

Local Administrator Rights Process & Requests

Division of Information Technology

Stevens Institute of Technology

Objective:

To maintain the security of Stevens workstations, and in accordance with the [IT Security Policy](#), all users of computers owned by Stevens must adhere to the Guidelines outlined in this document.

User Rights:

Since local administrator permissions provide users complete access to computers, there is a higher risk of devices and/or networks being compromised. Therefore, we restrict local administrator rights to Stevens-owned workstations. Generally, there are two designations for all Stevens workstations:

- Standard User: includes integrated access, guards against unintentional or deliberate system-wide changes, and can use most software and tools.
- Local Administrator: includes full and unrestricted administrator-level access to a device.

Procedures:

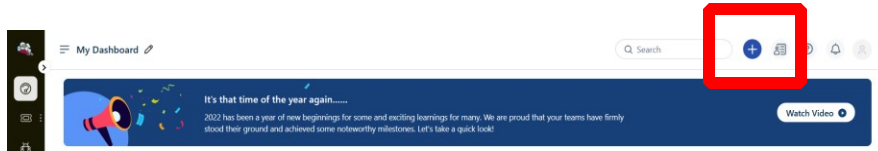
- Every Stevens employee workstation comes with Standard User privileges by default.
- If users need specific applications, software, or updates, it is recommended that they visit the TRAC office or submit an IT Support Ticket to have IT personnel address your request remotely or on site.
- If users need administrative rights on a long-term basis, these are the requirements:
 - Administrative privileges for Stevens workstations will only be granted to faculty and staff members with a legitimate defined need and approval from the appropriate dean or vice president.
 - All individuals with administrative privileges must complete mandatory privileged access user training each year.
 - For non-research and non-lab users, users must reapply for access on a yearly basis.
 - For researchers and lab users, a request can be made to extend the time frame beyond a year.
 - Request for administrative privileges can be submitted on [Stevens support portal](#) on <https://my.stevens.edu> using the steps outlined in Appendix A of this document.

Guidelines for Acceptable Administrative Use:

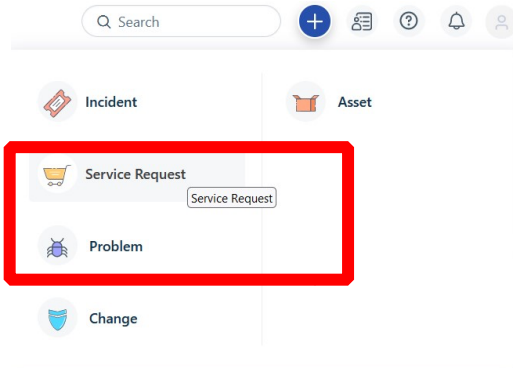
- Only software required for university business is to be installed on Stevens' workstations.
- Software that could expose Stevens networks to viruses and malicious attacks cannot be installed by users.
- Users should not download or install applications that are prohibited, unlicensed, or in violation of the University's Acceptable Use Policy or IT Security Policy.
- The responsibility for maintaining proof of the proper licenses rests with individuals who download or install applications that are not already part of the default setup for all Stevens computers.
- The occurrence of security-related issues or Operating System integrity problems may result in the removal of administrative-level access.

Appendix A: Local Administrator Privileges Request

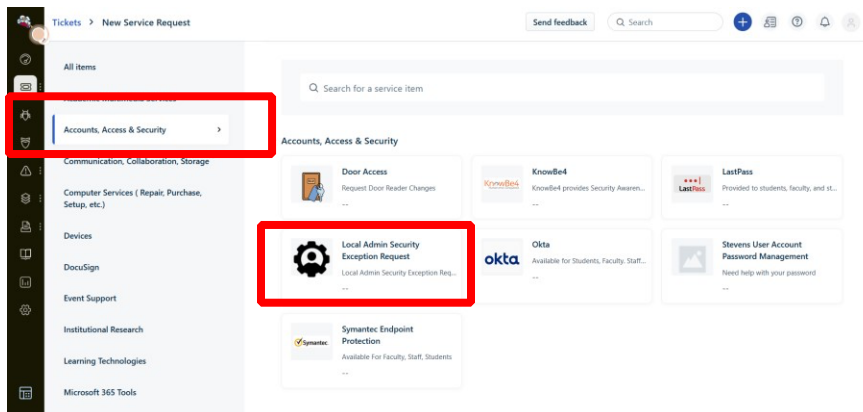
- Go to the mystevens portal: <https://my.stevens.edu>
- Look for Stevens Support Portal
- Click on + to create a new request.



- Select Service Request



- Go to Account Access and Security and select Local Admin Security Exception Request



- Complete the form and place request.
- We will further process your request and may contact you to validate the information provided or request additional details. Please allow 2-3 business days for this process.