

# Deploying Secure Endpoint Wireless Network Services

Whitepaper



## Summary

Constant incidents of data breaches, bandwidth stealing and denial of service attacks in wireless networks everywhere have made it a business requirement to deploy secure, authenticated wireless networks. No longer is it prudent to expect that basic security authentication protocols such as those using pre-shared keys and policies are sufficient. Wireless network deployments must balance user accessibility with hardened security. A combination of enhanced wireless devices with support for the latest encryption and authentication protocols and an easy to use network policy platform ensures that an appropriate level of role-based access and audit capability are set in place for today's wireless LAN deployments. The eTIPS platform offers a flexible and incremental approach to deploying secure and authenticated wireless networks.

## WLAN Uptake

Dell'Oro Group expects the enterprise WLAN market to increase to \$3.5bn in 2009, from \$1.1bn in 2008, a compound annual growth rate of 32%.

Growth is expected to be driven initially by healthcare, education and retail sectors, traditionally strong verticals for Wi-Fi.

The advent of built-in client gear in most notebook PCs has eliminated the cost of separate Wi-Fi cards and led employees to expect wireless capability.

Dell'Oro Group  
November, 2008.

## Increased User Mobility

Wireless LANs have become ubiquitous in organizations large and small as they offer increased mobility and the flexibility needed to enhance productivity and develop innovative new use cases, all while saving cost. These use cases range from retail inventory and healthcare communication to real-time enterprise collaboration networks. Wireless connectivity is also ubiquitous at home, and in many retail and entertainment establishments. But as users are offered convenient access to network services they are often exposed to security risks that are beyond their understanding. These risks must be considered by IT security departments prior to any enterprise or institutional deployments.

As wireless signals are pervasive and not contained by walls they are easily intercepted using readily available tools which have forced many organizations to no longer rely on open wireless networks. Many organizations have turned to WEP and WPA based encryption to provide secure wireless access. However, with the recent cracking of these encryption methods, it has become imperative for organizations to move toward strong authentication and dynamic key based encryption, which is provided by 802.1X based authentication methods. Unsecured data is only one of the risks in such a deployment though. In some cases employees can con The advent of built-in client gear in most notebook PCs has eliminated the cost of separate Wi-Fi cards and led employees to expect wireless capability nect malware-infected laptops or access the network in ways that are inconsistent with company usage and compliance policies.

The challenge is to ensure that there is a high level of security and consistent access permissions regardless of the user's role or where the connection is established. For certain types of organizations, challenges with wireless security are more complex. Universities may have a hybrid environment consisting of network access points from multiple vendors, and there might be conflicting demands for access privileges and accountability. Like many other organizations, universities are required to secure personal data to keep it private, as well as meet a host of compliance regulations that necessitate fine-grained access control and reporting.

This solution brief describes the challenges associated with deploying a secure, authenticated wireless network and shows how organizations can use eTIPS to automate user access control to ensure the appropriate level of security and permissions for WLAN deployments.

## Exploring the Wireless Challenge

In addition to potential bandwidth pirating by unauthorized users, wireless access can introduce some very real security issues, some of which are similar to those of wired networks. The underlying communications medium, airwaves, make it the logical equivalent of an Ethernet port in the parking lot. Unauthorized users can potentially gain access to intellectual property and information; they can corrupt corporate data, degrade network performance, launch DoS attacks or use corporate network resources to launch attacks on other networks.

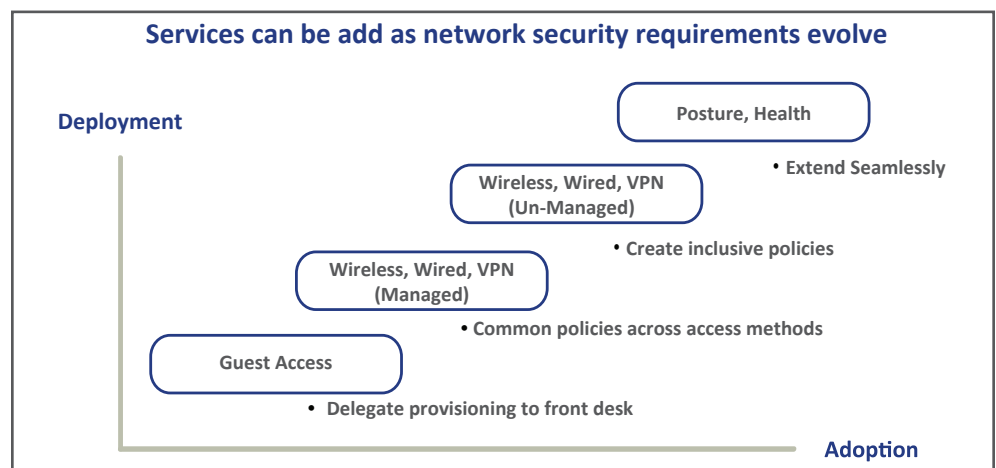
Anyone equipped with a laptop computer in close proximity to a wireless access point has the potential to use the organization's network. In most environments simply applying security settings to each access point is not only cumbersome, but also ineffective, as employees can deploy rogue access points that network administrators may not be aware of

These and other concerns are forcing organizations to implement security architectures that contain some form of higher level user authentication. In organizations where protection of data is crucial, such as the financial and health-care industries, a balance is needed that contains secure access that is managed and tracked. The type and strength of security needs to be appropriately applied, based on the sensitivity of the information transmitted over the network, the cost and the needs of the users. Designing for real end-to-end security is not a simple task, as network vendors offer many alternatives for access control that may not interoperate with other vendors' offerings which lock you into their products.

An overall security architecture that is built around an open standards platform for user access control, and also connects to disparate directories for identity data and to any network equipment from different vendors is needed. The IT administrators must also have the flexibility of creating and leveraging centralized role-based policies that control access to the entire network, including WLAN, wired Ethernet, VPN and dialup connections. When deploying secure and role based wireless access control, it makes operational and economical sense to acquire a system that allows the organization's IT administrators to incrementally roll out wired, VPN and guest and partner access.

### Deployment and Management Flexibility

When deploying secure and role based wireless access control, it makes operational and economical sense to acquire a system that allows the organization's IT administrators to incrementally roll out wired, VPN and guest and partner access



### Addressing Security and 802.1X Standards

Data encryption protocols for wireless LAN, such as WPA (Wi-Fi Protected Access) and TKIP (Temporal Key Integrity Protocol) allow all traffic on the network to be encrypted and have become a necessity of any secure wireless deployment. Recent WPA and WEP key attacks have accelerated the need for enterprises to adopt a more secure form of access. 802.1X and EAP based authentication offers the most secure form of access because of the inherent support for dynamic keys in encrypting wireless traffic. While secure access is an important component of 802.1X and EAP based authentication, these protocols also offer stronger user-authentication capabilities, such as role-based access, and can be deployed in a more manageable and cost effective manner. Deployment has been simplified as many popular operating systems and network equipment vendors now include 802.1X support in their products, allowing role-based access control technology to be a part of any network infrastructure upgrade or new installation.

Deployment of role-based access control has emerged as the preferred method for enforcing network access security on both the wireless and wired networks to ensure that users can use the network only in ways appropriate to their roles and needs. Widespread authorization and provisioning policies that enable IT administrators to configure different types of access for employees, contractors and guests are essential if the organization is to maintain a secure environment.

The compromise of lower level authentication methods, and the native embedding of 802.1X supplicants in popular operating systems, has accelerated the adoption of 802.1X as a means to secure and include role-based access; the added benefit is that the same 802.1X supplicant now can be used to also control access into wired networks. Networks based on 802.1X authentication require the RADIUS server to handle user credential verification with support for a wide variety of EAP methods; moreover, role based access control requires the server to support rich policies. Many existing RADIUS solutions were built with the service-provider market in mind and lack features an enterprise would require for role-based policies. The legacy Service Provider systems and freeware solutions available today cannot easily support any large sized deployments, nor do they offer needed manageability, scalability, support and troubleshooting mechanisms required for enterprise-wide use.

Furthermore, network equipment vendors often provide extensions and enhancements beyond the basic capabilities of RADIUS, and IT security administrative staff must have a deep understanding of 802.1X, EAP and the RADIUS protocol in order to use these capabilities. What is needed is a policy server that lets the IT administrators focus on the business logic and not worry about the details of the underlying access protocols.

### Simplifying a Secure Wireless Solution

The key to a secure wireless solution is end-to-end security with validation and sustainability at every step of the process. The solution must consistently provide an expected level of service that the users and IT administrative staff do not find cumbersome.

eTIPS® from Avenda Systems is a comprehensive role- and policy-based network identity system that provides the innovation and flexibility needed for any sized wireless deployment. Out-of-band control and performance augments wireless, wired, and VPN equipment alike by not creating a bottleneck or a single point of failure. Full featured clustering and data synchronization provides better manageability and scales from small deployments to deployments of tens of thousands of users. These unified policies span basic guest access to complex role-based policies for employees and managed and unmanaged end-points such as laptops, handhelds, printers, and ad hoc wireless access points. And, this single policy platform provides the ability to fine-tune a user's access by taking advantage of existing authentication sources, such as Microsoft Active Directory, LDAP directory, SQL database, and token servers.

High-availability clustering also allows eTIPS to scale to thousands of users across geographic regions. In conjunction with mobility controllers and access points from any networking vendor, the solution delivers extensive regulatory and compliance reporting, optional checks for endpoint posture or health along with remediation, port and vulnerability scanning of unmanageable devices, and a powerful help-desk dashboard for delivering expedient end-user support. This combined solution easily evolves from initial security applications like guest access to broad 802.1X and Microsoft Network Access Protection (NAP) based deployments, and can also support environments with mixed NAC, NAP or TCG-TNC framework based deployments.

### 802.1X Adoption Taking Off

“IEEE 802.1X’s fortunes might be about to change. For example, vendors are working to correct the technology’s shortcomings. In addition, some experts predict that wider adoption of Windows Vista, which offers improved support for 802.1X, which will spur increased deployment of the technology.”

The increased use of wireless networks, particularly for purposes requiring security, will spur more 802.1X use in mobile devices.”

Robert Whiteley  
Forrester Research  
2008

## End User Authentication and Compliance

End-user devices can be classified as managed (a corporate entity) or unmanaged (printers, smartphones, or a personal laptop) where each poses a separate challenge in regards to 802.1X, as both types need to exist on the same network. Regardless of device the goal is to create a process where the user is properly authenticated before gaining access to the network based on multiple attributes:

- user or device identifiers
- user role
- type of device
- location
- identity attributes (Active Directory, LDAP, etc)
- network device and protocol attributes

**Managed** devices require an 802.1X-enabled client called a supplicant to connect to the wireless network. The supplicant negotiates a secure communication tunnel with eTIPS and uses that tunnel to send the user's credentials. During this process, the wireless access point is responsible for forwarding packets between the supplicant and eTIPS.

eTIPS then performs the necessary authentication and authorization, including verification of the user's credentials and extraction of the user's identity attributes from LDAP directory, AD or SQL database. eTIPS then sends a message to the wireless access point or controller to deny or permit access. If access is permitted eTIPS can provide more granular access (VLANs, ACLs, QoS attributes) using the built-in features of the access point or controller. The wireless access point complies with the request and generates a RADIUS accounting message describing the event. A record of the user's access request is stored in the logging system to allow auditing and report generation at a later time.

As a further level of protection, all approved wireless access points are configured to submit authentication requests. Likewise, eTIPS only responds to requests from wireless access points it knows. Having one system handle authentication and authorization for the entire network provides a unified, real-time view of approved devices accessing the network.

**Unmanaged** devices consist of two types, some that may not be capable of supporting supplicants (printers and IP phones) and some that can support a supplicant (guest/visitor laptops) but are not a part of an organization's management domain. For those that do not support a supplicant, eTIPS allows or denies access based on a whitelist or blacklist stored in the local DB, or an external store such as an LDAP directory, AD or SQL store. Furthermore, eTIPS can also perform a network port scan or vulnerability scans to provide more granular access based on a device's type or its state of health.

For those users accessing the network via a device that can launch a browser, eTIPS uses a dissolvable agent and captive portal to provide web based authentication and optional device health checks.

Any user accessing an organization's network via an iPhone, personal laptop or other handheld devices will adhere to the same level of access policy as managed devices or possibly more stringent access put in place for unmanaged devices.

eTIPS works with all popular 802.1X supplicants, including the native supplicants available on Windows, Mac and Linux platforms. A new configuration utility that will ease the endpoint setup process for 802.1X is also in the works. Avenda Linux Agents are available for Linux based endpoints that do not natively support 802.1X supplicants.

### Full Featured 802.1X Support

eTIPS works with all popular 802.1X supplicants, including the native supplicants available on Windows, Mac and Linux platforms.

Avenda's Quick1X, a new configuration utility eases the endpoint setup process for 802.1X deployments. Users are directed to a captive portal where they initiate the self-guided wizard and are connected to the network in the final step.

IT administrators can push subsequent changes using the same utility.

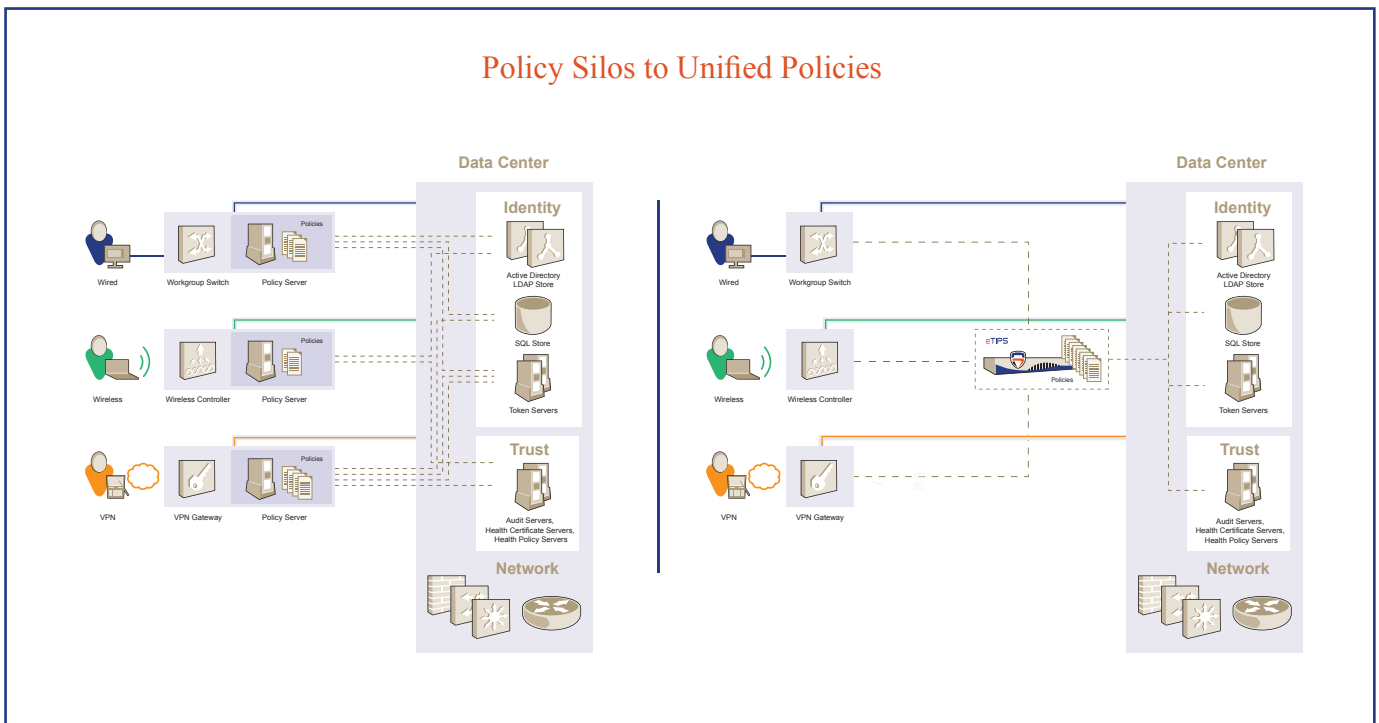
### Elimination of Policy Silos

IT administrators can leverage existing networking equipment and policy servers or they can consolidate multiple policy servers, audit servers, and management platforms across access silos to eliminate inconsistencies in order to better manage resources.

### Operational and Runtime Scalability

As wireless network usage grows, more wireless access points may be added to the network and users will expect a consistent experience from anywhere; the building, campus or remote location. Configuring user-access policies on each separate access point or controller, VPN concentrator and switch is not scalable and leads to security vulnerabilities, operational complexity and compliance headaches. With eTIPS, access policies are centrally configured and managed, ensuring there is network wide coverage and the entire network remains secure as it grows.

Enterprise-class clustering capabilities allow eTIPS to easily support additional users and access devices or new networking equipment regardless of vendor or location. A fully replicated cluster also means all management and configuration is done from a central place, instead of creating policy silos. IT administrators can leverage existing networking equipment and policy servers or they can consolidate multiple policy servers, audit servers, and management platforms across access silos to eliminate inconsistencies in order to better manage resources.



### Incremental Policy Enforcement

The modular architecture that eTIPS is built on allows IT administrators to incrementally fine-tune, enhance and extend policies for network access. When deploying 802.1X for wireless environments, it is prudent to start with identity and role based access control for managed endpoints, primarily those operated by employees. Once this is in place, the IT administrator can create policies for unmanaged and unmanageable endpoints using a MAC-address based whitelist; which can be further enhanced by also having eTIPS perform a network port scan or vulnerability scan of these endpoints. Policies for Guest Access on the wireless network could be next set service put in place. Further enhancements would include policies to perform health assessment of managed and unmanaged endpoints.

**A typical progression of incremental policy enforcement would be:**

1. **Identity and Role based policies** - 802.1X based secure wireless access for employees
2. **Whitelist policies** - wireless access for unmanageable endpoints
  - a. Enhance with port and vulnerability scan
3. **Captive Portal policies** - wireless access for guests, contractors and partners
  - a. Optionally add health checks, using dissolvable agent
4. **Endpoint Posture policies** - enhanced employee wireless access policies with health and posture based rules
5. **Unified policies** - leverage policies developed for wireless access for wired and VPN control

**Dynamic Deployment Monitoring and Simulation**

As customers roll out new wireless networks with richer authentication methods, built-in policy monitoring allows IT administrators to generate detailed reports regarding the health of the endpoints in their network before enforcing network access control. And a policy simulation utility allows administrators to ensure that identity and posture based policies give the expected results.

**Conclusion**

As organizations increasingly deploy wireless networks throughout their infrastructure, network administrators must address the security issues that accompany the technology. With the emergence of the 802.1X standard, most network equipment now offers the basic tools to address secure network access control. Without a strategy and tools to manage these controls, security administration becomes expensive, time consuming, and potentially unreliable. Avenda addresses this problem by offering a system that lets organizations harness the 802.1X controls built into their network equipment and endpoints to provide scalable, cost-effective user authentication and protection for their networks and intellectual property.

**Top 3 Reasons to deploy eTIPS for Secure Wireless Access Control**

- **Enterprise-class authentication and authorization** - industry-leading 802.1X and EAP with built-in RADIUS server for the most secure form of wireless access (no need to deploy yet another RADIUS server required by other NAC solutions)
- **Incremental policy deployment** - Start with simple identity and role-based network access policies, and enhance these, over time, to include posture and health based access. Extend this to include policies for unmanaged device and guest access
- **Global security and management** - use the same set of role and posture based policies for all access methods, regardless of location

**For further information:**

[info@avendasys.com](mailto:info@avendasys.com)



Avenda Systems, Inc.  
3255 Scott Blvd., Bldg. 2, Suite 102  
Santa Clara, California 95054  
408.748.0902  
[info@avendasys.com](mailto:info@avendasys.com)  
[www.avendasys.com](http://www.avendasys.com)