ACS and Network Rights and Permissions

Most network operating systems, as well as advanced workstation operating systems like Windows 2000 Professional, Windows XP, and Windows Vista allow an administrator to set security settings at the file and/or directory level. Often, a network administrator restricts certain users to read-only access to certain files and no access to others for security purposes.

This restriction to files presents a conflict with ACS. ACS routinely writes temporary files into the various ACS directories on both the server and workstation. Because of this, users need full access to the \acsnet directory and all of its sub-directories on the server. On workstations that use Windows XP, 2000, or Vista, users need full access to the \winacs directory and all of its sub-directories. Please note that this is full access and not administrative rights.

Many network administrators and church officers are concerned that this allows uncontrolled access to sensitive data. ACS data files cannot be read in a text editor. These files must be read with special database software. Any files with sensitive information that can be easily discerned are password protected.

For information on how to set network rights and permissions, check your network operating system documentation, or contact your network administrator.