

# AEROHIVE<sup>®</sup>



Security and Control for all Devices on the Access Network



**AEROHIVE<sup>®</sup>**  
NETWORKS

# Aerohive® A<sup>3</sup>™

**Aerohive A<sup>3</sup> is an innovative Cloud-Managed Network Access Control (NAC) solution. It secures, manages, and controls all devices on your Access Network – from standard wireless and wired clients to IoT and BYOD.**

A<sup>3</sup> provides complete functionality for device onboarding, guest management, automated device provisioning, device profiling and access control. The industry-first cloud management option significantly streamlines the deployment and management of A<sup>3</sup>. A<sup>3</sup> is vendor-agnostic and runs on access networks from all major vendors.

## Key Features & Benefits

### Supports all devices and users on the access network

A<sup>3</sup> secures standard wireless and wired corporate clients, BYOD, IoT and guest devices alike. It also supports the creation and administration of granular network policies (e.g., by access to applications, time of day, location on the network) depending on the user's role.

### Complete onboarding for guest and corporate devices

A<sup>3</sup> includes a highly customizable captive web portal (*CWP*) that supports self-service onboarding for visitor devices, while a comprehensive management interface and automated device provisioning of 802.1X certificates enables onboarding of corporate devices.

### Comprehensive authentication toolset

For authentication of corporate devices, A<sup>3</sup> supports 802.1X certificates with its built-in RADIUS server. Where certificates are not practical, A<sup>3</sup> provides alternative authentication methods like Pre-Shared Keys (*PSK*) or Social Login (e.g., for Guest authentication).

### Compliance and Remediation

A<sup>3</sup> provides complete functionality for security posture enforcement that ensures authorized devices stay secure over time. Features include device scanning for security compliance, quarantining of non-compliant devices to prevent network access, and guided self-remediation to reduce IT helpdesk calls.

### Security for the Internet of Things (*IoT*)

Connected user-less "things" like thermostats and lighting systems present a unique set of challenges for IT security. A<sup>3</sup> is equipped to onboard, secure and control "Things", with the ability to automatically identify IOT, and then onboard them with appropriately restricted network access rights.

### Seamless integration with existing IT security infrastructure

A<sup>3</sup> can directly integrate with the market leading firewalls, MDM and endpoint security systems, Intrusion Detection Systems (*IDS*) and Posture Assessment solutions they already have installed. These integrations boost overall network security and allows customers to continue to leverage their existing security investments.

### Cloud or on-premises management

A<sup>3</sup>'s industry first cloud-management option enables centralized deployment and ongoing management of local A<sup>3</sup> instances, which greatly streamlines setup and maintenance of the solution and ensures consistent policy application and enforcement. On-premises management of A<sup>3</sup> instances is also supported.

### Device fingerprinting and profiling

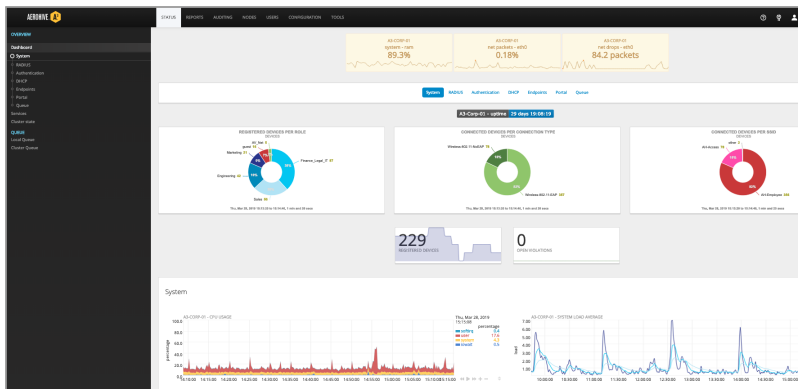
A<sup>3</sup> includes the world's largest continuously updated device fingerprint database. Device fingerprinting is the most comprehensive method for identifying a device type (e.g. laptop vs. smartphone vs. HVAC sensor) automatically when a device requests network access. A<sup>3</sup> can then leverage this information to grant appropriate network access rights to each device based on its type.

### Supports access networks from all leading vendors

Access networks typically include wired and wireless infrastructure components from multiple vendors. A<sup>3</sup> supports WLAN equipment and switches from Aerohive and other leading vendors, which provides customers added deployment flexibility.

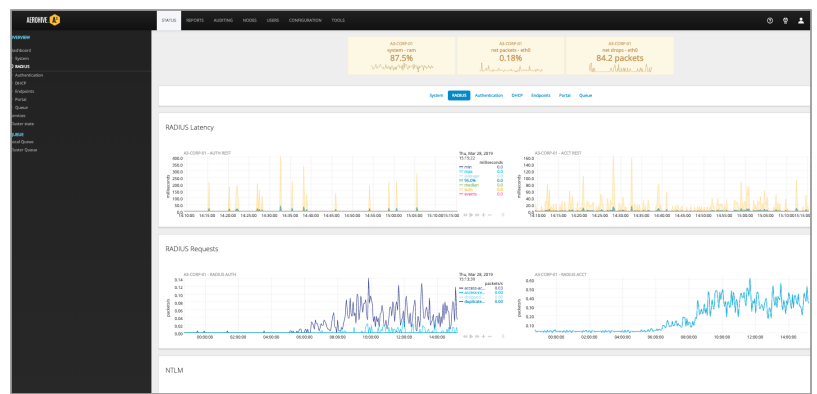
### Usability

One of the design tenets of A<sup>3</sup> is streamlining workflows to help simplify complex tasks. For example, the setup of new Virtual Appliances and clusters can be performed directly from the UI, and can be completed in as little as 30 minutes. A comprehensive set of troubleshooting tools is also available through the UI. These powerful tools remove the need for tedious, error-prone CLI configuration and allow administrators to be more efficient.

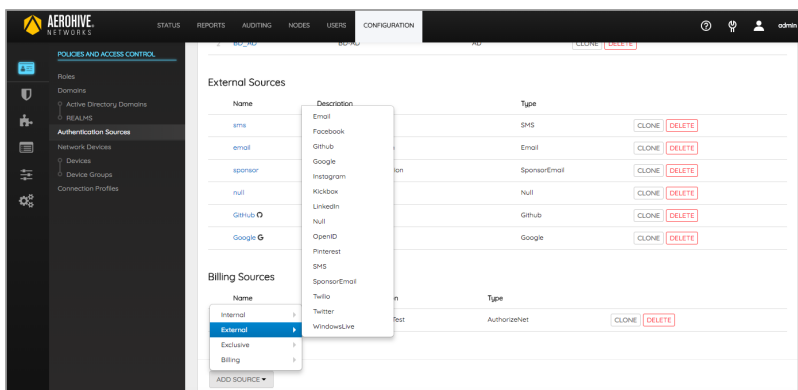


Intuitive graphical dashboard

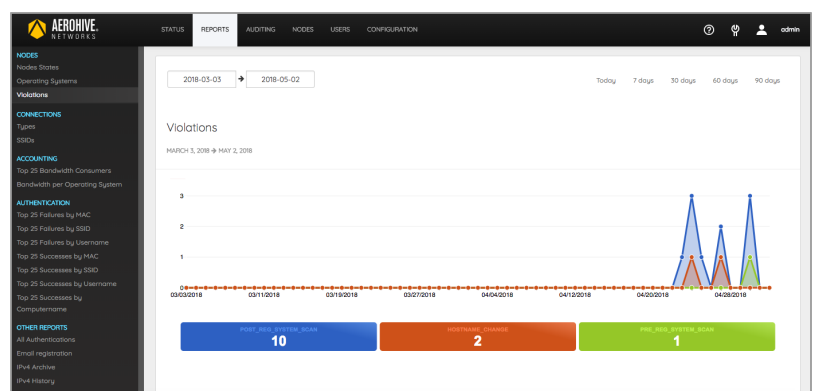
Detailed RADIUS analytics



Configuration of external authentication sources



Extensive reporting capabilities



## Management Features

---

- **Role-based Access Control (RBAC)**

- Per User
- Per Switch
- Per VLAN
- Per Client
- Per Client Category
- Per Device Type
- Per Time
- Per Location

- **Object based configuration management**

- Define roles, domains, authentication sources, switches and WLANs, and connection profiles easily

- **Automated checkpoint and fix permissions tasks**

- **Accounting based on several criteria**

- Node, switch groups, user, role, OS, source, realm, SSID, profile and domain
- Violations, failures, successes, registration type and state

## Guest, BYOD and IoT Management

---

- **Customizable Captive Web Portal (CWP)**

- **Wireless ISP Roaming (WISPR), Eduroam and Hotspot 2.0**

- **Supports billable hotspots**

- Billing and service tiers
- Payment processing through Paypal, Mirapay, Authorize.net, Stripe

- **Guest Access Self Registration**

- With or without credentials
- Self- registration with Social login

- **User device registration**

- **Employee sponsorship**

- **Email Validation**

- **SMS Validation**

- **Password-of-the-day**

- **“Device profile” or “device fingerprint” based onboarding**

- **Aerohive Private Pre-Shared Key (2019)**

## Authentication

---

- **EAP Protocols**

- EAP-FAST, EAP-PEAP, EAP-TTLS, EAP-TLS, PAP, CHAP, MSCHAPv1 and 2, EAP-MD5

- **802.1X Support**

- RADIUS to AD/LDAP server support for 802.1X authentication
- 802.1X (PEAP) or Certificate (TLS) BYOD automated onboarding
- User Authentication Portal (AD/LDAP)
- PKI with EAP EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAPv0, EAP-PEAPv1, EAP-MSCHAPv2

- **Authentication Types**

- **LDAP**

- *Microsoft Active Directory*
- *Novell eDirectory*
- *OpenLDAP*
- *Any LDAP-compliant servers*

- **RADIUS**

- *Cisco ACS*
- *RADIUS (FreeRADIUS, Radiator, etc.)*
- *Microsoft NPS*
- *Any RADIUS-compliant servers*

- **Local user file (Apache htpasswd format)**

- **OAuth2**

- *Facebook*
- *Google*
- *GitHub*
- *LinkedIn*
- *Microsoft Live*
- *Twitter*

- **SAML**

- **Additional built-in SQL DB for User store for deployments without LDAP**

- **Aerohive Private Pre-Shared Key (2019)**

## Secure Provisioning

---

- **Provisioning agents**

- Android
- Windows

- **APIs for all Apple devices**

## Network Access Control

---

- **Realtime security policy assessment (posture assessment) & notification for multiple OS**

- **Gradual Deployment**

- Pre-registration
- Per location/switch/port deployments

- **Automated Device Registration**

- By network device
- By device fingerprinting
- By MAC address vendor
- Integrates with 3rd party solutions to extend device registration capabilities
  - *Short, Nessus, OpenVAS, Browser User-Agent and more*
- VLAN isolation and quarantining (*See supported switches below*)

- **Netflow / IPFIX**

- **Bandwidth accounting**

- **Floating device support**

- Switches and APs

## Profiling

---

- **Functionality**

- Profiling of devices/ IoT device recognition
- Group based policies for network devices
- Device visibility and identification

- **Device Fingerprinting**

- World's largest device fingerprinting database
- DHCP v4 & v6
- User Agent
- MAC address Patterns
- OUI
- TCP fingerprints
- Behavioral analysis

## Integration Capability with Complementary Security Infrastructure

---

A<sup>3</sup> optionally integrates with these 3rd party IT security solutions:

- **Intrusion Detection (IDS):**

- OPSWAT Meta defender
- Snort
- Suricata
- Fortigate
- TrendMicro

- **Vulnerability / Posture Assessment**

- Nessus
- OpenVAS
- Windows Management Interface
- TNC Statement of Health protocol

- **Endpoint Security**

- OPSWAT Meta defender Agent
- Symantec SEPM
- Sentinel One

- **Mobile Device Management (MDM)**

- Mobile Iron
- JAMF
- AirWatch (*2HY 2019*)
- Microsoft inTune (*2HY 2019*)

- **Firewalls**

- Barracuda
- Checkpoint
- Cisco
- Fortinet
- Fortigate
- iBoss
- Juniper
- PaloAlto Networks
- Watchguard

- **Microsoft PKI**

- Simple Certificate Exchange Protocol (*SCEP*)
- Network Device Enrollment Service (*NDES*)



## Deployment Flexibility

---

- **Simplified Deployment**
  - Out of band deployment
  - Hybrid out of band
- **High Availability**
  - Active/Active Clustering
  - Supports deployments of millions of devices
- **Supported deployment models:**
  - Virtual Appliance (VA)
  - Cloud-based management (*monitoring Q3 2018, configuration Q2 2019*)
- **Supports WLAN Infrastructure from the following vendors:**

Aerohive, Aruba Networks, AnyFi, Avaya, BelAir, Brocade, Cisco, D-Link, Dell, Extreme Networks, Enterasys, Extracom, Hewlett-Packard, Huawei, Juniper, Meraki, Meru Networks, MicroTik, Mojo Networks, Motorola/Zebra, Ruckus Wireless, and Xirrus Networks
- **Supports network switches from all leading vendors:**

Aerohive, Alcatel-Lucent, Avaya, Brocade, Cisco, Dell, D-Link, HP, Huawei, Juniper, Linksys, Ubiquiti, and more
- **VoIP support, also in heterogenous environments, for multiple switch vendors**

Avaya, Cisco, HP and more

## Hardware Requirements

---

- **Virtual Appliance Support**
  - Deployed as VA
  - VMWare ESXi 4.0 and above
- **Minimum System requirements**
  - Intel or AMD CPU 3 GHz
  - 16 GB of RAM
  - 250 GB of disk space (RAID-1 recommended)
  - 1 network card (2 recommended)
- **High Performance Active Clustering**
  - Minimum recommended cluster is 3 hosts for HA, load balancing and failover
  - Significantly increases capacity and throughput
  - Enables sharing of device licenses across different customer sites.
- **Contact your Aerohive partner or representative for configuration assistance**

## Professional Services

---

- Optional professional services are available through A<sup>3</sup> Authorized and A<sup>3</sup> deployment partners (in North America) or A<sup>3</sup> Authorized VAD (in EMEA).

AEROHIVE A<sup>3</sup> - SKUs

| SKU                           | DESCRIPTION   |
|-------------------------------|---|
| <b>AH-A3-VA</b>               | Software license for A <sup>3</sup> Virtual Appliance (VA). Required with A <sup>3</sup> subscription.          |
| <b>AH-A3-HA</b>               | High Availability software license for 2 additional VA for cluster configuration; optional for all deployments. |
| <b>AH-A3-1K-SL-1Y/3Y/5Y</b>   | 1/3/5 Year subscription for up to 1,000 concurrent clients/endpoints. Includes support.                         |
| <b>AH-A3-5K-SL-1Y/3Y/5Y</b>   | 1/3/5 Year subscription for up to 5,000 concurrent clients/endpoints. Includes support.                         |
| <b>AH-A3-10K-SL-1Y/3Y/5Y</b>  | 1/3/5 Year subscription for up to 10,000 concurrent clients/endpoints. Includes support.                        |
| <b>AH-A3-25K-SL-1Y/3Y/5Y</b>  | 1/3/5 Year subscription for up to 25,000 concurrent clients/endpoints. Includes support.                        |
| <b>AH-A3-50K-SL-1Y/3Y/5Y</b>  | 1/3/5 Year subscription for up to 50,000 concurrent clients/endpoints. Includes support.                        |
| <b>AH-A3-75K-SL-1Y/3Y/5Y</b>  | 1/3/5 Year subscription for up to 75,000 concurrent clients/endpoints. Includes support.                        |
| <b>AH-A3-100K-SL-1Y/3Y/5Y</b> | 1/3/5 Year subscription for 100,000 (and more) concurrent clients/endpoints. Includes support.                  |

