eLogger Security

eLogger

Product info

Electronic Logbook software replaces paper log books and disconnected systems, allowing for collection, storage and distribution of real-time data about your operation to those who need to know.

" Brilliant tool that makes everyone's job easier, faster and more efficient."

-Garry, City of Riverside

Log In Options

Database Log In
Users log in to the browser and authenticate against a database

Forms Active Directory
Users log in to the browser to authenticate AD

Windows Active Directory (AD)
Browser pass through authentication

Six Permission Levels: Applied by Location, Log, Group and/or User

1. No Security
2. View-Only permission
3. Append permission, including view-only
4. New Permission, including view-only, appending
5. Edit permission, including view-only, appending and creating new entries
6. Delete permission, including all of the above permissions

Location Permissions

Add New	Location	Permissions	
Edit	Power Plant	View	Delete
Edit	Power Plant->East Facility	Append	Delete
Edit	Power Plant->North Facility	New	Delete
Edit	Power Plant->South Facility	Edit	Delete
Edit	Power Plant->West Facility	Delete	Delete

User Security

Users can be assigned specific security permissions based on the needs of your facility. For example, users may only be allowed access to one of many locations, or they may only have access to specific log types. This is all based on the needs of your facility and set up by your system administrators.

Security can be set up for each individual user, or can be set up for groups of users. Your IT department can also access eLogger for IT help/support, but they don't count against your licenses.

eLogger provides in the software a full audit report that details changed to each and every entry. And, deleting records inactivates the log entry in the database; they are still retrievable.

Log Permissions

Add New	Log	Permissions	
Edit	Alarms	View	Delete
Edit	Fire Ext. Report	Append	Delete
Edit	Incident Report	New	Delete
Edit	Maintenance	Edit	Delete
Edit	Operations	Delete	Delete

Security

eLogger Administrator More Info	admingroup
IT Administrator Role More Info	adminitgroup

System Administration

System Administration security allows only your group of administrators access to the setup and configuration of your eLogger system.

eLogger Security FAQ's

Is eLogger's data encrypted? Data encryption is controlled in SQL Server, and can be enabled with the correct version of SQL Server.

How does eLogger connect to Active Directory (LDAP)? eLogger connects to Active Directory through a service account provided by the client. No special permissions are necessary for the service account.

Are files stored within eLogger scanned for malware? Files stored within eLogger are not scanned for malware, however, certain file extensions are restricted (we can provide a list, upon request).

eLogger's strong security model assists companies in keeping data safe, as well as meeting legal obligations and federal regula-

"VVWRA is better informed and more knowledgeable about their operations as a result of using eLogger."
- Latif , Victor Valley Water Reclamation Authority