Solution Brief

Aerohive NETWORKS

HOWARD™ | TECHNOLOGY
www.howardcomputers.com | (888) 912-3151

Aerohive and Impulse

Powerful Network Security for Education and Enterprise

Introduction

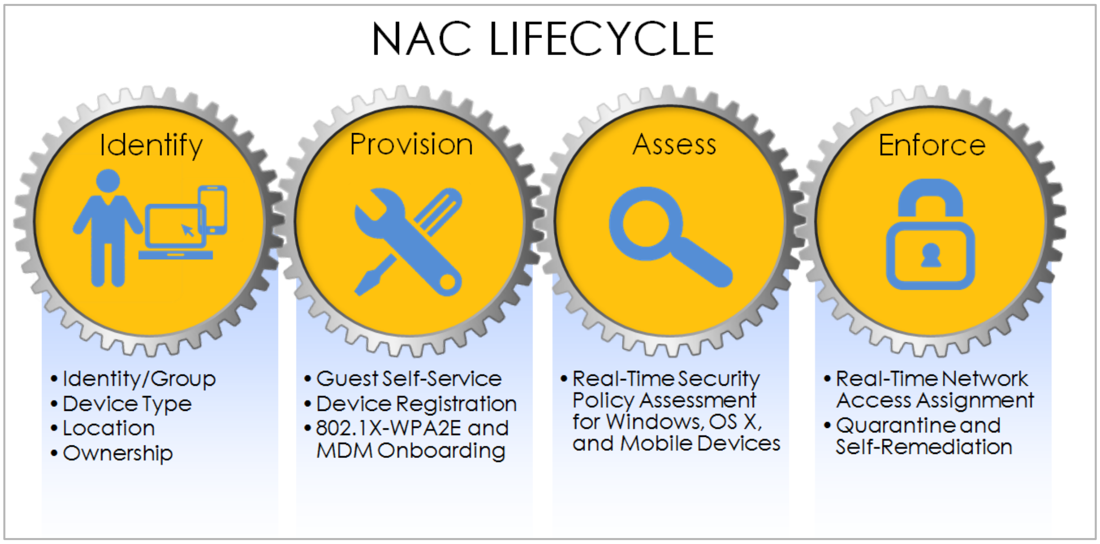
In today's highly connected organizations, end users expect secure Wi-Fi access across the campus and from any of their devices. While this requirement is essential for today's learning and corporate environments, it also opens up a secure network to a multitude of potential issues with Bring-Your-Own-Devices (BYOD), rogue devices and possible threats to secure data from the Internet and unknown applications.

Protecting the organization's networks, data and end user privacy are essential business requirements, but their realization is more challenging than ever. Highly distributed environments, the need to support BYOD and an ever-growing number of device types and applications, as well as depth of content require powerful network security solutions. And while the demands on IT are increasing, both the complexity of deployments and the cost of ownership need to be reduced. In educational institutions like colleges and K-12 schools, IT resources are often much more limited than in enterprises, which is a challenge in itself.

A Network Access Control (NAC) solution automates and enforces an organization's Acceptable Use Policies (AUP) for enterprise-owned, BYOD, and guest devices. A comprehensive offering should:

- Identify and assign security and network access policies based on user identity/group, device type, location, time, and ownership.
- Provide self-service tools to easily provision an end user device without help desk involvement.
- Deliver real-time device security assessment, enforcement and user self-remediation guidance.

In addition, the ability to deploy and support a NAC system with minimal technical resources and network changes while providing a superior user experience are key factors for success.



- Identity/Group
- Device Type
- Location
- Ownership

- Guest Self-Service
- Device Registration
- 802.1X-WPA2E and MDM Onboarding

- Real-Time Security Policy Assessment for Windows, OS X, and Mobile Devices

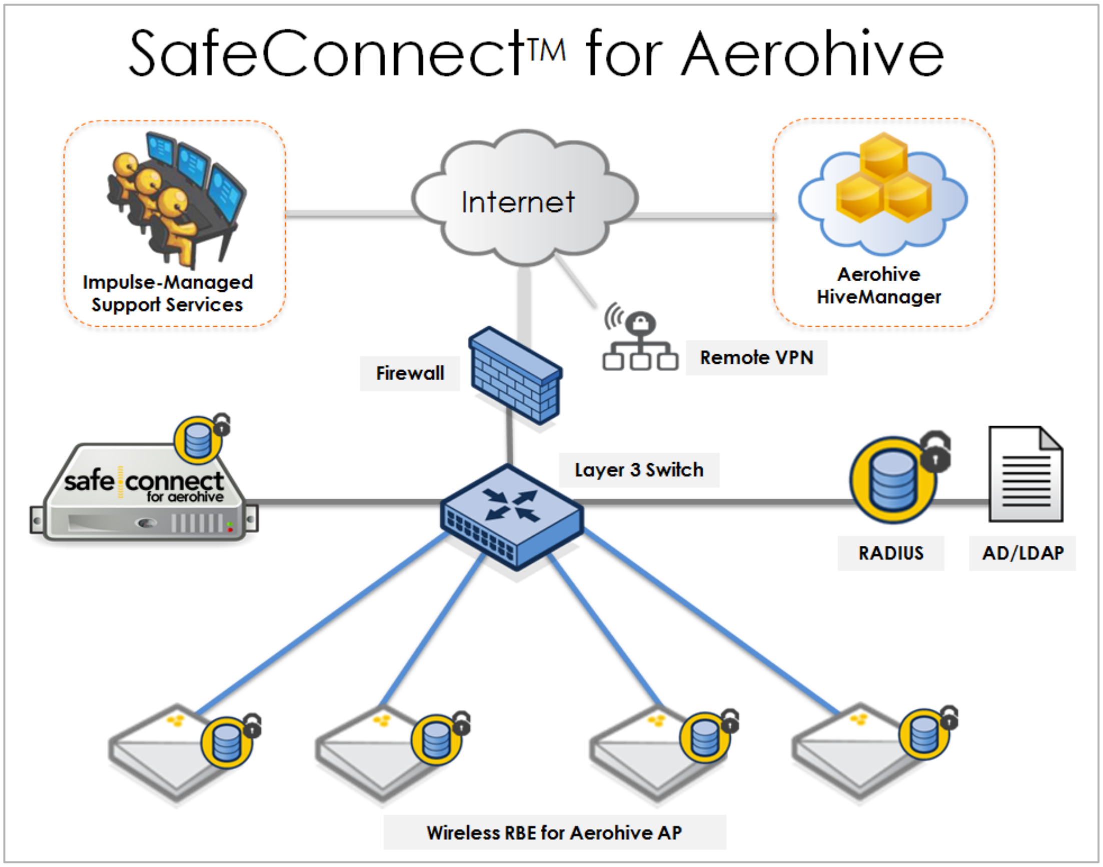
- Real-Time Network Access Assignment
- Quarantine and Self-Remediation

Combining Aerohive's and Impulse's solutions helps address the network security challenges encountered in today's educational institutions and enterprises. It provides enterprise-grade network security in a highly economical manner to ensure safe access to networks and resources for all.

The Aerohive and Impulse Solution

Impulse delivers industry-leading network access control (NAC) with its SafeConnect™ solution. It reduces the risk and impact of security breaches by providing secure onboarding of devices, and then by constantly monitoring devices to ensure they remain in compliance with IT-defined policies. When integrated with Aerohive's controller-less network architecture, the distributed intelligence in the access points ensures that the security policies are enforced on all devices in the network. In other words, Aerohive access points effectively become enforcement points for SafeConnect's policy definitions.

The joint solution supports a multi-vendor network environment for all client devices, whether they are wireless, wired or VPN. It enables automated 802.1X-WPA2 Enterprise (wireless data encryption) provisioning and security compliance enforcement before and after admitting devices to the network. Non-compliant devices can be quarantined immediately and offered remediation guidance. Features like agentless device-profiling, end-user authentication and real-time visibility into device and application usage enable a superior level of network security. At the same time, the user experience, installation, and ongoing management of the solution is greatly simplified, thereby reducing demands on IT.


SafeConnect™ for Aerohive
Impulse-Managed Support Services
Internet
Aerohive HiveManager
Remote VPN
Firewall
safe connect for aerohive
Layer 3 Switch
RADIUS
AD/LDAP
Wireless RBE for Aerohive AP

The combined solution has many benefits including:

- A consistent experience for end users: SafeConnect's device-centric approach enables user identity persistence across network segments and access points. This feature eliminates the need to frequently re-authenticate. Other UX-enhancing features are automated 802.1X/WPA2E provisioning, self-registration for guests and non-browser devices (e.g., gaming, media, etc.), and ongoing real-time device security assessment and enforcement. There is no need to schedule periodic scans of the client population, or to ensure ongoing compliance by forcing clients to re-authenticate periodically.
- No need for VLAN steering: SafeConnect integrates directly with Aerohive controller-less access points to assign access privileges like application permissions and firewall rules dynamically by leveraging Aerohive's user profile firewall-based technology. This removes the need to reconfigure a Layer2 switch port to reassign devices between production and trusted VLANs. It also results in a better end user experience, since devices don't need to be re-authenticated every time the IP address changes. SafeConnect can also utilize Layer3 switches for policy enforcement of wired devices, alleviating the burden of deploying and supporting Layer2 802.1X or SNMP-based alternatives.
- Simplified installation and deployment:
    - Aerohive's HiveManager allows for zero-touch configuration of access points and their associated, unified user profiles and policies. Once the devices are installed, they will automatically contact their assigned HiveManager and will be auto-configured. The result is a highly simplified installation process that can be accomplished by technicians, without involvement from IT.
    - SafeConnect has been designed for remote customer setup and deployment. The system is pre-loaded with the customer's configuration information, and Impulse's customer support center provides remote guidance through the installation and deployment process. Systems can usually be installed in hours by leveraging the managed support services capability.
- Integration with the customer's existing network infrastructure and directory services:
    - SafeConnect integrates seamlessly with Aerohive's Access Points (AP), utilizing their distributed network architecture. No additional networking hardware or changes are needed.
    - SafeConnect also utilizes existing directory services infrastructure (LDAP, MS AD, RADIUS) to authenticate end user devices. Identity and role-based profiles are supported, and enforcement rules can be defined for each profile.
- Contextual Intelligence: SafeConnect for Aerohive provides real-time device-based information (i.e., user profile, application usage, location and time of access, compliance status) to other network management and security systems like web content filters, bandwidth managers, firewalls or SIEMs. This translates to single-sign-on, one-time authentication,

granular policy assignment and enhanced analytics that enable more informed and timely security decisions.

- Cloud-based, centralized management:
  - The Aerohive HiveManager supports cloud-based management that allows administrators easy access from anywhere to remotely manage connected devices, clients and security policies.
  - SafeConnect is supported by a proactive cloud-based managed service that provide continuous system monitoring, problem determination/resolution, daily system updates, and application of future software upgrades which reduce the maintenance burden on the IT department.

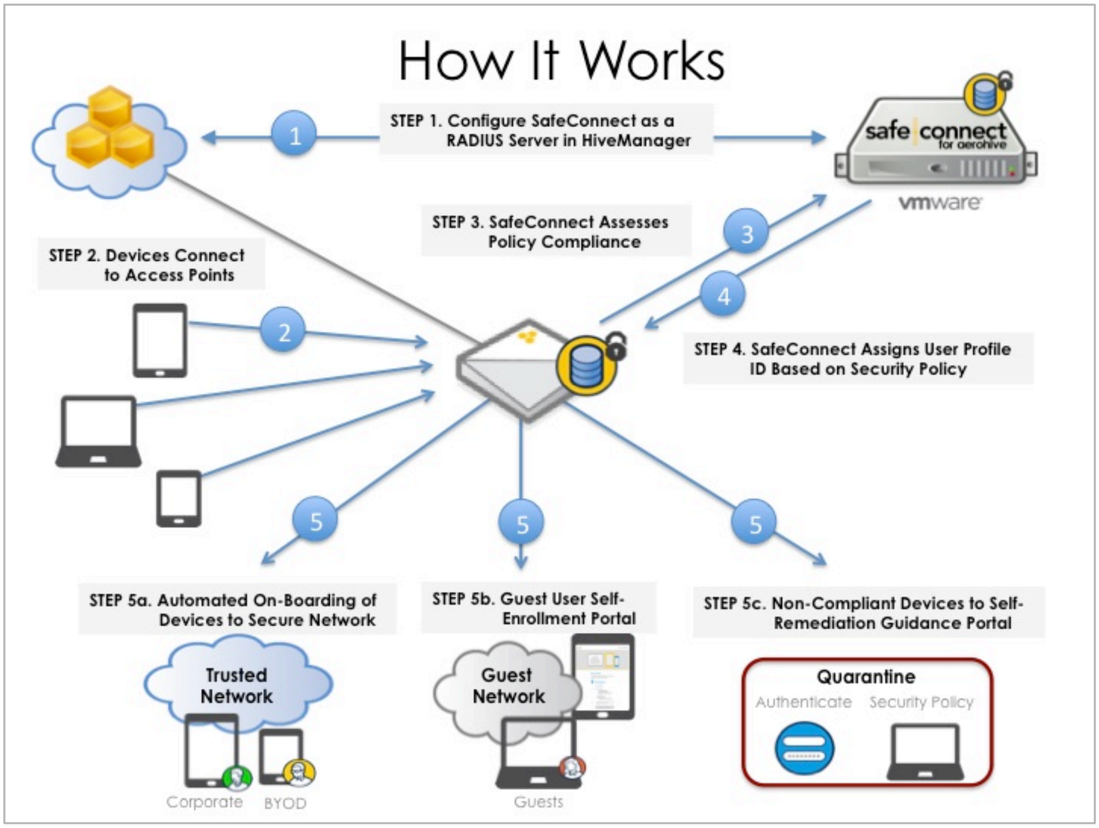
How It Works

Combining the Aerohive and SafeConnect solutions utilizes key advantages of both architectures: Impulse's device-centric access control approach, coupled with the ability to leverage Aerohive's Layer7 application and quality-of-service technologies, enables enterprise-grade NAC, while ensuring the best possible network performance and user experience. To achieve this, SafeConnect integrates with Aerohive's access points, so that they can act as enforcement points for SafeConnect's security policies**.**

Once a new device connects to an access point, it is placed in an initial quarantine mode by the access point's firewall policy and assessed immediately for policy compliance by SafeConnect. After examining the device's level of compliance and associated policy-driven network access privileges, SafeConnect returns a specific user-profile ID. Depending on the result, the access point will authorize the device for:

- Full access to the trusted network.
- Limited access rights, as defined for different user roles (e.g., guests, contractors and employee personal devices). Guests and other unknown users will be re-directed to a self-registration Web page to receive their access credentials. Each of these user roles can be supported with different policies and associated network privileges. Access rights for each user role can be defined by device type, ownership, application usage, VLAN, access duration and location, security compliance and other criteria.
- Quarantine, where it is blocked from the trusted network. To reduce help-desk calls, user devices are guided through self-remediation options:
  - Windows and Mac OS X devices may be re-directed to a remediation Web page with the option to address AUP compliance (e.g., anti-virus software, OS patch policy, encryption software) or provided direction to cease usage of non-compliant applications like P2P file sharing, Skype, gaming, etc.
  - Mobile devices may be re-directed to install the organization's designated Mobile Device Management (MDM) software. They may also remain in a quarantined state if the device does not fulfill other compliance criteria, like being jail broken or missing password or data encryption protection.

Once the devices are authorized, they will be assigned applicable network access privileges and monitored continuously in real-time to ensure ongoing compliance.


How It Works
STEP 1. Configure SafeConnect as a RADIUS Server in HiveManager
safe connect for aerohive
vmware
STEP 2. Devices Connect to Access Points
STEP 3. SafeConnect Assesses Policy Compliance
STEP 4. SafeConnect Assigns User Profile ID Based on Security Policy
1
2
3
4
5
5
5
STEP 5a. Automated On-Boarding of Devices to Secure Network
STEP 5b. Guest User Self-Enrollment Portal
STEP 5c. Non-Compliant Devices to Self-Remediation Guidance Portal
Trusted Network
Corporate
BYOD
Guest Network
Guests
Quarantine
Authenticate
Security Policy

The actual integration of the two solutions is a straightforward process.

In HiveManager, SafeConnect is configured as an Authentication and Accounting RADIUS Server. By creating Access-Lists and leveraging features available in the Aerohive environment, SafeConnect will be enabled to dynamically block, redirect or limit device access based on SafeConnect Policy Group definitions.

The steps of the configuration process are as follows:

1. Add Safe Connect Enforcer as a RADIUS Authentication Server.
2. Create IP objects for the SafeConnect appliance and for the landing page where users are sent after passing their compliance check.
3. Add firewall policies for the different device authorization options:
   - Initial device quarantine
   - Full access to the company network
   - Limited access to the network, differentiated by role (e.g., guest, contractor, BYOD)
   - Quarantine, with remediation options

4. In HiveManager, create user profiles that reference the defined firewall policies.
5. Create RADIUS local user groups for each of the user profiles so that the RADIUS server can send initial and new authorizations.

A detailed configuration guide is available.

Summary

Providing high-performance, enterprise grade networking and security in today's mobile world is key to ensuring productivity for all users, regardless of whether their device is corporate-issued or personal (BYOD).

Aerohive and Impulse deliver a unique industry solution to address the challenges of managing mobile devices in a highly simplified manner that minimizes the technical resources required to deploy and support a secure, high-performance network environment.

By combining Aerohive's controller-less architecture with Impulse's simplified NAC and managed support service approach to automating device security policy management, we created an unmatched offering and value proposition.

About Aerohive

Aerohive (NYSE: HIVE) unleashes the power of enterprise mobility. Aerohive’s technology enables organizations of all sizes to use mobility to increase productivity, engage customers and grow their business. Deployed in over 16,000 customers worldwide, Aerohive's proprietary mobility platform takes advantage of the cloud and a distributed architecture to deliver scalable, simplified, secure and cost-effective networks. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. For more information, please visit www.aerohive.com, call us at 408-510-6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community or become a fan on our Facebook page.

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
The Courtyard
16-18 West Street
Farnham
Surrey, UK GU9 7DR
+44 (0)1252 736590
FAX +44 (0) 1252 713094