

The logo features the word "Intermec" in a bold, sans-serif font, oriented vertically. To its left is a blue square containing a white graphic of three interconnected circles. The entire logo is set against a background of thin, light blue curved lines.

Intermec

White
Paper

**MAXIMIZING MOBILE DEVICES IN
EXTENDED RETAIL ENTERPRISES**

Intermec



Handheld computers have come a long way.

Back in the '80s, handheld computers were little more than lightweight data collectors that used lightweight DOS-based applications. A clerk would scan a bar code, enter an order amount or log an inventory position, and go to the next item. Then the computer was dropped into a docking unit where the data collection file would be transferred. They were little more than fixed function tools that rarely changed.

The '90s brought real-time wireless communications to store systems—and the handhelds became even less sophisticated. Tied to a server in the backroom through a proprietary system, the handheld computer was reduced to simple terminal emulation. Handhelds became little more than “smart bricks.” In fact, one well-known store handheld was affectionately referred to as a “brick on a stick” by many in the industry. Managing a device that virtually never changed and ran only a single simple application was easy.

Sophisticated handhelds, complex management

In the current decade, things changed dramatically. Wireless networking became mainstream, handheld operating systems became sophisticated, wide area networking became inexpensive, and with it handheld computer management became a nightmare! Low-cost wide area networking brought great benefits, like rapid credit card authorization, real-time email to stores, real-time access to flash reports, cross-store inventory inquiry, and the elimination of nightly polling of store data and the ever present polling failures.

Today's sophisticated handheld operating systems, like WinCE and Windows Mobile, mean handheld computers can do much more with less development work. Audio and voice capture/playback, video capture and playback, Voice over Internet protocol (VoIP), sophisticated email, Web browsing, Java applets, and other capabilities open up new possibilities for improving the work environment for the front line worker on the store floor.

Mainstream wireless networking was made possible by the creation of networking standards (e.g. WiFi), which has led to the proliferation of standards-based hardware. This lowered the cost of wireless networking to the point where it became ubiquitous.

Now retailers have an environment where mobile workers use sophisticated computing tools on high-speed wireless backbones, connecting thousands of stores through high-bandwidth, dedicated data links. These advances in mobile computing technology are empowering retailers to do more than ever before.

There are only two problems: security and management.

Major challenges, major headaches

Consider the network security issues facing a big box retailer, which could have:

- 2,000 stores located in every major city and every major country in the world.
- 2,000 wireless network access points covering all the stores' retail space and parking lots.
- Accessibility to every device in the store (e.g. POS register, in-store processor, and desktop computers) and the centralized management systems (e.g. HR, WMS, payroll, and billing) from computers no bigger than the palm of your hand.

Considering the number of security patches released during one year alone, the job of keeping the entire enterprise secure can be a nightmare.

Now add the management of in-store handheld devices. They have become an important component in extremely large and complex enterprise systems, with store operations and merchandising groups running a variety of applications on them, which they will modify over time.

Take the 2,000 stores, add 30 handhelds per store and you have 60,000 handhelds spread across a global enterprise. With no support personnel on site, you have a disaster waiting to happen.

Retail IT managers are faced with limited choices:

- Keep running proprietary wireless networks with terminal emulation,
- Quit and find an easier job, or
- Develop a strategy to deal with the environment properly.

A solid device management strategy means managing all handheld computers from a central network operations center using device management software. DMS enables retailers to maximize their IT investment by enabling IT staff to centrally manage devices remotely through the company's wireless network at any time. Simply put, DMS lets IT perform the majority of its management and support tasks from their desks instead of traveling to every site.

DMS allows devices to stay working with no support or maintenance handoffs at the end of the day and no downtime due to installations or upgrades. The software also allows managers to check the status of all the company's devices and send specific settings for all mobile computers and operating systems over the network, keeping them up and running.

DMS enables retail IT managers to:

- **Keep track of the company's investment in mobile devices.** DMS allows real-time visibility into the status and availability of each and every mobile computer that should be on the network. If a device is unavailable for an extended period of time, DMS alerts IT staff to investigate so they can get it back into service.
- **Maximize uptime and productivity** by keeping the handhelds and software in optimal working condition. Updates, upgrades, and other maintenance can be automatically sent out to the devices, without interrupting the workday.
- **Keep the network safe** by quickly and easily installing the latest security updates on all the devices in the network with a few clicks of a mouse. This extends wireless device security and keeping unwanted users off your network.

All of these improvements drive the TCO down by reducing—even eliminating—hands-on device management.

DMS also provides:

- **A better "out of the box" experience for users.** In-store personnel are not paid to be technicians, so mobile computers need to be ready-to-go. Handhelds equipped with pre-installed device management software can be configured remotely right out of the box. No need to train users; no downtime for the configuration.
- **A uniform approach.** Using one common method for managing all devices reduces mistakes and the need for training, and improves overall system reliability.
- **Reduced WLAN traffic.** Distributed agent technologies reduce network traffic and enable remote and unattended management.
- **An easy to use, graphical console interface.** A properly designed device management system provides network administrators with a readily understood, intuitive window into all the devices on the network.

Without a strong DMS system, your IT staff is destined to be inundated with calls from users and disgruntled store managers. The inefficient operations will ultimately have a negative impact on your customers—and your bottom line.

For example, a large retailer might have an extended enterprise of this magnitude:

30,000,000	square meters of wireless network coverage
300,000	mobile computer users
120,000	battery packs
60,000	mobile computers
60,000	WinCE operating system licenses
15,000	battery chargers
10,000	wireless access points
2,000	wireless networks
2,000	WAN gateways
180	T1 line equivalent network capacity or more

Without centralized control and device management, a well-designed, secure network, and an IT staff operating under the best practices, this retailer will never be able to compete in the global economy.

Best Practices

Implementing and managing a large enterprise is not the time for learning as you go. Fortunately, there are best practices that have been established to help make the task easier.

Adhere to industry standards

Diverging from industry standards for what appears to be a unique value-add will cost you in the long run for two reasons:

1. Every time the base system changes, is updated, or evolves, any proprietary piece must be brought forward. If it isn't, you can't move forward.
2. You lose your freedom of selection. In order to continue to get the proprietary piece, you must stay with your current provider. Even worse, you completely lose your bargaining position for pricing.

Keep security protocols up-to-date and deployed in a timely fashion

Security implementations continually evolve and hackers are never far behind any security upgrades. To have a robust, secure system you must have a plan and process to acquire, test, deploy, and verify the installation of patches and security upgrades in your network, all the way down to the device level.

Fully test before you deploy

Set up a strict and thorough testing procedure for system and application updates before deploying them to the field. Make certain you build a test plan that provides good coverage or your systems will have operational problems causing help desk calls, erosion of user confidence, and a difficult recovery.

Make sure you have a roll back plan and methodology

No matter how well you test before roll out, there is a chance the system will have a flaw that is catastrophic. Make sure your system will allow you to easily roll back a release and re-deploy/ reset mobile devices remotely from a central location. Have a plan in place with identifies who, why, and how such a roll back can occur. Be sure the roll back is communicated to the field in a timely, well-articulated manner.

Communicate versioning at the use level

Build versioning communications into your systems so users know when and how the system is changing and how it affects them. Make sure this is done at the user, not the device, level.

Run a pilot

On any major install or upgrade, start by running a single store and then multi-store pilots. If you have unique regions or countries, make sure to run pilots in each area. Look for functional as well as process and user acceptance validation.

Provide a method for soliciting and collecting feedback from the field. Monitor the usage, collect the data and build it into the system including reports to corporate.

Monitor and verify deployment of changes and updates

It is imperative that the systems in the field be on a common base to make support manageable. Make certain when your DMS system deploys fixes or updates that the installation is verifiable. If mobile assets are missing from the system, make sure they are found and updated. If a mobile asset doesn't get reinserted into the network before multiple revisions are deployed, make sure the system can manage it.

Centrally manage your battery pool and enforce swap outs to keep the system healthy

Batteries are a cause for many field failures, so maintaining a healthy battery pool keeps the entire system strong. It is important to treat battery packs as assets in the system and monitor their location, use, and age. Pro-actively cycle old batteries out of the network before they become a problem.

Constantly monitor wireless network coverage and take corrective action before it becomes a problem

One of the main reasons for perfectly good mobile devices to be sent for repair is a problem with the WLAN coverage. Store reconfigurations and stock placement in the store can impact network coverage and cause users to think their mobile devices are not working.

Actively monitor network coverage in the store. Look for dead spots and communicate issues to store management, proactively putting in place repair recommendations. Tie RMA requests, failure reason codes and store conditions to weed out network-driven problems before units are shipped for repair.

SIDEBAR:

Problem: I just learned that six of the handheld computers at my Miami store have been down for three days, so the staff there haven't been able to restock 15 percent of the shelves. Now goods that should be in the stores are still sitting in the back room. How can I keep these devices up and running?

Solution: DMS keeps track of the health of every device on the network. If a device goes down, IT staff is notified immediately; in most cases they can troubleshoot and repair the device instantly from their desks. More importantly, IT can perform preventive maintenance on devices during off hours keeping your staff productive and goods moving.

Monitor and track your computing asset base in real time

The only way to maintain control is to know where all the system's devices are at any point in time. This can be especially difficult with mobile computers on wireless networks, which can be temporarily lost, sent in for service, or walk out the door. These computers can get out of sync with changes, updates, and retrofits, which can impact the health of the network and the ability of the call center to satisfy user problems.

A strong DMS system will proactively monitor and manage network assets from a central point. Make sure that trip points can be set and corrective action taken in real time.

Control device settings and periodically re-initialize and reset the computers in the field

When initially deployed, configuration settings need to be assigned to the default. For example, screen backlight brightness, backlight timeout settings, and key assignments need to be set specifically for the device and its usage.

Over time, mobile workers may alter computer configuration settings, causing it to be perceived as “not functioning properly.” Having the ability to remotely reset a computer’s configuration settings enables IT staff to check the health of the device before performing any additional service.

Monitor for rogue access points and wireless interference constantly

Hackers may try to intercept communications or access your host by fooling your system into thinking it’s a valid access point and then stealing access information so that your network can be penetrated.

Given the immense footprint of the publicly accessible real estate found in a retail chain, it is critical that the network be monitored and controlled centrally from a data center.

SIDEBAR:

Problem: The handhelds in the store in Cleveland have newer software than the ones in Dallas and the distribution center in Denver has handhelds with old security software, which has allowed hackers onto the network once already. How can I get all these devices on an equal footing?

Solution: With DMS, IT can define a standard configuration for every device. As new software versions become available, they are sent to all the devices over the wireless network during off hours so there’s no loss in productivity. Security software and settings are sent out the same way and can be changed immediately if a new threat to the network is discovered. DMS keeps the network safe and all devices at peak performance from one central location.

Integrate your wireless infrastructure into your wired infrastructure

Retail enterprises have extensive wired data networks that are controlled centrally from a network operations center capable of monitoring thousands of nodes. Historically, wireless store networks have been isolated islands of locally controlled connectivity.

With wireless beginning to proliferate throughout the enterprise, it’s imperative to build a comprehensive network control strategy that fully integrates wired and wireless. Make sure you are building your network to encompass the entire enterprise and that your stores are being treated as nodes on the network, not as separate networks.

SIDEBAR:

Problem: We have a Cisco network installed in our front office. What’s the best strategy for rolling out an integrated wired and wireless network across our entire enterprise?

Solution: Building your infrastructure around standards-based industry leaders will make network management easier. Extending the Cisco network through the wireless enterprise will provide a solid platform from which to run a DMS system. Your mobile devices should be Cisco Compatible Extensions (CCX) compliant, to ensure that they will work on a Cisco network right out of the box, saving time and money by eliminating configuration and troubleshooting.

Intermec is an active participant in Cisco’s Solutions Technology Integrator program as well as in the Cisco Compatible Extensions (CCX) program, incorporating Cisco’s wireless technology into its handheld devices.

Give your help desk remote control and diagnostic capability

Without local technical support, it is sometimes difficult to understand a user's problem. This is especially true when the user community renews itself 100 percent every 12-24 months.

DMS provides your help desk with remote control and diagnostics capabilities so they can see what the user sees and diagnose problems without having to send a technician on-site or send a computer in for repair.

Build a database of device profiles and manage them centrally

To effectively manage thousands of handheld computers, it is important that the base of computing assets be closely tracked, configured and managed.

Variations in configurations and settings will lead to help desk diagnostic problems and difficulty in assessing situations. Make certain that:

- You keep a central database of all units deployed in the field.
- Computing assets are self-reporting so that any alterations can be matched against the database.
- Assets are easily reconfigured to a known state so that diagnostics are easily done.
- Versioning is centrally controlled, monitored, and reported for likewise reasons.

SIDEBAR:

Problem: My sales associates have never used computers, so when the handhelds come into the store, they sit there until someone can configure them.

Solution: Pre-kitting the devices (i.e. installing all the necessary software applications before the handhelds are sent to the store) means end user need only know how to turn the device on. When the handhelds are powered up, the network will identify it as a new device and the DMS system will automatically configure it. Your sales staff is up and running in minutes with no technical knowledge or training needed.

Centrally monitor device health and put in place pro-active corrective action

Don't wait for units in the field to fail. Make sure the devices are functioning within standard parameters and that you can diagnose and/or pull units from the field that fall outside standard operating parameters.

Devices should be able to periodically and asynchronously report their condition and any failures to a central log. The DMS system should be configurable for rules and actions so that preemptive activity takes place automatically and smoothly.

Control updates and installs from a central console

With no technical resource in the field, it is important that you know the assets you have deployed and can control their configuration down to the individual device. DMS allows IT to manage and install new software from a central console as well as reverse and install by device type or group if necessary.

DMS Reduces TCO, Increases Profitability

As mobile devices are increasingly becoming part of the extended retail enterprise, the importance of a robust device management system is growing. A solid device and network management strategy will significantly reduce the total cost of ownership for mobile devices, increase the productivity of workers throughout the enterprise, and free IT resources to focus on tasks other than device support.

Ultimately, DMS allows retailers to be more competitive, drive costs out of their supply chain, and increase profitability.

For more in-depth information on device management, visit www.intermec.com and download the white paper "Lowering Total Cost of Ownership Through Device Management."



SIDEBAR:

Intermec SmartSystem™ – Simplified Device Management

SmartSystem™ from Intermec Technologies enables enterprises to deploy and administer mobile systems with a fraction of the time and resources traditionally required, while reaping all the productivity gains and operational improvements that mobile computing and data collection applications provide.

SmartSystem is a core suite of technologies that embed advanced management functions and features in Intermec products. These technologies automate and streamline management at the device, system, and enterprise levels.

SmartSystem-enabled devices and software applications are designated by the **Intermec Ready-to-Work Indicator (IRWI)**, a blue light LED or icon on the device that indicates it is ready to take advantage of SmartSystem control, configuration and management features.

The **SmartSystem Console** provides the main functionality and gives system users access to new capabilities as they become available. The console software has a graphical interface that provides a simple, central view to all system clients and is the gateway for more powerful features. It provides a convenient way for system administrators to view, manage, and configure all the devices on the system and can be used to develop custom applications and features. Together, IRWI-enabled SmartSystem devices and software create a fundamental infrastructure for managing mobile computers, access points, bar code printers, scanners, RFID readers, other data collection equipment and even software applications. The SmartSystem infrastructure provides a common, consistent interface so data collection and mobile computing system elements can be managed as a system, rather than as a collection of disparate pieces with separate configuration and support tools.

SmartSystem simplifies the initial configuration and deployment, allows ongoing monitoring and proactive management, creates a single, consistent platform for managing different types of devices, and provides control at the device level to serve as the foundation for advanced system and enterprise management operations. As a result, companies get a platform to manage their systems more efficiently, which allows them to automatically deploy application enhancements without incurring all the traditional high costs of upgrading.

North America
Corporate Headquarters
6001 36th Avenue West
Everett, Washington 98203
tel: 425.348.2600
fax: 425.355.9551

Systems & Solutions
550 2nd Street S.E.
Cedar Rapids, Iowa 52401
tel: 319.369.3100
fax: 319.369.3453

Media Supplies
9290 Le Saint Drive
Fairfield, Ohio 45014
tel: 513.874.5882
fax: 513.874.8487

Canada
7065 Tranmere Drive
Mississauga, Ontario
L5S 1M2 Canada
tel: 905.673.9333
fax: 905.673.3974

**Europe/
Middle East & Africa**
Headquarters
Sovereign House
Vastern Road
Reading RG1 8BT
United Kingdom
tel: 44.118.987.9400
fax: 44.118.987.9401

Asia
Asia Regional Office
26-16 International Plaza
10 Anson Road
Singapore 079903
tel: 65.6324.8391
fax: 65.6324.8393

Intermec International Inc
14 Floor, IBM-Pacific Century Place
2A Workers Stadium
Chaoyang District, Beijing 100027
P.R. China
Tel: +86 (010).6539 1012
Fax: +86 (010).6539 1025

Australia
Level 7, 200 Pacific Highway
Crows Nest, NSW 2065
Australia
tel: 61.2.9492.4400
fax: 61.2.9954.6300

South America & Mexico
Intermec South America Ltda.
Rua Samuel Morse 120 9 andar
Brooklin CEP04576-060
São Paulo, SP
Brazil
tel: 55.11.5502.6770

Intermec Technologies de Mexico
Av Tamaulipas #141, Primer Piso
Col. Hipodromo Condesa
Mexico, DF, 06140 Mexico
tel: 525.55.211.1919
fax: 525.55.211.8121

Internet
www.intermec.com

Sales
800.347.2636
(toll free in N.A.)
tel: 425.348.2726

Service and Support
800.755.5505
(toll free in N.A.)
tel: 425.356.1799

Copyright © 2004 Intermec Technologies Corporation. All rights reserved. Intermec is a registered trademark of Intermec Technologies Corporation. All other trademarks are the property of their respective owners. Printed in the U.S.A.
611581-01A 10/04

In a continuing effort to improve our products, Intermec Technologies Corporation reserves the right to change specifications and features without prior notice.