Administrative Rights to University-Owned Computers

Created by Webster, James D, last modified by Okulate, Temiloluwa D on Jan 04, 2017

The UMES IT department does not grant administrative rights on University-owned computers. We do understand, though, that there is a need for elevated rights in order for our teammates to do their jobs. To enable that ability, we have implemented a privilege management solution. This allows IT administrators to enable privilege elevation through computer and user policy. There are two ways to request elevation:

At UMES, we take IT security seriously, so we have implemented new privilege management solution to allow trusted software to run and elevate if required. A privilege management solution is a security software solution that uniquely integrates three proactive technologies to stop malware at the endpoint. Below is a standard message that notifies the user that the application identified will be running with elevation. The user is then required to click yes or no to either allow the application to execute or not. If the program you see listed in the popup is not recognized please cancel and contact IT for assistance.

If you are interested in more detail about the technologies behind our privilege management solution, please read on…

Privilege Management

The purpose of Least Privilege is to increase the security and compliance of the operating environment. Our solution enables us to do this while seamlessly maintaining user functionality.

Why:

Standard users are highly secure, yet severely restricted. Conversely, admin users are totally free, but security is compromised. By enabling everyone to work efficiently with standard user accounts, we create a much safer business environment.

What:

We achieve security objectives without creating a barrier for you, the end user. Privilege management solution allows us to strike a balance by enabling the complete removal of admin rights across the organization yet ensuring that individuals can still be productive.

How:

Privilege management solutions provide all the tools we need to successfully manage a least privilege operating environment. With this flexible approach, individuals can still access the documents, tasks and scripts they need to perform their job roles so that they can be productive.

Application Control

Application Control ensures that you, the user, are free to access the applications you need to perform your day-to-day role. With Application Control, we are able to enhance usability without compromising security.

Why:

Ensuring you are free to access the applications you need, without compromising security, is critical for business. The Council on Cyber Security lists application control as the most essential strategy for mitigating threats, based on real-world data.

What:

We gain immediate control of applications with a proactive approach to whitelisting that improves security and protects our software environment. Privilege management solution application control offers usability as well as security.

How:

With the advanced capabilities of Privilege management solution, we can take a more pragmatic approach to whitelisting so that users retain the flexibility they need to be productive. Simple yet highly effective management makes it possible to maintain application control across even the largest enterprise

Sandboxing

Sandboxing allows us to safely contain web threats and isolate any malicious activity without restricting your ability to perform your day-to-day role.

Why:

Vulnerabilities in web browsers and known business productivity software, create opportunities for malicious code to enter your network. With sandboxing we can safely contain web threats and isolate any malicious activity, without restricting you.

What:

You are free to use the internet in the knowledge that you are protected by a safety net, a last line of defense. If you visit a compromised website or open an infected document, malware is restricted to a safely contained environment, so that corporate data is protected.

How:

Privilege management solution Sandboxing extends security coverage to the most common entry point for malware and hackers - the internet. Using Windows native security to isolate web-borne threats, your corporate data is protected by a safety net, while the end user experience remains seamless.