syncsort

PRODUCT SHEET

Cilasoft EAM

The Elevated Authority Management Solution for IBM i

Having too many powerful user profiles leaves the security of your IBM i system and data exposed. Security and compliance auditors prefer that IBM i users be given only the authorities required to perform their jobs, and that they be granted additional authority only when needed and only for the time required.

Cilasoft Elevated Authority Manager (EAM) enables you to reduce the number of powerful IBM i user profiles in your environment by allowing you to easily elevate the authority of user profiles on an as-needed basis. Elevated authority can be granted by an administrator upon request or automatically based on preconfigured rules, and it can be limited to a specific command, day, time, IP address or other parameters.

Cilasoft EAM also provides comprehensive monitoring and reporting. A graphical dashboard shows the users who are elevated, how long they've been elevated and more. The activities of elevated profiles are also exhaustively logged using multiple sources to create a full audit trail.

EAM gives you complete control of IBM i user authorities to help your company meet the most stringent regulatory requirements mandated by SOX, PCI-DSS, HIPAA, GDPR and more.

Benefits

- Makes it easy to manage user requests for elevated authorities on demand
- Satisfies security officers by reducing the number of powerful user profiles
- Produces necessary alerts, reports and a comprehensive audit trail
- Enforces segregation of duties
- Limits user access to sensitive data
- Significantly reduces security exposures caused by human error

How Cilasoft EAM Works

With Cilasoft EAM, when a user needs elevated authority for a specific action, they ask for elevation of authority within their job. That request must specify a profile with the authority needed and the command to be run. Requests can be accepted by the administrator, or when configured to automatically grant requests, rules defined by the administrator are consulted to determine whether the request should be granted.

EAM's powerful rules are defined for pairs of requesting and requested profiles based on group profiles, supplemental groups, lists of users and command line access. Rules provide the context around which requests can be granted, including day of the week, date range, time range, job name, IP address, IASP and more. They also determine whether profile swapping or adopted authority methods will be used for elevating authority and the duration of the elevation. EAM can also be instructed to log all user activity without changing the user's authorities.

If EAM accepts the request, it grants the user's job the authority of the target profile, launches the initial command, places the job under its control and starts logging job activity. Multiple sources are used to log activity including job logs, screen captures, exit points, and system and database journals to ensure a complete audit trail. When the command completes, EAM restores the authority of the initial profile, stops logging the job activity and records the log.

EAM also controls how long the job runs with the authority of the target profile. If a job exceeds its duration, EAM alerts the user. Based on rules configuration, the job can then be held or canceled.

Key Features

- Offers users a fast and easy process for requesting authority
- Allows authority requests to be granted manually or automatically based on rules
- Enables powerful rules to be defined for source and target profiles based on group profiles, supplemental groups, lists of users and command line access
- Rules determine the context around which a request can be granted, including day of the week, date range, time range, job name, IP address, IASP and more
- Rules define whether *SWAP or *ADOPT methods are used for elevating authority
- Provides a *JOB option that logs all user activity without changing the user's authorities
- Supports external processes connecting through ODBC, JDBC, DRDA and FTP
- Maintains a complete audit trail of activities from elevated profiles based on multiple sources, including job logs, screen captures, exit points, and system and database journals
- Supports management from a graphical console or full-featured 5250 menus
- Displays currently elevated users and duration of elevation in a graphical dashboard
- Provides ability to drill into logs of statements executed and view screen captures of activity
- Able to enrich joblogs with SQL statements, FTP functions and critical commands
- Allows rules management to be delegated with a complete audit trail
- Delivers alerts on events, such as exceeding authorized time, via e-mail, popup or syslog
- Logs and reports on all requests with customizable filters
- Produces reports in PDF, XLS or CSV formats
- Can be integrated with external helpdesk solutions for ticket management
- Able to interface with leading SIEM consoles