UADA Policy 915.5
Information Technology Administrative Rights Access Policy

Purpose

Administrative rights refer to the level of access and control granted to individuals within the UADA systems and networks. These rights enable users to make significant changes to computer systems, including the installation and removal of software, configuration adjustments, and access to sensitive data. While administrative rights can be essential for certain tasks, their indiscriminate distribution poses substantial security risks. The purpose of this policy is to establish guidelines for the responsible management of administrative rights within the UADA ITS managed environments. This policy aims to:

- Enhance cybersecurity by minimizing the potential for unauthorized changes, malicious activities, ransomware, export control violations, licensing, compliance issues, data loss, and data breaches.
- In accordance with the Principle of Least Privilege (see the definition below), ensure that administrative rights are only
  granted when necessary. Exceptions must be approved by UADA ITS Executive Leadership team and only for
  specific roles and purposes.
- Promote efficient information technology operations by streamlining administrative access to those who require it for legitimate purposes.

Scope

This policy covers local Administrator rights for UADA devices and users with privileged administrative rights in the UADA Microsoft Entra/InTune identity access management tenant or environment. It also applies to local Administrator rights for UADA purchased devices within the UARK Microsoft Entra/InTune tenant's UADA AgriTech organizational grouping.

Definitions

AES ITS Site Lead: The Director of Infrastructure & Academic/Research Technologies.

CES ITS Site Lead: The Deputy Chief Information Officer.

Principle of Least Privilege: Refers to the practice of granting individuals or systems the minimum level of access, permissions, or privileges necessary to perform their specific tasks or functions, and no more. In essence, it limits users and processes to only the resources and permissions they need, thereby minimizing potential security risks and limiting the potential for misuse or abuse of privileges.

UADA ITS Executive Leadership Team: Includes the AES ITS Site Lead, CES ITS Site Lead, Chief Information Security Officer, and Chief Information Officer.

Policy

At UADA, we prioritize the security and integrity of our UADA ITS environment. To this end, we strictly adhere to the Principle of Least Privilege, which dictates that administrative rights are granted only to individuals when administrative rights are essential to fulfilling that individual's specific job responsibilities. This approach ensures that users are granted the minimum level of access required to carry out their duties, thereby mitigating potential security risks and minimizing the potential for misuse of privileges. Based on this principle, administrative rights will only be granted by request to those who meet specific criteria for having administrative rights.

For software installations, users can request administrative access through Admin By Request© software. This practice not only streamlines the process for software installations but also reduces the risk associated with widespread administrative access.

Administrative rights will only be granted for specific exceptions and under carefully controlled circumstances. Such exceptions must be thoroughly justified and documented, and approval will be subject to review by the UADA ITS Executive Leadership team. These exceptions are granted sparingly and exclusively when there is a clear and compelling need.

Valid Reasons for Granting Administrative Rights

Administrative rights should only be granted when individuals have a legitimate need for them to perform their job responsibilities timely and effectively. Valid reasons for granting administrative rights include:

- Specialized Software/Hardware: Faculty or staff members who require administrative rights to install, maintain, and operate specialized software and/or hardware that would require frequent use of administrative rights critical for their academic or research activities.
- Exceptional Circumstances: In exceptional circumstances, administrative rights may be granted on a case-by-case basis with approval from the UADA ITS Excutive Leadership team and appropriate Senior Associate Vice President. Such cases should be rare and well-documented.

Administrative Rights Restrictions

Users receiving administrative rights will agree to the following restrictions:

- Users will receive a separate Administrative Account.
- Administrative accounts will last for 1 year and then must be re-requested/re-evaluated.
- Administrative accounts will not be used for general day-to-day activities such as logging into your computer, e-mail, or web access.
- Administrative accounts will only be used to perform tasks requiring administrative privileges.
- Administrative accounts will not be used to remove or modify any hardware or software without Information Technology Services (ITS) permission.
- Administrative accounts will not be used to remove or modify antivirus/security software.
- Administrative accounts will not be used to disable or reconfigure the remote management services used by ITS.
- Administrative accounts will not be used to create additional user accounts, give any other accounts administrative rights, or otherwise tamper with the administrative account.

- Administrative accounts will not be used to install any software not purchased by UADA ITS through the appropriate procurement processes or free software that has not been approved.
- Administrative accounts will not be used to install applications that may establish network share protocols which result in an increase in bandwidth utilization as this may cause network congestion and degradation of network performance across wide areas of the campus. Examples include peer-to-peer (P2P) applications such as BitTorrent, Gnutella, etc.
- Administrative account users will allow for the removal of any software that adversely affects system efficiency or introduces a significant risk to system security as determined by ITS.
- The administrative account holder will be responsible for patching the software that they install.

Additional Warnings

- The use of cloud services (Microsoft) for UADA business requires a contract that has been approved by UA System Legal Counsel. The only approved cloud storage for UADA is Microsoft OneDrive/Teams/SharePoint. If you use cloud services that are not approved, then you are responsible for any and all implications that result, and you may not be represented and will not be indemnified by UADA.
- Non-standard software will be removed as part of a normal repair process if necessary to restore system functionality.
- Administrative accounts that are not used or deemed a security risk may be revoked at the discretion of UADA ITS Executive Leadership team.
- Systems may be placed in special protected networks to reduce risk at ITS discretion.
- Users with Administrative accounts on shared systems must consider the consequences of their actions on other users of those systems. For instance, users may unintentionally or intentionally modify system settings, which can disrupt network connectivity, cause software conflicts, or reduce the overall stability of the system by performing certain actions.

Procedure(s)

You can request administrative rights by using one of the following procedures:

1. **Admin by Request**
   To request administrative rights, UADA employees can request access to their devices through Admin By Request.
   - Request administrative access by clicking the Request Admin Access (Admin By Request) icon on desktop or by opening the task tray on the desktop and selecting the Admin By Request checkmark icon.
   - Review and approval:
     - By UADA ITS Executive Leadership team.

2. **Local Administrator Access**
   To request administrative rights, UADA employees should follow a formal process that includes:
   - Submit an Administrative Rights to Computers (login credentials required) request explaining the specific reasons and justifications for needing administrative rights.
   - Review and approval:

    - By Supervisor, AES or CES ITS Site Lead, Chief Information Security Officer, Chief Information Officer, and Senior Associate Vice President.
    - Complete annual UADA Cybersecurity Security Training in Workday
- Provision of administrative rights for a limited and defined duration, with periodic reviews and audits.

Revocation of Administrative Rights

Administrative rights may be revoked under the following circumstances:

- The individual no longer requires administrative rights for their job responsibilities.
- No use of Administrative Account for 6 months.
- Violation of UADA IT policies or security practices.
- Non-Compliance with UADA Cybersecurity Training.

Accountability

Persons in violation of this directive are subject to the full range of sanctions, including, without limitation, the loss of access privileges to resources, disciplinary action, dismissal from UADA, and legal action. Some violations may constitute criminal offenses, as outlined by federal, Arkansas, and all other applicable laws. UADA will carry out its responsibility to report such violations to the appropriate personnel.

The Chief Information Officer for UADA is charged with the responsibility to periodically review this policy and propose changes as needed.

Reference Documents

UADA Policy 910.1 Division Acceptable Use of Computers and Networks Policy
Request for Administrative Rights to Computer (login credentials required)