



Computer and Network Policies: Bradford Campus Manager Network Access Control Policy

eSupport immediate help online: <http://support.cumc.columbia.edu>
5-Help (212-305-4357) • 5help@columbia.edu • <http://www.cumc.columbia.edu/it>

The Columbia University Medical Center is instituting Network Access Control (NAC) to help provide a more secure computing environment for all students, faculty and staff. **Bradford Campus Manager**, a NAC management tool/appliance, is being used to institute these controls. Bradford will also give connectivity to new computers registering for wired network access within two hours, as long as they meet the basic network security policies.

These basic policies are that each computer using the CUMC network has:

- Current operating system updates
- Working antivirus and antispyware programs with their current virus and spyware definition updates

The Bradford Campus Manager does this by registering computers via a short online form and a running a quick (typically less than a minute) scan of the computer. The scan only checks for the policies and programs listed above, and removes itself from the computer upon completion of the scan. No other data is scanned or checked in any way, and no program is left installed or running on the computer. The form and initial scan can be found at <http://www.cumc.columbia.edu/it/bradford>

Additionally, anyone connecting to the wired network in areas managed by Bradford must now authenticate by logging in with their Columbia UNI and password. This allows us to accurately match owners to their computers, and provides Network Security a more efficient way to contact those using an infected computer.

A list of the specific steps involved in registering, scanning and authenticating with Bradford Campus Manager can be found on the other side of this document or http://www.cumc.columbia.edu/it/getting_started/bradford_steps.html



Why has CUMC implemented the Bradford Campus Manager?

We have decided to use Bradford Campus Manager both to provide significantly quicker registration and access for new computers on the wired network, and to provide a more secure campus network.

Faster Registration and Access to the Network

Registration and wired access previously took one business day or more. Registration using Bradford Campus Manager now allows access to the wired network within two hours of registering for those computers that meet the basic required security policies. NOTE: Computers registering between midnight and 5am will not be able to connect until after 5am.

Providing a More Secure Campus Network

Viruses, spyware, bots and other malware can cause serious problems for any private network and the computers connected to it. By using Bradford Campus Manager we are insuring that computers on the campus network have the most basic security software programs to prevent infection from malware and in doing so, help to provide a much more secure network for all.

Viruses and other exploits in recent years have targeted computers that do not have current working security programs. There have been numerous incidents of widespread attacks that manage to bring down thousands of unpatched, unsecured computers at a time in addition to causing serious congestion on affected private networks. The rise in identity theft by malware also poses a serious problem for all, but is a special concern for the campus network which must maintain compliance with HIPAA regulations.

FAQs About Bradford Campus Manager

Please visit http://www.cumc.columbia.edu/it/getting_help/faq-student-network.html#bradford for more FAQs.

Computer and Network Policies: Bradford Campus Manager Network Access Control Steps

There are three facets involved in the Bradford tool's management of the network:

- Registration
- Re-scans
- Authentication

Registration and Initial Scan

The steps involved in initial registration via Bradford are:

1. A new system* plugs into the wired network at a Campus Manager managed location on campus. Currently, these locations are Bard Hall, Georgian, and Towers I, II, and III.
2. When the system launches a web browser, it will be redirected to the Bradford registration form. The form requests basic contact information and the person's Columbia UNI and password. Information on the computer's make, model, OS version and Hardware Address are collected automatically.
3. A prompt to download and run the Client Security Agent (CSA) appears in the browser with instructions.
4. Upon download and opening of the CSA, a brief scan is run on the computer. The CSA only checks for OS updates, antivirus and antispyware programs and their updates. The CSA displays the status of the scan and what it is inspecting as it runs.
5. The web browser displays whether the scan was successful or the computer failed to meet the network policy requirements of having these updates and programs.



- **Success:** the computer is allowed on the campus wired network within the following two hours. NOTE: Computers that pass registration between midnight and 5am will not connect until after 5am.
 - **Failed**
 - I. The web browser displays a specific message regarding which policies it failed to meet, and links to download required programs and/or updates.
 - II. Until it passes registration, the computer will be in a Remediation network on the campus where the only sites that can be accessed are those needed to install and update security programs.
 - III. Any time the computer reboots or re-opens a web browser, it will be directed to the Bradford registration page until it is able to pass.
6. The CSA program removes itself from the computer whenever it completes a scan

* As the network access management tool is rolled out in various locations on the CUMC campus, a "new system" is considered one that has not previously registered via the Bradford form. Any that had already registered via the old student Wired (Ethernet) Registration Request form will need to re-register so we may verify that security programs are installed and working properly.

Re-scans/Remediation

Every seven days, registered computers are prompted to re-scan via Steps 3 through 6 above. This allows CUMC to verify that computers continue to receive needed updates to their security programs and remain in compliance with required network policies.

Authentication

Every 72 hours a user will be required to authenticate their computer to the CUMC network. The Bradford Campus Manager Authentication page will appear when the computer's web browser is launched. This only requires login with Columbia UNI and password, no scan is performed.