

# Identity-based Network Access for Educational Institutions

## Secure Campus Wireless and Guest Access



### Introduction

This paper introduces the steps that IT departments can take to securely connect all users to networks within diverse educational environments. Faced with the rapid adoption of wireless networks, smartphones and the need for campus-wide access, we discuss new trends and outline a sample deployment that takes advantage of Avenda's eTIPS™ policy platform. Operational value and savings by using a centralized approach for differentiating a users wireless access, controlling managed and unmanageable devices, such as laptops, iPhones and game consoles and policy enforcement are addressed throughout.

### The Diverse Campus

#### Challenges Maintaining a Secure Network

Today's campus initiatives must satisfy the computing needs of a broad population of students, researchers, faculty, non-academic personnel and guests. The challenge for the IT staff is to maintain consistent network security while providing users differentiated, or role-based, access to network resources regardless of their location-on or off campus.

The requirements for secure networking have grown to include support for the numerous types of end-user devices, the changing versions of operating systems used, and the potentially risky integrity of the endpoint devices. How do you identify and hold accountable students or guests that access the network with their own computers, and spread malware and viruses?

Another pressing issue involves deploying a simple method to distribute campus-wide login and password privileges for the large number of visitors that take advantage of public wireless access. IT staffs are often tasked with creating and then deleting information pertaining to the user, distributing login information and ensuring proper network access.

The challenge increases as individual departments, campuses, or schools within an institution maintain their own user repositories. This decentralized approach frequently means that no single, comprehensive store of user and policy information exists. Updating or accessing a user account or a user's group affiliation may mean searching multiple department or remote directories.

When a problem does arise in a segmented environment, users often encounter challenges identifying the appropriate IT staff to help determine why they cannot access the network.

### Connected Campus



## Risk Mitigation

The proliferation of low level authentication methods on wireless networks has made it easy for unauthorized users to gain access to network resources and confidential student information.

## Sponsored Access

Easy-to-use, self-provisioning capabilities allow trusted “sponsors” or users to define roles, duration periods and appropriate access authorization.

## Removing the Complexity

### Centralized policies for wireless, wired and remote access (VPN) networks

Wireless networks have become a standard method of access on every campus as students and faculty have come to expect availability of resources from any location. Initially deployed in common areas of the campus (libraries, plazas, etc.), wireless is now expanding to classrooms, research departments and dormitories, offering a wide umbrella of coverage across the entire campus. Unfortunately, existing wireless networks have frequently been deployed using fairly low level authentication and authorization methods. This methodology represents troublesome security risks as wireless deployments grow in scope and users are provided access in more areas of the campus network.

The proliferation of low level authentication methods on wireless networks has made it easy for unauthorized users to gain access to network resources and confidential student information. Easy-to-deploy encrypted wireless access methods and role-based policies can now provide a systematic way to control who has access to the network. This provides a higher degree of trust for the institution and the user community.

## A New Approach

A centralized identity-based network security platform is the first step to ensuring consistent policies for:

**Role-based access** - the ability to automatically provide network privileges to an end user based on their identity (role, title, function, department, etc.). For example, by adding identity based, conditional policies, staff can be placed on one network segment while students can be placed on a less-privileged segment, using identity, location or time-of-day. In addition, access for students can also differ in a common area (library) versus when in a classroom during an examination. This same principle applies to any wired or VPN connection within the campus domain. For example, VPN access for collaborative projects among schools, private businesses, or government agencies can be differ for staff, non-staff, non-student users based on the network resources needed for the project. By applying consistent policies, the IT staff can easily administer appropriate access, generate audit reports and provide necessary security compliance.

**Visitor Access** - satisfies a requirement to offer network access for short durations in support of activities such as conferences or meetings. Easy-to-use, self-provisioning capabilities allows trusted “sponsors” or users to define roles, duration periods, and appropriate access authorization. This relieves the provisioning burden from skilled IT staff members. In the past, the IT team would need to provision and then remove users from existing identity stores.

**Device or endpoint access** – provide access privileges based on a user’s identity which can include the type of endpoint - laptop, desktop or Smartphone that is used to access the network. Granular policies can be created that give greater access to network resources for approved laptop devices versus limited access for iPhone™ or BlackBerry® devices in less secure or common areas.

**Endpoint Health** - advanced policies can also be created that will require users to perform periodic health checks (anti-virus, anti-spyware) before accessing more secure areas of the campus network. This method can help alleviate a non clean endpoint device from possibly corrupting critical resources that contain confidential or private information.

## The Connected Campus Solution: Avenda’s eTIPS®

The eTIPS platform allows for the consolidation of user identity attributes from different departments and from multiple identity stores to be centrally managed from a single platform. Granular policies can then be created that match a service offering for an entire group of users and their requirements to create more predictable access results. With eTIPS’ powerful Policy Engine, security rules can be easily created to support a wide variety of equipment that makes up your existing access security infrastructure. For example, all students accessing the network from common areas, regardless of where their identity information is stored will receive appropriate authorization privileges. eTIPS is unique in that it is able to use the information from multiple identity stores with a single policy.

**Ease of use** is also a trait of eTIPS Policy Manager Interface. Templates are provided that allow the IT staff to readily create policies for common network services; general wireless access, visitor access, wired access for administrative staff. Policy Simulator and Monitor Mode tools ensure that policies are correctly authored and that the effects of these policies will be tested before turning on enforcement.

**Extensive management**, troubleshooting and reporting views streamline the implementation and data gathering process to avoid excessive helpdesk calls, as well as provide fast-track problem resolution. eTIPS also provides the ability to easily consolidate reports from datapoints across the entire campus to ensure that regulators and auditors will receive required periodic reports needed to meet compliance standards

**eTIPS support for today’s industry standards** allows institutions to consistently enforce policies and leverage further value from existing identity stores, endpoint devices, and networking equipment, from any vendor.

- Microsoft Active Directory, Sun ONE, Novell eDirectory, Open LDAP and other LDAP-compliant identity stores
- Any wireless AP, switch, router, VPN and RADIUS-enabled networking devices
- Agentless and dissolvable agent support for Microsoft Windows®, Apple®, and Linux endpoints/computers

### Strong Security

Security rules can be created to support a wide variety of equipment that make up your existing access security infrastructure.

## Higher Education Use Case – Stronger wireless authentication deployments

As the need to provide cutting-edge wireless and voice technology becomes a requirement, many institutions are revamping their wireless LAN infrastructure with 802.11n capable access points (APs). This has prompted IT departments to simultaneously roll-out stronger WiFi Protected Access (WPA2) or 802.1X authentication. This new security element means that the user's endpoint device must be updated to support this stronger method of authentication. Because of the new endpoint requirement and the need to replace large numbers of wireless APs, institutions are approaching these upgrades with a phased deployment strategy.

The goal throughout each deployment is to ensure that the user (student, staff, visitor) is authenticated properly regardless of the status of their endpoint (802.1X capable or not).

In this scenario, the deployment of Avenda's eTIPS identity-based networking platform provides uninterrupted access via unique built-in 802.1X, Web Authentication and policy creation features.

**Phase 1:** Wireless APs and associated controllers are upgraded within a targeted area of the campus.

- Access to attributes for affected identity stores is defined within eTIPS, 802.1X authentication is enabled and proper policies have been simulated

- Users are notified which areas of the campus are affected and require endpoint changes

- Users who then log into the upgraded portion of the wireless network using up-to-date devices (.1X capable) are provided seamless access to the network based on identity, role and access privileges

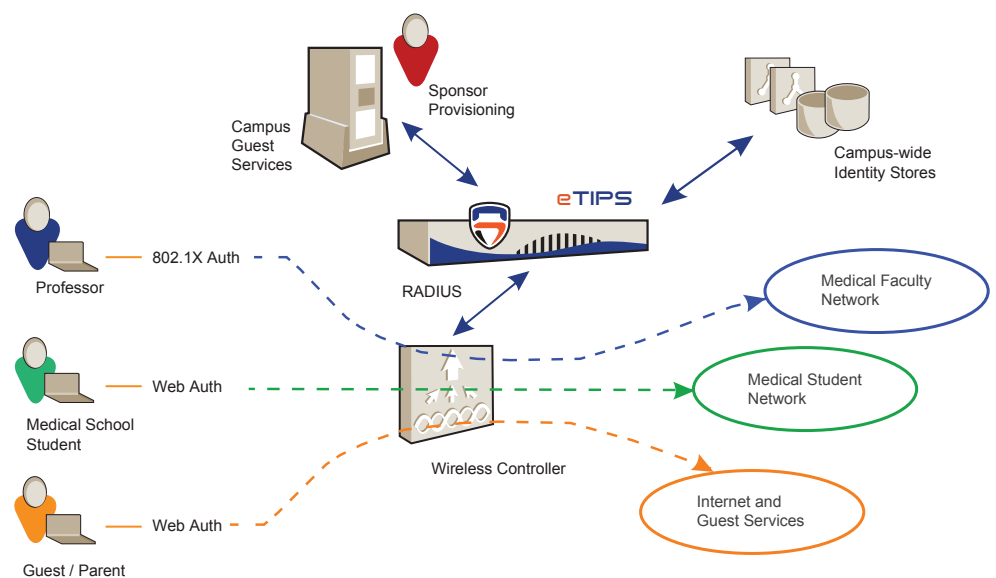
- Users who log into the upgraded portion of the wireless network using out-to-date devices are re-directed to a captive portal where eTIPS communicates with the device via dissolvable agent to authenticate and authorize proper network connection privileges

- Any User (.1X capable or not) who logs into areas of the campus containing older wireless equipment will receive seamless access based on original authentication methods (WEP, Pre-shared keys)

### Subsequent Phases:

- As the wireless 802.1X deployments progress, the above process is repeated

- After a certain comfort level has been reached, additional authentication security can be applied to wired ports and VPN connections; eTIPS uniquely allows IT staffs to re-use the policies previously created for wireless access



In addition to centralized administration, Avenda's eTIPS delivers the following unique capabilities:

- Support for all 802.1X EAP (Extensible Authentication Protocol) types, which are native on all major brands of desktops and laptops; Microsoft, Apple and Linux operating systems
- The eTIPS Dashboard™ provides a real-time display of all users currently authenticated across all network services which helps identify the percentage of users that have complied with the update for stronger authentication. And, in all cases can quickly assist to resolve help desk issues.
- Visitors and guests who access the campus network will be unaffected by any changes in the network and will continue to login via eTIPS built-in Guest Access portal

For the use case described above, the flexibility provided by eTIPS campus-wide policy and enforcement improved security, and wireless key and passphrase management, reduced operating costs, and delivered the ability to painlessly roll-out new services and infrastructure when needed, without interruption.

## Conclusion

Avenda offers institutions of all sizes the ability to automate and control users network access and endpoint security. Differentiated end user service is centrally managed for all staff, student and visitors regardless of location or connection method. Broad support for open standards allows for the integration of secure policies in any heterogeneous network.

Avenda's eTIPS provides a cost-effective solution for centralized management and trouble-shooting across wireless, wired and VPN networks. IT staff members in the network, security and computing departments can work together to create campus-wide policies that map each user to appropriate services.

- Supports all existing identity stores, network and AAA resources, endpoints, and anti-virus, anti-spyware and firewalls
- Provides the ability to differentiate access for all users and endpoint types
- Offers a complete Campus and Guest Access solution with sponsor administrative account creation and control
- Industry's easiest to deploy and maintain policy system

Avenda Systems, Inc.  
3255 Scott Blvd., Bldg. 2, Suite 102  
Santa Clara, California 95054  
408.748.0902  
www.avendasys.com

*Securely Connecting Users to Networks*

## About Avenda

Avenda Systems introduced the industry's first multi-function platform for network access security that breaks through past deployment barriers – complexity, compatibility, compliance and cost.

Avenda's flagship eTIPS™ solution is a scalable AAA platform that utilizes identity-based policies for access control, endpoint health and device authorization across wired, wireless and VPN networks.

