



THE INDUSTRY'S MOST COMPLETE MOBILITY-WIDE MANAGEMENT SOLUTION

MSP4 CONTROL EDITION

CENTRALIZED AND REMOTE MANAGEMENT OF ENTERPRISE AND BYOD DEVICES

Get complete control over your enterprise mobile devices as well as the tablets and personal mobile phones your employees are bringing to work with MSP4 Control Edition. With MSP4, you get a powerful single pane of glass that allows you to manage a heterogeneous device environment — including devices with different operating systems from different manufacturers and their attached peripherals, regardless of whether they are inside the enterprise or out in the field. With this comprehensive management solution, you get the centralized automated management capabilities you need to maximize uptime and utilization of your mobile devices and their associated peripherals, protecting mobile worker and IT staff productivity. Get true end-to-end control with three core capabilities. Staging redefines the user out-of-the-box experience — enterprise-owned devices are ready to use the moment they power on, and employees can register their own devices via an easy-to-use web-based enrollment system in less than a minute. Provisioning allows the automatic updating of operating systems, firmware, applications, configurations and more. Control provides rich day-to-day management functions, including anywhere, anytime access to the granular information required to proactively monitor and analyze device performance as well as quickly identify, troubleshoot and resolve day-to-day user issues — regardless of whether those issues are related to the device, the applications on the device or the wireless network.

The result? Mobile device reliability is improved, protecting mobile worker productivity. With the MSP client on board, your IT staff no longer needs to physically handle devices, minimizing management time and associated costs. And you get the constant availability required to get the most of your mobility solution.

FEATURES

Manage and secure enterprise and BYOD devices

Manage virtually any mobile device and peripheral — Motorola and non-Motorola; operating system support includes Microsoft® Windows Mobile®, Microsoft WinCE, Apple iOS 4 and 5 and Android™ 2.2+; peripheral support includes printers, debit and credit card readers, biometric fingerprint readers and more

Full management capabilities for Motorola 'hardened' Android

Motorola's Android-based devices, including the ET1 tablet, have additional operating system improvements that provide support for all MSP4 management features

Device metrics

Access to device, network, battery utilization, application metrics as well as OS and firmware versions provide the visibility required to remotely identify and resolve device issues

GET A SECURE CONNECTION TO ALL YOUR DEVICES

A fully integrated secure tunnel enables remote control of all your mobile devices — even if they are behind a firewall.

DEPLOY READY-TO-USE APPLICATIONS IN RECORD TIME — COMPLETE WITH DYNAMIC CONTENT

Just because an application is loaded doesn't mean it's ready to launch. There may be user-specific information required, such as a user name and password or unique security certificate. MSP4 allows devices to be configured completely, with any required dynamic information, so applications are always truly ready to use — without any user action.

COLLECT THE RICHEST SET OF METRICS FOR THE MOST ROBUST MANAGEMENT CAPABILITY: DEVICE, BATTERY, WI-FI, CELLULAR AND GPS

MSP4 collects the world of available metrics to provide the most holistic view possible — enabling the most granular management of every individual mobile device and its peripherals. Device metrics include available memory and storage, battery usage information, number of power cycles as well as the number of attempted and completed scans. The ability to track changes in the device registry provides valuable historical information to help with troubleshooting. Wireless LAN (WLAN) and wireless WAN (WWAN) metrics include signal quality, signal strength and the number of network connection attempts. If devices have integrated GPS capability, visibility into the GPS information allows you to pinpoint the location of any device at any time for the most complete asset tracking functionality available today. In addition, the GPS data can be exported for use in a fleet management application to enable new capabilities, such as geofencing — the ability to spot when a driver takes a vehicle 'off route'.

COLLECT THE METRICS YOU WANT, WHEN YOU WANT

Choose which metrics to collect, and when to collect the data for an individual device, a group of devices or for all devices to support long term trending analysis as well as short term troubleshooting. For example, a standard set of metrics can be defined for daily collection as a part of day-to-day routine device monitoring and trend analysis. But if an individual

device is performing poorly, the IT administrator can define and collect specific metrics for that device as often as every five minutes to provide deeper insight into potential problem areas. If there are issues noted in a particular enterprise location — for example, a specific retail store with an unusual number of failed scans or device reboots — IT administrators can collect information from all devices in that store every hour or as often as every five minutes for a 24 hour period, providing a richer data set to better troubleshoot the geographically isolated problem.

PROACTIVE ISSUE MANAGEMENT MAXIMIZES DEVICE UPTIME — AND PROTECTS STAFF PRODUCTIVITY

Armed with a full set of data and the ability to completely control your mobile devices and peripherals, your IT staff is equipped to spot issues and take proactive steps to avoid device downtime, protecting the productivity of one of your most valuable business assets — your employees. Developing device issues become apparent before users may become aware of a problem. For example, IT administrators can spot and determine why the number of scans for a particular device has sharply declined and take the appropriate action to correct the situation — there may be a technical issue with the scanner, wireless network connection or application, or the device may be in the hands of a new employee who simply needs additional training.

Corrupt software, including line of business applications, the operating system and firmware can be easily and remotely re-installed on demand. And with the ability to take complete control of a device, regardless of where in the world it might be located, administrators can take whatever real-time action is necessary to quickly correct an issue, from rebooting a device to restarting a process.

In addition, one of the toughest mobility assets to manage is improved — batteries. IT can detect devices that do not have ample battery power for the remainder of a shift and send users a text message to change batteries before the device powers down — eliminating unnecessary worker downtime. And since IT can monitor how fast batteries drain on each shift, they have visibility into the health of the battery pool — aging batteries are easily identified and replaced to ensure an adequate supply of fully functional batteries is always on hand for mobile workers.

Wi-Fi/cellular metrics

Troubleshoot any wireless connection on any network with visibility into the signal quality, network connection metrics, call duration and more

Battery performance metrics including battery cycle time and remaining battery time

Provide visibility into the metrics of a specific battery, or the entire battery pool to support troubleshooting; also supports Motorola's new Smart Battery

Enhanced device security

Enhanced Lock and Wipe allows you to block the use of specific peripherals and features, such as Bluetooth, media card slots and the camera and automatically lock the device when an incorrect password is entered; Secure Storage enables the encryption of files on the device hard drive and media in media card slots

Tunnel Service

Fully integrated secure tunnel eliminates the need to purchase and manage a standalone VPN solution, simplifying the mobility architecture while ensuring secure connections with all your mobile devices and peripherals

Active Directory/ LDAP Integration

Eliminates the need to issue a separate user ID and password to administrators, preserving the integrity of the Active Directory and improving network security

FLEXIBLE ASSET IDENTIFICATION AND MANAGEMENT

Comprehensive asset identification and grouping capabilities allows you to segment your devices in the manner that will best support management. Assign fully customizable asset identifiers, including asset name and tag number, IP address, region, model number, store number and more. Comprehensive searching and filtering capabilities allow you to use those asset identifiers to create literally any device group — such as similar device types or devices in a specific division, country, zone or office.

IDENTIFICATION AND MANAGEMENT OF MISSING DEVICES

Often enterprises have no way to immediately identify missing devices — critical in environments such as healthcare and retail, which must comply with strict government regulations for security of personal and credit card information. With Control Edition, IT can simply configure a time frame to flag when a device should be noted as missing — for example, if the device has not checked in with MSP4 once a shift, once a day, or once a week. Devices flagged as missing can be automatically locked and disabled when policy time frames are exceeded — or a visual cue can appear on the MSP4 console to notify administrators, who can then contact a local manager or IT administrator to determine the disposition of the missing device.

MAXIMIZE MOBILE DEVICE UTILIZATION

When purchase requisitions for new mobile devices are received, IT can quickly determine if there are unused devices in other enterprise locations that could be re-allocated to fill the need — prior to purchasing new devices. There may be locations with more devices on hand than employees due to staffing changes. Or there may be locations with shift workers where devices are under-utilized — for example, used for only one shift instead of three. As a result, the enterprise has the knowledge needed to better rationalize device inventory — and control associated device capital and operational expenditures.

EASY TO INTEGRATE AND MANAGE

MSP4 integrates easily into your existing environment. This software-only solution can be deployed on an existing server and does not require the purchase of additional hardware. In addition, the plug-in framework allows you to easily integrate MSP4 with your existing Help Desk function, including trouble-ticket systems and existing knowledge bases, greatly enriching the knowledge and the capabilities of your Help Desk workers. Active Directory/LDAP integration enables the linking of the Active Directory with the MSP4 role directory database, simplifying company-wide password administration and better protecting the company network. Audit Logging provides an audit trail of each and every administrator and each and every action that they performed in the system, improving accountability and network security. And granular definition of administrator roles minimizes risk during training — for example, you can restrict new administrators from performing critical updates to operating systems or crucial line of business applications.

MOTOROLA — YOUR TRUE END-TO-END ENTERPRISE MOBILITY PROVIDER

To help you achieve the highest levels of functionality and support for your mobility systems, Motorola offers a full suite of enterprise services that span the entire solution lifecycle. Five services practices — Design, Implementation, Management, Security and Support — provide the comprehensive framework to help you address every stage of your mobility deployments. Tiered MSP4 commissioning services incorporate server configuration, training, testing and a rapid deployment process into a single streamlined program, so you simply select the level that best meets your requirements. And once your mobility solution is in place, services such as MSP4 Software Support give you full access to technical support resources, the rights to download and use software releases and more — helping ensure all elements of your solution work at peak performance levels.

Asset management

Customizable asset identifiers, including asset tag number, serial number, model, IP address, region, store or office location identifier; enables easy location of devices; enables granular definition of device groupings for monitoring and analysis

Full real-time remote device control for Motorola mobile devices

Allows IT staff to take complete control over the remote device for troubleshooting and issue resolution; drag and drop folders and files from the desktop to the remote device to simplify troubleshooting and issue resolution

Best practices policy-based management

Allows IT administrators to monitor key performance indicators (KPIs) and tolerance thresholds to simplify management; on-screen reports ensure staff is immediately alerted when devices are out of compliance

Dynamic Deployment

Mail merge style simplicity enables the automated mass deployment of configurations that required unique information — such as a user name and password or a unique security certificate

Device-side scripting

Based on the popular LUA language, this feature allows you to easily deploy and run scripts, significantly enhancing the flexibility and power of MSP management of Motorola Solutions' Windows-based devices

Take control of your enterprise and BYOD devices today.

To find out how, visit www.motorolasolutions.com/msp or access our global contact directory at www.motorola.com/enterprisemobility/contactus

SPECIFICATIONS

Without Data Collection and Long Term Analysis		With Data Collection and Long Term Analysis
RECOMMENDED HARDWARE CONFIGURATION		
Processor:	3 GHz processor	Dual 2.33 GHz dual-core processors
Memory:	2 GB	4 GB
Hard Drive:	40 GB	40 GB
Supported Operating Systems:	Windows Server 2003 Standard/Enterprise/Web editions x86/x64 with SP2 or higher Windows Server 2003 R2 Standard/Enterprise editions x86/x64 with SP2 or higher Windows Server 2008 Standard/Enterprise/Datacenter editions x86/x64 with SP1 or higher Windows Server 2008 R2 Standard/Enterprise editions x86/x64 with SP1 or higher	
VALIDATED CONFIGURATIONS USING RECOMMENDED HARDWARE (CONFIGURATION 1)		
Mobile Devices:	100,000	250,000
Relay Servers:	20 (5K devices per relay server)	2 (5K devices per relay server)
Database Support::	SQL Server Express	SQL Server 2005/2008 Standard Edition with SQL Server Analysis Services (SSAS) enabled (External to MSP4 server in an enterprise grade cluster)
VALIDATED CONFIGURATIONS USING RECOMMENDED HARDWARE (CONFIGURATION 2)		
Mobile Devices:	5,000	5,000
Relay Servers:	1 (5K devices per relay server)	1 (5K devices per relay server)
Database Support::	SQL Server Express Edition	SQL Server 2005/2008 Standard Edition with SQL Server Analysis Services (SSAS) enabled (External to MSP4 server)
NOTES:	Please note that these specifications are the same for MSP4 Stage and Provision Editions and should be used as a basis for comparison and estimation. Actual performance will vary by hardware and configuration. For an exhaustive list of validated configurations (including 250,000 devices under management), please reference the MSP 3.3.1 User Guide.	These are the recommended minimum specifications as the Analysis feature set is resource intensive and requires the use of SQL Server 2005/2008. There may be additional scalability gains when the SQL Server 2005/2008 instance is running external to the MSP4 server. These specifications should be used as a basis for comparison and estimation. Actual performance will vary by hardware and configuration.

Missing device support

Define maximum length of time between device 'check-in' times to automatically and instantly identify, lock and/or wipe devices that have been misplaced, lost or stolen; ensures compliance with regulations such as PCI by securing sensitive data

Non-intrusive updates

Schedule device updates without disrupting the workday and risking downtime — updates can be downloaded in the background throughout the day and applied when it will not interrupt the flow of work

Expedited updates

Notify a device to pick up a critical update — even if a device is not scheduled to 'check-in' for hours

Complementary integrated Add-on Kits

Enables seamless deployment of four Motorola mobile software solutions: AppCenter for control over device-level features; SSL VPN for government-grade security; and user applications created with Motorola's PocketBrowser and Terminal Emulator (TE) development environments

Automated 802.11x certificate deployment and renewal

MSP 4 can now obtain and incorporate data from other applications into MSP4 policies and payloads that are distributed to managed devices; can automatically obtain certificates from certificate authority (e.g. SCEP) servers and deploy to MSP-managed devices; can automatically obtain new certificates when existing certificates are nearing expiration