DATASHEET

ACL MANAGER

What is ACL Manager?
The function of ACL Manager is to present permissions to local resources and shared resources (local and network). This is made possible by retrieving user permissions via a special API. ACL Manager is fully integrated with the Microsoft service Active Directory.

WHY USE **ACL MANAGER** FEATURES?

- Simpler data analysis, thanks to the implementation of tree structures,
- real-time monitoring of user accesses to individual directories,
- integration with Microsoft Active Directory,
- real impact on increasing protection against leakage of confidential information from the organization's directories,
- monitoring of local and shared resources,
- possibility of any filtering of permissions due to folders, groups, or users.

FULL CONTROL OVER RESOURCES IN THE ORGANIZATION

ACL Manager allows any administrator to fully monitor the permissions of users working in the organization (including those who work remotely). In terms of security, it is important to have always up-to-date information, so a special schedule has been implemented in ACL Manager, which allows you to set any frequency of data reading.

DATA PRESENTATION USING TREE STRUCTURES

To make it easier and faster to find data in tables, tree structures have been implemented in the eAuditor system. This allows for easier handling of sorted data. Depending on the selected groups (folders, users, groups, owners), the parent elements in the structure change dynamically, presenting other subordinate elements.

DATA DIVISION INTO 3 GROUPS OF ACL DIMENSIONS

Folder

- all folders inventoried in the system
- only shared folders
- only local folders

User

- list of all users
- user list domain users
- user list local

User group

- list of all groups users
- list of domain groups
- list of local groups

MONITORING 13 TYPES OF RESOURCE ENTITLEMENTS

Abbreviation	Name	Explanation
RD	Read Data	Specifies the right to read the file.
WD	Write Data	Specifies the right to open and save to a file or folder. Does not include the right to open and write file system attributes, extended file system attributes file system, and access and audit policies.
AD	Append Data	Specifies the right to add data.
D	Delete Specifies	Specifies the right to delete a folder.
DS	Delete Subdirectories and Files Specifies	The right to delete a folder and any files contained in that folder.
EF	Execute File	Specifies the right to run the application file.
RA	Read Attributes	Specifies the right to open and copy file system attributes from a folder or file. For example, this value specifies the right to view the creation or modification of a file. It does not include the right to read data, extended file system attributes, or rules access and auditing.
REA	Read Extended Attributes	Specifies the right to open and copy extended file system attributes from a folder or file. For example, this value specifies the right to view information about the author and content. It does not include the right to read data, file system attributes, or access and audit.
RP	Read Permissions	Specifies the right to open and copy access and audit rules from a folder or file. Does not include the right to read data, file system attributes, and extended file system attributes.
WA	Write Attributes	The right to open and write attributes of the file system in a folder or file. It does not include the ability to write data, extended attributes, and access and audit rules.
WEA	Write Extended Attributes	Specifies the right to open and save extended file system attributes in a folder or file. Not includes the ability to write data, attributes, or rules access and auditing.
CP	Change Permissions	Defines the right to change security and audit policies related to folders.
TO	Take Ownership	Specifies the right to change the owner of the folder. You should Note that the owners of the resources have full access.