RAZ-LEE

AUTHORITY ON DEMAND

Significantly reduces the number of user profiles with special authorities

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world's leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee's flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

We build solutions that work with other companies' technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva IBM McAfee™

Akamai RSA® SEA™ SOFTWARE ENGINEERING OF AMERICA

About iSecurity Suite

Advanced Threat Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Optional Client/Server for Antivirus

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** Journal, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

Authority On Demand

Significantly reduces the number of user profiles with special authorities

When do we need to use Authority On Demand?

Use case examples:

- Need to control and monitor the activities of “non-corporate” personnel such as consultants, auditors, contractors, etc.

- Need to provide emergency access to critical application data and processes on an “as needed” basis (i.e. Dev Team / R&D)

- Need to maintain documentation of activities of to comply with regulations and auditor’s security requirements

- Need to provide enough rights to a user to carry out unique assignments that his security level rights normally don’t allow

What is so special about Authority On Demand?

Authority On Demand leads the market with Unique or Semi-Unique capabilities:

- Most important: Adding authority without changing the user profile. This allows the logs and journals to record the actual user who is responsible for the activity
- Elevating user authority in system wide approach
- Verify by TOTP (Time-Based One time password), and One time password and even
- Be part of a Program. Wrap just the required part with elevated authority
- Can run in Batch. Can be used as part of your GUI
- Best screen recording. Allows playback and search. Compresses 1000 screens to 1MB
- Include database activity during elevated authority in field mode, highlighting changes
- Most comprehensive logs and activity end reports
- And more…

How is authority elevated?

All regulations require that authorities, particularly Special Authorities (*ALLOBJ, *SECADM, *AUDIT etc.), should be provided on an as needed basis.

Authority on Demand simplifies the process of temporarily granting special or regular authorities. A set of rules designates how a user can elevate his authority. To elevate the user authority in his job or throughout the system, all that is needed is to enter the Get Authority On Demand (GETAOD) command.

This command is usually requires verification measures such as:

- Pin code
- One time password
- TOTP (Time-Based One time password)
- Approval by an administrator

Based on previously defined rules, user gets temporary elevated authority and his activity is thoroughly logged

This ends by the user or when the set time expires. Auditor then automatically receives a report via email, which includes commands used, recorded screen activity and list of Database updates.

Types of elevation of authority

Authority on Demand can elevate authority in different ways, mainly:

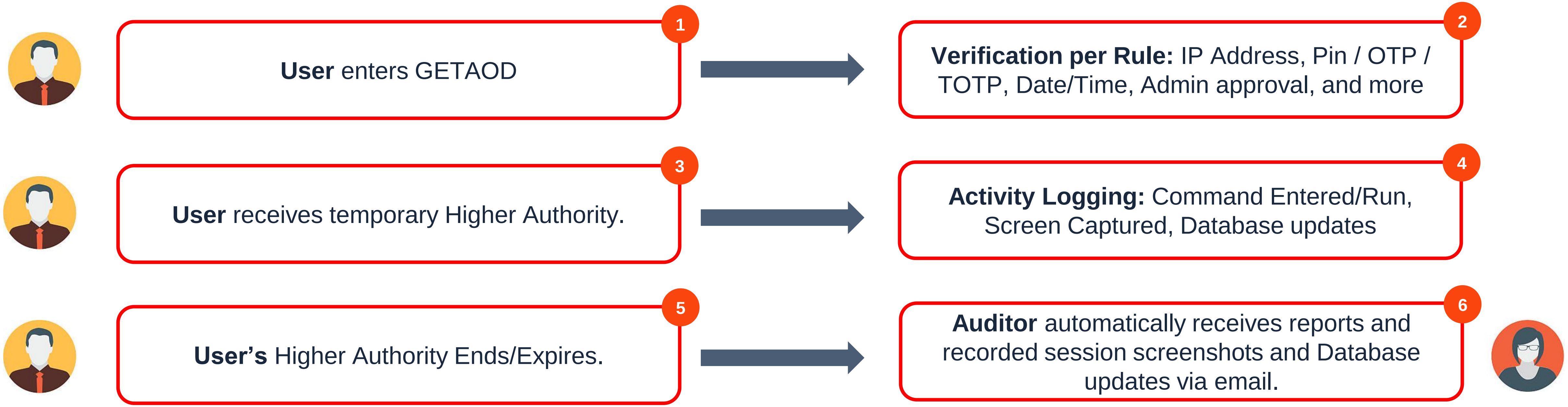
- By adding authority (without changing the current user) for the job
  This unique feature logs the real user as responsible to his activity.
- By swap (changing the current user of the job)
- By adding authority to the user throughout the system
  This semi-unique feature enables elevated authority for all user jobs
- By using trace (Does not elevate authority, but follows and report the user’s activities)

The Get Authority On Demand (GETAOD) command works in:

- Interactive or Batch environments
- Native or GUI
- Programs or Menus

Workflow

Authority on Demand saves valuable time and resources, enforces segregation of duties and enables relevant personnel to obtain access to approved information when needed. Its real-time audit of access rights protects sensitive corporate assets and significantly reduces the number of profiles with powerful special authorities.



1 **User** enters GETAOD

2 **Verification per Rule:** IP Address, Pin / OTP / TOTP, Date/Time, Admin approval, and more

3 **User** receives temporary Higher Authority.

4 **Activity Logging:** Command Entered/Run, Screen Captured, Database updates

5 **User's** Higher Authority Ends/Expires.

6 **Auditor** automatically receives reports and recorded session screenshots and Database updates via email.

Emergency rules can be defined for use during night shifts.
These rules require the agreement of 2 or 3 people.

Authority Reports

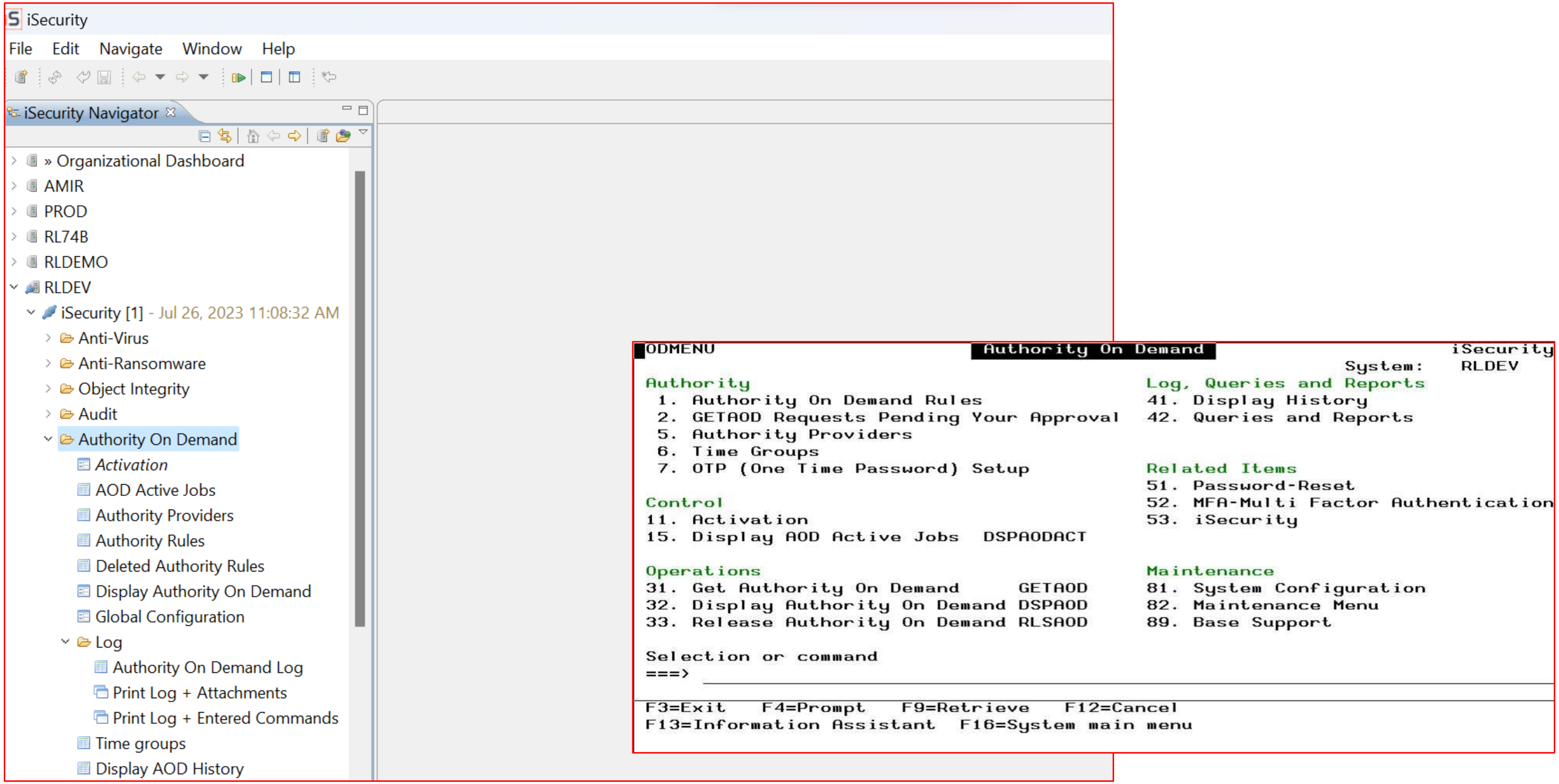
During the elevated session, the product records:

- Screens observed
- Entered commands
- Database changes (in the field level, comparing the before-after values).

These recording are composed in a document which is sent to the auditor, providing a comprehensive log of activity. This is how sensitive and potentially dangerous capabilities are controlled.

Emergency rules are also enables to enable secured access for faster recovery from different types of emergency situations with minimum chances for human error.

Authority On Demand in Action



iSecurity

File Edit Navigate Window Help

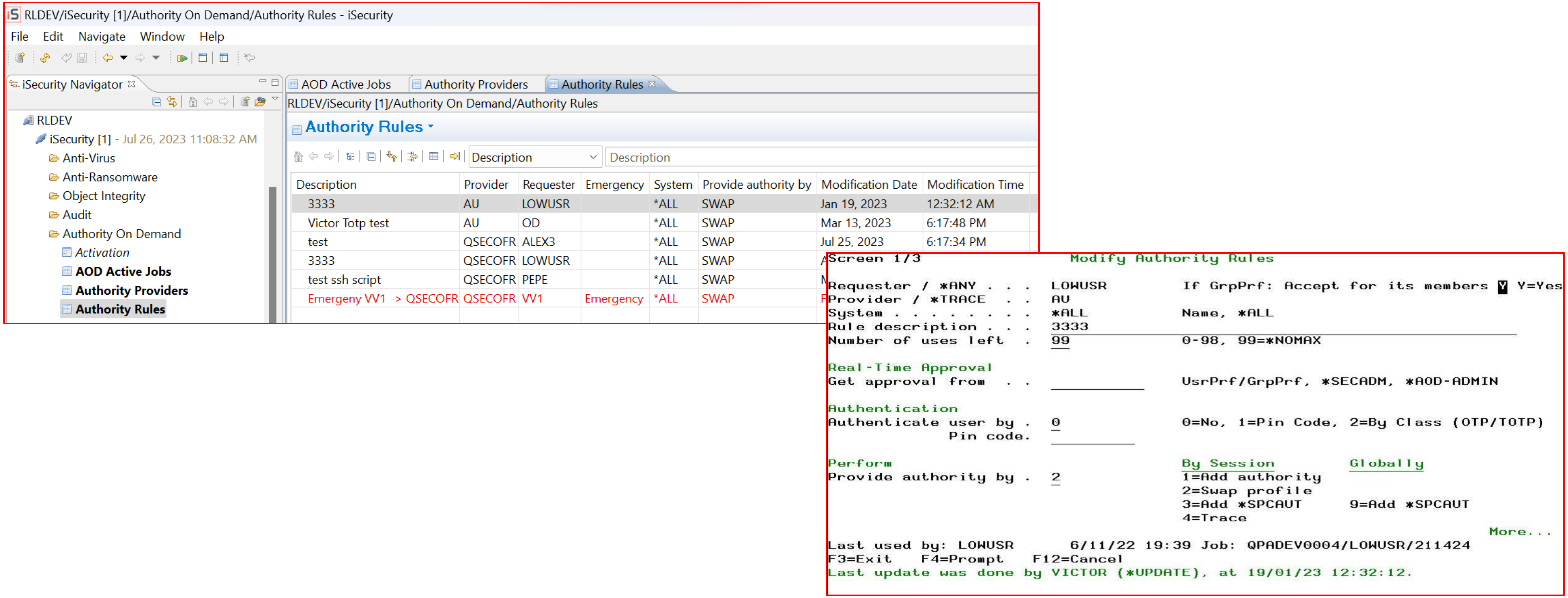
iSecurity Navigator

- » Organizational Dashboard
- AMIR
- PROD
- RL74B
- RLDEMO
- RLDEV
  - iSecurity [1] - Jul 26, 2023 11:08:32 AM
    - Anti-Virus
    - Anti-Ransomware
    - Object Integrity
    - Audit
    - Authority On Demand
      - *Activation*
      - AOD Active Jobs
      - Authority Providers
      - Authority Rules
      - Deleted Authority Rules
      - Display Authority On Demand
      - Global Configuration
      - Log
        - Authority On Demand Log
        - Print Log + Attachments
        - Print Log + Entered Commands
      - Time groups
      - Display AOD History

```
ODMENU                          Authority On Demand                   iSecurity
                                                            System:   RLDEV
Authority                                         Log, Queries and Reports
 1. Authority On Demand Rules                     41. Display History
 2. GETAOD Requests Pending Your Approval         42. Queries and Reports
 5. Authority Providers
 6. Time Groups
 7. OTP (One Time Password) Setup                 Related Items
                                                  51. Password-Reset
Control                                           52. MFA-Multi Factor Authentication
11. Activation                                    53. iSecurity
15. Display AOD Active Jobs  DSPAODACT

Operations                                        Maintenance
31. Get Authority On Demand       GETAOD          81. System Configuration
32. Display Authority On Demand DSPAOD            82. Maintenance Menu
33. Release Authority On Demand RLSAOD            89. Base Support

Selection or command
===>

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

Rule Definition

Authority on Demand simplifies the process of granting special authorities temporarily, when necessary, by a set of rules which designated who and how can a user authority be elevated.

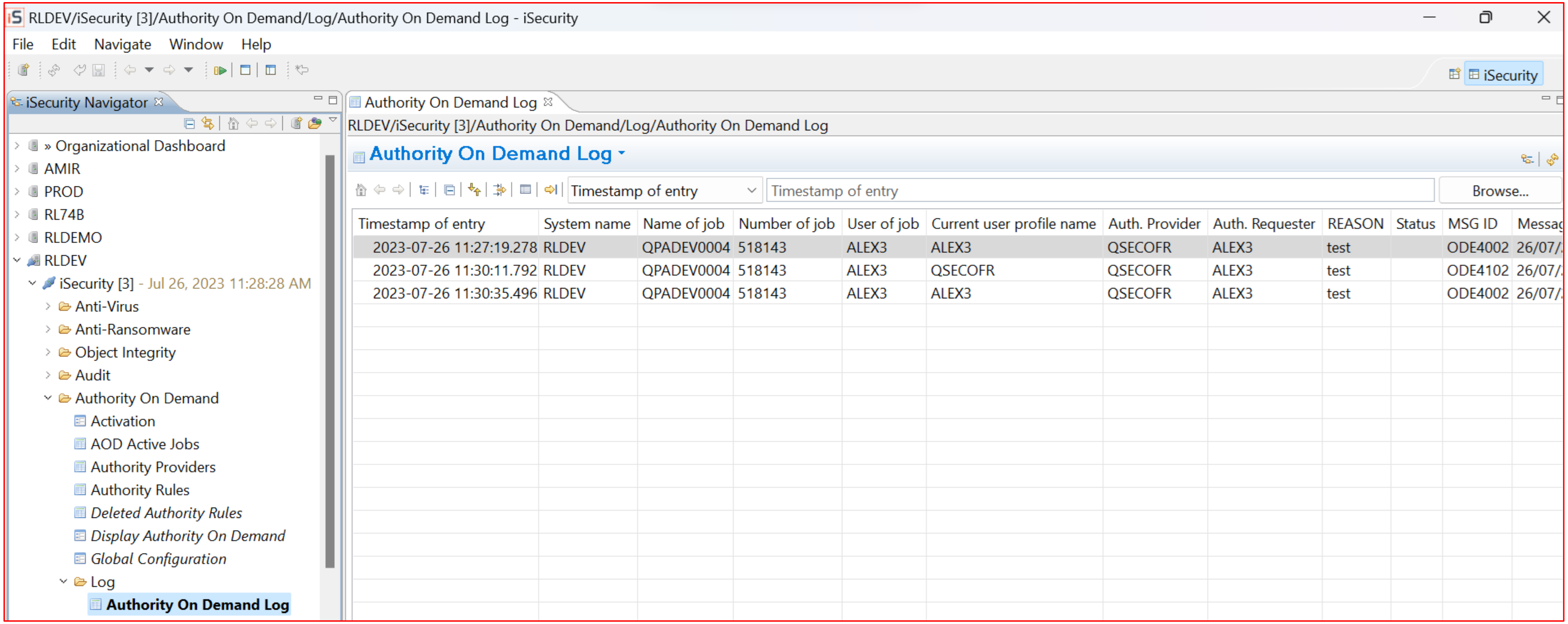


Description	Provider	Requester	Emergency	System	Provide authority by	Modification Date	Modification Time
3333	AU	LOWUSR		*ALL	SWAP	Jan 19, 2023	12:32:12 AM
Victor Totp test	AU	OD		*ALL	SWAP	Mar 13, 2023	6:17:48 PM
test	QSECOFR	ALEX3		*ALL	SWAP	Jul 25, 2023	6:17:34 PM
3333	QSECOFR	LOWUSR		*ALL	SWAP	A	
test ssh script	QSECOFR	PEPE		*ALL	SWAP	M	
Emergeny VV1 -> QSECOFR	QSECOFR	VV1	Emergency	*ALL	SWAP	F	

```
Screen 1/3                    Modify Authority Rules

Requester / *ANY . . .  LOWUSR        If GrpPrf: Accept for its members Y Y=Yes
Provider / *TRACE  . .  AU
System . . . . . . . .  *ALL          Name, *ALL
Rule description . . .  3333
Number of uses left  .  99            0-98, 99=*NOMAX

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

Authentication
Authenticate user by .  0             0=No, 1=Pin Code, 2=By Class (OTP/TOTP)
             Pin code.  _________

Perform                               By Session        Globally
Provide authority by .  2             1=Add authority
                                      2=Swap profile
                                      3=Add *SPCAUT     9=Add *SPCAUT
                                      4=Trace
                                                                   More...
Last used by: LOWUSR     6/11/22 19:39 Job: QPADEV0004/LOWUSR/211424
F3=Exit    F4=Prompt    F12=Cancel
Last update was done by VICTOR (*UPDATE), at 19/01/23 12:32:12.
```

Authority Logs

These recording are composed in a document which is sent to the auditor, providing a comprehensive log of activity. This is how sensitive and potentially dangerous capabilities are controlled.



Timestamp of entry	System name	Name of job	Number of job	User of job	Current user profile name	Auth. Provider	Auth. Requester	REASON	Status	MSG ID	Messag
2023-07-26 11:27:19.278	RLDEV	QPADEV0004	518143	ALEX3	ALEX3	QSECOFR	ALEX3	test		ODE4002	26/07/.
2023-07-26 11:30:11.792	RLDEV	QPADEV0004	518143	ALEX3	QSECOFR	QSECOFR	ALEX3	test		ODE4102	26/07/.
2023-07-26 11:30:35.496	RLDEV	QPADEV0004	518143	ALEX3	ALEX3	QSECOFR	ALEX3	test		ODE4002	26/07/.

iSecurity Authority On Demand Advantages

- Provides users higher authority as needed according to pre-defined rules
- Logs all activities as well as all users' activities while operating with a different authority
- Site-definable email message alerts and SYSLOG messages
- Capabilities for restricting requestors
- Real Time approval request
- PIN number verification
- OTP Verification
- User-friendly GUI interface

RAZ-LEE

Thank You

For more information about our company and products please visit

www.razlee.com