VMware Patient Engagement Design Guide for Healthcare

WHITE PAPER

vmware® airwatch® | GROUND CONTROL™

Table of Contents

About Design Guides

VMware design guides are created through architectural design development and review by subject matter experts. The guides provide overviews of solution architectures and implementations. As a reference asset, each document illustrates a design framework to support proof-of-concept, pilot, and full implementations.

Design guides incorporate generally available products into the design and employ repeatable processes for the deployment, operation, and management of components within the solution.

Design guides ensure the viability of logical designs or concepts in real-world practices. This document complements product specifications and installation guidelines published for each product. All detailed technical and functional product-level questions should be referred to appropriate product documentation.

Introduction

This guide provides an overview of the Patient Engagement solution using VMware AirWatch® and GroundControl, its logical architecture, and validation of the capabilities by VMware experts. Based on products from VMware, GroundControl, Apple, and Bretford, this architecture represents the foundation on which customers and partners can build comprehensive healthcare solutions providing a rewarding, personalized patient experience, ensuring the security of personal information, and requiring the absolute minimum attention from nursing staff.

This document will be updated as newer capabilities are incorporated in the AirWatch and GroundControl solution.

Audience

This document is for enterprise architects, solution architects, sales engineers, field consultants, advanced services specialists, and customers who plan to design, configure, and deploy an iOS-based patient engagement solution.

Business Case

Simply put, *Patient Engagement* is healthcare providers and patients working together to improve outcomes. The more a patient is engaged in their healthcare decision-making process, the healthier that patient becomes. Patient Engagement provides patients with tools that involve them in the process of their own treatment and care, including diagnosis, information gathering, education, and even personal entertainment while staying at a healthcare facility. Evidence is growing that shows these programs dramatically improve outcomes in patients across all types of treatment.

Providers are leveraging digital tools as the tip of the spear in this effort—predominantly through Apple iPads. While this might seem easy at first glance, the challenge in delivering a solution is complicated by the need to adhere to strict privacy rules to manage Electronic Protected Health Information (ePHI) as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and similar privacy regulations worldwide.

A common solution is to attempt to "lock down" patient iPads to keep ePHI off the devices. In many cases, healthcare institutions discover that lock down is often too restrictive for patients, as it places limits on the device usability and capabilities. In addition, the lock down approach can prove difficult to maintain, with devices subject to changes to apps, operating systems, and other requirements that can impact device availability.

Fortunately, the joint solution offered by GroundControl and VMware AirWatch offers a powerful alternative that meets patient desire for expanded device and application usability while protecting ePHI. The joint solution, outlined in this document, takes a different approach: iPads are set up with *minimal restrictions*, allowing relatively open access by patients who are free to do (nearly) whatever they will with the devices. On patient discharge, iPads are easily and quickly reset to "factory condition"—removing all ePHI—then automatically reprovisioned with no burden on staff.

This AirWatch and GroundControl solution is not only a better experience for patients, it is actually safer for ePHI, because the device is electronically wiped clean after every patient. Additionally, the software solution scales to meet potential Patient Engagement demand in the largest hospital infrastructures, multiple campuses, buildings, and units, each requiring variations and compliance rules.

What Is GroundControl?

GroundContol is a software platform that manages iOS device setup, configuration, and supervision. The solution offers critical capabilities in key areas:

- Tethered management for complete control
- Cloud administration for enterprise security and scale

Tethered Management for Complete Control

Perhaps unintuitively, GroundControl manages Apple mobile devices over USB, not over the air. Tethered USB management is critical because mobile devices have no wireless capabilities when factory reset. There are only two ways to get these devices online: tap on the screen, or use USB. Because hospitals do not want to add additional burdens to their nursing and clinical staff, USB is strongly preferred. The reduction in time, labor, and errors is particularly great with Patient Engagement, since each device may require re-provisioning several times a day.

GroundControl allows for several key tasks—traditionally performed by tapping on the screen—to be completely automated:

- Factory reset, wiping all known and unknown ePHI
- Initial Wi-Fi provisioning, even to a certificate-based WPA2 Enterprise network
- Apple device supervision, unlocking critical MDM restrictions
- Touch-free, agentless AirWatch enrollment, including APIs to set AirWatch organization group and tags

A single GroundControl "Launchpad" station can provision dozens of Apple iPads at once, using an appropriate USB charge/sync cart like those manufactured by Bretford.

Cloud Administration for Enterprise Security and Scale

Like AirWatch, GroundControl is centrally managed by a Web browser. Designated administrators have a single place to set up device images and automation rules. Once configured, all endpoints have access to the same assets and adhere to the same rules. All work done on devices—in fact all changes to any aspect of the system—is centrally and securely logged for auditing. GroundControl is commonly set up for single sign-on (SSO) to your existing Active Directory system, allowing you to maintain control over your users, administrators, and permissions.

Critically, the GroundControl cloud never comes into contact with private data and GroundControl cannot pull ePHI *from* devices.

What Is VMware AirWatch?

VMware AirWatch simplifies mobility for healthcare organizations, while empowering end users—whether the end user is a patient or a clinician. AirWatch is a comprehensive enterprise mobility platform built to manage any endpoint including smartphones, tablets, laptops, rugged, printers, wearables, and IoT devices across all major operating systems in a single management console throughout the device lifecycle. With a multi-layered security approach across the user, endpoint, app, data, and network, AirWatch provides complete protection of corporate data and intelligent access controls, compliance monitoring, and threat detection. The AirWatch apps suite enables mobile productivity and collaboration with consumer-simple and integrated business apps that unlock mobile micro-moments and drive digital transformation.

Patient Engagement Software and Hardware Stack

The following functions and associated products are incorporated in the Patient Engagement design guide.

COMPONENT	VENDOR	DETAILS
GroundControl Management Cloud, Enterprise Edition	GroundControl Solutions	Web management console
GroundControl Launchpads	GroundControl Solutions	Software running on Windows PCs or Macintosh
VMware AirWatch	VMware	Enterprise Mobility Management
iPad or iPad Pro	Apple	
Device Enrollment Program	Apple	Optional for additional security (**Note:** GroundControl automates DEP enrollment and fully supports DEP as a customer option for iOS devices.)
iTunes Volume Purchase Program	Apple	Third-party app licensing and distribution
Charging/Syncing Carts	Bretford	High-quality components are critical.

Table 1: Patient Engagement Software and Hardware Stack

Patient Engagement Architecture and Topology

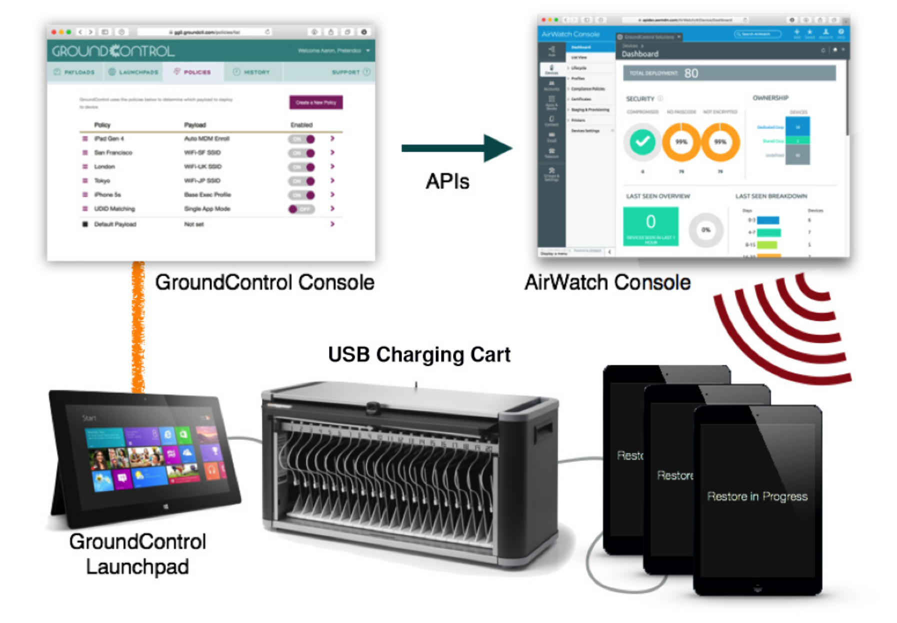
The following section describes the solution design, illustrated in two perspectives:

- **Functional stack** – Shows functional layers in a typical implementation as well as interconnections between layers in terms of dependencies.
- **Component-level architecture** – Shows products required within the layers identified in the logical stack.

Functional Stack

Figure 1 shows the shows the functional relationships among the components of the solutions.

The iPads are plugged into the USB charging cart. A Mac or Windows PC is attached as the host for the cart. The GroundControl Launchpad software running on the Mac or Windows machine detects the newly connected devices, and informs the GroundControl Console, running in the cloud. The console evaluates the devices against predefined rules, and if appropriate, initiates a deployment to the devices. That deployment will typically factory-erase the device then re-apply apps and configurations. The Launchpad has already cached any required apps and configurations, and operating systems, requiring very little bandwidth to perform the deployment. As the deployment ends, the GroundControl console sends commands to the AirWatch server via the AirWatch API. AirWatch then takes over management of the devices, via Wi-Fi, applying additional policies and compliance rules.



Policy	Payload	Enabled
iPad Gen 4	Auto MDM Enroll	ON
San Francisco	WiFi-SF SSID	ON
London	WiFi-UK SSID	ON
Tokyo	WiFi-JP SSID	ON
iPhone 5s	Base Exec Profile	ON
UDID Matching	Single App Mode	OFF
Default Payload	Not set	

Figure 1: Functional Stack

Component-Level Architecture

Figure 2 details the products required in the logical stack layers.

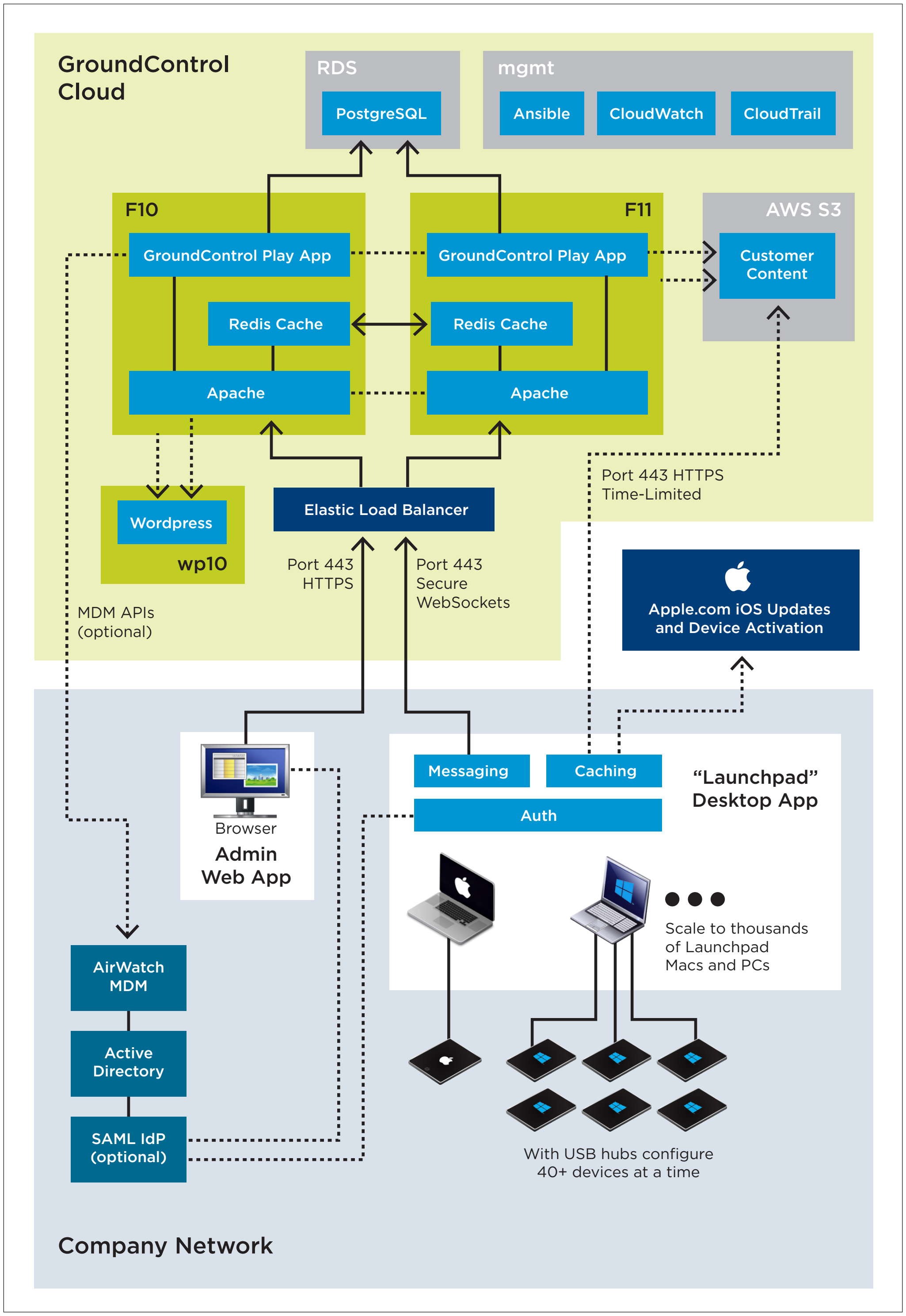


Figure 2: Component-Level Architecture

GroundControl is typically deployed with hooks into existing corporate systems. Specifically, GroundControl integrates deeply into the VMware AirWatch EMM solution, providing robust device management without redundant administration. In addition, GroundControl is often connected to an organization's Active Directory infrastructure via SAML 2.0. This allows GroundControl to leverage single sign-on (SSO), making role-based user administration simple.

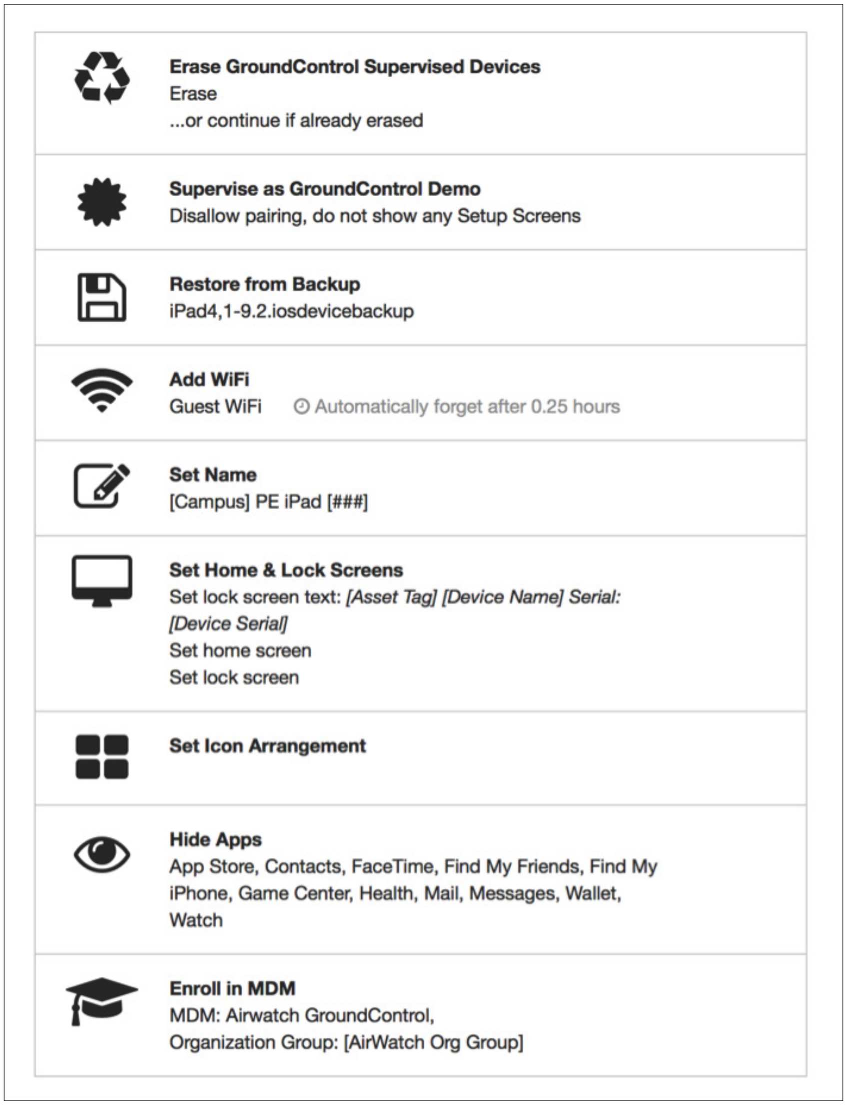
The GroundControl Cloud management system has been architected to ensure robust security and high availability. All inbound and egress traffic is monitored and filtered against expected patterns. All data is encrypted, whether in transit or at rest. All assets are checked against known hashes during each device deployment to prevent tampering.

GroundControl Setup and Best Practices for Patient Engagement

This section outlines the setup and best practices of the Patient Engagement solution.

Setup

A typical Patient Engagement image is set up in GroundControl with a single image, and a single automation rule.



Erase GroundControl Supervised Devices
Erase
...or continue if already erased

Supervise as GroundControl Demo
Disallow pairing, do not show any Setup Screens

Restore from Backup
iPad4,1-9.2.iosdevicebackup

Add WiFi
Guest WiFi Automatically forget after 0.25 hours

Set Name
[Campus] PE iPad [###]

Set Home & Lock Screens
Set lock screen text: *[Asset Tag] [Device Name] Serial: [Device Serial]*
Set home screen
Set lock screen

Set Icon Arrangement

Hide Apps
App Store, Contacts, FaceTime, Find My Friends, Find My iPhone, Game Center, Health, Mail, Messages, Wallet, Watch

Enroll in MDM
MDM: Airwatch GroundControl,
Organization Group: [AirWatch Org Group]

Figure 3: GroundControl Image

The GroundControl image shown in Figure 3 is typical. This image shows the actions GroundControl will perform on an iPad when it is plugged into a PC running the Launchpad app.

1. On connect, GroundControl will use AirWatch APIs to delete the device from the AirWatch system, clearing the way for a clean re-enrollment later.
2. GroundControl erases the device to factory defaults (the same as “Erase all content and settings”).
3. GroundControl will supervise the device, placing it in “enterprise mode,” allowing AirWatch to place additional restrictions later on. Supervision also prevents the device from connecting with any other hosts, such as a rogue laptop or Workstation on Wheels.
4. GroundControl will restore a master image to restore app settings and system settings such as Bluetooth.
5. GroundControl connects the device to the Guest Wi-Fi network, but sets a 15-minute timeout. During those 15 minutes, the device will connect to AirWatch and receive the certificate required to connect to the hospital’s enterprise Wi-Fi network.
6. GroundControl sets the device name to include the campus name and a unique three-digit sequential number.
7. GroundControl sets the device home and lock screens. This can alternatively be done by AirWatch. But GroundControl also will burn-in unique identifying text on the lock screen, including device name, asset tag, and serial number.
8. GroundControl will arrange the apps on the home screen into multiple folders and pages, as needed.
9. GroundControl will hide specified built-in apps that are not appropriate for Patient Engagement, such as Mail, FaceTime, and others.
10. GroundControl will enroll the iPad into AirWatch MDM for ongoing, over-the-air management. GroundControl will also use AirWatch API calls to move the device into a specific AirWatch organization group, which can be unique per device. These organization groups determine which apps and restrictions are sent to the device, allowing for differences between children and adults, and other specific groups.

This list is just a sample, as GroundControl can also perform actions such as iOS updates, setting time zone, setting device language, and API calls to additional systems.

Patient Engagement Best Practices

Our experience with many healthcare providers has produced an evolving list of best practices. We list several here.

Set up the AirWatch API Within GroundControl

GroundControl can perform either basic or advanced integration with AirWatch. With basic integration, GroundControl can enroll your devices to a common staging group, touch-free. Advanced API integration includes three additional features:

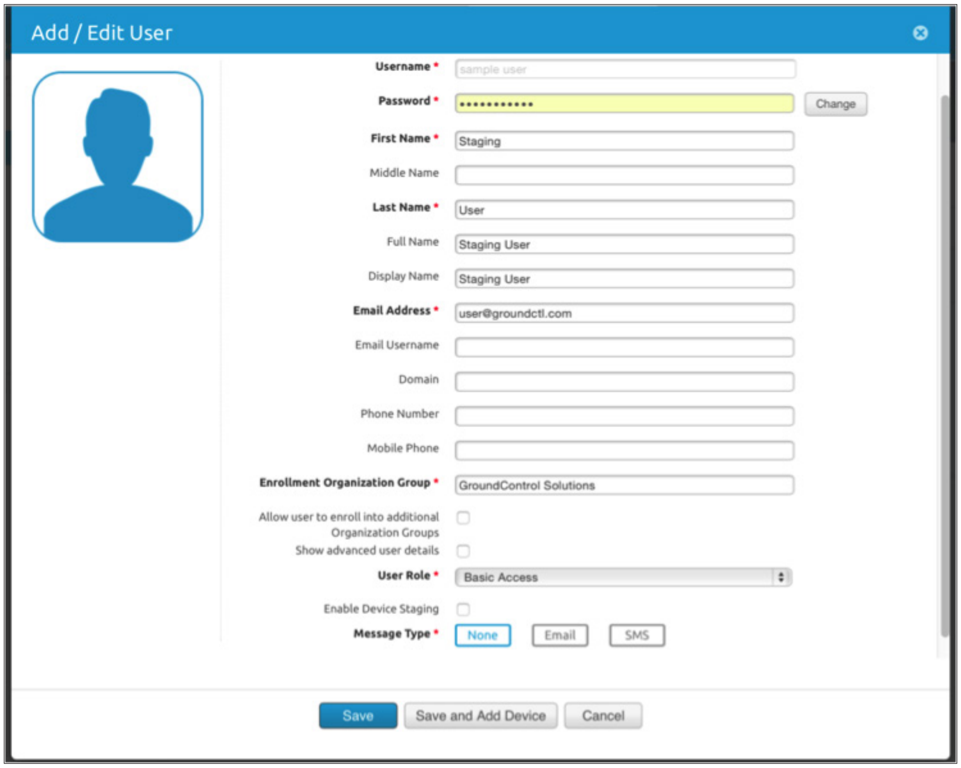
- Unenrolling before deployment, to make sure AirWatch sees devices as “new”
- Assigning devices to a specified user
- Moving devices into the correct organization group, post-deployment

Basic Integration

To enroll devices with basic integration, obtain an enrollment configuration profile.

1. Navigate to your organization group – Basic integration will enroll devices into this group. If you are going to use API integration to personalize an organization group, we recommend using your top-level "global" group.

2. Create a staging user – AirWatch requires that every device is associated with a user. You will need to create a user (not administrator) to associate devices. Create this user in your staging organization group. You only need to enter the required fields, as shown below:



Add / Edit User

Username *	sample user
Password *	●●●●●●●●●●●
First Name *	Staging
Middle Name	
Last Name *	User
Full Name	Staging User
Display Name	Staging User
Email Address *	user@groundctl.com
Email Username	
Domain	
Phone Number	
Mobile Phone	
Enrollment Organization Group *	GroundControl Solutions
Allow user to enroll into additional Organization Groups	□
Show advanced user details	□
User Role *	Basic Access
Enable Device Staging	□
Message Type *	[✓ None] Email SMS

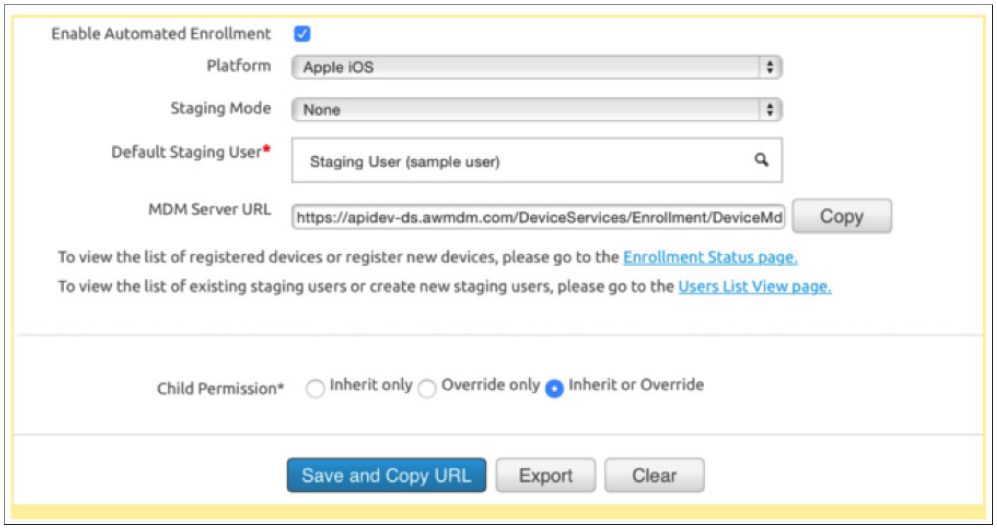
If you are sharing devices, then this configuration is sufficient. All devices will belong to the same staging user.

3. Click **Save** (do not add a device).

4. Download the enrollment configuration profile – The section to download the enrollment configuration profile is buried deep within Settings. Go to **Groups & Settings** > **All Settings**. Then, click **Devices & Users** > **Apple** > **Apple Configurator**.

5. Ensure the correct staging organization group is selected at the top of the screen.

6. At the bottom of the screen, check the box **Enable Automated Enrollment**.



Enable Automated Enrollment ☑

Platform: Apple iOS

Staging Mode: None

Default Staging User*: Staging User (sample user)

MDM Server URL: https://apidev-ds.awmdm.com/DeviceServices/Enrollment/DeviceMd

To view the list of registered devices or register new devices, please go to the Enrollment Status page.

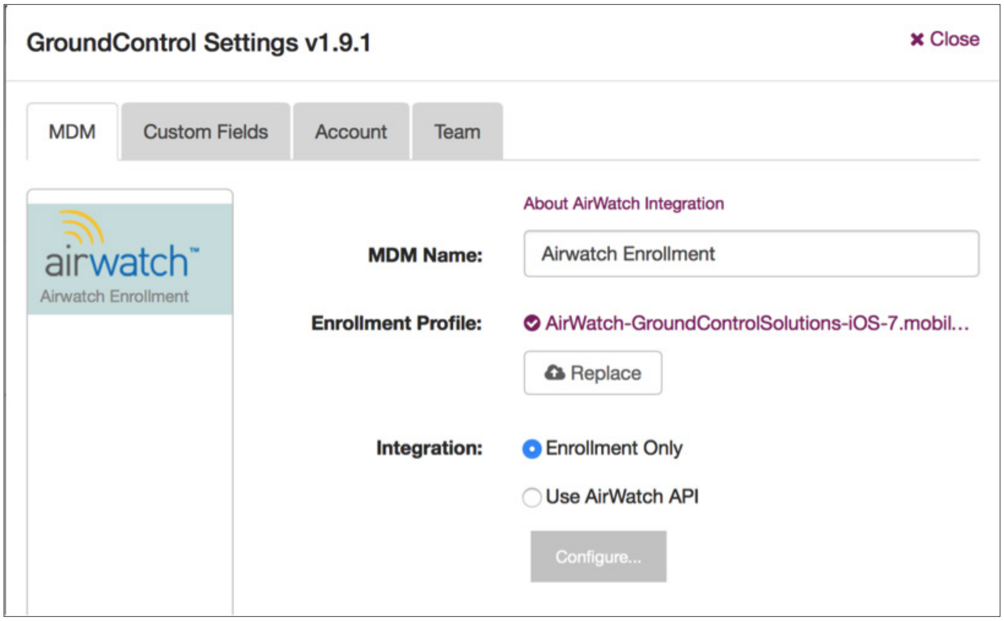
To view the list of existing staging users or create new staging users, please go to the Users List View page.

Child Permission*: ○ Inherit only ○ Override only ● Inherit or Override

7. For shared devices, Staging Mode should be **None**.

8. Click **Export** to download a configuration profile containing this enrollment information. **Note:** If you are on a Mac, your Mac will attempt to install this configuration profile. Click **Cancel** or you will enroll your Mac into AirWatch.

9. Locate the downloaded configuration profile on your Mac or PC. Go to the MDM tab of GroundControl Settings to upload this file.



GroundControl Settings v1.9.1

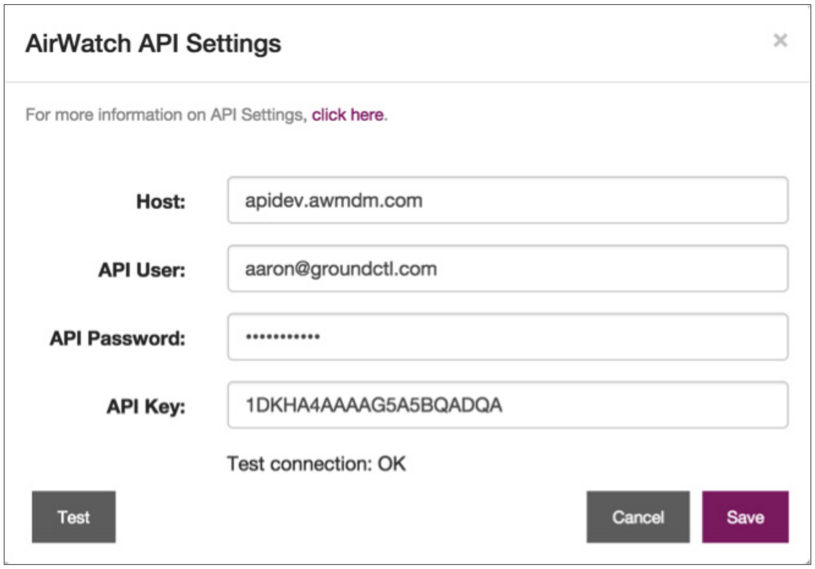
MDM Name: Airwatch Enrollment

Enrollment Profile: ✓ AirWatch-GroundControlSolutions-iOS-7.mobil...

Integration: ● Enrollment Only ○ Use AirWatch API

Advanced API Integration

To enable advanced API integration, you will need to fill in several additional fields in GroundControl:



AirWatch API Settings

For more information on API Settings, click here.

Host: apidev.awmdm.com

API User: aaron@groundctl.com

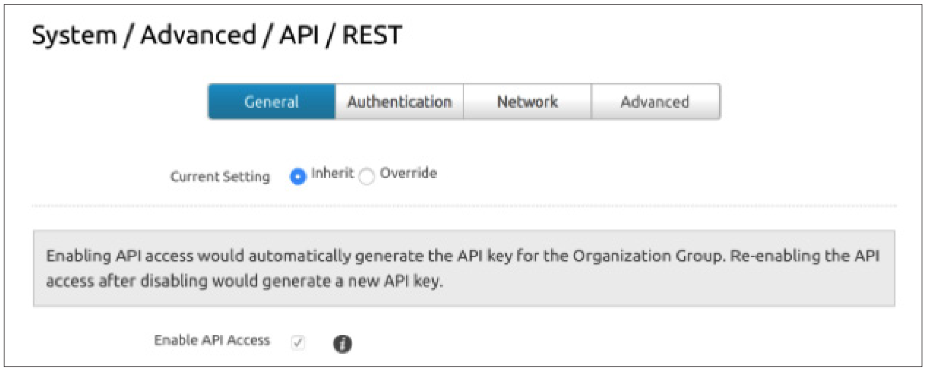
API Password: •••••••••••

API Key: 1DKHA4AAAAG5A5BQADQA

Test connection: OK

- **Host** – Enter the hostname of your AirWatch console. Do not include the `https` or trailing slash.
- **API User** and **API Password** – In your AirWatch console, navigate to **Groups & Settings** > **All Settings** > **System** > **Advanced** > **API** > **REST API** > **Authentication**. Make sure Basic authentication is enabled.
- Now you need to enable API access for one of your administrator accounts. Go to **Accounts** > **Administrators** > **List View**. You may want to create a new user for GroundControl. Fill in the required fields. In the API tab, make sure Basic authentication is enabled. Add a role of Console Administrator or above.

  In GroundControl, enter the newly created administrator username and password.
- **API Key** – In your AirWatch console, go to **Groups & Settings** > **All Settings** > **System** > **Advanced** > **API** > **REST API**.



System / Advanced / API / REST

Current Setting ● Inherit ○ Override

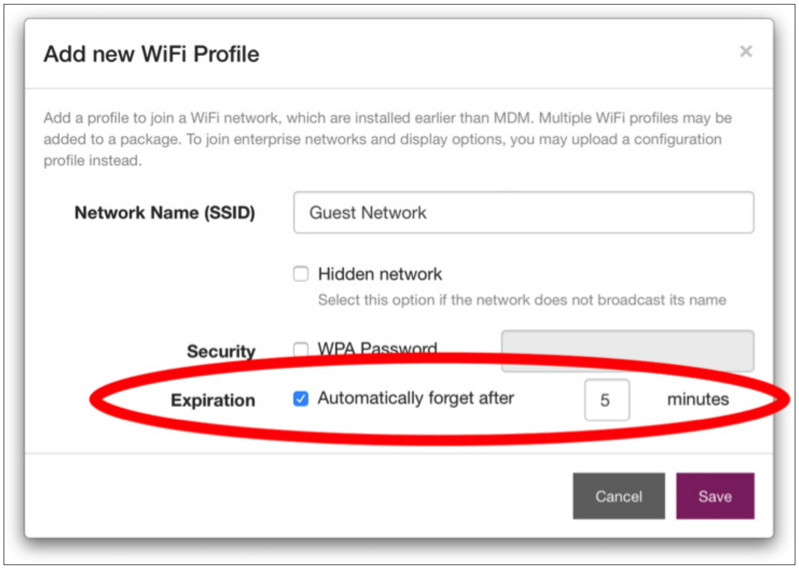
Enabling API access would automatically generate the API key for the Organization Group. Re-enabling the API access after disabling would generate a new API key.

Enable API Access ☑

  Make sure **Enable API Access** is checked. Copy the API Key and paste it into the GroundControl **API Key** field.
- **Test** – Click **Test**. GroundControl will verify the settings.

Bootstrap Devices onto Secured Wi-Fi Networks

If your Wi-Fi network has WPA2 certificate-based authentication, how can you make sure each iPad gets the correct certificate in a zero-touch enrollment? First, set up GroundControl to install a common, more open, but *expiring* Wi-Fi profile. That profile will be sufficient for the device to reach and enroll into AirWatch. Once enrolled, AirWatch can leverage a Simple Certificate Enrollment Protocol (SCEP) server to provide certificates and push the Wi-Fi profiles. Once the initial provisioning Wi-Fi profile expires, after 5 minutes for example, the iOS device automatically switches to the enterprise network with the proper credentials, forgetting the guest network.



Add new WiFi Profile

Add a profile to join a WiFi network, which are installed earlier than MDM. Multiple WiFi profiles may be added to a package. To join enterprise networks and display options, you may upload a configuration profile instead.

Network Name (SSID): Guest Network

☐ Hidden network
Select this option if the network does not broadcast its name

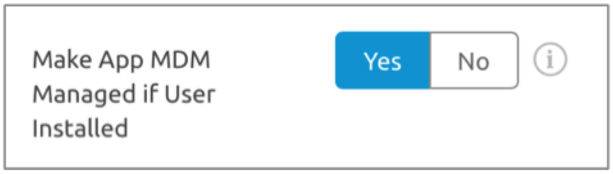
Security: ☐ WPA Password

Expiration: ☑ Automatically forget after 5 minutes

Figure 4: Set Expiration to Forget Guest Network

Side-Load Apps with GroundControl While AirWatch Manages Licenses

As a security measure, iOS devices only trust apps pushed from the App Store or from MDM. Apps installed via USB are not implicitly trusted. An option in AirWatch bridges this gap. If you select **Convert unmanaged apps to managed**, then you may side-load apps using GroundControl, and AirWatch will ask the device to trust that app. The app is then installed on the device without burdening Wi-Fi, and the app simply "works."



Make App MDM Managed if User Installed: [✓ Yes] No

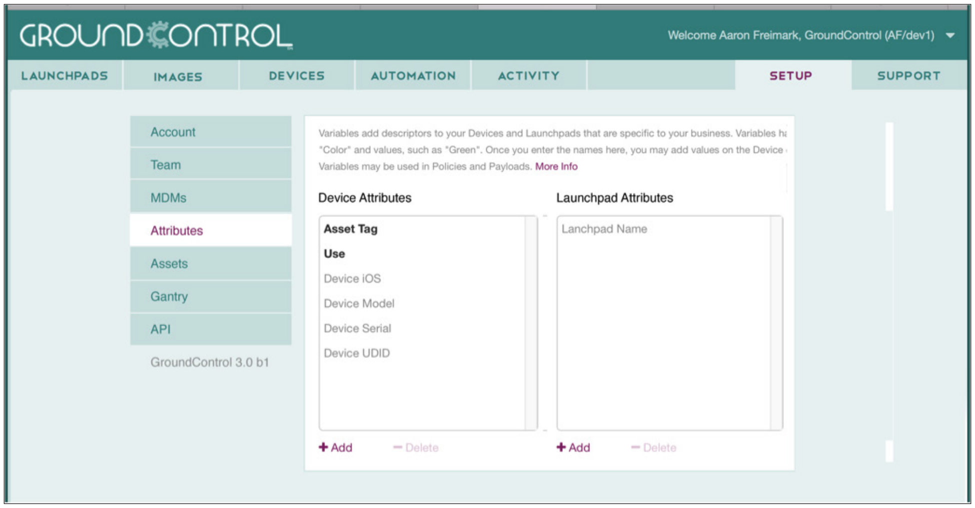
Figure 5: Side-Loading App Using Ground Control

This system currently works for enterprise (in-house) apps only.

Use Custom Attributes to Set up Multiple Device Images

By default, GroundContol will image every device in the same way. But it is easy to set up different groups of devices—or different groups of Launchpads—that push different images. The key to this differentiation is custom attributes.

Built-in Device Attributes include read-only data such as serial number, device model, and iOS version. GroundControl allows you to define as many additional attributes as you need for your workflow. For example, you may create new attributes for Use or Asset Tag.



Variables add descriptors to your Devices and Launchpads that are specific to your business. Variables h
"Color" and values, such as "Green". Once you enter the names here, you may add values on the Device
Variables may be used in Policies and Payloads. More Info

Device Attributes

- **Asset Tag**
- **Use**
- Device iOS
- Device Model
- Device Serial
- Device UDID

Launchpad Attributes

- Lanchpad Name

Figure 6: Defining Device Attributes

When you create a new Use attribute, each device may then be assigned a use such as “Patient Engagement” or “Nursing.” You may add attribute values to each device serial number in bulk with a CSV file or with the GroundControl API.

Once you have the attributes defined, you may use them in Automation rules or as variables in Images. Rules may be very simple, for example, “IF ‘USE’ IS ‘PATIENT ENGAGEMENT’…” You may also add more complex rules, to limit by device type, iOS version, and more. GroundControl evaluates Automation Rules from top to bottom, and the evaluation continues until a match is found.

In Images, you may use these attributes as variables in many fields. For example, you may include the Asset Tag you defined as text in the device lock screen. Or define an attribute to represent the AirWatch organization group, and the GroundControl API will move the device into the correct AirWatch group every time.

About VMware End-User Computing Solutions for Healthcare

VMware end-user computing solutions for healthcare help providers transform the cost, quality, and delivery of patient care. To learn more about VMware end-user computing solutions for healthcare, visit www.vmware.com/industry/healthcare/point-of-care.html.

To learn more about GroundControl healthcare solutions, visit www.groundctl.com/healthcare.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com