

Authority on Demand

One of the greatest challenges of system administrators is reducing authorities while still allowing the organization to function properly. Permissions are generally granted on a permanent basis meaning users are granted higher system authority for a longer time than necessary. Consequentially, there are too many users with too much authority – a potentially dangerous situation which could lead to security breaches.

Authority on Demand (AOD) is a unique product for controlling user permissions while responding to emergency security needs of an organization. AOD can provide users with temporary authorities, while fully monitoring individual user's activity when the higher authorities are active.

AOD reduces the number of profiles with high authorities, while enabling relevant personnel to easily obtain access to processes and critical information when needed.

AOD uses advanced logging and reporting facilities to provide internal and external auditors with complete audit trails. Users running with higher authority can be monitored through actual user screenshots and lists of user activities that are logged with iSecurity Capture. These capabilities enable AOD to save valuable time and resources.

EASY TO USE

Simplifies the process of granting special authorities when necessary, and incorporates advanced reporting and monitoring mechanisms.

ADD/SWAP SECURITY LEVELS

Can grant an alternative authority level or add additional security rights to an existing user profile.

FULLY MONITORED TEMPORARY PERMISSIONS

Provides temporary authority that is fully monitored through system audit log (QAUDJRN), which can be printed or delivered to the System Administrator by email. iSecurity Capture can provide screen captures of a User's activity while provided the senior system authority.

AUTHORITY TRANSFER RULES & PROVIDERS

- Enables pre-defining special authority “providers” and special authority transfer rules such as time-limited authority transfers and PIN codes.
- Safe Recovery from Emergency
- Enables recovery from various emergency situations with minimum risk and/or error.

EXTENSIVE MONITORING

Logs and monitors relevant activities, producing regular audit reports, real-time e-mails, text messages and/or SYSLOG alerts when higher authority is requested.

AOD Modify Rules

CONTROLLED ACCESS

Allows only relevant personnel to access critical data and processes.

Controlled Access

AOD allows only relevant personnel to access critical data and processes.

Reporting

Detailed reports containing critical information are automatically generated with:

- User who requested authority (requester)
- User whom provided authority (provider)
- Operation type
- Job name (workstation)
- Time groups
- And Many More...

Three Levels of Product Usage

- Full
- Auditor (read-only)
- Emergency