

RAZ-LEE

Authority on Demand ^{iSecurity}



iSecurity
Authority on Demand

Rule Definition to Elevate Authority

iSecurity Authority on Demand Provides temporary extended authorization by Swap or by Adding authority.



When do we need to use Authority On Demand?

iSecurity Authority on Demand helps you for example in the following cases:

- ✓ 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.



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



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 requiring verification measures such as:

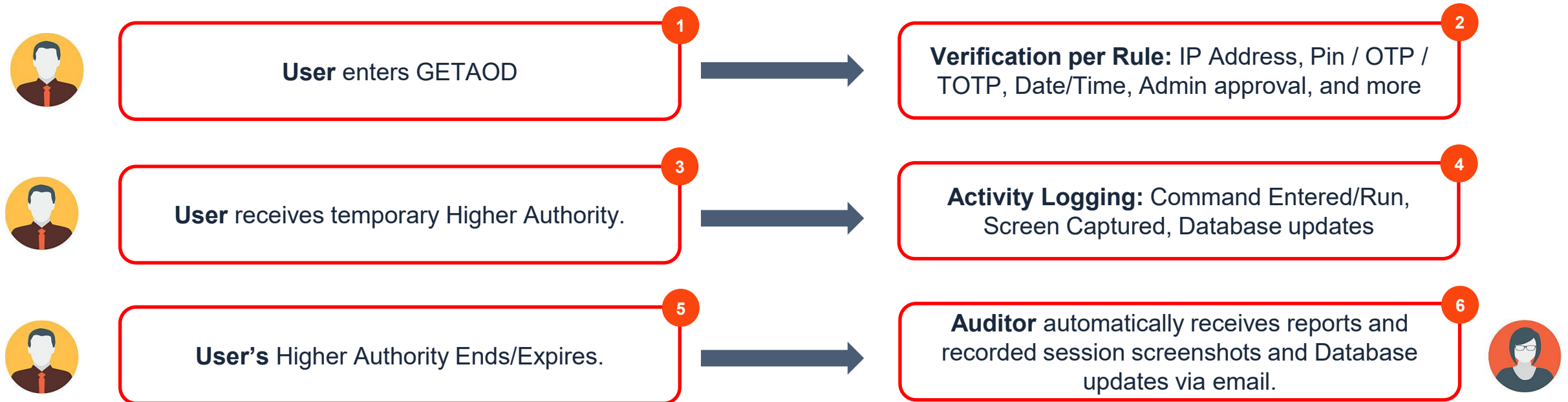
- ✓ Pin code
- ✓ One time password
- ✓ TOTP (Time-Based One-time password)
- ✓ Approval by an administrator

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.

Workflow

iSecurity 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.



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

iSecurity Authority on Demand Insights

We proudly say that **Authority On Demand** leads the market with Unique or Semi-Unique capabilities

Our Solution:

- ✓ Adds authority without changing the user profile. This allows the logs and journals to record the actual user who is responsible for the activity.
- ✓ Logs all activities as well as all users' activities while operating with a different authority.
- ✓ Real Time approval request.



iSecurity
Authority on Demand

Let's see our Product in Action!

The best way to see how it works is a demo with **iSecurity Authority on Demand** running on a real environment.



RAZ-LEE

Authority On Demand in Action (Green Screen)

```
ODMENU                               Authority On Demand                               iSecurity
                                                                              System:      RLDEV

Authority
 1. Authority On Demand Rules
 2. GETAOD Requests Pending Your Approval
 5. Authority Providers
 6. Time Groups
 7. OTP (One Time Password) Setup

Control
11. Activation
15. Display AOD Active Jobs   DSPAODACT

Operations
31. Get Authority On Demand      GETAOD
32. Display Authority On Demand DSPAOD
33. Release Authority On Demand RLSAOD

Log, Queries and Reports
41. Display History
42. Queries and Reports

Related Items
51. Password-Reset
52. MFA-Multi Factor Authentication
53. iSecurity

Maintenance
81. System Configuration
82. Maintenance Menu
89. Base Support

Selection or command
==> _____

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

Rule Definition (Green Screen)

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.

```
Screen 1/3                               Modify Authority Rules
Requester / *ANY . . . LOWUSR             If GrpPrf: Accept for its members  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
Provide authority by . 2                By Session                Globally
                                     1=Add authority
                                     2=Swap profile
                                     3=Add *SPCAUT                9=Add *SPCAUT
                                     4=Trace

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.

More...
```

Rule Definition (GUI)

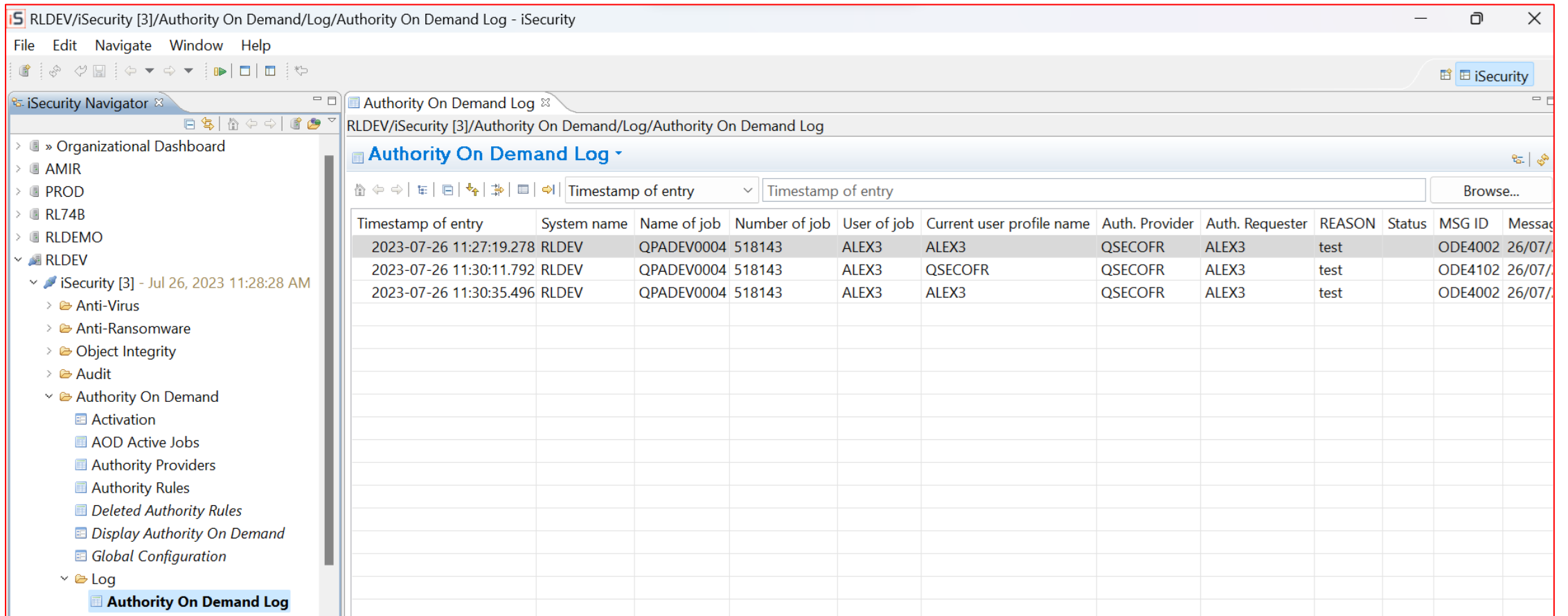
Authority on Demand simplifies the process of granting special authorities temporarily, when necessary, by a set of rules which designated who and how can a user authority be elevated.

The screenshot shows the iSecurity GUI interface. On the left is a tree view under 'RLDEV' with 'Authority Rules' selected. The main pane shows a table of Authority Rules with columns: Description, Provider, Requester, Emergency, System, Provide authority by, Modification Date, and Modification Time. The table contains several entries, with the last one highlighted in red.

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	Apr 19, 2023	2:47:12 PM
test ssh script	QSECOFR	PEPE		*ALL	SWAP	Mar 1, 2023	5:48:39 PM
Emergency VV1 -> QSECOFR	QSECOFR	VV1	Emergency	*ALL	SWAP	Feb 16, 2023	5:39:59 PM

Authority Logs (GUI)

These recordings 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.



The screenshot displays the iSecurity Authority On Demand Log GUI. The interface includes a menu bar (File, Edit, Navigate, Window, Help), a toolbar, and a navigation pane on the left. The navigation pane shows a tree view of the system structure, with 'Authority On Demand Log' selected under the 'Log' folder. The main area displays a table of log entries with the following columns: 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, and Message. The table contains three entries, all with a REASON of 'test' and a Status of 'Success'.

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	Message
2023-07-26 11:27:19.278	RLDEV	QPADEV0004	518143	ALEX3	ALEX3	QSECOFR	ALEX3	test	Success	ODE4002	26/07/2023 11:27:19.278
2023-07-26 11:30:11.792	RLDEV	QPADEV0004	518143	ALEX3	QSECOFR	QSECOFR	ALEX3	test	Success	ODE4102	26/07/2023 11:30:11.792
2023-07-26 11:30:35.496	RLDEV	QPADEV0004	518143	ALEX3	ALEX3	QSECOFR	ALEX3	test	Success	ODE4002	26/07/2023 11:30:35.496

iSecurity
Authority on Demand

| Advantages on our Solution

iSecurity Authority on Demand significantly reduces the number of user profiles with special authorities.



New Generation Features

Secure Privilege Elevation

Protect temporary authority with strong identity verification.

What's New

- MFA-secured GETAOD command.
- Stronger control of privileged access.

Why It Matters

Reduce the risk of privilege escalation and insider threats.



Authority Reports

During the elevated session, the product records:

- ✓ Screens observed.
- ✓ Entered commands.
- ✓ Database changes (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.



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.
- ✓ 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...

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 or OTP Verification.
- ✓ User-friendly GUI interface.



RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

Authority on **D**emand ^{iSecurity}

