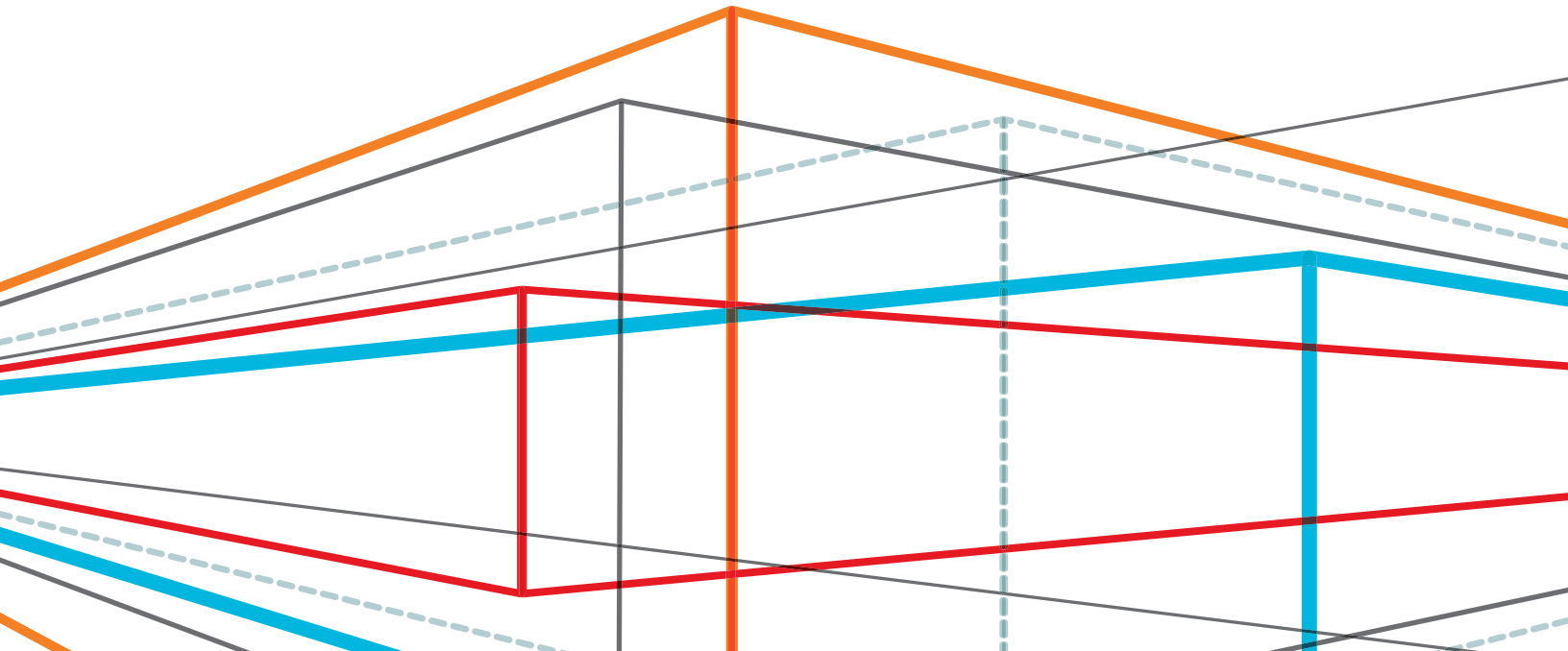
CENTRALIZED DEVICE MANAGEMENT HELPS DRIVE BUSINESS EFFICIENCIES

Improve device security, availability and cost-effectiveness

ZEBRA TECHNOLOGIES

SEE MORE. DO MORE.



CENTRALIZED DEVICE MANAGEMENT HELPS DRIVE BUSINESS EFFICIENCIES

IMPROVE DEVICE SECURITY, AVAILABILITY AND COST-EFFECTIVENESS

Executive Summary

With the increasing proliferation of mobile devices, each requiring its own unique provisioning, configuration, and reporting requirements, businesses face enormous challenges ensuring consistency and control over connected devices. IT is responsible for purchasing, setting up, and maintaining mobile devices, including printers and other peripherals. IT must ensure that these devices deliver the highest availability so users can run their applications and business operations smoothly.

However, device management tasks can overburden IT departments, and they become even more difficult as the number of devices scale into the hundreds, or even thousands of units. The challenge grows as technology refreshes inject more varieties of products. Device administration can scope out of control if IT does not have a device management strategy and plan defined early in the deployment process. As a result, business operations can suffer from poor efficiencies, higher costs, and lost opportunities.

To ensure maximum uptime and optimal configuration, all the devices in workflows and processes must be smart, connected, and manageable, which also extends to mobile printers. Businesses require a solution that centralizes device management so IT can deliver consistent device configuration, higher availability, tighter security, and future-proofed scalability throughout the device lifecycle.

In this paper, Zebra® shows how a solid device management solution can provide consistency and visibility into device status to maximize uptime and business efficiencies. Ensuring visibility of all assets whether they are directly on premise or at remote locations is another key benefit—for both IT and finance. Doing so helps maximize productivity where the devices are used, streamlines inventory management and compliance operations, and helps to create a more agile enterprise.

INTRODUCTION

Mobile devices are becoming a part of the critical infrastructure across a wide range of industries, from manufacturing and healthcare, to logistics and retail. And these devices are not just smartphones, tablets, and handheld computers. Printers have joined the sea of mobility, requiring the same IT attention as other mobile systems. To gain the maximum benefits from mobile devices, IT must ensure that users can run their mobility-driven applications in the most optimal manner. Device management is all about eliminating risk to the business, its operations, data and networks—delivering an infrastructure for continuously connected, '"always available" operations.

The Need for Device Management is Real

For many organizations, mobile devices—including printers and terminals—are mission critical and a key part of the business process. IT must solve initial device provisioning and production management issues, while having visibility into device status and solution usage. Consider the following sample of industries that require mobile device management solutions.

Healthcare

Medical centers are a complex jungle for IT. Multiple departments have unique IT needs and compliance requirements. There is a wide range of "end-of-point" printing devices that includes hand-carried, cart-top, stationary, and desktop printers. For example, phlebotomy tasks require specialized blood- and liquid-resistant labeling. Patient administration tasks require barcoded wristbands to comply with positive identification mandates. Pharmacy departments require individually printed instructions and warning labels.

Each healthcare task is unique, and may require the printing of critical information that must accompany a

patient's medical records, samples, documentation, and medication. Ensuring uptime and network integrity for all of these departmental needs is essential, and must be the primary objective of any device management solution.

Retail

Retailers use large numbers of mobile devices that are highly disbursed throughout their stores. For large chains, stores are geographically diverse, which requires a centralized, consistent method for performing device management. Mobile printers produce brand-approved signage, price markdown and shelf-edge labels, along with many other in-store applications. These tasks require high print quality, precise scannability, and data accuracy. Labeling must be synchronized with store promotions and sales activity. Proper device management helps ensure that all approved devices are available when and where sales associates need them.

Transportation and Logistics

Supply chain and distribution enterprises deliver thousands of unique packages per day. Warehouse, transportation, and enterprise planning systems are optimized for highly efficient and accurate picking, packing, and labeling. The end-of-point printing device is the final, vital piece of the workflow puzzle. The printer readies the package for distribution, closes the sale, and triggers revenue recognition. Device management ensures uptime and enables proactive attention to printers that need replacing, upgrading, and servicing.

Regardless of the industry, IT often struggles with how to apply consistent provisioning, configuration and regular updates to their wired and wireless devices. Ad hoc device management places unnecessary burdens on IT resources, exposes the business to security and compliance risks, reduces efficiency and productivity, and ultimately drives costs higher.

COMMON DEVICE MANAGEMENT CHALLENGES

Mobile and wired devices require software and firmware patches, updates, and other management attention throughout their lifecycle. From a business perspective, the volume and performance throughput of the devices must match the required speed of the workflow, reliably and accurately. From an IT perspective, device management includes the following three primary tasks:

- Updating the device operating system – Firmware upgrades, OS patches and updates provided by the original manufacturer pulled by, or pushed to, the device from a centralized, secure location.
- Device configuration – Initial device set up and security provisioning, including software objects stored on the device, and optimizing settings for specific workflows and compliance requirements.
- Status reporting – Centralized visibility into devices to help ensure uptime and availability through error and exception reporting.

The first device management challenge is the initial provisioning for hardware just out of the box and still in an "as-shipped" factory state. Each device must be brought up to corporate standards, which include network and performance settings, security and encryption settings, and granularity of status reporting. Wireless devices add an extra layer of difficulty, especially when it comes to security, Bluetooth, and IP subnet requirements.

Another challenge is that the device configuration task is not always a one-time, "set it and forget it" process. Production workflows change as the enterprise adjusts to meet the requirements of new products. Facilities are upgraded and expanded; IT refreshes networks, servers, and storage systems. The need for continual change requires IT to regularly ensure that devices maintain proper configuration throughout their usage lifecycle.

Managing Change

Like any other part of the IT ecosystem, devices require continuous control and change management. Ad hoc device management can result in non-uniform upgrades, missing patches, or outright security holes—costing money and exposing the business to risk. Fact is, IT must inject the same management rigor applied to the IT environment (network, storage, and server infrastructure) and apply it to mobile and wired devices.

What's more, the ability to visualize device utilization and performance obtained through the device management applications can bring value back into the organization and improve efficiencies. Printers often present challenges because IT only has minimal control over them, since they are complex mechanical devices that require consistent oversight to ensure operation.

Most businesses purchased barcode label printers over a number of years, so they must manage legacy printers that are off the network, or that do not have a webpage or do not support remote monitoring. Just as challenging are mobile printers, which are offsite, wireless, mechanical and not manageable remotely—all an unhappy combination for IT administrators.

Scalability and Flexibility

As the number of devices scale, so does the management burden. Large organizations often deploy hundreds, thousands, or even tens of thousands of devices. Mixing and matching of hardware, versions, and workflow usage often forces IT to maintain separate configurations, which is an enormous load on IT resources.

Unfortunately, it is nearly impossible to scale using ad hoc and manual techniques, and presents enormous challenges when it comes time to refresh the device population. Changes to security provisioning, firmware/OS upgrades, and configuration must be scalable. In many cases, the only solution is to hire an army of outside consultants to maintain the IT ecosystem, which increases both costs and complexity.

In some environments like at retail stores, expert IT resources are not always available. Lacking centralized device management, IT departments must send specialists into the field to configure, connect, and maintain devices. Doing so spreads the organization thin, creates downtime, and presents obstacles to productivity.

As can be seen above, solving the device management challenge calls for a consistent, auditable way to perform the three primary management tasks of OS updates, configuration, and status reporting. To achieve this goal, IT requires a uniform method to perform device management across the entire enterprise—regardless of geographical location.

STREAMLINE AND CENTRALIZE DEVICE MANAGEMENT

Optimally, devices should be good network citizens, supporting enterprise standards and preferences for security and connectivity. But this is clearly the exception, and not the rule. A device management solution that addresses these risks is highly valuable to any mobility-driven enterprise. Optimally, the device management solution should support both "push" and "pull" operations.

"Push" refers to when the device management application has the ability to discover devices on a network. This approach allows IT to reach deep into mobile devices and push content down to them. It is often used during initial setup and deployment, and typically offers the best path for troubleshooting issues. Push operations provide strong IT control over devices, source content, and planned downtime windows.

"Pull" is when the devices manage themselves, and contain settings directing them when and where to retrieve configurations, updates, and reassignments.

However, without a secure, central repository; encryption; and certificate verification, the business could be exposed to security issues because devices should not just go out to the internet and grab unverified data.

Improve Efficiencies and Reduce Expenses

Centralized device management governance creates a single repository of configuration "truth". Centralization allows printers to use a certificate technology that is at both the device and server level. When the device connects, if there is no matching certificate, the device management tool denies it access. When IT is pushing or pulling data it is always at one location, and the organization has overriding access control based on "allow or deny" authentication.

The optimal device management solution includes both the certificate and encryption technology that IT can apply or withdraw at their discretion. It provides the control to allow or deny requests to the centralized location

based on the organization's unique security needs. IT only has to manage one location that is encrypted, authenticated, and under full control. Centralization forces a structured, auditable, and scalable security and management plan for all devices.

As printers and devices turn on, they can connect to the network and pull the required configuration information, or, IT can specify controlled, time-based configuration changes. Now IT can ensure the device pool is synchronized and updated, and provides a common management tool for status monitoring. IT can collect device uptime statistics and analyze where problems are occurring to be more proactive in resolving issues. Centralized device management saves IT operations time and money, and ensures devices are functioning with the right configuration at the right time.

Team Up With the Right Partner

Zebra's 40-year history, and resulting network of trust, has enabled Zebra to create and develop innovative solutions, tools, and printers to help pave your path to a centralized, streamlined device management solution. Zebra's extensive portfolio of asset-tracking, location, and printing technologies, including barcode, passive and active RFID, and RTLS—along with unmatched domain expertise—turns the physical into the digital to give devices and operational events a virtual voice. This enables you to know the real-time location, condition, timing, and accuracy of the events occurring throughout your value chain. Once you can see the events, you have the opportunity to create new value from what is already there. We call it the Visible Value Chain™ solution.

Zebra device management solutions are Cloud-aware and capable, enabling Cloud migration both today and tomorrow for an infrastructure- (public/private/hybrid Cloud) and provider-agnostic solution. These device management solutions pair a multiplatform powerful software development kit and software applications with smart Zebra devices. The solutions allow users to easily integrate, manage, and maintain Zebra's suite of printers from multiple locations.

To save enterprises time and effort, Zebra can pre-configure printers coming out of the factory with customer-unique wireless setup in a secure manner. Upon deployment and installation, IT can connect the device to their network and complete confidential security provisioning and configuration on their terms.

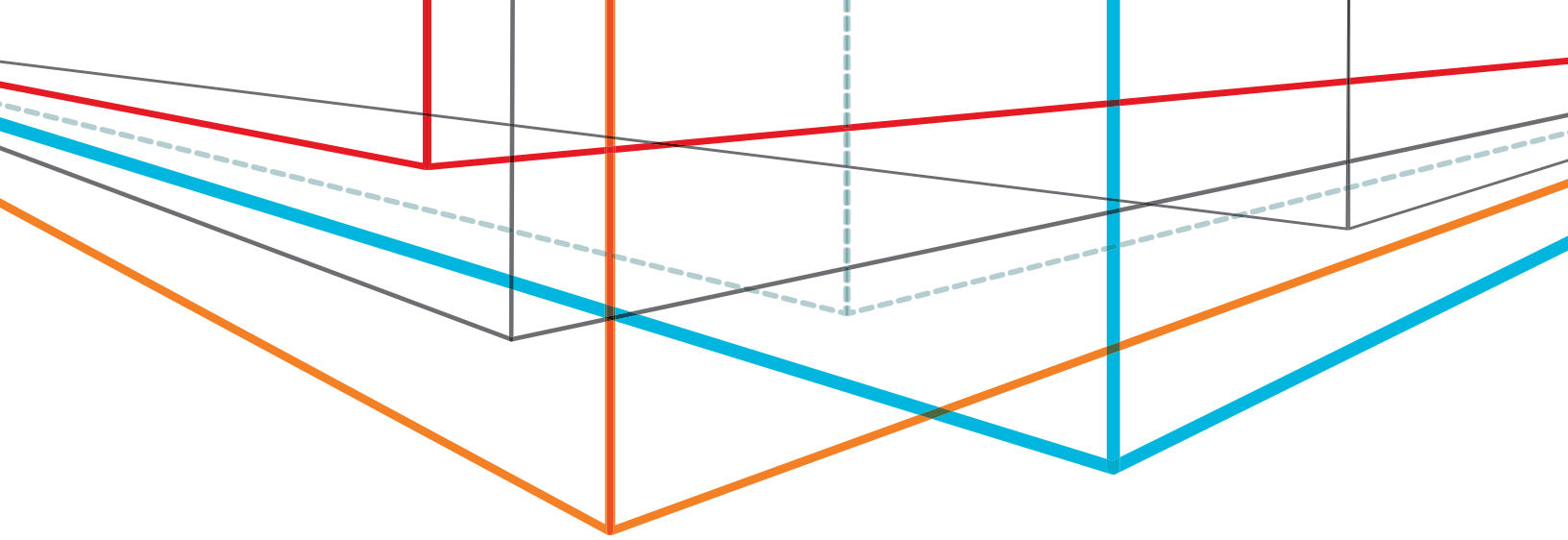
SUMMARY AND CONCLUSION

Device management tasks can overburden IT departments and become even more difficult as the number of devices scale into the hundreds, or even thousands, of units. If IT does not have a management strategy and plan defined early in the deployment process, device administration can scope out of control. As a result, business operations can suffer from poor efficiencies, higher costs, and lost opportunities.

Centralized device management solutions enable IT to deliver consistent device configuration, tighter security, and future-proofed scalability through a governed, single repository of "truth". The solution helps ensure the device pool is synchronized and updated, and provides a common management tool for status monitoring, saving the enterprise both time and money, while improving efficiencies.

To help ensure success, businesses should work with a company that has a history of device management across a wide range of verticals A global leader respected for innovation and reliability, Zebra offers technologies that illuminate organizations' operational events involving their assets, people and transactions, allowing them to see opportunities to create new value. We call it the Visible Value Chain.

Zebra's extensive portfolio of marking and printing technologies, including barcode, active and passive RFID, and RTLS, turns the physical into the digital to give operational events a virtual voice. This enables organizations to know in real-time the location, condition, timing and accuracy of the events occurring throughout their value chain. Once the events are seen, organizations can create new value from what is already there. For more information about Zebra's solutions visit **www.zebra.com.**



Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
apacchannelmarketing@zebra.com

EMEA Headquarters
+44 (0)1628 556000
mseurope@zebra.com

Latin America Headquarters
+1 847 955 2283
inquiry4@zebra.com

Other Locations / USA: California, Georgia, Illinois, Rhode Island, Texas, Wisconsin **Europe:** France, Germany, Italy, the Netherlands, Poland, Spain, Sweden, Turkey, United Kingdom **Asia Pacific:** Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam **Latin America:** Argentina, Brazil, Colombia, Florida (LA Headquarters in USA), Mexico **Africa/Middle East:** Dubai, South Africa

(10/13)