Aerohive and Airwatch

Partner Solution Brief

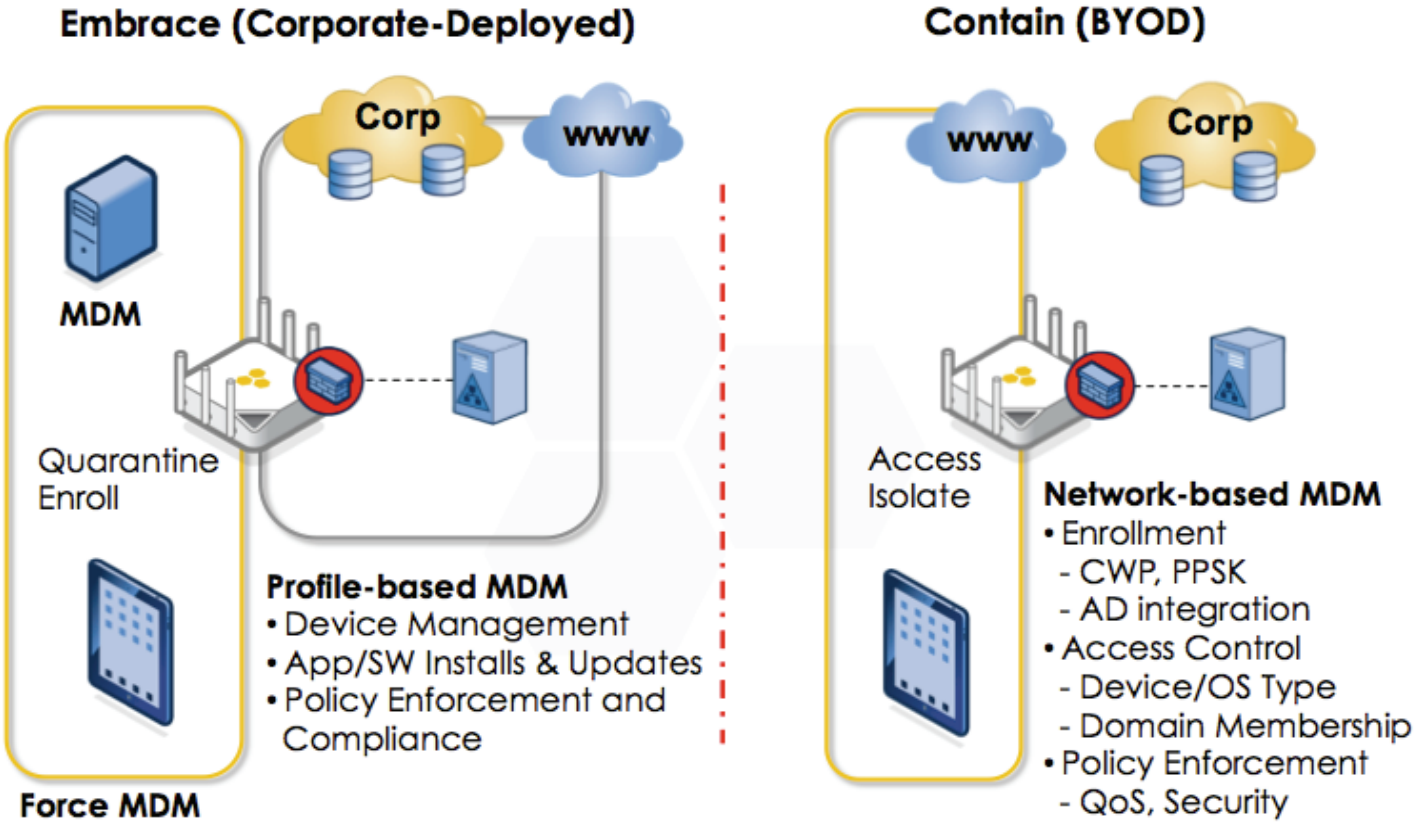
Introduction

The Aerohive and Airwatch Solution

Aerohive next-generation controller-less Wi-Fi paired with Airwatch mobile device management streamlines and automates connectivity, management, and monitoring of mobile devices and BYOD. IT administrators can use these two best-of-breed solutions to increase efficiency, productivity, and security of all mobile assets by enabling control and containment of mobile devices, forced enrollment and re-enrollment of agent profiles, enforced installation and uninstallation of applications, and even compliance checking to ensure devices meet requirements before accessing network resources.

In order to corral the iEverything explosion on today's enterprise networks, IT administrators must be able to control and contain the devices joining the network. There are two main ways to do this, either by installing an agent or profile on the devices to ensure compliance, or by relying on intelligent network infrastructure to use context-based information to implement network permissions. Since "BYOD" and "Mobile Device Management" are very broad terms that cover a wide range of users and devices, the most successful implementations will actually be a combination of both agent-based and context-based enforcement.

Context-based enforcement, also known as Network MDM, is essential to any successful network implementation. The ability to define network permissions based on identity, device type, location, and time is critical to ensure network resources are protected from all types of users and devices. Aerohive uses the highly-intelligent cooperative control capabilities built into HiveOS to control what, how, and when each device can access network resources based on the available context. However, in this age of smarter and smarter mobile devices, sometimes additional control is required to ensure security policy enforcement, application and software installation and updates, and licensing can be controlled centrally. In these situations, an agent or profile based MDM solution is required.



Agent or Profile-based Mobile Device Management allows an administrator to tightly control devices on the network by enforcing security parameters such as requiring a passcode on the device, remotely wiping the device in the event of misuse or mishandling, controlling app and software installation and updates, and distributing configuration information. The most common issue with profile-based mobile device management solutions is simply getting the profile installed on the device itself and then ensuring an enterprising user doesn't simply uninstall it once it is there. The Aerohive and Airwatch solution solves this dilemma for administrators who want to use a profile-based MDM solution for managing mobile devices.

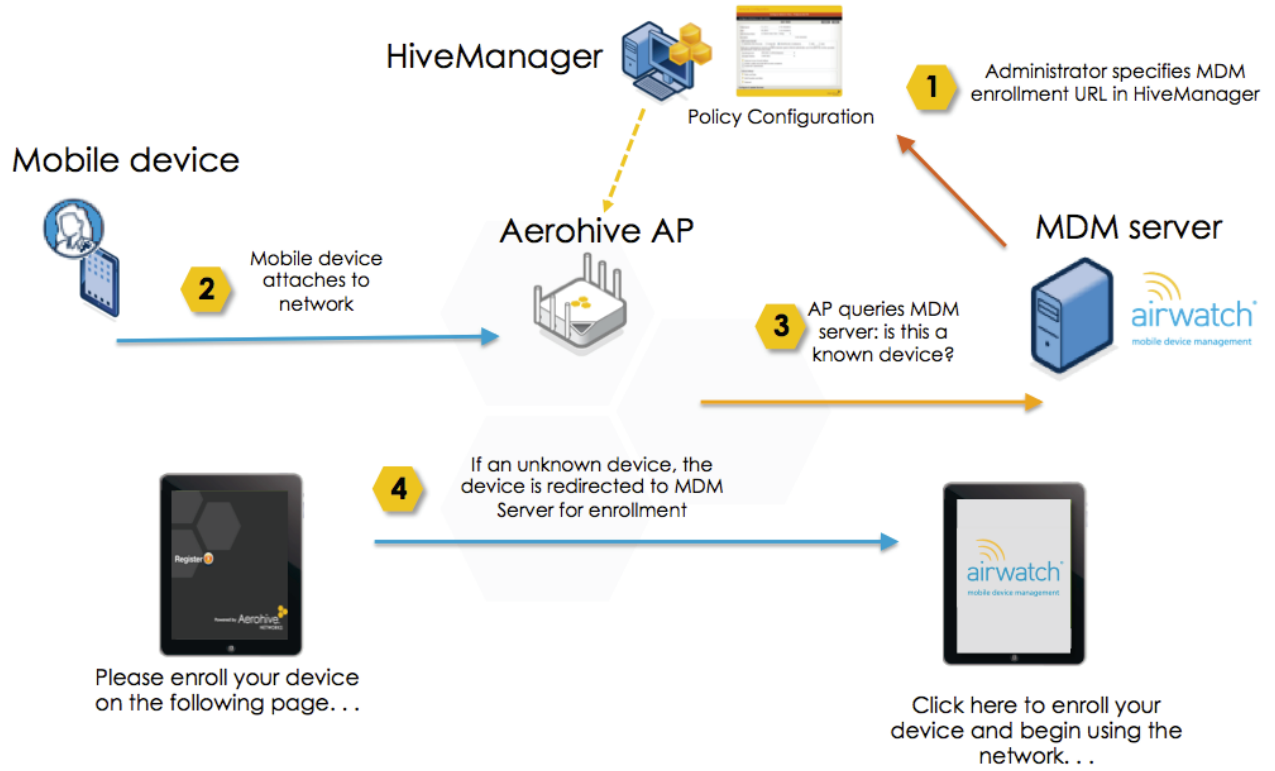
The Aerohive and Airwatch Solution

Aerohive's Cooperative Control networking infrastructure equipment along with Airwatch provides a comprehensive and robust solution for managing smart mobile devices. Together the solution provides many benefits, including:

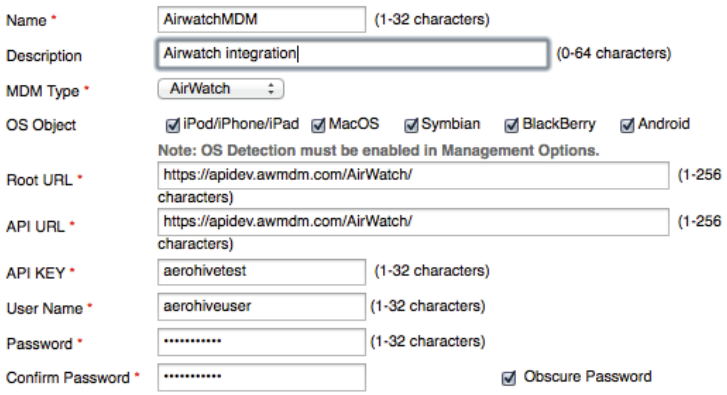
- **Automated Enrollment and Re-Enrollment** – New or unmanaged devices joining the network are automatically redirected to the Airwatch server to enroll and acquire the MDM agent profile. No network access is available unless the profile is installed, and if the profile is uninstalled for any reason, network access is again revoked until the profile is re-installed. This takes the guesswork out of initial enrollment for connected devices as well as ensures devices connected to the network remain under management.
- **Robust Multi-Vendor Support –** Enterprise-class control for deploying, securing, and monitoring Android, Apple iOS, Mac OS X, Blackberry, Symbian, Windows Mobile and Windows Phone devices.
- **App Distribution/Updates –** Full support for managing internal, public, and purchased apps across devices in the organization. Integrated with a comprehensive Enterprise App Catalog to distribute, track, update, and secure applications over the air, including integration with the Volume Purchase Program.
- **Configuration Profiles –** Streamlined asset management across corporate, employee-owned, and shared devices with automated profile distribution by user roles, groups, or device type, including configuration for corporate policies, settings, certificates, email, and VPN access.
- **Integrated Compliance Checking –** Administrators can configure compliance requirements for connected devices, including options like passcode policies, whitelist or blacklist applications, and content requirements. If any of the devices fail to meet the requirements, Aerohive can notify the user to correct the problem and use the context-based enforcement built into HiveOS to quarantine the device until the problem is corrected.
- **Comprehensive Monitoring and Reporting** – Data and usage tracking based on contextual information with pre-defined thresholds, customized alerts, and remote diagnostics. Detailed reports provide usage data over time, top users by SSID, client device information, and many other perspectives that can filtered based on connection type, identity, and network information to provide a single pane of glass view into mobile device usage.
- **Network-Based Mobile Device Management –** If the connected devices are not corporate or school-issued or if they are not Apple devices, an administrator still has the ability to implement network access controls based on identity, device type, connecting location, application, and time of day. These controls are independent of the MDM profile and require no acceptance or installation of any software on the end-user device, but rather rely on the intelligence of the infrastructure to enforce permissions to network resources.

How It Works

The Aerohive and Airwatch solution is supported from HiveOS/HiveManager version 6.0r1. The administrator simply specifies the configuration parameters for the Aerohive devices to enable Airwatch integration, and then whenever a new device joins the network, the Airwatch server is queried to determine if the device is known and whether the agent profile is currently installed on that device. If the Airwatch server reports that the device is unknown or the agent profile is currently not installed, the device is immediately redirected to the enrollment page and is required to download the profile before gaining access to the network.

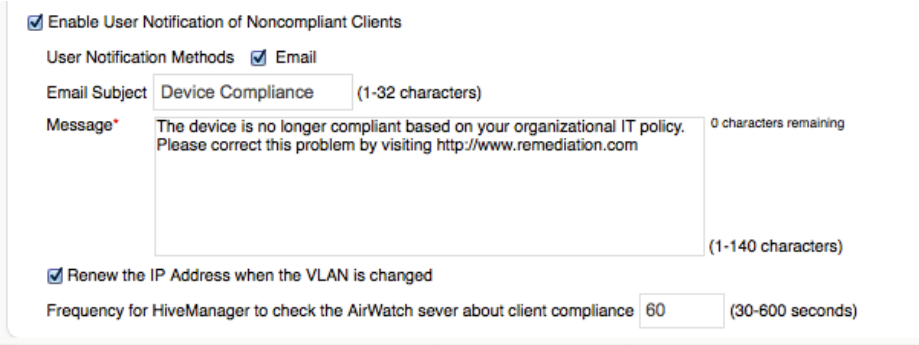


Configuring forced and reinforced MDM enrollment on the Aerohive access points and routers is a simple process that only requires specifying the enrollment and API URLs and then adding the API key, all of which can be found within the Airwatch management interface. This feature can be enabled per-SSID, so the administrator can determine which mobile devices are forced to enroll to get the Airwatch agent profiles.

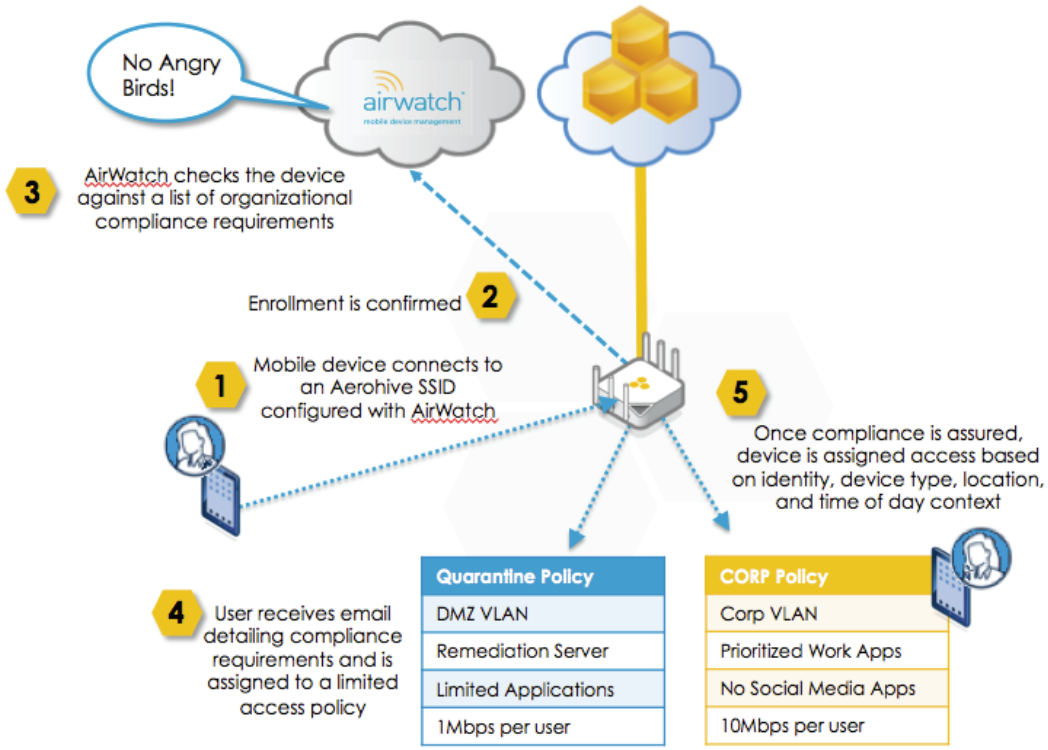


Integrated Compliance Checking with Network Access Control

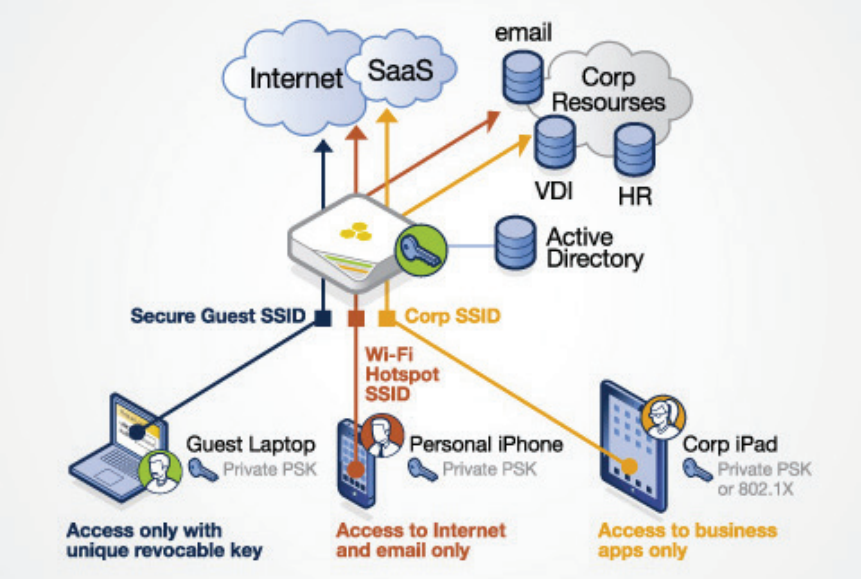
In addition, the Aerohive and AirWatch solution tightly couples network control with device control by combining device requirements with network access privileges. The administrator can specify an organizational compliance policy for options like passcode change requirements, blacklisted applications, or operating system updates, and then assign customized VLAN, firewall, and application permissions based on the compliance status of the device. An administrator can also configure email notifications to notify the user account defined for the client device in the AirWatch dashboard.



For example, if a user joins the wireless network for the first time, the device will be redirected to install the AirWatch profile before he/she can go any further, as shown above in How It Works. Then this additional functionality checks the posture of the device against an organizational compliance policy that may restrict installing a certain application. If the user has that application installed on the device, the device will be quarantined on a limited-access network until the application is uninstalled. Once the user remediates the device and is in compliance with the organization policy, full network access will be granted to the device.



In addition, devices that do not require or do not support the AirWatch profile can still be easily managed using Aerohive's Network-based MDM functionality. Policies can be configured to assign VLAN, firewall, QoS, application permissions, time-of-day schedule, and tunneling permissions based on the detected context of the device, including identity, device type, and location. Device type can be determined using DHCP option 55 or the HTTP user agent, or both, to ensure all devices are properly identified and permissions are granted. This feature can also be configured on a separate SSID to enable all guest devices limited access based on identity, device, location, application, and time.



Summary

Enforcing security on mobile devices connected to the network is absolutely necessary to ensuring a successful enterprise Wi-Fi deployment. Regardless of whether the devices are corporate-issued or BYO, permissions must be enforced based on context. By combining two best-of-breed solutions to embrace and control consumer devices issued by the enterprise or brought in by users, Aerohive Networks and Airwatch have given administrators an easy and comprehensive solution to deploy, configure, monitor, and control the mobile device explosion in the enterprise.

About Aerohive

Aerohive (NYSE: HIVE) unleashes the power of enterprise mobility. Aerohive's proven technology enables organizations of all sizes to use mobility to increase productivity, engage customers, and grow their business. Deployed in over 13,000 enterprises worldwide, Aerohive's proprietary mobility platform takes advantage of the cloud and a distributed architecture to deliver unified, intelligent, simplified 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.

About Airwatch

AirWatch was founded in 2003 with the belief that mobile technology would completely revolutionize the way companies do business. Their mission is to develop solutions that empower companies to focus on innovative uses of mobile technology rather than the complexities of managing mobility. Based in Atlanta with offices worldwide, AirWatch provides enterprise mobility solutions to thousands of companies worldwide. AirWatch is continually recognized for their innovation in mobility by top analyst firms. Gartner recently named AirWatch a Leader in the 2012 Magic Quadrant for Mobile Device Management Software.

Aerohive NETWORKS