Protecting Institutional and Research Information
Workstation Security and Administrative Rights
Executive Summary

Cybersecurity threats are increasing and, as the university increases its security posture, the bad actors have increased their focus on individual desktops and servers. Maintaining a layered security approach is critical to protecting everyone's information. As technology advances, we must adapt our security posture to take advantage of new tools and methods in our battle to fight back against attempts to compromise our systems as well as software licensing and other challenges. Operating system advances coupled with better tools to manage and support systems have now made it possible to further protect our information by limiting administrative rights in most cases.

These threats are not a problem you only hear about on the news, they are here at Rutgers and SAS IT staff have been dealing with an increasing number of incidents. Ransomeware, cryptojacking, back-doors, and other vulnerabilities rely primarily on deception and security vulnerabilities to propagate and workstation administrative rights both smooth the way and increase havoc the attacker can cause. These rights vastly increase the risk of data loss, theft of resources, loss of intellectual property, financial liabilities, and reputational damage.

We have also seen an increase in issues related to software licensing and the things that have been done on systems where administrative rights have been granted. The university has been forced to pay substantial licensing fees for software that was inappropriately installed on systems, administrative rights have been used to disable systems protections, and they've been used to grant students and others inappropriate access to systems and information.

To minimize these risks, the process by which administrative rights are being granted has been changed. We've always tried to minimize the granting of these rights but, once granted, the need for those rights was never revisited. Under the new process, when a new system is purchased, the user is notified that these rights are no longer granted by default. To obtain these rights on the new system, a request and a conversation are required to review the need and determine if they are still needed.

In most cases, because of new operating system capabilities and support tools, the need for these rights has significantly decreased. However, if during the review process, we discover that the user still needs administrative rights, the IT staff will recommend that they be granted. This process will include a consultation with the user's Chair or Director and, if necessary, the Vice Dean for Administration and the appropriate Divisional Dean.

Users without administrative rights will have the configuration of their systems adjusted, to the extent possible, to minimize their reliance on IT support. This includes granting targeted rights to perform tasks that have required full rights in the past. We are a creating installer packages that can be used to easily install software without the need for admin rights and re-prioritizing our IT support procedures to minimize the response time, with a goal of responding in under 15 minutes when administrative rights are needed.

Our goal is to always provide the best IT support possible, including striking the right balance between security and usability. We understand that having administrative rights makes it easier to get things done quickly but the risks that these rights present warrant taking some extra time.

Please review the full document below for complete details on this change.

Protecting Institutional and Research Information

Workstation Security and Administrative Rights

The Goal

Cybersecurity threats increase every day with bad actors finding new ways to infiltrate systems using any means open to them. As the university's security posture has increased on our larger systems, those bad actors have increased their focus on individual desktops and laptops ("systems") as well as mobile devices. When a system is compromised, the impacts reach far beyond that system. All data that system accesses become vulnerable and the system can become a launch pad to attack other systems on the local network.

Maintaining appropriate access controls, management, and malware protection on these systems is a critical component of layered security approach that protects everyone. This includes the restriction of administrative rights where possible.

Our goal is to provide you with a secure system that can meet your needs with a minimum amount of interruption because of necessary security so you can focus on your research and teaching. Let IT worry about making sure software is properly licensed, that software is safe, that patches are installed, and the many other requirements that will ensure that everyone's data is as secure as possible.

The Threats

There are specific threats that we regularly see at Rutgers and their incidence is increasing. Here are examples of issues that the information technology staff in the School of Arts and Sciences have been confronting recently. These are only some of the highlights and it is by no means a complete list.

- Backdoors – The most dangerous of the system compromises, backdoors are used to create havoc in many ways. They can allow an attacker to delete or change files, steal data, or even remote control your machine, doing anything you can do - sending emails from your account, logging into your bank account and transferring money, etc. Once a backdoor has been installed on a system, it essentially lets an attacker do anything on the computer that the logged in user can do, including monitoring your activity on the system, even capturing what you type and activating your camera.
- Ransomware – Attacks using this type of malware have been in the news but there is much more activity than is reported because many of its victims simply pay the ransom and don't report it. There are many variants, but their main goal is to encrypt as much of your data as possible in order to extort money. All your data becomes unrecoverable unless you pay the ransom. In some cases, the attacker will use the system and the data they steal to determine how much it's worth and how much the victim can afford to pay.
- Cryptojacking – Bitcoin and other types of cryptocurrency can be "mined" by running software that runs calculations to find unregistered tokens and then register them. As of 9/12/2022, a single bitcoin is worth over $22,000 so there is a significant incentive to find them by using as many systems as possible, especially when they can rely on someone else's system, power and networking. Once installed on systems, this software is often stealthy, varying how much power it uses based on whether the system is idle. Many variants of this software try to compromise other machines and some exfiltrate data from the computers.
- BotNets – Rutgers was a victim of a major attack using a botnet between 2014 and 2016. At times, these attacks crippled the university's networks, severely impacting operations. In that case, we were victimized by being attacked but our systems have also been used to attack others. In addition to mounting virtually untraceable attacks on other systems, this malware is typically used to send spam or flood other machines with traffic to knock them offline.
- Poisoned Repositories – Many people believe that open-sourced software is safe because the availability of the code for open inspection means it is widely reviewed. Unfortunately, that's not always true and even widely

used software that people have relied on for years can be a risk. For example, there have been cases where the underlying libraries have been compromised or repositories cloned to include malware. In these cases, an update to a trusted program can result in malware being installed.

- Software Licensing – Software license agreements are long and tedious documents that most people simply ignore and, while that isn't typically a problem on home systems, institutionally owned systems are a different story. One provision that's typically in those agreements that few people read gives the vendor permission to report back information about the system on which it's running. This could include the IP address, serial number, etc. Using this information, vendors have reached out to compel payment of license fees. This has happened at Rutgers and typically is the result of a misunderstanding like the belief that software that is "free for personal use" can be installed on an institutional device, which isn't usually the case. Keep in mind that any device purchased with university funds, including those purchased on grants, is institutionally owned. By allowing IT staff to review the license agreement before installing the software, we can ensure that all software is properly licensed and avoid surprise costs or penalties later.
- Misuse – Users with administrative rights often use those rights to further degrade the security of the system. Examples include, but are not limited to, adding administrative level accounts for other users, disabling malware protection, blocking IT's ability to manage the system, and disabling or postponing system updates.
- Accidents – No one is perfect and it's easy for someone to accidentally or reflexively click on the "Allow" or "OK" button. When the user has administrative rights, these accidents allow the malicious software to run with admin rights as well.

To provide some sense of scope, as of August of 2022, the university logged over 450 separate security incidents and this represents only a fraction of the total number because many go unreported. Specifically, in the SAS, IT staff have dealt with RansomWare that required the victim to pay the ransom to get their data back, CryptoJacking of several systems, as well as backdoors and botnets.

On the licensing front, the university recently had to pay Oracle for numerous copies of Java that were only licensed for use on personal systems. Oracle has been particularly aggressive in searching out people who are violating their license agreements, reaching out via email, phone and contacting the university to threaten audits.

The IT staff also regularly monitors and adapts our countermeasures to protect against ongoing attacks. Our systems are a significant enough target that as recently as August of 2022, FBI agents were on campus because, during another investigation, one of our systems was being targeted for attack.

In short, this is an ongoing problem that is already impacting our university, our school, and our departments. Just because it might not have happened to you yet, doesn't mean it won't or can't. As the former head of the FBI, Robert Muller, said, *"There are only two types of companies: Those who have been hacked and those that will be hacked."*

The Risks

Some of the risks are obvious from the details above but more details and some examples help to bring the point home. For more information, please see this Deloitte review article from 2016 that still very much applies.

- Loss of Data – Whether it's because of a virus that deletes the contents of a drive to simply be malicious or Ransomware, the loss of data is a real risk that happens regularly. Ransomware was discovered on systems in 2022 and the user impacted was forced to pay the ransom to get their data back. The user in question had administrative rights on their system and didn't realize they had allowed the software to install until it was too late.
- Theft of Resources – Multiple systems have been discovered running cryptomining software that was consuming system resources and slowing down other work as well as compromising the security of the data accessible to the system. It also drives up real costs because of additional wear and tear on the machines and the much

higher level of power consumption. All the users' systems were compromised using a known vulnerability that was unpatched on the system because the users prevented the system from installing updates.

- Loss of intellectual property – In a relatively recent case from a peer institution, a faculty member's system was compromised, and research data was stolen. That data and posted on the Internet and, because of that public disclosure, the faculty member lost their intellectual property rights to their own research. Furthermore, it was later discovered that the classified research that was stolen was being used by a foreign power to enhance their military's capabilities.
- Financial Liabilities– In addition to the case of ransomware, the university (and possibly individuals) could be held liable if proper steps were not taken to secure the information.
- Reputational Damage – When a system is compromised an investigation is required to ensure that the system has been secured and to determine what damage was done. This includes an analysis of the malware to determine if it is known to exfiltrate or modify data. If there is any evidence that unauthorized access to data was granted, the law requires that those who were impacted be notified (N.J. Stat. § 56:8-163). Granting agencies like the NSF also have requirements related to the breach of Personally Identifiable Information (PII). This includes notifications of various agencies and timely notification of those impacted, including students, even if the only thing found on the computer is a class grade roster.
- Collegial Responsibility – The university maintains a multi-layer security model that includes firewalls, private networks, network analysis, wireless network isolation, malware protection software and system monitoring. Almost all of these measures become ineffective if malware is installed on a system connected to the Rutgers network. Network firewalls that protect from outside attack are ineffective against inside attacks and malware protection that is disabled or overridden can't protect against the installation of malicious software. Malware will often seek out other vulnerable system on local networks, especially those made more vulnerable because software updates have been suspended and/or management software has been hobbled in the name of speed or convenience. Essentially, failure to maintain proper security on one system impacts everyone, not just the person making that choice.

Granting of Administrative Rights

Security is a balancing act, and the challenge is finding the right balance between security and accessibility. The most secure system is one that is only used by one person and doesn't connect to the network, but this setup would fail the accessibility test. On the other hand, removing vital security mechanisms in the name of convenience would be equally irresponsible.

To be clear, this procedure isn't about denying users administrative rights to their system. To state it plainly, we aren't saying NO. We're saying that we need to discuss your needs.

Our procedures are meant to determine when administration rights are truly needed and, when we believe that is the case, we will recommend that they be granted. However, if the user's needs can be met without granting blanket administrative rights, that's the preferred way to proceed for all the reasons stated above.

Why The Change?

As mentioned previously, the threats are increasing in complexity and volume but, our tools to combat these threats have also improved. New Windows and Mac operating systems have added capabilities allowing for additional security and more granular control over security settings. These developments have made it much less likely that administrative rights are required.

Software updates can be pushed to systems automatically or configured to update on their own, even allowing the user to delay for a short period when desired. Additional access rights can be granted to allow new software versions to be installed, modules added, and configurations changed, all without unrestricted administrative rights. Remote control software can be used by IT to easily and quickly handle issues that still require administrative rights without the need to bring the system to campus or wait for an in-person appointment.

These and other improvements make it possible to secure our systems more effectively and ensure appropriate license compliance without significant disruptions in system useability.

Of course, there will be times when users without administrative rights will need to wait for IT to do something. While this is more inconvenient, SAS IT will prioritize these requests and ensure that they are handled as quickly as possible. In turn, this relatively minor inconvenience helps us maintain a more secure environment for everyone.

Making it easier

We understand that this necessary change in our security posture is inconvenient and we're making several changes to minimize those impacts. These changes are both technological and procedural.

On the technology front, we are working to package software packages so they can be installed, even without administrative rights. We will publish a catalog of software packages so that users can simply click to install them without having to wait for IT to do it. This will also ensure that the software is properlyconfigured and updated.

In many cases, especially in labs, faculty have been managing accounts on local machines manually, often having to create and maintain accounts on multiple systems, share files and remove those accounts when they are no longer needed. We are working on a process to allow faculty to continue to create and remove those accounts on all machines in their labs at once, linking these accounts to user NetIDs which will make the accounts more secure and simplifying the current manual process.

Procedurally, we are updating the way we respond to requests that require administrative rights. Over the past several years we have standardized the way we support and manage our systems. This standardization means that systems can be supported by any IT staff member who handles workstation support. When tickets are submitted into the new ServiceNow ticket system, they are seen by everyone and any IT staff member, regardless of their location, can respond. We are prioritizing requests for administrative rights with the goal of responding to these requests within 15 minutes of submission during normal business hours.

As we try to strike the right balance between security and convenience, we will continue to work to minimize the inconvenience that these necessary security measures create.

What if IT isn't available when I need something?

The most frequent reason for requesting administrative rights is convenience. Whether it's the need to install software frequently or when working outside of regular business hours. We understand that adding delays is problematic and we are taking several steps to minimize those delays. Beyond that, we are tasked with ensuring that the software being installed won't negatively impact security and is appropriately licensed for use on the system, and so the occasional delays are necessary. When administrative rights are truly needed, they will be granted but it must be done after an appropriate review of the need so that the granting of these rights can be justified should an issue occur.

The Procedure

This procedure is currently only being used for new purchases because new computers have the newer hardware and software capabilities that minimize the need for administrative rights.

- When the IT staff receives a request to generate a quote, included in the conversation about the user's needs will be a reminder about the new procedure surrounding administrative rights. Additionally, language about this procedure will be included in the email that includes the purchase quote.

- If the user wishes to request administrative rights, they can submit that request as a ticket. The request should include the reason for the administrative rights request and a basic description of the system or systems to be included.
- The IT staff member handling the case will provide the requesting user a copy of the agreement they will have to sign later for their review, and then have a conversation with the user to gather information about why administrative rights are required. This includes reviewing the software that is on any existing systems and reviewing any history regarding any security issues that the user may have experienced in the past.
- The IT staff member will then forward that request, including any relevant details and making a recommendation as to whether they believe administrative rights are needed and why. That request is then forwarded to SAS IT Management.
- SAS IT management reviews and discusses the request with the Department Chair or Center Director.
- If the Chair or Director and the Executive Director of IT agree on the recommendation, that decision is implemented.
- If administrative rights were approved, SAS IT will fill out the aforementioned agreement form in DocuSign and send it to the faculty member for signature. The faculty member is also given instructions to request an administrative NetID. Once the faculty member signs that agreement and has received their administrative NetID, administrative rights are granted.
- If the Department Chair or Center Director, and Executive Director of IT do not agree, the Divisional Dean and Vice Dean for Administration are consulted to make the final decision.

Administrative rights can be granted temporarily if there is a time limited need. This can include granting these rights when the system is first delivered so that the necessary initial setup can be performed before the user's account is returned to standard user status and IT re-reviews the system to ensure that the work done while rights were temporarily granted hasn't introduced additional risk. This period will be brief because the risks of administrative rights still exist, especially when many changes are being made. Barring extraordinary circumstances, this period should not exceed two weeks.

Approved Administrative Rights

When administrative rights are approved, the user will be required to request an administrative NetID. Once created, this account will be granted administrative rights. In accordance with established best security practices, those rights will never be granted on the primary account that is used for day-to-day activities. When administrative rights are needed, the operating system will prompt for the user's administrative credentials.

When Will Administrative Rights be Recommended

There is no set of specific circumstances when administrative rights will be recommended or not because several factors come into play. Some of those factors include the system type (Mac, PC or Linux), the devices portability (laptop or desktop), primary use location (on or off campus), the installed software, connected devices, etc. We will also consider what mitigating factors can be put in place to offset the additional risk of granting administrative rights. For example, computers that are connected to data collection instruments sometimes have poorly written software that requires administrative rights and/or require out-of-date operating systems. In these cases, administrative rights can be granted but there could be a requirement to prohibit general Internet access from that system and placing it on a restricted network connection to protect other systems on the network.

Grouping Requests

If there are several substantially similar systems that are being purchased and the faculty member wishes to request administrative rights for all of them, only one request is required. Substantially similar means that the system configuration, installed software, and type of use for the machines are all similar. Five computers that are used to do the same type of data processing in a lab would be an example of substantially similar systems. A desktop and a laptop system that are being used by the same person wouldn't be considered substantially similar because one is stationary and the other could be connected to any number of private and public wireless networks that introduce additional risk.

This Process is Evolving

Just like the threats and the measures we use to protect against them, this process is evolving. We would appreciate any suggestions to improve upon the process. Please know that our primary goal is always to provide the best IT support possible. We appreciate your patience, cooperation, and insights.