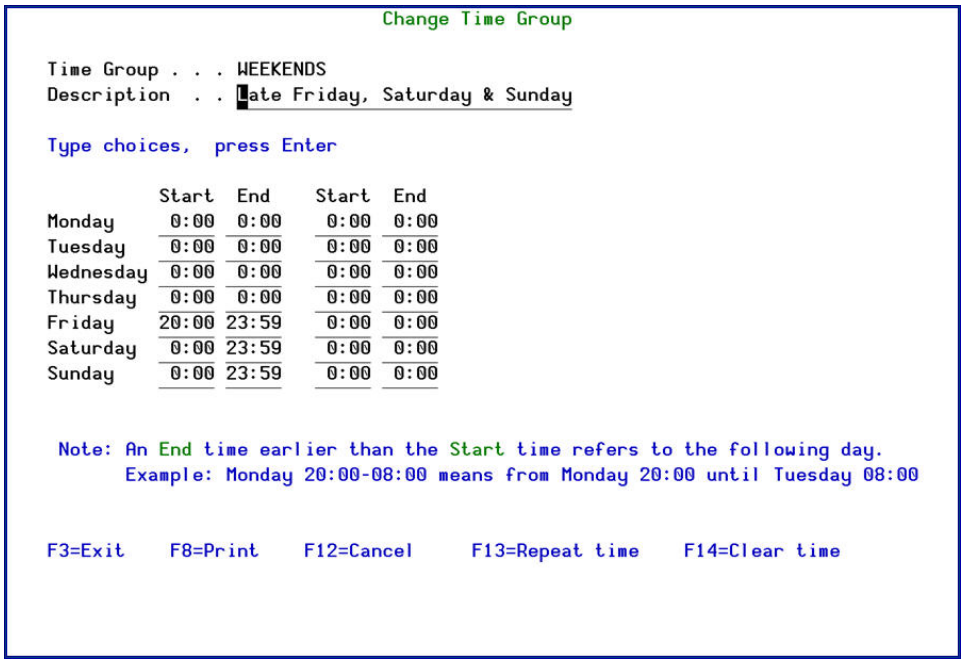
Time groups are sets of time and day parameters that can be used as filter criteria when working with authority rules.

1. Select option **6. Time Groups** from the main menu



Define Time Groups

2. Type **1** to select a time group for modification or press **F6** to add a new time group



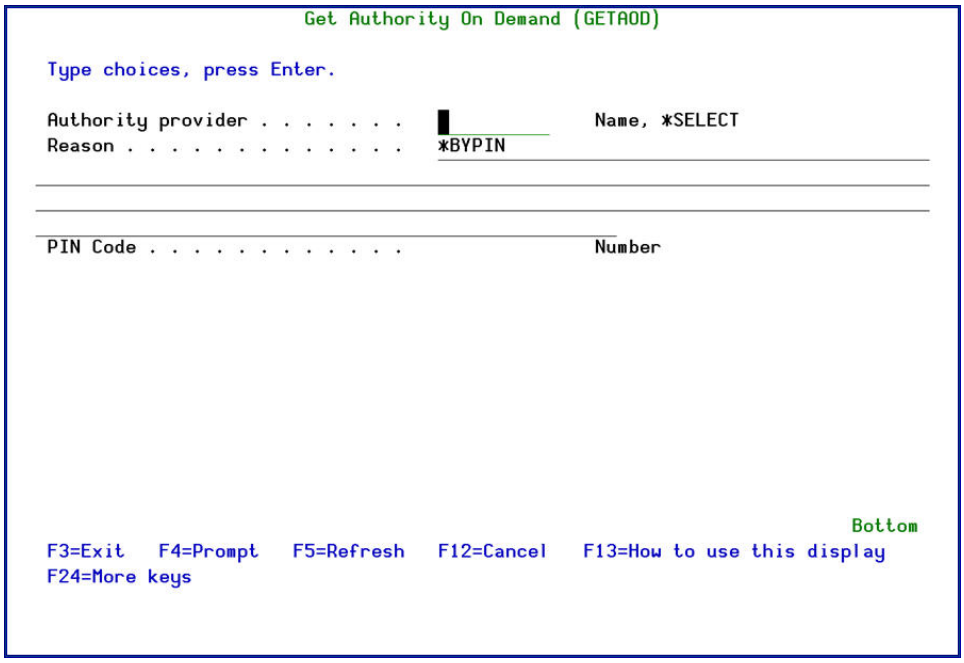
Add Time Group

3. Type a time group name and description
4. Enter start and end times for each period using 24 hour notation

Option	Description
F13	Copy start and end times from cursor line to all subsequent days
F14	Erase the start and end times for the cursor line and below

Get Authority on Demand

To activate Authority on Demand, log in with the requester user profile, type the command ***GETAOD*** on a command line or ***STRAOD*** and select option **31. Get Authority on Demand**



Get Authority on Demand

1. Insert the authorities provider user profile
2. The Reason field has been extended to 240 chars and its default is to *BYPIN. This value is acceptable only if PIN number was specified.
3. Enter the PIN code as defined in the previous step: *Authority Rules*

Display Authority on Demand

To display the new authorization currently in use, type the command ***DSPAOD*** on a command line or ***STRAOD*** and select option **32. Display Authority on Demand**

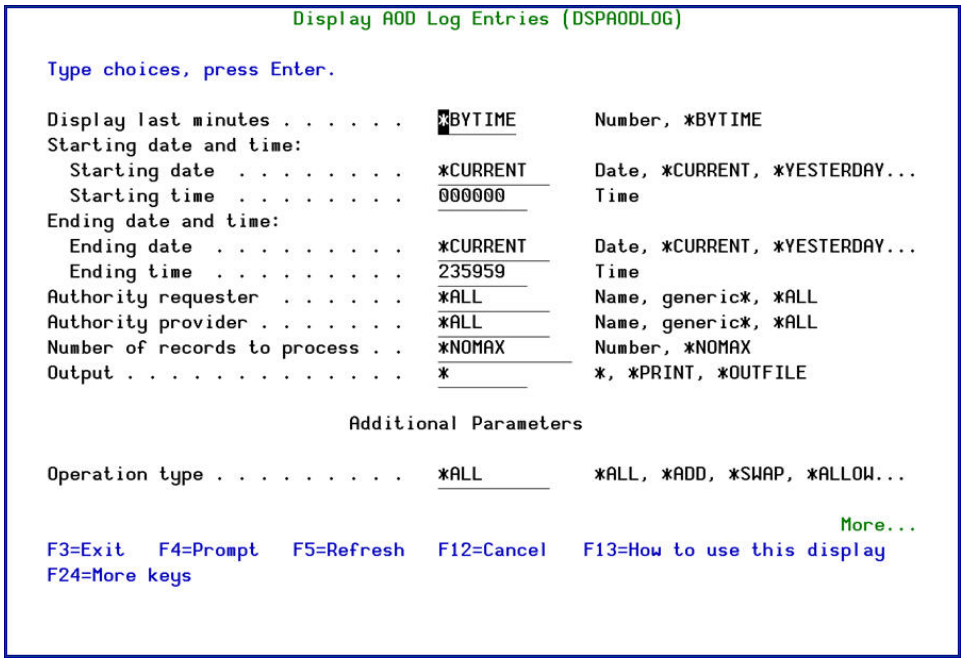
Release Authority on Demand

To release Authority on Demand and work with the standard authorizations, type the command ***RLSAOD*** on a command line or ***STRAOD*** and select option **33. Release Authority on Demand**

Log

Display the Authority on Demand activity log to view the contents of the history log quickly and easily in a standard format using basic filter criteria.

1. Type ***DSPAODLOG*** on a command line or ***STRAOD*** and select option **41. Display Activity Log**



Display AOD Log Entries (DSPAODLOG)

Parameter	Description
Display last minutes	Selects only those events occurring within the previous number of minutes as specified by the user **Number** = Enter the desired number of minutes ***BYTIME** = According to start and end times specified below
Starting date & time **Ending date & time**	Selects only those events occurring within the range specified by the start and end date/time combination **Date and time** = Enter the appropriate date or time ***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
Authority requester	User profile who requested the authorization
Authority provider	an existing user profile that provides the authorization
# of records to Process	Maximum number of records to process

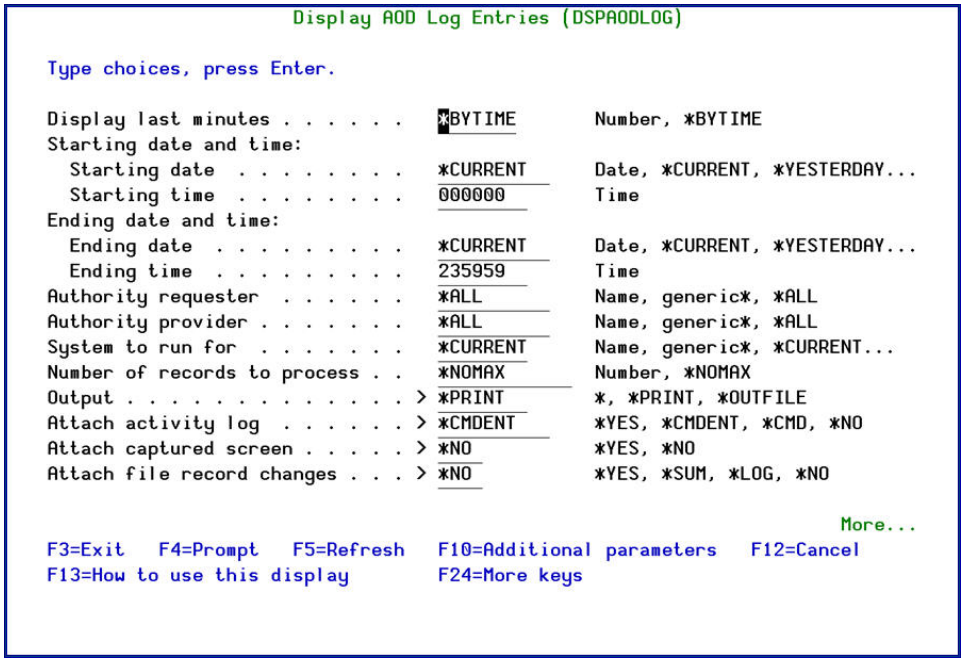
	***NOMAX** = No maximum (Default)
Output	***** = directly from the screen ***PRINT** ***OUTFILE**
Operation type	***ALL** ***ADD** ***SWAP** ***ALLOW** ***REJECT** ***RELEASE**
Job name - User	Selects a subset of records by OS/400 job name
Job name - Number	Selects a subset of records by OS/400 job number
Filter by Time Group – Relationship	***IN** = Include all records in time group ***OUT** = Include all records not in time group ***NONE** = Do not use time group, even if included in query definition
Filter by time group - Time group	**Name** = Name of time group ***SELECT** = Select time group from list at run time

2. Select option **42. Print Log + Entered Commands** to print activity log with commands entries. The activity log is composed of audit and journal logs.

```
                    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
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
Attach file record changes . . . > *NO      *YES, *SUM, *LOG, *NO

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

Print Log and commands info

3. Select option **43. Print Log + Attachments** to print activity log, captured screens and journaled updates. This option prints Captured screens + FileScope updates summary

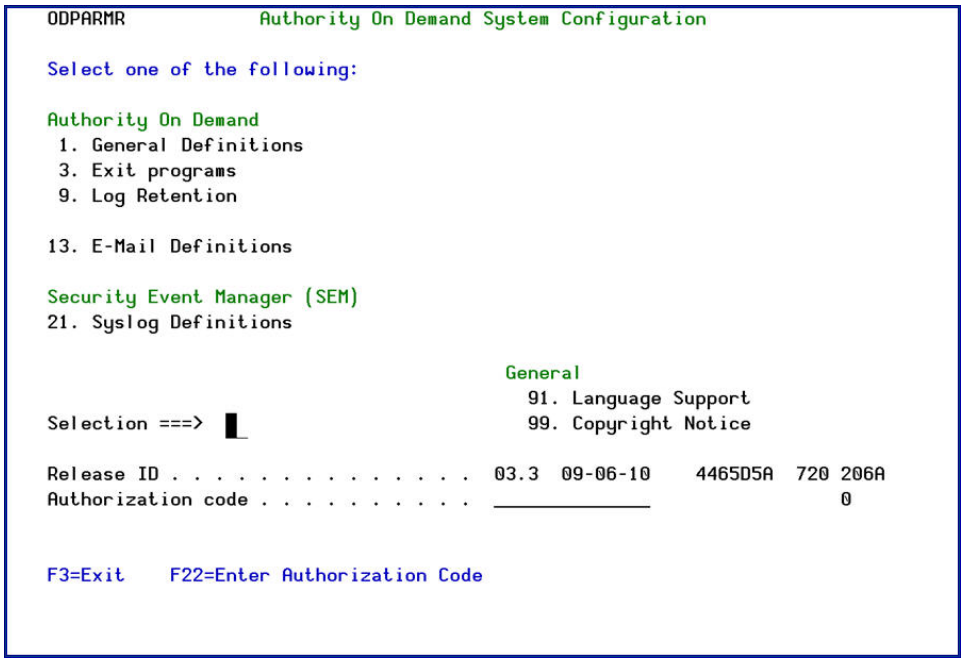


Print Log and full Audit info

Parameter	Description
Attach activity log	*YES = Attach a log with full **Audit** log entries information *CMD = Attach a log with full **Audit** commands entries information *NO = Do not attach
Attach captured screen	*YES = Attach captured screen *NO = Do not attach captured screen
Attach file record changes	*YES = updates from journal as long as the receivers are online. If the system also has Raz-Lee's AP-Journal, you will receive a print in field mode. Otherwise, the changes will be printed using the system commands as character strings. *SUM = Journal sum *LOG = Journal log *NO = Do not attach journalled record

Chapter 3: System Configuration

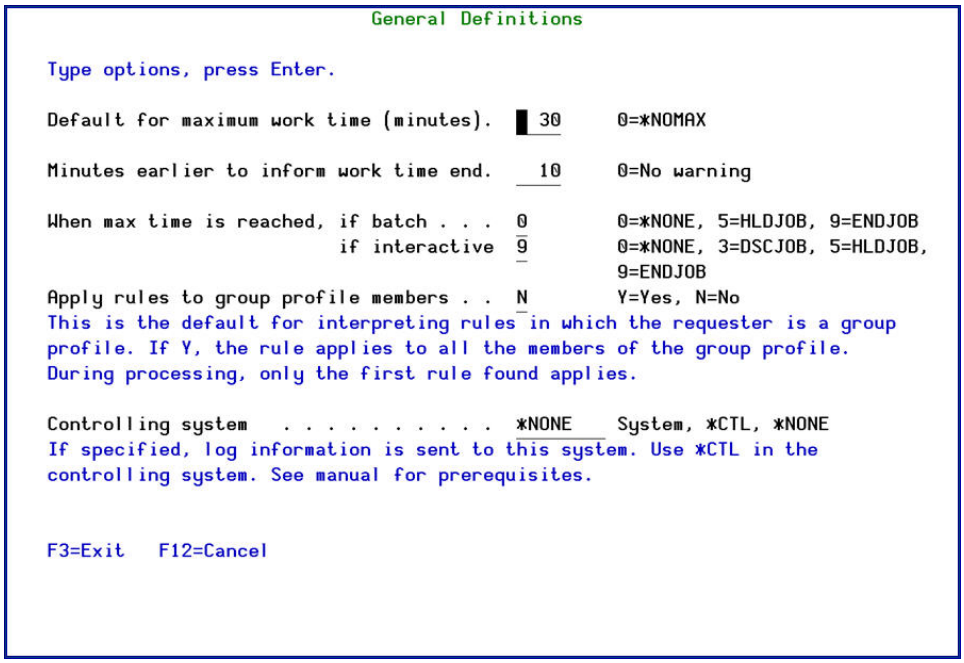
Select option **81. System Configuration** from the main menu



Authority on Demand System Configuration

General Definitions

1. Select option **1. General Definitions** to set the temporary authorization work span and define how to handle the ending of this work span.



General Definitions

2. Set general maximum work time in minutes. Maximum work time can also be defined individually for each rule, which will be the dominant definition of the two.
3. Type the number of minutes to inform a user with temporary authorization that the work time is about to end.
4. Set an action to be executed (in batch or interactive) when the work time has ended.
5. Type **Y** in the **Apply rules to group profile members** if rules can be applied to group profiles members.
6. Define the name to specify of the Remote Location as can be seen in the DSPNETA of the remote location at the **Controlling System** field. "Behind the screens" the product is using DTAQs.

   *Read more about this option in **Multi Site Support**.*

Multi Site Support

Multi site support ensures that a control location will collect others sites Log info (besides its own). To access it, use the parameter ***SYSTEM()*** in the ***DSPAODLOG*** (Display Authority on Demand Log) command. The SYSTEM parameter supports *CURRENT, *ALL, generic* and name,

To define the controlling system name, select option **81. System Configuration > 1. General Definitions**

First time activation

1. Select option **81. System Configuration > 1. General Definitions** to define the **Controlling System: **CTL***
2. Select option **82. Maintenance Menu > 59. Force DTAQ re-creation.**
3. To activate select option **11. Activation** from the main menu, and activate by selecting option **1. Activate Authority on Demand Now.**
4. To add more systems enter the controlling system name by selecting option **82. Maintenance Menu > 59. Force DTAQ re-creation**.

Communication parameters

To add more connection parameters, install iSecurity/Base with SMZ4* libraries. Enter the information by ***STRAUD*** > Option **83. Central Administration > 1. Work with network definitions**.

At present we support MODE.

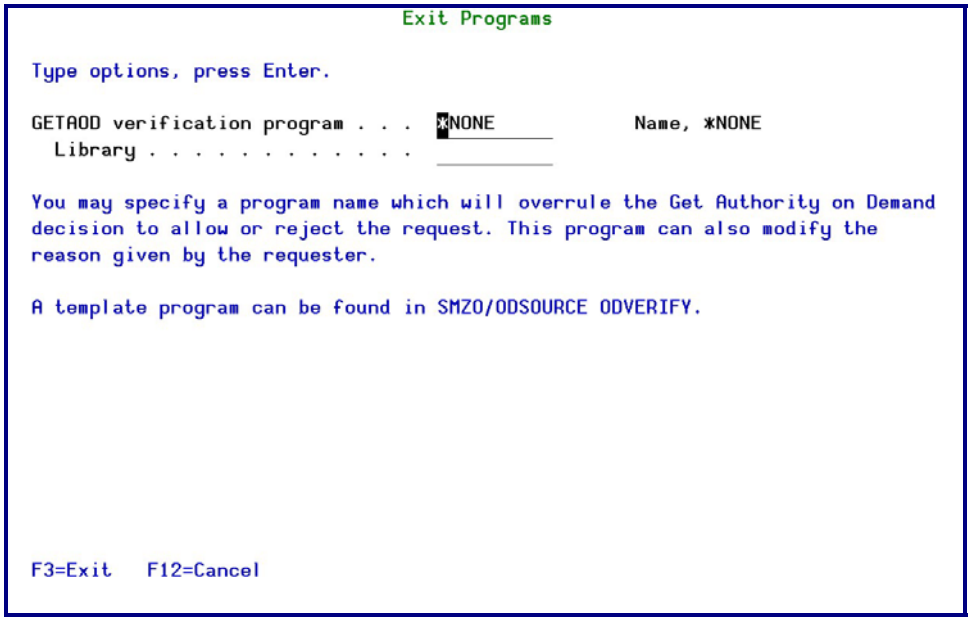
> **Note:** To change parameter in the network definitions, select **82. Maintenance Menu > 59. Force DTAQ re-creation** and force DTAQ re-creation.

Exit Programs

With user **Exit Program**, a user can specify a program name which will overrule the **Get Authority on Demand** rule definitions of allow or reject the request. This program can also modify the reason given by the requester for the temporary authorization.

A template program can be found in SMZO/ODSOURCE ODVERIFY.

Select option **3. Exit programs**



Exit Programs

Retention Period

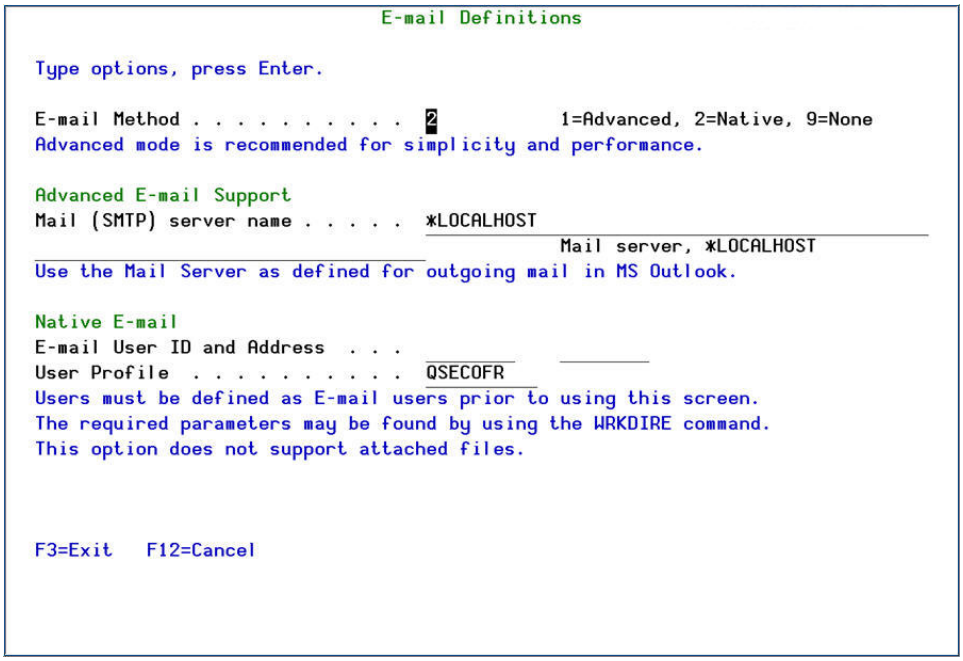
1. Select option **9. Log Retention** to set the number of days during which the log is retained, and to define a backup program for the collected data

AOD Log Retention

2. Define the data retention period days.
3. Specify the backup program you would like execute before the recorded data is deleted.

E-Mail Definitions

1. Select option **13. E-Mail Definitions** off the **System Configuration** menu



E-mail Definitions

2. Select Email sending method
3. Define mail server
4. Define user ID and Email address

SYSLOG

Overview

Current security regulations and auditing best practices dictate that log files from network access attempts and critical system components be monitored by a real-time alert system tracking potential security failures and abnormal changes to application data. Until recently, iSecurity satisfied this requirement by sending real-time e-mail and operator message alerts and executing CL scripts when such events occurred.

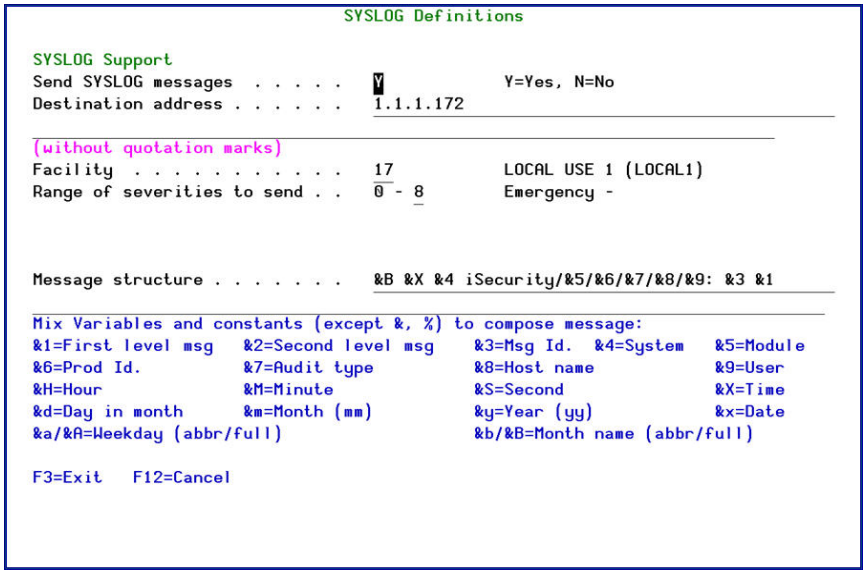
However, with the increasing prevalence of site-wide Intrusion Detection and Security Information Management systems, which present managers with an end-to-end view of security related events at different network nodes, it has become increasingly important to display security-related events from the System i in the same manner.

iSecurity's new Syslog capability sends events from various System i facilities (such as logs and message systems) to a remote Syslog server, and categorizes the events according to a range of severities such as emergency, alert, critical, error, warning, notice, informational and debug.

The Syslog feature enables the system administrator to decide under which conditions the System i should send a Syslog message, to choose the IP address of the Syslog server, the facility from which the message is sent, the severity range and the recipients, as well as decide whether the Syslog message should contain all events from iSecurity Firewall or only the rejected entries.

Using Syslog

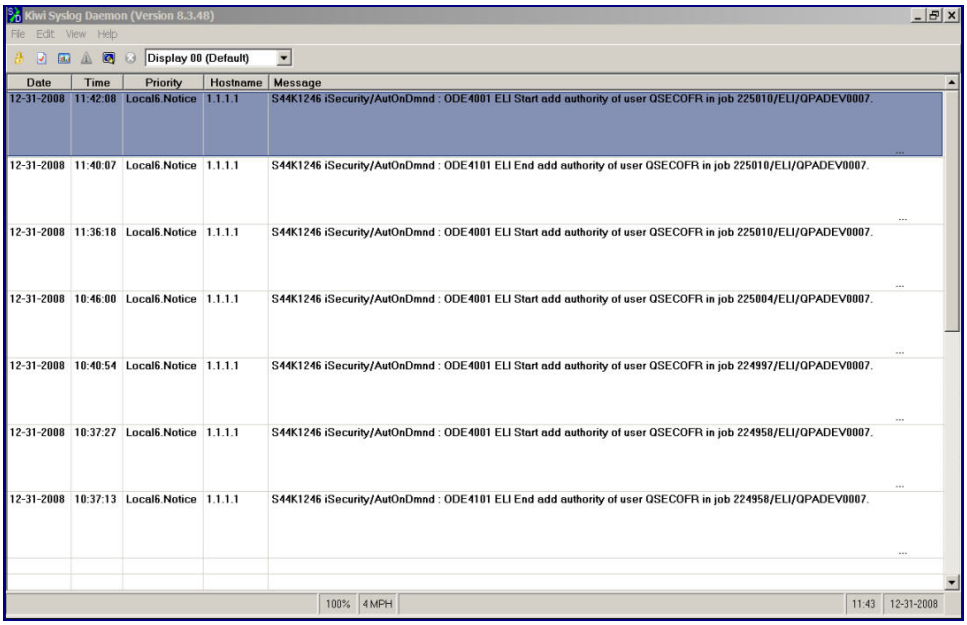
Select option **21. Syslog Definitions**, and define whether to send a Syslog message, to what IP address, from which facility (list of optional facilities below), in what range of severity (list below) and how the message looks.



SYSLOG definitions

To see how the Syslog definitions work without actually setting up a software on an IP address, and to receive the Syslog messages, follow this procedure:

1. Download Kiwi Syslog Server from http://www.kiwisyslog.com
2. Enter the PC IP address in the field on the Syslog definition screen. Syslog works very easily using this product. The command entry of **Get Authority on Demand** (***GETAOD***) writes a Syslog message and can be seen immediately in Kiwi Syslog Server.



Kiwi Syslog Server

****SYSLFC - SYSLOG FACILITY:**

KERNEL MESSAGES
USER-LEVEL MESSAGES
MAIL SYSTEM
SYSTEM DAEMONS
SECURITY/AUTHORIZATION MESSAGES
SYSLOGD INTERNAL
LINE PRINTER SUBSYSTEM
NETWORK NEWS SUBSYSTEM
UUCP SUBSYSTEM
CLOCK DAEMON
SECURITY/AUTHORIZATION MESSAGES
FTP DAEMON
NTP SUBSYSTEM
LOG AUDIT
LOG ALERT
CLOCK DAEMON
LOCAL USE 0 (LOCAL0)
LOCAL USE 1 (LOCAL1)
LOCAL USE 2 (LOCAL2)
LOCAL USE 3 (LOCAL3)
LOCAL USE 4 (LOCAL4)
LOCAL USE 5 (LOCAL5)
LOCAL USE 6 (LOCAL6)
LOCAL USE 7 (LOCAL7)

****SYSLSV - SYSLOG SEVERITY:**

EMERGENCY
ALERT
CRITICAL
ERROR
WARNING
NOTICE (SIGNIFICANT)
INFORMATIONAL
DEBUG

Maintenance Menu

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

For more information, please contact Raz-Lee at 1-888-RAZLEE4 (7295334) or at +972-9-9588860, or contact your local distributor.