Empower Hospitality Teams and Transform the Guest Experience with Mobility: Best Practices

Mobility is changing every aspect of hospitality, from improving customer service to streamlining back-end operations. Incorporating mobile devices is allowing hotels, restaurants and other businesses in the hospitality industry to facilitate employee workflows and improve the guest experience with mobile point of sale, line busting and custom apps. Some are even implementing mobile payment solutions, digital menus and mobile check-in.

A mobile device management (MDM) platform such as AirWatch® by VMware® is central to the mobility strategy of many hospitality organizations. MDM provides IT administrators with a way to track assets and ensure organizations maintain compliance with industry regulations, while enabling owners and operators to streamline processes such as training, updating materials, managing workflows and ensuring guests enjoy their stays. The following whitepaper outlines best practices for mobile device implementation in a hospitality environment, from the board room to the guest room.

PCI Compliance

Mobility is ubiquitous today, and consumers rely on their mobile devices to plan every aspect of their trips and outings. They use apps to find discounts and coupons, book reservations and pull up directions. It’s likely that eventually, many consumers will rely on their mobile devices to complete transactions at hotels, restaurants and other destinations. According to Hospitality Technology, experts agree mobile wallets are the future of payment, and some hospitals are already piloting solutions to accept these payments or integrate mobile point of sale (MPOS) into existing point of sale systems.

But before hospitality organizations can embrace the payment preferences of the future, their IT departments must ensure they meet the requirements of the payment card industry (PCI) Data Security Standard, a regulation which ensures consumer data is kept secure. The standard, already widely implemented in the retail industry, includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Though PCI has not yet released formal requirements for accepting payments with consumer grade mobile devices, AirWatch partners with leading sled hardware providers to ensure all mobile transactions are secure and meet PCI’s most recent recommendations.

In May 2012, the PCI council released an “At a Glance” document called “Accepting Mobile Payments with a smartphone or tablet.” It is likely that the guidelines within this document lay the framework for future requirements. AirWatch recommends taking the following preliminary steps to secure mobile devices used in a hospitality setting and be prepared to meet mobile-specific PCI compliance requirements.
Prevent Rooting and Jailbreaking

AirWatch® Mobile Device Management enables devices used as mPOS systems to be monitored remotely from the AirWatch administrative console. Each device under management is routinely queried to ensure that the device is operating as designed. Rooted or jailbroken devices pose an immediate and potentially costly threat. All transactional or credit card data that is temporarily stored on the device is no longer secure if the device is compromised. AirWatch defends against attempts to jailbreak or root devices by applying a proprietary compromised device algorithm that automatically detects jailbroken or rooted devices. As soon as devices are detected as compromised, AirWatch can automatically remove access to all corporate content enabled through MDM.

Ensure App Security

Distributing apps to employees can boost productivity and maintain lines of communication. But because apps are built with the intentions of accessing data, it is important for owners and operators to ensure the security of all applications, especially those that access or transmit customer information, before deploying them to devices in the field. From the administrative console, administrators can run AirWatch® App Reputation Scanning to test app security before deployment.

AirWatch App Reputation Scanning analyzes apps to help IT administrators identify potential security breaches and data loss threats. Though most apps do not contain malicious malware, many are built without the appropriate security features and APIs that make them safe for enterprise use. The tool will alert IT administrators to apps that pose security risks by flagging risk areas. App Reputation Scanning determines an app’s risky behaviors, such as network connections, access to contacts, access to GPS location and access to other personal information. Based on those findings, App Reputation Analysis identifies high, medium and low risk areas on the app. Within the AirWatch console, administrators can determine which apps users download most frequently, scan those apps, and make a decision about whether or not they should be allowed to remain on the devices. Administrators can add applications that are deemed risky to blacklists and notify users to remove them. In the future, administrators will be able to set profiles that enable automatic removal of applications that do not meet the minimum security requirement. AirWatch also partners with app security vendors Appthority and Veracode for more advanced testing capabilities.

Require Complex Passcodes

Passcodes can stop threats in their tracks. AirWatch MDM can strengthen the power of passcodes by requiring longer passcodes, requiring alphanumeric passcodes with complex characters, or by setting the amount of time a device is able to remain open without re-entering the passcode. With AirWatch MDM, administrators can set specific compliance policies that require end-users to apply passcodes that meet their requirements.

Enable remote device wipe

Devices performing transactions often store sensitive consumer data. With AirWatch, owners and operators can enable remote device wipe on lost, stolen or compromised devices. AirWatch is designed to keep mobile data secure, and in the case of emergency, wiping the device of all transactional history will prevent data loss. For example, if a device is detected as rooted, jailbroken or otherwise compromised, administrators can set policies that automatically trigger an enterprise wipe, removing all corporate data, via the AirWatch compliance engine.
Prevent data loss on lost or stolen devices

A major concern for client-facing devices is the risk of the device being stolen – along with all the data stored on the device. AirWatch helps IT administrators keep tabs on all devices in their environment and take action quickly as soon as a device is reported or detected as lost or stolen. If an employee reports a lost or stolen device, the administrator can lock or wipe the device from the management console. On devices that have GPS tracking enabled, AirWatch can detect the location of a device that has been lost or stolen.

Ensure secure transmission of data over the network

PCI recommends, at a minimum, a rotating key for accessing the private network over Wi-Fi. AirWatch takes secure network access one step further by offering the use of certificate-based authentication through a public key infrastructure (PKI). Because many owners and operators choose to deploy Wi-Fi only mobile devices, it is essential to ensure network access is secure. PKI integration ensures high security while reducing IT burden – because PKI integration exceeds the rotating Wi-Fi key requirement, administrators do not have to notify users each time the key changes.

Content

Training

With AirWatch® Secure Content Locker™, owners and operators can provide up-to-date training materials to new associates in real time. AirWatch Secure Content Locker integrates directly to backend content repositories in order to provide a seamless and real-time mobile content storage system. AirWatch Secure Content Locker can be used to send all major file types out to mobile devices across an organization. With videos, text, audio and photos, hospitality organizations can create an immersive digital training hub for all employees, at both the corporate and field levels.

Taco Bueno, a US-based fast food chain, is using AirWatch Secure Content Locker to train cooks and ensure recipes are consistent across locations. A digital recipe book deployed through AirWatch Secure Content Locker ensures that anytime a recipe is added or updated, all locations can access the same information.

Promotions

Prior to the digital age, introducing new marketing campaigns was a time-intensive process. Technology has hastened that process. With Secure Content Locker, marketing promotions can be created at a global – or even local – level, and then distributed to all locations with mobile devices set up to display content. Hotels and restaurants are using single app mode to display promotional content, such as room, activity or menu specials. With AirWatch, a mobile device becomes a revolving door of content and an asset to any hospitality organization, large and small businesses alike. Whether an executive is in a beach chair or airport terminal, he or she can push content down directly to display tablets, reducing the time it takes to initiate a large-scale marketing campaign.

Some large hotel chains are using AirWatch Secure Content Locker to distribute data-rich planograms for hotel pantries and gift shops. The ability to automatically push the latest version of a store or lobby layout to managers in multiple locations helps to ensure visual consistency and proper representation of the brand.
Apps

With AirWatch, hotel IT administrators can manage the entire application lifecycle, from testing to deployment to new versions to retirement. Administrators and developers can test applications in AirWatch with a controlled release, limiting deployment to a control group to test for issues before widely deploying the app. AirWatch offers application versioning, which enables IT administrators to require application updates, an action that can be performed organization-wide or through a phased rollout.

Administrators can make applications available to users through the AirWatch® App Catalog, a custom app catalog for your organization where employees and guests can access and download both internal and third-party applications that are managed with AirWatch. Apps for inventory, mPOS, time logging, instant messaging or guest-specific apps can be uploaded into the AirWatch console and pushed down simultaneously to specified devices.

Apps can be distributed based on organization group, which enables IT admins to push down apps based on geographical location, job function or device type, such as housekeeping and facilities, front of house, management or guest devices. For example, administrators could push room service or hotel event apps to all devices, then select hospitality and facilities staff smart groups to push maintenance, workflow and inventory apps that help facilitate more efficient room preparation. After the IT administrator selects the relevant organization groups within the console, apps can be pushed (or all users can be prompted to download).

Taco Bueno, a U.S.-based fast food restaurant chain, is using AirWatch® Mobile Application Management to manage a digital checklist app for managers and a recipe book app for cooks. Managers use the checklist app to digitally perform restaurant quality assurance checklists including food temperature readings, pictures of the dining area demonstrating cleanliness, a readiness check prior to lunch and dinner and security audits. “The biggest driver for exploring mobility was the need for digital checklists rather than paper,” explains senior director of IT Tim Collins. Having the digital checklists also help if there is a lawsuit or workers compensation claim. “If someone slips and falls in the dining room, we can provide evidence that at 10 a.m. we checked that the floors were clear and dry,” Collins says. “This checklist app, supported by AirWatch, has been instrumental in protecting Taco Bueno.”

In Taco Bueno kitchens, cooks use tablets to access recipes so they do not have to memorize them and so updates or new recipes can be automatically updated from the central office. Everything is prepared fresh - the meat, guacamole, beans – and team members using tablets will know what the final result of the product should look like.

Corporate-level Devices

The AirWatch multitenant architecture is designed to support a large number of devices and scale as a hospitality organization expands its mobility initiatives. Administrators can manage all devices across corporate headquarters, brands and global locations in a single console. The entire device fleet can be managed at a global level while empowering different groups or divisions to maintain visibility and control of devices.

Some hospitality owners and operators choose to start mobility initiatives at the corporate level and implement mobility on location later. The AirWatch solution enables administrators to enroll devices quickly, configure and update device settings over-the-air and secure mobile devices. With AirWatch, administrators
can manage a diverse fleet of Android, Apple iOS, Blackberry, Mac OS, Symbian, Windows Mobile, Windows PC/RT and Windows Phone devices from a single management console. Starting at the corporate level, hospitality organizations can give corporate employees secure access to email, calendar, contacts, apps, content and more. Through the secure container solution **AirWatch® Workspace**, hospitality organizations can enable access to these resources on BYOD devices.

**Shared Devices**

AirWatch provides the most innovative multiuser management solution that meets the hospitality industry’s security and management requirements for corporate devices while providing the personalized experience users demand. The AirWatch Shared Device feature can seamlessly provision a single managed device with settings and features specific to multiple predefined user roles. For example, an hourly employee can check out a shared device and access material that is unique to him or her. At the end of the shift, the employee can check in the device, setting the device back to a blank, unassigned state, while still under management. The AirWatch Shared Device feature is integrated within the AirWatch® Agent to ensure the most streamlined user experience. It does not require re-downloading of apps or re-provisioning of the device, so there are no gaps in management, and the device is always locked down and secured.

Several AirWatch hospitality customers have plans to deploy the check-in/check-out feature. These organizations will import authentication information for their employees by syncing with existing back-end systems. Device-level authentication will enable owners and operators on a budget to use the same device for multiple purposes and/or user types.

**Kiosk Devices (Guest-facing)**

Devices that have been enrolled and staged in Apple Configurator can be used as customer-facing devices in supervised mode, which enables administrators to lock devices into a single app, such as AirWatch® Browser, or a set of apps. The same features are available for Android devices through the Android Secure Launcher. Several organizations are using this feature to display their website or a custom app, such as apps that display menus, suggest wine pairings, provide a list of upcoming on-site entertainment or facilitate hotel check-in.

Guests at Mohegan Sun at Pocono Downs, a casino, racetrack and resort in Pennsylvania, are greeted with in-room iPads equipped with a full room-service menu and a concierge request app. “If a guest needs an extra pillow, they can actually go on the iPad and submit an order and the housekeeping team member on duty can get the order on their iPod Touch.” Guests can still pick up the phone and call in requests, but many now choose the mobile option. Guests can also scroll through the entire room service menu, which can be updated across devices over-the-air, saving time and printing costs when changes are made.

Other organizations are using kiosk mode to ensure that associates and hourly employees only have access to the app or apps they need to do their jobs. Others are using single app mode to lock devices into child-appropriate games and apps to give parents a break and allow them to enjoy some rest and relaxation.
### Grouping

#### IP-based Groups

Large deployments across multiple locations, such as large hotel groups with several brands, may want to apply unique configurations and different enterprise content to devices based on the location where they are ultimately used. In order to simplify the process of staging enrollment for numerous devices, enterprises can leverage Network Range Assignments to provision devices based on their IP address. With this method, administrators don’t have to worry about the assignment group of the original enrollment user because devices will be re-assigned based on the network range from which they report back to AirWatch.

Existing Active Directory users that reside in different user groups based on location can use existing AD credentials. Administrators should ensure that users without AD credentials reside in different organization groups to receive different configurations. Administrators then simply define the process to stage enrollment for numerous devices, either with a shared basic user account or through Apple Configurator. Devices are then shipped to their various locations, and once the devices check in from their new Network Ranges, they will be re-assigned to the users defined above, and configured with the associated settings.

#### Smart Groups

The AirWatch feature Smart Groups can simplify the grouping process. Smart Groups are custom groups of devices that administrators can define for application, profile or content assignment. Administrators can create logical Smart Groups based on a number of criteria, including ownership type, device platform, user group, model and OS. Administrators can configure smart groups that apply to a group of specific devices and/or users, and devices and users can belong to multiple Smart Groups. Once defined, administrators can reuse Smart Groups for assignment to any applications. Multiple Smart Groups can be assigned to a single application. This feature is useful for fine-tuning who should receive certain apps. Creating Smart Groups is simple and can be done on-the-fly when creating an application. By default, a Smart Group will include all devices in the Organization Group in which it was created.

In addition to refining results based on criteria selections, administrators can specify devices or users that should be included and excluded with the Additions and Exclusions categories. To add or exclude a device or user, begin typing the device friendly name in the input box and select an entry from the menu, which filters as you type. Click Add to add the selected device or user.

After administrators select criteria, a list of devices matching your selections appears under Devices in Smart Group. They can also use this field to find devices and users if you are unsure of their assigned Smart Group.

### Staging and Enrollment

The simple AirWatch enrollment process provides a consistent agent-based enrollment flow for all major platforms, and allows both administrators and end users to enroll devices. When users enroll, they are authenticated and the appropriate restrictions, apps and content are pushed automatically.
Enrollment through the AirWatch Agent or URL

To enroll in AirWatch, IT can direct employees to the app store on their devices, where they can download the AirWatch Agent. When opened for the first time, the AirWatch Agent will prompt users to enter Active Directory credentials to enroll. Users then simply follow a series of prompts, and the device is automatically configured over-the-air (OTA) based on profiles administrators have configured in the AirWatch console. This enrollment method works across device types.

For employees without Active Directory credentials, such as hourly or seasonal employees, URL-based enrollment provides a simple alternative. Administrators can direct these users to a URL that will prompt them to enter a set of credentials.

QR Code

Organizations can enroll iOS devices by scanning a QR code, rather than typing in the environment and user information. Using a QR code generator, administrators can prepare QR codes based on environment URL and group ID. Within the MDM Agent, users can select the “QR Config” button to scan the QR image and automatically connect to the correct environment.

Apple Configurator and Device Enrollment Program

The Device Enrollment Program (DEP) from Apple can help hospitality organizations maximize the benefits of iOS devices enrolled in MDM programs. Administrators can install a non-removable MDM profile on a device and automatically provision devices over-the-air, a good option for devices issued to guests. For Apple devices that are not part of the DEP, AirWatch enables administrators to take advantage of OTA updates, mass configuration and remote management.

Preparing Wi-Fi Networks

As a best practice, AirWatch recommends setting up two Wi-Fi networks for each location: one secured network for employees and MPOS and a separate public network for customers. AirWatch network access control partners can assist in the network management process through automated enrollment. Aerohive redirects new or unmanaged devices that attempt to join the store’s secure network to the AirWatch Agent or enrollment URL to enroll (or re-enroll) a device.

AirWatch is in the process of creating a solution to allow organizations to leverage distributed nodes over store networks. Individual stores will be able to host content received from the central AirWatch server and then deploy that content to devices in that network. This method of content distribution will significantly reduce bandwidth load.

Printer Management

Hospitality organizations that need to print receipts may want to use wireless mobile printers for on-site and on-demand needs. Mobile printers can improve efficiencies across organizations, processes and workforce by helping associates print materials quickly from their mobile devices.
AirWatch partners with several printer manufacturers to enable management of in-store wireless printers. AirWatch will ensure that any data that is transmitted to wireless printers, such as customer information on receipts, pricing information and barcode labels are kept private and secure.

**Rugged Device Management**

AirWatch provides complete mobility management solutions for rugged devices. AirWatch supports multiple rugged operating systems, such as Android and Windows Embedded. AirWatch rugged management provides the features our customers have come to expect, such as rapid deployment, cold boot persistence and product provisioning, while also adding proven industry solutions in mobile content management, security and extended asset tracking.

With AirWatch, hospitality customers now have a complete, integrated platform for managing both consumer based and rugged products.
Additional Resources

For additional information, visit:
www.air-watch.com/industries/hospitality
To get started with a free trial of AirWatch, visit www.air-watch.com/free-trial.

AirWatch Global Headquarters
1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch by VMware
AirWatch® by VMware® is the leader in enterprise mobility management, with more than 12,000 global customers. The AirWatch platform includes industry-leading mobile device, email, application, content and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at www.air-watch.com.