



## SARBANES-OXLEY & UMP

User Manager Pro rapidly mass manages security settings on servers and workstations by allowing system administrators to report on and make global changes to administrative and user credentials, groups, rights, registry settings, and more across an entire network in a single operation. User Manager Pro also provides extensive reporting capabilities to show security auditors any information they require about the Windows based computer systems on your network.

Sarbanes-Oxley sections 302 and 404 require maintaining internal controls to ensure that data is available only to the individuals who require access to the data and give proof that these controls are effective. Furthermore, deficiencies of the internal controls must be identified and their weaknesses corrected.

User Manager Pro helps maintain SOX compliancy by providing the following controls:

- Reporting on the existence of all user accounts on any system or domain.
- Identifying those users roles in the network or system as an administrator or other role.
- Deleting or disabling users that should not exist or do not comply with security requirements regarding password age or other criteria.
- Randomize administrative passwords across the network ensuring peer level control cannot be gained by unauthorized users.
- Randomized passwords can be stored and secured using 3DES security and provide logging of access to those passwords.
- Reporting on the existence of all local and global groups that exist on any system or domain and giving the ability to delete the groups as necessary.
- Change protected built-in groups such as the Administrators group to ensure that no changes to the groups memberships can be made.
- Modifying the group memberships to ensure an appropriate level of access to network resources.
- The ability to grant or remove rights to a user or group.

*Weeks of Work Cut Down to Seconds*



## SARBANES-OXLEY & UMP

...continued

- Report on and edit the shares and permissions of shared folders.
- Report on and edit NTFS permissions for any file and folder on an NTFS partition.
- The ability to create password and account lockout policies for all systems.
- Report on Audit and security policy settings on each machine and domain.
- Report on and manipulate all registry settings on any system including users that are not presently logged in.
- Change permissions of the computer's registry to protect access to vital system controls and services.
- Report on and eliminate computer accounts that no longer exist in the network.
- Push service packs and hotfixes to machines and applications to ensure compliancy.
- Provide proof of the current patch and security level of all systems.
- Gather information from the systems event logs including the security logs.
- File reporting allowing verification of files and version information. As necessary allowing the lockout or deletion of that file.
- Reports can be stored indefinitely in a SQL database or exported into a format of your choosing such as HTML or CSV.
- Every action of the tool is logged within the tool and additionally can be stored in the event logs of the machines being managed.