Lowering Total Cost of Ownership Through Mobile Device Management

Intermec®

CIOs, IT managers, road warriors, warehouse staff – we all love our mobile devices and the productivity and convenience they bring to everyday work tasks. Although handheld devices are terrific tools, the fact is, managing and maintaining them can be prohibitively expensive. Gartner estimates the annual total cost of ownership (TCO) for mobile devices equipped with wireless modems – a must in most industrial environments – is around $4000 per device per year.

Gartner also notes that, "When assessing the total costs of wireless mobile products, we found that the more capable the device the higher the cost. The more processing power it has, the more applications it can store, leading to higher support and operational costs." And as anyone in the IT business will tell you, a large part of those support costs are spent just in keeping devices updated with current software and security.

The cost to support and secure mobile and wireless devices skyrockets each time a device needs attention, whether it be for a software version update, device reconfiguration or to upgrade firmware. IT labor, diagnosis and training costs, plus the user's time lost to "docking" a device or handing it over to sit in the IT department can add up to a significant number of hours of wasted employee time. The user may be left without a device until the IT administrator can perform the necessary upgrades, further increasing the cost of non-working devices.

"Hands-on" maintenance becomes even pricier when companies support devices at multiple locations, such as branch offices. In these cases, an IT administrator must take time out to travel to the site and upgrade that location's devices, or the branch manager must take the devices away from users and out of productive work time, then pay to ship them to the administrator – risking loss or theft in addition to the cost of the downtime. Some companies deal with these situations by purchasing spare devices, which increases the cost and complexity of ownership.

Introducing Mobile Device Management
Mobile device management software (DMS) directly addresses all of these issues, allowing IT staff to manage devices remotely through the company's wireless LAN at any time of the day or night from a central console. That means the devices stay in action, with no support or maintenance handoffs at the end of the day, no downtime due to installations or upgrades. The software also allows managers to check the "health" of all the company's devices and deploy specific settings for a host of popular mobile computers and operating systems.

This paper will offer guidance on how to select a device management software package to ensure maximum reduction in total cost of mobile device ownership. The paper also will explain the benefits of DMS and illustrate how it can help IT managers track their companies' devices, keep them maintained and updated with the most current software and security, and ensure a uniform mobile environment for their users – all while relieving them of the chore of hands-on maintenance, and at the cost of about one hour of labor – approximately $50 per device.

Benefits of DMS
Simply put, device management software cuts labor costs and boosts productivity by freeing IT staff to do their work without the time, effort and cost required for physical contact with the devices they manage. Among the administrative tasks that can be accomplished and resulting benefits to be gained with remote device management are the following:

- Keep track of your 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.

- Maximize uptime and productivity by keeping software applications running and in optimal working condition. Updates, upgrades and other maintenance can be automatically "pushed" out to users by device management software, without interrupting the workday. These updates can be timed to the IT administrator's schedule, not just when users have gone home.

- Quickly and easily install the latest security updates, such as SSID, WEP, EAP, LEAP and 802.11x, on all the devices in the network with a few clicks of a mouse, immediately enhancing and extending wireless device security.

All of these improvements positively affect the bottom line, driving the total cost of ownership down by reducing and even eliminating hands-on device management. Other benefits of using a device management software system include:

- Better "out of the box" experience for users – Devices equipped with pre-installed device management enablers can be configured remotely by IT staff, even if they're brand new, right out of the box. No need to train users, no downtime for the configuration.

- 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

Centralized vs. Decentralized Management

Ideally, a device management software solution controls policies and versioning from one location, or "centralized." The solution should "push" software updates and setting changes out to each device on the network. As the enterprise grows, the DMS system should offer a method for distributing the workload and network traffic effectively throughout. If the DMS includes web-based technology, IT managers and users with authorization also can browse or contact the entire network of devices – including those off-site or at remote locations – from the central console.

Additionally, a wide variety of devices are available with pre-installed "device management software enablers" that correspond with popular DMS packages. These enablers help the device management software "recognize" new devices or devices that have been reset to factory settings, such as would happen in the case of a drained battery. DMS enablers make for exceptionally easy and low-cost remote device management, ensuring that users have nothing to load when they get a new device, and that the DMS works with all devices right out of the box.

Centralized device management software can be programmed to manage and track devices around the clock, not just when administrators are on the job. Once set in motion, a DMS system can maintain itself and the devices within the network indefinitely, and should not require a person to monitor or manage devices day to day.

Other, decentralized approaches to device management are available but can be prohibitively expensive, costing around $100,000 for an enterprise-class solution and $10,000 per point solution. These options usually are not ready to use right out of the box and involve lengthy implementation cycles, or offer very generic device management configuration capabilities. Also, many of these solutions have roots in wired network technologies and occasionally miss the mark when it comes to wireless devices and the complexities they introduce, especially concerning security in the enterprise.
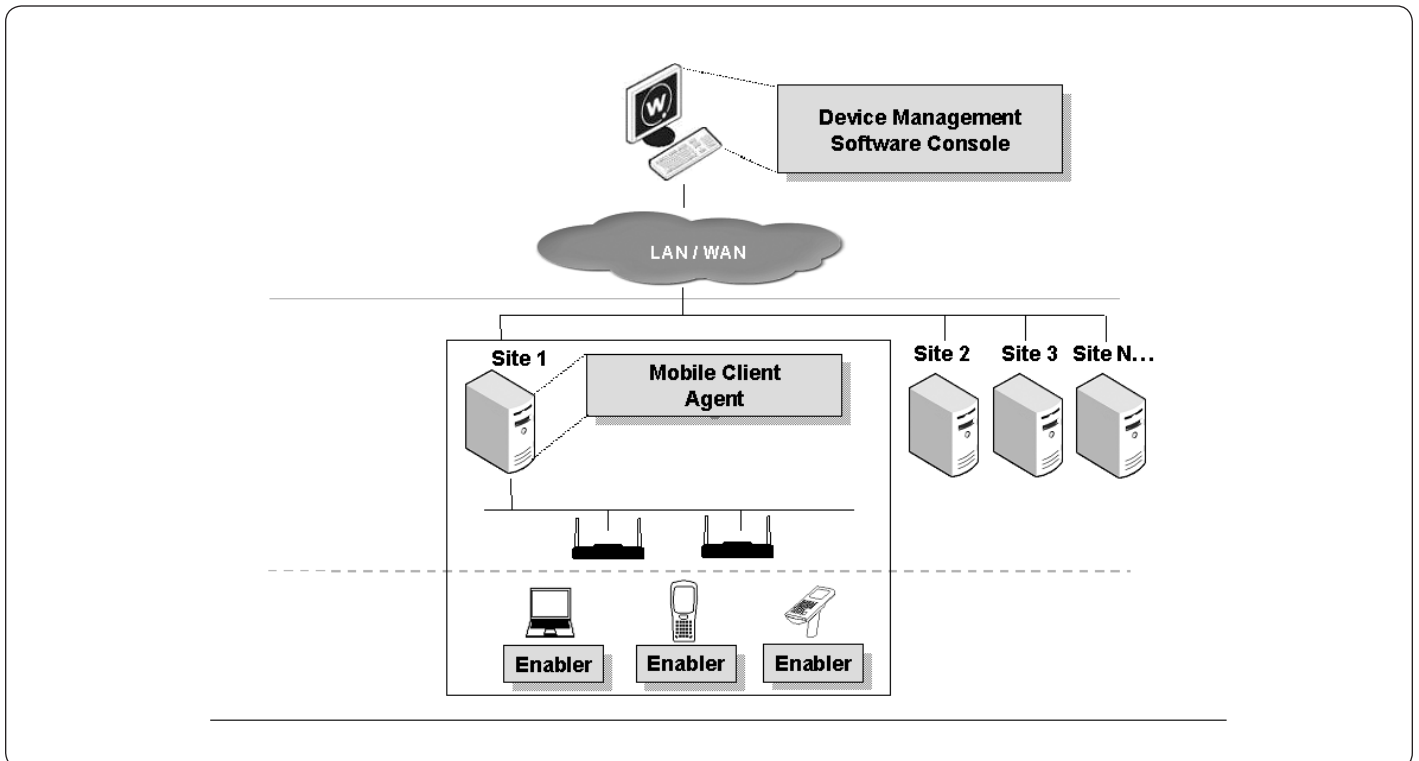
Why Use Device Management Software?
Get Ready - Automating Device Configuration

Networks, like companies, must be able to grow and change according to the demands of their customers. A device management system should do the same for mobile devices, allowing companies to add new ones, hassle-free. DMS recognizes a new device on the network and configures it accordingly, without the need for IT staff to manually configure, restart, or interrupt work to add the device to complete the addition.

Device management software also allows IT administrators to create network profiles for each type of device or application – organizing devices by model number, MAC address, network address – with provisions to include appropriate security level and their "home" location. When a new device is added to the network, the DMS then automatically assigns the appropriate configuration settings to the device, depending upon its specific network profile.

DMS also enables IT management to define and enforce advanced security parameters such as setting encryption keys, configuring 802.1x, LEAP and EAP parameters and WEP key rotation. Additionally, gateway and IP address assignments and routing directions all can be set within these profiles. This remote configuration capability eliminates manual configuration, saving considerable time and IT costs. Once a configuration has been standardized or created, the 'packaged' setting can be delivered to one, some, or all managed devices.

Get Set - Deploying Software

Once a device is "accepted" onto the network and configured, it must be loaded with all the software the user will need to do their job, stay secure, do reporting, etc. A device management software system allows IT administrators to load all user software – hands free – from the central console. Programs can be selected and sent one by one, or some DMS solutions offer a "package builder" utility by which administrators can create a pre-selected group of applications based on user requirements. Again, the IT department never has to touch the device to get these applications loaded – all are sent wirelessly by the DMS over the corporate LAN.

Software upgrades and updates also can be customized to specific groups; for example, new accounting software updates can be sent out only to users with accounting job functions. These updates can be transmitted centrally or users are given the option to download them at their convenience, no device handoffs or training time required. IT managers also can update firmware, radio drivers or other software settings at the touch of a button.

Get Healthy - Accessing Device Condition

Properly equipped device management software can take the pulse of the devices in its purview, monitoring their general health and usability. Comparing individual devices with a list of pre-determined properties and settings, the DMS can monitor and control which devices have components that need to be updated. Device management software can even list the current software packages that are deployed on a device, indicating the software versions they are running and current status. Software may be also recalled from the device, and the device reset back to a previous configuration.

The information collected by the DMS is kept as a continuous history that can be turned into easy-to-read, detailed reports to include vital stats on your company's mobile devices such as IP addresses, MAC addresses, device types, device names or IDs and operating systems. This log even allows IT management to check how long a device has been off the network. If, for example, a device has not logged on in three weeks or so, the administrator should investigate its whereabouts. Is the user just on vacation or has the device been stolen?

Device management software also can help maintain the general functionality of your entire wireless network by monitoring and controlling device bandwidth consumption. If most users update their devices at the end of the day, the number of simultaneous updates can use up a lot of bandwidth quickly, slowing the network. With DMS, IT management can monitor bandwidth consumption to determine when peak network utilization occurs, and then limit the number of simultaneous updates. By staggering the timing of these downloads, the burden on the network is lightened. DMS also allows IT management to monitor the status of ongoing global updates and check the results of the last completed update.

Get Safe - Increasing Security

Perhaps one of the most important yet time consuming responsibilities of IT managers is keeping all devices compliant with the company's security policies. When wireless security standards change and improve – and they do so about ever six months – the security software and settings on each wireless device on the network must be updated to reflect the new standard. DMS greatly eases this burden, allowing for hands free security updates, all initiated from a central console – and without the need for user intervention or knowledge that anything on their device has changed.

Device management software also allows authorized IT staff to control which applications users can access from their devices and even permits them to "lock down" applications, requiring a password for access. Occasionally referred as "kiosk" mode, this ability is especially useful when users are experienced with only a specific application on the device or – for security or company policy reasons – are not permitted to launch alternate programs; for example solitaire. Users do not have to know when they are locked out of a particular part of the device or operating system; the applications that they are not allowed to access simply do not appear on their device's screen. Nor are users offered navigation paths to unwanted programs.

Device management software also helps IT administrators manage third party client utilities and configuration tools such as the Intermec ICCU, Cisco's ACU and Funk Odyssey, and security settings including LEAP and WPA parameters and multiple connection profiles. The device management system can serve as a conduit between the administrator and the managed device, providing additional opportunities for management tasks like remote control, help desk functions, diagnostics or general assistance to the user.

Get to work - Device side functionality and enablers

Device users can spend an enormous amount of time initiating new software updates, be they files, applications, utilities, firmware and operating systems. These chores become especially time consuming when the user or administrator finds it necessary to turn off and restart the device with each upgrade. Device management software allows all these new additions to be initiated by the IT department, without user intervention – and even without their knowledge.

DMS also helps ensure the integrity of devices if programming is lost and a unit returns to factory settings, as would happen with a drained battery. Devices that come loaded with embedded device management enablers prove to be the easiest to put back into service if the software and settings are lost. Without this internal "receiver" to talk to the device management software and get help in "remembering" its programming, the device must be handled by the IT administrator to be reset, negating many of the total cost of ownership benefits of managing remotely from a central console.

Devices pre-loaded with device management enablers also stand a better chance of receiving all the information "pushed" out by the DMS console, especially if there is an interruption in the transmission of information. If a software or data transfer is interrupted before completion, devices without an internal enabler must start the transmission over from the beginning. Devices with an enabler can "tell" the DMS package where they left off in the data transfer, and only the remaining files will be transmitted when the device reconnects to the network.

Where do we go from here?

Remote device management technology will continue to improve, especially in its ability to configure applications and the settings within those applications. Imagine being able to set specific application parameters like timeouts (no more empty batteries!), host names, screen colors, language of operation, even scheduling the devices in your network to initiate backlighting after 5pm or turn down the beeper volume after the presses are finished running for the day. These features and more are on the horizon, all to help companies reduce the amount of money they spend on maintaining devices and training personnel to use them.

Summary

As companies embrace mobile technologies in quest for new economies, the need to contain costs while supporting an ever-expanding base of mobile users and devices becomes an enormous challenge for IT operations staff everywhere. Device management software can make a tremendous contribution toward lowering total cost of ownership, allowing customers with multiple network devices to upgrade and configure device software remotely, saving the time and cost of manual, one-at-a-time upgrades. The remote management capabilities reduce or eliminate the need for workers to physically "dock" devices, greatly increasing user efficiency while reducing the total cost of ownership.

Device Management, Intermec Technologies and Wavelink

Intermec Technologies understands that controlling the total cost of device ownership is paramount when selecting a device management software solution. To ensure its customers maximum savings and the best in device management and control, Intermec offers SmartSystems™ Foundation, a software platform that provides a single, integrated environment for hands-free deployment and management of devices located anywhere in the enterprise – on-site or remote. Foundation works with the Intermec components of your system including mobile computers, RFID readers, printers and bar code scanners, to make the most of limited IT resources, and lower your total cost of ownership for data collection equipment.

Foundation lets you view and configure all of the settings contained in a device from one convenient location for quick set-up, and provides easy access to the wide range of features integrated into Intermec equipment. An intuitive administrator's console provides centralized access to remote devices. Administrators can change device settings, send OS upgrades, update software applications, and execute other changes directly from the console to save time and significantly cut costs. SmartSystems-enabled devices appear on the console, providing real-time visibility to device status and information.

SmartSystems Foundation integrates with industry leading device management solutions which enables you to take advantage of additional management features. You have the option of managing your Intermec devices from the same console that you use to manage other devices in your enterprise, yet you get full visibility and access to the unique device features and settings.

Many SmartSystems-enabled devices feature the Intermec Ready-to-Work Indicator, a blue LED that gives users visual confirmation that the device is on the network and functioning properly. Check with Intermec for the latest list of SmartSystems-enabled products.

Intermec®