Aerohive and JAMF Software

Simplified & Powerful Management & Enrollment for Apple Platforms

Partner Solution Brief

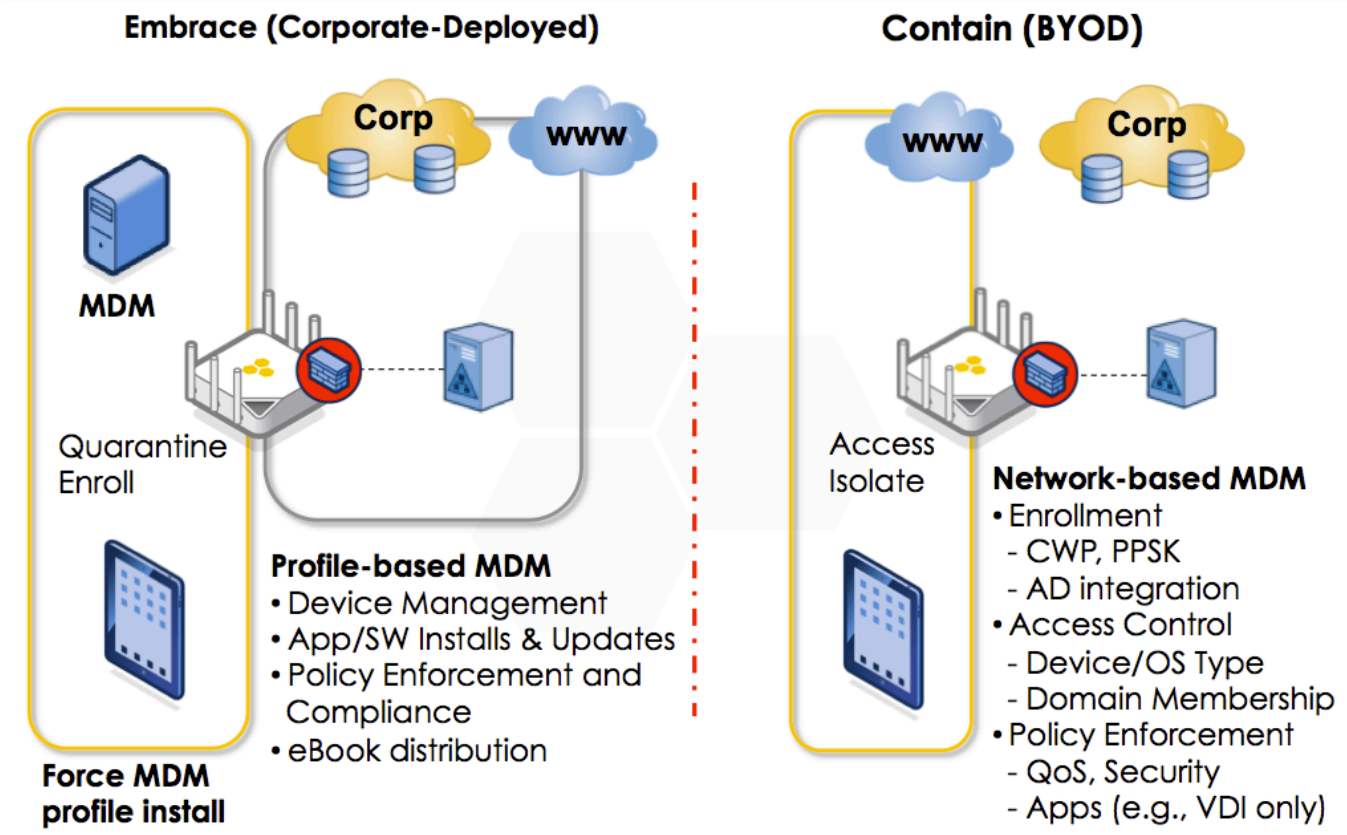
Introduction

The Aerohive and JAMF Software Solution

Aerohive Cooperative Control Wi-Fi along with JAMF Software Casper Suite provides a simple, robust, and comprehensive mobile device connectivity and management solution for Apple devices. By combining best-of-breed solutions, Aerohive and JAMF Software allow administrators to increase efficiency and productivity when managing mobile devices in schools and enterprises by enabling control and containment of mobile devices, forced enrollment and re-enrollment for mobile device profiles, inventory management, app and eBook distribution, and security policy enforcement.

One of the major problems facing IT administrators in this highly mobile age is how to enforce security and access controls on the myriad of devices that may be connected to the corporate network. There are basically two main options when it comes to controlling and containing mobile devices – an agent/profile-based solution or using intelligent network infrastructure to enforce permissions to resources based on identity, device type, location and time. In order to be truly successful in corralling the iEverything explosion, the ideal infrastructure solution will support both.

Using network infrastructure to enforce mobile device management, otherwise known as Network MDM, is an absolutely essential feature for any networking vendor. Aerohive uses the highly-intelligent cooperative control capabilities built into HiveOS to enforce network permissions based on identity, device type, location, application, and time. This allows administrators to control what, how, and when the device can access network resources, but does not extend to controlling access on the device itself. In order to support functionality such as security policy enforcement, app and software installation/updates, and licenses, a 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 JAMF Software Casper Suite integration solves this dilemma for administrators who want to use a profile-based MDM solution for managing Apple devices.

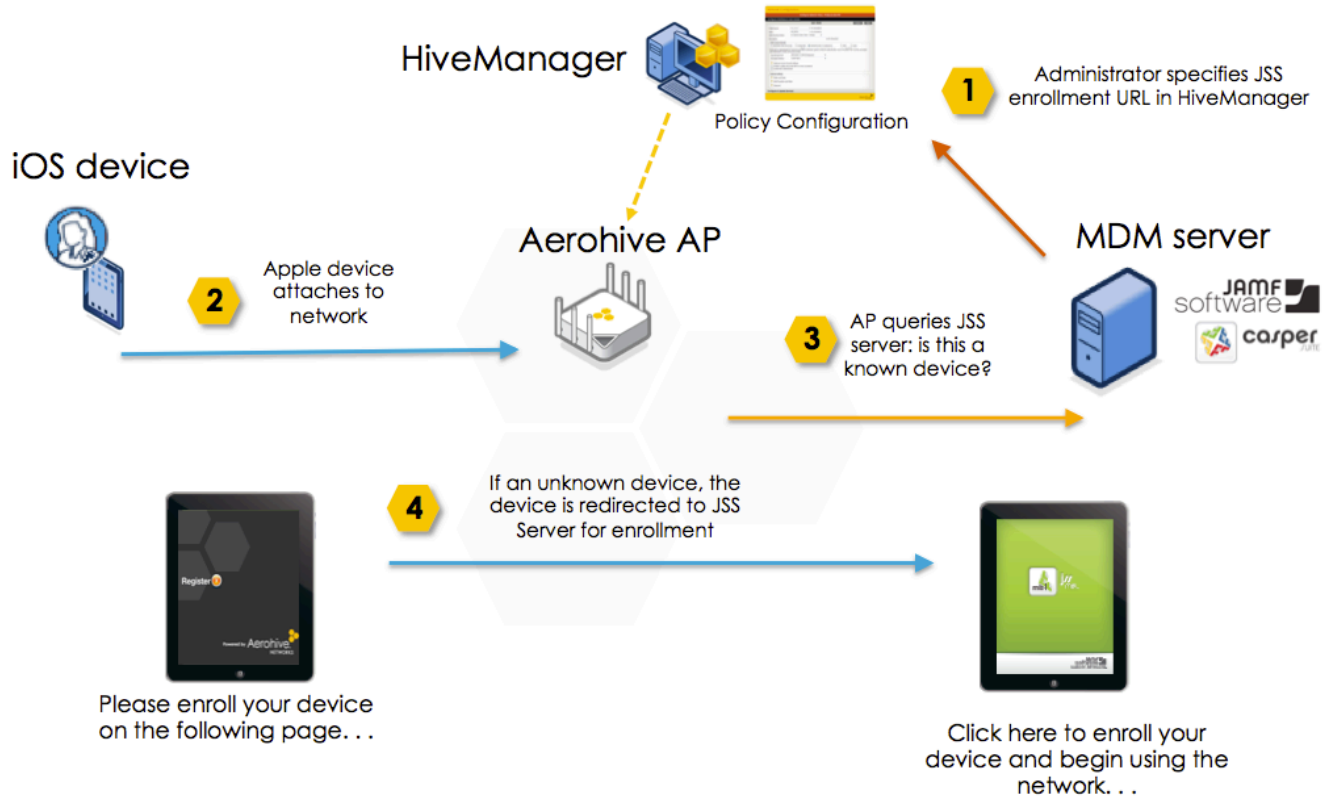
The Aerohive and JAMF Software Solution

Aerohive's Cooperative Control networking infrastructure equipment along with the JAMF Software Casper Suite provides a robust and comprehensive solution for managing Apple devices. Together the solution provides many benefits, including:

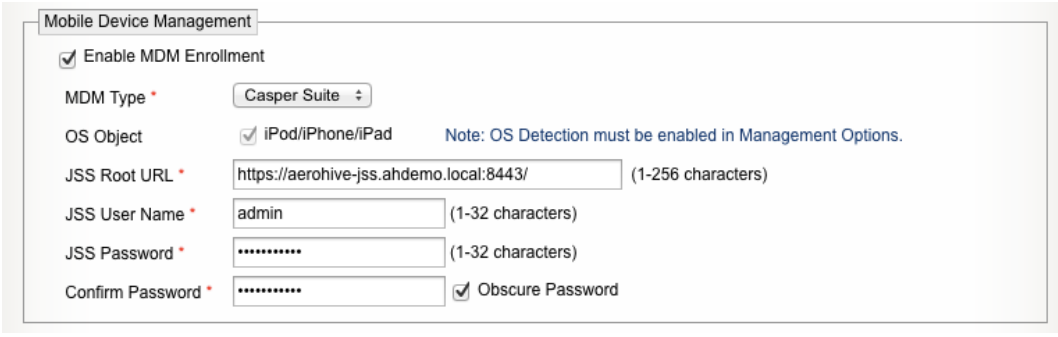
- **Automated Enrollment and Re-Enrollment** – New or unmanaged Apple devices joining the network are automatically redirected to the JAMF Software Server (JSS) to enroll and acquire the MDM profile. No network access is available unless the profile is installed, and if the profile is uninstalled for any reason, network access is again revoked until the profile is re-installed. This takes the guesswork out of initial enrollment for Apple devices as well as ensures devices connected to the network remain under management.
- **App and eBook Distribution/Updates –** Full support for deploying, updating, and configuring App store apps and privately-distributed apps, as well as uploading, distributing, managing, and tracking Volume Purchase Program (VPP) codes**.** In addition, administrators can deploy, manage, and update iBookstore, in-house, and public-domain books in iBook, ePub, and PDF file formats.
- **Configuration and Security Profiles –** Administrators can configure the entire range of configuration profile settings available on iOS devices, build new configuration profiles, or upload configuration profiles previously created with the iPhone Configuration Utility. Administrators also have the ability to require that users enable security passcodes on their devices, configure a wide range of settings and policies, and configure account access through integration with LDAP. They can even require that users enable data encryption on their devices, and in the event that a device is lost or stolen, have the ability to quickly lock or wipe the device remotely.
- **Inventory and License Management** – Management capabilities include the ability to gather a full inventory of device information, installed apps, and settings. Administrators can easily reference purchasing and warranty information from Apple's Global Service Exchange (GSX) database and populate user information with LDAP. Devices check in regularly (every 24 hours by default) to provide inventory information, which can be utilized in a variety of ways for configuration and compliance.
- **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 JAMF Software solution is integrated into HiveOS and HiveManager 5.1. The administrator simply specifies the configuration parameters for the Aerohive devices to enable JSS integration, and then whenever a new iOS (or in the next release, Mac OS X) device joins the network, the JSS server is queried to determine if the device is known and whether the profile is currently installed on that device. If the JSS server reports that the device is unknown or the profile is currently not installed, the device is immediately redirected to the JSS MDM Profile enrollment page and is required to download the profile before gaining access to the network.

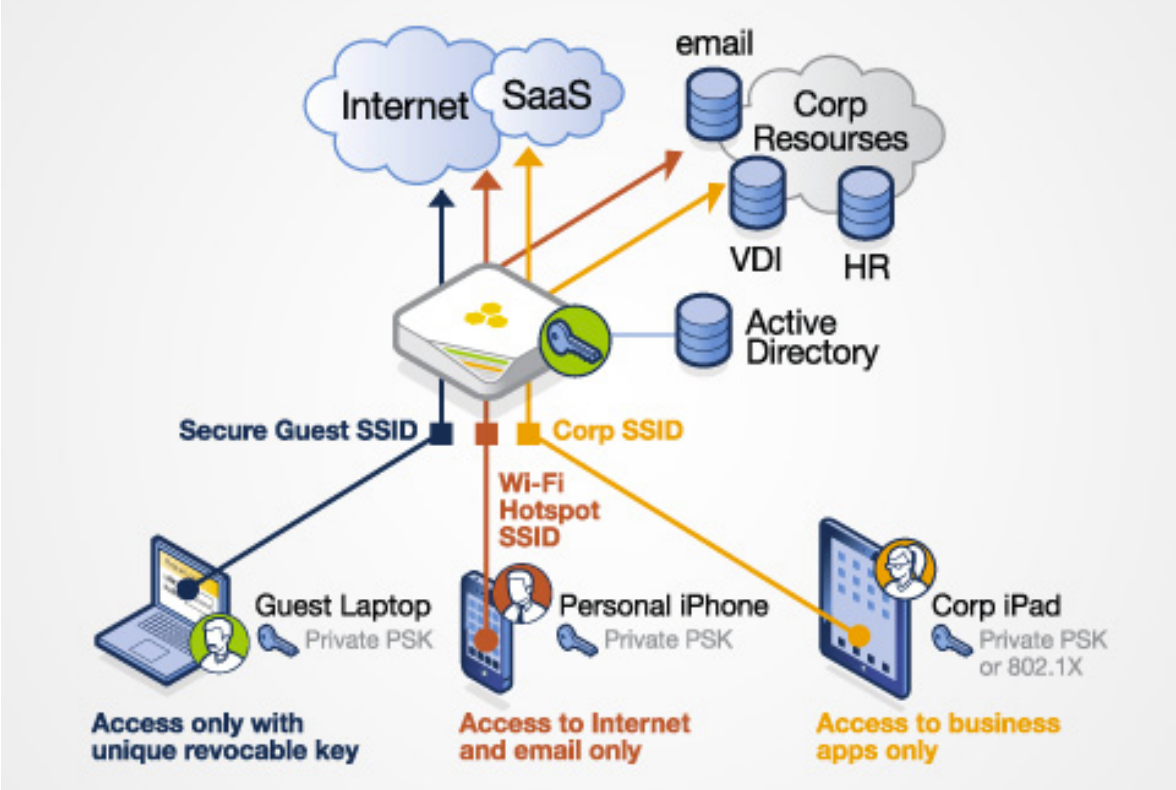


Configuring forced and reinforced MDM enrollment on the Aerohive access points and routers is as easy as checking the box to enable the service and specifying the JAMF Software Server (JSS) enrollment URL. This feature can be enabled per-SSID, so the administrator can determine which iOS and OS X devices are forced to enroll to get a JSS profile.



If the connected device is not an Apple device, the administrator can specify additional parameters for containing access for that device using Aerohive Network-based MDM. This functionality allows an

administrator to configure customized network, firewall, QoS, time-of-day schedule, and tunneling policies based on the identity of the user and the device type. 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 (even Apple 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 identity, device type, location, and time. 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 JAMF Software have given administrators an easy and comprehensive solution to deploy, configure, monitor, and control Apple and other mobile devices in the enterprise.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

About JAMF Software

By listening to colleagues, customers and thought leaders in the industry, JAMF Software has grown into the world leader in Mac OS X and iOS management. JAMF Software continues to develop software made to support Macs and iOS devices in an enterprise environment. From their offices in Minneapolis, Minnesota and Eau Claire, Wisconsin, JAMF Software builds innovative solutions and has assembled a support and services team dedicated to helping customers manage Macs and iOS devices.

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

International Headquarters
Aerohive Networks Europe LTD
The Court Yard
16-18 West Street
Farnham, Surrey, UK, GU9 7DR
+ 44 (0) 1252 736590
Fax: + 44 (0) 1252 711901