



CAROLINA ADVANCED DIGITAL, INC.
IT INFRASTRUCTURE | SECURITY | MANAGEMENT

SOLUTION SET

www.cadinc.com | 800.435.2212

CAMPUS MANAGER™

Delivers highly-effective network access control and security policy enforcement for educational institutions of all sizes.



College, university, and K-12 computer networks are evolving rapidly to give students, faculty, and staff anytime, anywhere access to ever-increasing multi-media content. With countless PCs, laptops, handhelds, and gaming devices requiring access, education networks are extremely vulnerable to disruptions from unauthorized access and unprotected endpoint devices.

Bradford Campus Manager, a solution set built on Bradford's Network Sentry™ platform, automatically identifies authorized users and verifies security policy compliance of endpoint devices before granting network access. If users fail to gain access, Campus Manager provides remediation options allowing non-compliant users to update their systems themselves. Campus Manager continuously enforces security policies, records detailed historical data to document network activity, and generates reports for security threat analysis and regulatory compliance.

User Identity and Device Registration

Automates user authentication, as well as registration and tracking of all authorized devices on the network.

Endpoint Compliance Validation

Performs security posture assessment via persistent or dissolvable agents, or via integration with existing directory services as part of the normal user login process.

Isolation of Unauthorized or Non-Compliant Users and Devices

Isolates "at risk" users and devices from the rest of the network.

Automated and User-Assisted Remediation

Allows users to correct policy compliance issues themselves without engaging IT staff.

Role-based Access Policy Enforcement

Enforces role-based access policies for all authorized users and compliant devices.

Emergency Notification and Broadcast Messaging

Allows important messages and emergency notifications to be sent instantaneously to all network users running the persistent agent.

Location Tracking for All Devices On Network

Enables Help Desk staff or other authorized administrative users to quickly and easily locate specific users and devices.

Detailed Historical Reporting

Provides detailed log data and reporting functionality to satisfy internal and external regulations, such as DMCA, CALEA, FERPA, PCI, HIPAA and others.

CHALLENGE

Securing network access for a diverse set of users (students, faculty, staff, others) and a variety of devices, while simplifying IT administration.

SOLUTION

Comprehensive network access control with identity management, endpoint compliance, and usage policy enforcement.

BENEFITS

Enhanced network security and control, as well as increased productivity for IT staff.

- Register computers, game consoles, PDAs, etc.
- Assess OS patch, anti-virus, anti-spyware, and P2P applications status
- Automatically remediate at-risk devices
- Secure wireless deployments
- Broadcast emergency messages to all users
- Track network access and usage

"Students registered with virtually no assistance from IT Services. Prior to having Campus Manager, that's something that was unheard of - ever."

*Andrew Watson
Colorado College*



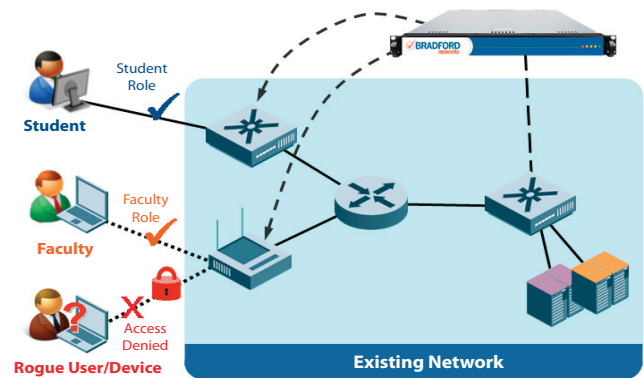
HOW IT WORKS

When a user attempts to connect an endpoint device to the network, the edge switch or wireless access point alerts Campus Manager, which determines whether the device is registered and requires the user to authenticate (log in). As part of the login process, the endpoint device is quickly scanned to check for up-to-date OS patches, anti-virus and anti-spyware software, and/or other system checks defined by IT.

If the scan is successful, Campus Manager instructs the switch or wireless access point to allow network access—typically by assigning the user to an appropriate VLAN, such as a Student VLAN or Faculty VLAN.

If a problem is found when scanning the device—such as anti-virus software that is out-of-date or not turned on—a Remediation VLAN is used to limit or prevent network access. Campus Manager can also provide users with easy instructions for updating their systems themselves so they can get normal network access.

If a rogue user attempts to log in without a valid username and password, Campus Manager prevents network access by telling the switch or wireless access point to assign a Quarantine VLAN or to disable the user’s physical connection. An alert can also be sent to let IT know that an unauthorized user has attempted to access the network.



UNMATCHED VENDOR INTEROPERABILITY

Campus Manager integrates with an extensive range of network and security infrastructure equipment, operating systems, and security applications, and offers the ability to leverage unique features and properties of each network element to maximize all of the available security features.

Network Infrastructure	Switches, Routers, Wireless Controllers and Access Points from dozens of leading vendors
Security Infrastructure	IDS/IPS, NBA, SIEM, DLP, and other 3rd-party security systems
AAA, Directory Services	RADIUS, LDAP-based directory services, and other AAA services
Host Operating Systems	Microsoft Windows, Apple Mac OS X, and Linux
Endpoint Security Suites	Anti-virus, anti-spyware and other host security software suites from numerous vendors

A NETWORK SENTRY™ FAMILY SOLUTION SET

Campus Manager is built upon the Bradford Network Sentry family, an Adaptive Network Security platform that greatly enhances security and automates IT operations. The Network Sentry family consists of the Foundation, an intelligent base platform, along with software-based Solutions and Extensions which can be deployed in combination to meet the needs of any environment. The Campus Manager solution set consists of the following combination of hardware and software components from the Network Sentry family:

Foundation	Intelligent base platform, deployed either on hardware appliances or as a virtual server application
Access Manager	Software solution providing visibility and control of all users and endpoint devices
Device Tracker	Software solution providing management and monitoring of all known endpoint devices
Endpoint Compliance	Software extension enabling validation of security posture of endpoint devices
Integration Suite	Software extension allowing integration of multi-vendor security systems to enhance security & control



Address 162 Pembroke Road, Concord, New Hampshire 03301, USA
 Toll Free +1 866.990.3799
 Phone +1 603.228.5300
 Fax +1 603.228.6420
 Email info@bradfordnetworks.com

Bradford Networks offers the best network security solutions for evolving IT environments. The company’s flexible Network Sentry platform is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. Unlike vendor-specific network security products, Network Sentry provides a view across all brands of equipment and devices so nothing falls through the cracks. Hundreds of customers and millions of users worldwide rely on Bradford to secure their IP networks. Visit www.bradfordnetworks.com

Copyright © 2010 Bradford Networks. All rights reserved. Printed in USA. Bradford Networks and the logo are registered trademarks of Bradford Networks in the United States and/or other countries. Adaptive Network Security, Network Sentry, Campus Manager and NAC Director are either trademarks or registered trademarks of Bradford Networks or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Bradford Networks reserves the right to change, without notice.