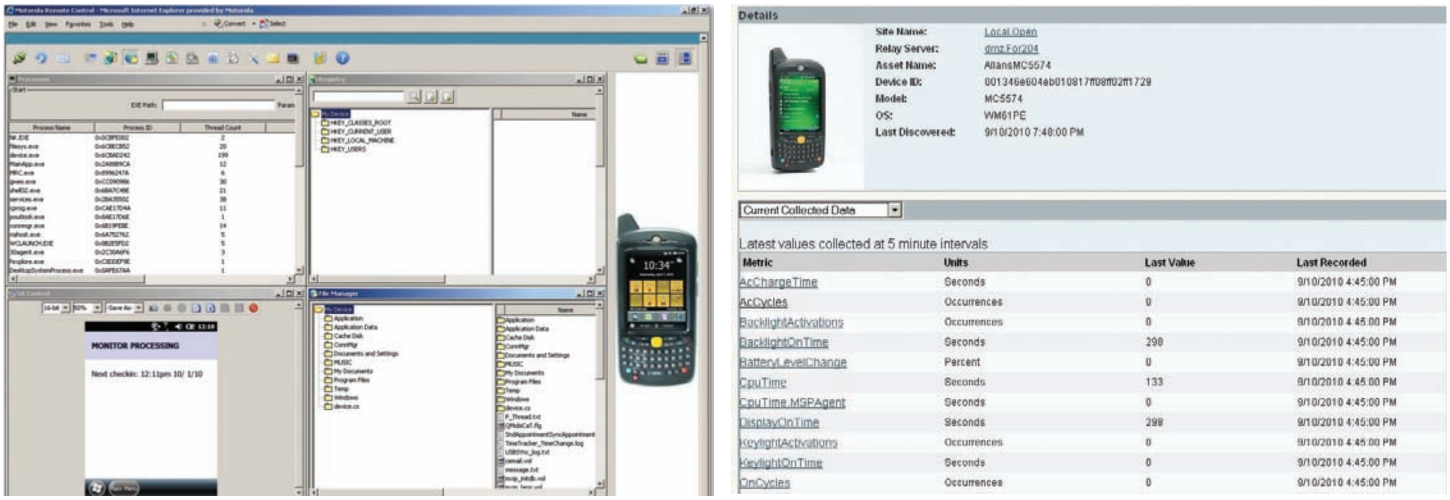
MSP4: THE COMPREHENSIVE MOBILE DEVICE MANAGEMENT SOLUTION BUILT FOR A BYOD WORLD

MOTOROLA SOLUTIONS SERVICES



MONITOR PROCESSING

Next checkin: 12:11pm 10/ 1/10

Details

Site Name: Local Open
Relay Server: dmz.For204
Asset Name: AllansMC5574
Device ID: 001346e604eb010817ff08ff02ff1729
Model: MC5574
OS: WM61PE
Last Discovered: 9/10/2010 7:48:00 PM

Current Collected Data

Latest values collected at 5 minute intervals

Metric	Units	Last Value	Last Recorded
AcChargeTime	Seconds	0	9/10/2010 4:45:00 PM
AcCycles	Occurrences	0	9/10/2010 4:45:00 PM
BacklightActivations	Occurrences	0	9/10/2010 4:45:00 PM
BacklightOnTime	Seconds	298	9/10/2010 4:45:00 PM
BatteryLevelChange	Percent	0	9/10/2010 4:45:00 PM
CpuTime	Seconds	133	9/10/2010 4:45:00 PM
CpuTime.MSPAgent	Seconds	0	9/10/2010 4:45:00 PM
DisplayOnTime	Seconds	298	9/10/2010 4:45:00 PM
KeylightActivations	Occurrences	0	9/10/2010 4:45:00 PM
KeylightOnTime	Seconds	0	9/10/2010 4:45:00 PM
OnCycles	Occurrences	0	9/10/2010 4:45:00 PM

Get all the information you need to troubleshoot the mobile devices your enterprise owns as well as the personal devices your employees bring to work (BYOD) — without ever touching any of the devices.

THE CHALLENGE:
THE BYOD MOVEMENT AND ITS IMPACT ON MOBILE DEVICE MANAGEMENT

Until recently, you had complete control over which mobile devices were in the hands of your workers. From fully-featured mobile computers to smart phones, you were in charge of specifying the operating system and the type of device. As a result, you could ensure that the mobile devices you purchased were compatible with your mobile device management (MDM) application, allowing you to maintain centralized control and to effectively minimize the management effort required to put and keep devices in the hands of your workers.

But the world has changed. Mobility is everywhere, embraced by your workers in their home lives as well as their work lives. Many workers want to bring their own devices into the workplace simply because they prefer their devices over those you specify. And while the 'bring your own device' (BYOD) movement is only a few years old, it is spreading like a wildfire — more than half of businesses in 2011 were confronted with the many issues that come with a BYOD mobile device environment.[1]

In virtually every industry sector, from retail and healthcare to field service and state and local government, businesses are allowing workers to turn their personal devices into 'dual-use' devices they use at home as well as work — from mobile phones to tablets. While there is a substantial upside for the enterprise — the capital investment in mobile devices is reduced — there is also a serious downside. When workers use their own personal iPhones and Android- or Windows Mobile-based smartphones or tablets for work instead of a corporate specified mobile device, they are accessing sensitive corporate data such as email and line-of-business applications. And since many of those devices utilize consumer-based operating systems that the typical enterprise mobile device management system does not support — such as Apple iOS and Android — how can you manage those devices and keep your corporate data secure?

[1] – Mobile and BYOD, InfoWorld Special Report, December 2011

THE SOLUTION: MSP4*

A GROUNDBREAKING COMPLETE MANAGEMENT SOLUTION FOR A HETEROGENEOUS MOBILE DEVICE POOL

MSP4 solves the heterogeneous mobile device management conundrum by providing a single management interface that provides complete control over mobile devices with different operating systems — and their peripherals. Through a powerful single pane of glass, you can deploy, manage and troubleshoot devices, applications and configurations, as well as the peripherals that are attached to those devices.

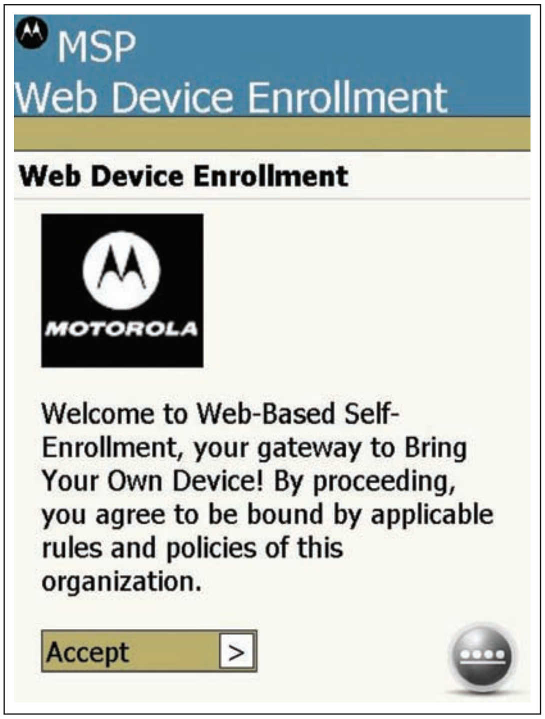
MSP4 gives you control, allowing you to centrally manage the personal mobile phones and tablets your employees are bringing into work, as well as the rugged enterprise-class mobile computers you deploy for your workers.

KEY BYOD MANAGEMENT FEATURES

While this fourth generation of Motorola's mobile device management (MDM) solution continues to offer all the features which have made it one of the most valuable mobile device management solutions available, it now extends management capabilities to many 'BYOD' devices. Features have been added to address the specific challenges of BYOD management, including:

- **Multiple operating system (OS) support**
  To date, MSP supported all versions of Windows Mobile plus Windows CE, the standard enterprise mobile operating systems. Now, MSP4 adds support for Android v2.2+, Apple iOS 4 and Apple iOS 5, with additional operating systems planned in the future.

- **Self enrollment**
  One of the most challenging issues with enterprise management of BYODs is the act of registering the device with the MDM software to ready it for remote management. Workers often need to physically bring their device to IT personnel, who must then load the application onto the device. But with MSP4, your workers can quickly and easily enroll their device via an easy-to-use web-based enrollment system, which allows the management software, enterprise settings and enterprise applications to be loaded onto the device over the air. No hands-on time is required from your IT department, dramatically reducing the time and cost associated with initial device preparation.



MSP
Web Device Enrollment

Web Device Enrollment

Welcome to Web-Based Self-Enrollment, your gateway to Bring Your Own Device! By proceeding, you agree to be bound by applicable rules and policies of this organization.

EASILY SUPPORT BYOD INITIATIVES WITH POWERFUL SELF-ENROLLMENT.

Let your workers register their personal devices in less than a minute in the MSP4 easy-to-use web-based enrollment system. Enrolling can be as simple as asking workers to enter their credentials (user name and password) and tap the 'Accept' button on the Web Device Enrollment screen.

- **Configuration and application management**
  With MSP4, all devices report all configurations, device settings, applications resident on those devices — and their version. Any deviations from the policies you have set for particular devices are automatically detected and corrected. Now, with virtually no effort, all devices remain compliant, with the proper settings and application versions. And since applications can be loaded complete with dynamic content, such as a unique security certificate or user name and password, they are ready to use instantly, without any user interaction.

- **Remote over-the-air (OTA) control**
  MSP4 gives you complete control of your BYOD and other enterprise mobile devices, all from a central location — no hands on required. Whether you are initially staging or updating device settings and applications, the entire process takes place in the background — users are never disturbed. You control when the device updates are installed — for example, late at night.

* BYOD features require MSP4 Control Edition.

In addition, you can also collect and monitor many different device metrics, providing the visibility required into issues that are brewing and allowing you to take proactive steps to prevent costly user and device downtime. And when enterprise mobile device users have an issue, IT can take complete control of the device to identify and resolve device issues — regardless of whether the problem is in the device itself, the applications loaded on the device or the wireless network connection.

- **Remote lock and wipe**
  BYODs present a major security concern — they are utilized at home and at work for both personal and business use, yet sensitive company data may be resident directly on the device or the device may have access to sensitive information in line of business applications on your computer network. If devices are lost or stolen, in accordance with regional privacy statutes, they can be automatically wiped or locked to protect sensitive company data. In the event a missing device is located, it can simply be unlocked to reinstate device access.

GET FULL MANAGEMENT FUNCTIONALITY ON MOTOROLA ANDROID DEVICES

Managing Android-based devices presents a unique challenge. While these devices can be adopted by a variety of competitive MDM solutions, the Android operating system (OS) itself limits the management functionality.

To address this issue, Motorola has incorporated a new set of hooks into the Android OS version that is utilized in Motorola Android-based mobile devices, such as the ET1 Enterprise Tablet. The result is a version of Android that is fortified for the enterprise, a 'hardened' Android able to support true enterprise-class management capabilities.

Specific management capabilities that are available only on Motorola's 'hardened' version of the Android OS include:

- **Enhanced data security**
  Devices can be configured to encrypt not only the data resident on the device itself, but also on any media card in the external media slot. So no matter where the data is located, it is protected. Data is encrypted using AE256, the same encryption protocol used by governments around the globe to protect the most sensitive information. And encrypting data is easy and transparent for your users — they simply drop files into a specific folder. All files stored in the specified folder are automatically encrypted.

  In addition, keys are centrally managed, so your data is safe, yet easy to recover. If keys are lost, unreadable or inadvertently wiped from a device, keys can be instantly restored, so device and user are back up and running instantly.

- **Forced updates**
  One of the major issues with the Android operating system is the fact that updates require acceptance by the user — so users can actually opt out of the update. But Motorola allows the hardened Android OS to automatically accept updates, without any user action. Updates simply run silently in the background, ensuring devices remain in compliance with your policies to protect your data and worker productivity.

- **Application white list**
  Users can only access applications you place on the Application White List, preventing employees from downloading or accessing applications that could allow the copying or downloading of corporate information.

The following chart lists the major features that have been added to Motorola's hardened Android operating system — features that are not supported by the standard consumer version of the Android OS.

MSP4: THE INDUSTRY'S FIRST HARDENED SECURITY AND MANAGEMENT SOLUTION FOR ANDROID-BASED DEVICES

KEY ENTERPRISE FEATURE	MOTOROLA HARDENED ANDROID	STANDARD (CONSUMER) ANDROID
Integrated management	Yes	No
Silent forced updates (applications, operating system updates, security certificates, etc.)	Yes	No (user must opt-in)
Application White List	Yes	No
Encrypt data on the hard drive and media cards	Yes	No

SUMMARY: ROBUST MANAGEMENT OF THE HETEROGENEOUS MOBILE DEVICE POOL

MSP4 offers the richest set of management tools for the mobile devices in use in your enterprise. Regardless of whether your workers are carrying traditional Motorola mobile computers with the Windows Mobile or CE operating systems, Motorola's Android-based mobile devices (including tablets) or BYODs based on consumer Android or Apple iOS, Motorola's MSP lets you manage them all.

MSP4. Mobile management in a heterogeneous device environment made simple.

THE BYOD MOVEMENT IS HERE TO STAY. STAY IN CONTROL WITH MSP4.

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

MOTOROLA