

Administrative_Privileges

Administrative user accounts are by far the number one target for someone trying to gain illegal access to a network and its resources. This type of account must be protected above all other accounts to ensure that users are not left vulnerable to the tools, tricks, and exposure that this account accommodates.

If you log on to your computer as an administrator to perform common everyday tasks, you make the computer vulnerable to malicious software and other security risks because malicious software will run with the same privileges you used to log on. If you unknowingly visit a malicious Internet site or open an e-mail attachment, the computer can be compromised by malicious code that will download and execute on your computer. Malicious code can, among other things, reformat your hard disk drive, delete your files, steal your passwords or personal information, and create a new administrative account that can give a hacker full access to your computer and the college network. When a computer has been compromised in this way, the resulting problems often affect other computers on the local network as well.

Because of the risks associated with local administrative user accounts we employ ?The Principal of Least Privilege?.

The principle is simple, and the impact of applying it correctly greatly increases our security and reduces our risk. The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. Most security-related training courses and documentation discuss the implementation of a principle of least privilege, yet organizations rarely follow it.

In order to facilitate the end result of this principal, administrative privileges will not be granted on newly deployed computers. Also, as these privileges are discovered on existing machines, they will be removed to comply with this policy. Before removing these rights, we will ensure that doing so does not impede anyone's job functions. In a large majority of cases, removal of administrative rights does not affect users in a negative way.

We do have an alternative available for the rare cases where administrative rights are absolutely necessary. In the cases where a user must be constantly installing and removing software on a Windows PC, we can provide a virtual environment to do so. This keeps your main computer "clean" and allows users to install, test, and remove software at will in a "sandbox" environment. This "sandbox" is a fully functional installation of Microsoft Windows but it is "contained," so anything you may do will not affect your "real" computer.

- Related topic: [Requesting Additional Software](#)