

System Center Mobile Device Manager SP1 Overview and FAQ

As the use of enterprise mobile devices increases, IT staff must efficiently support those devices while updating them with the latest software, enforcing corporate security and usage policies, and opening an ever-growing number of network resources to users. Microsoft® System Center Mobile Device Manager 2008 SP1 helps solve these challenges by providing IT professionals with complete tools for managing and securing Windows Mobile® devices. Easily deployed alongside existing Microsoft infrastructure, it uses Active Directory®/Group Policy and updates devices over-the-air (OTA). It enables you to manage and secure mobile devices as easily as you do networked PCs and laptops, and gives users secure, remote access to line of business (LOB) applications and corporate data.

How does Mobile Device Manager enhance security?

Mobile Device Manager 2008 SP1 empowers IT professionals with a robust security management platform for Windows Mobile devices, including:

- Integration with Active Directory, the most widely deployed enterprise network directory in the world, allowing you to easily extend existing security policies to mobile devices.
- More than 125 built-in policies, including the ability to lock down hardware features and camera functionality, giving you greater control over which applications can be installed and run.
- On-device data encryption and remote device wipe to help protect data if devices are lost or stolen.
- PIN Reset to enable users to request a new PIN, reducing helpdesk calls and unnecessary device wipes.

How does Mobile Device Manager 2008 SP1 help me manage mobile devices?

Mobile Device Manager 2008 SP1 enables you to provision, inventory, and update Windows Mobile devices OTA. Other device management features include the following:

- One installation of Mobile Device Manager 2008 SP1 can manage tens of thousands of devices, reducing total cost of ownership and providing for future capacity needs.
- Rich inventory and reporting tools based on Microsoft SQL Server™ 2005 help you track devices and better understand how they are being used.

- Role-based administration, Microsoft Management Console (MMC) snap-ins, and Windows PowerShell™ commandlets increase your efficiency by giving you more control over how you implement the solution.
- Software distribution and updating based on Windows Server Update Services (WSUS) 3.0 SP1 enables automatic, OTA updates.
- Open Mobile Alliance Device Management (OMA DM) 1.3 compliance enhances interoperability and programmability.

What is Mobile VPN?

Mobile VPN is the technology in Mobile Device Manager 2008 SP1 that helps deliver increased worker productivity with a single point for security-enhanced, behind-the-firewall access to corporate data and LOB applications from Windows Mobile 6.1 and later devices. Mobile Device Manager VPN features:

- Session persistence and fast reconnect to help workers stay productive even when using less-than-reliable connections.
- Machine authentication and double-envelope security to help protect corporate data and networks.
- Standards-based architecture to provide greater choice in how other networking servers interface with Windows Mobile devices.

Mobile Device Manager 2008 SP1 is designed to provide a seamless user experience across different data connection environments, as users may access their corporate assets using the Windows Mobile device's cellular or Wi-Fi connection.

What's new in Mobile Device Manager 2008 SP1?

Mobile Device Manager 2008 SP1 helps provide organizations with even greater security management and device management with performance improvements, bug fixes, and enhanced feature updates. For added device management capabilities, Mobile Device Manager 2008 SP1 now offers the following enhanced features:

- Windows Server® 2008 compatibility allows Mobile Device Manager 2008 SP1 to run against a domain/forest running Windows Server 2008 functional level Active Directory Domain Services.
- Multiple Instance enables organizations to deploy more than one instance of Mobile Device Manager 2008 SP1 within the same Active Directory forest, and helps support enterprises deploying more than 30,000 mobile devices within a single forest. With Multiple Instance, customers with independent IT organizations that want to manage devices independently can now do so.
- Enrollment Auto Discovery (available at Self Service Portal) eases the user enrollment experience by allowing the user to initiate the enrollment process without entering complex

Fully Qualified Domain Names (FQDN) or URLs. Enrollment Auto Discovery matches the user with the correct Mobile Device Manager 2008 SP1 instance, eliminating guesswork and mismatch.

- PIN Reset (available at the Remote Console) allows users to request a PIN reset on their current device, which can be initiated by the IT helpdesk or directly by the user via the Self Service Portal. If the user is unable to unlock his or her device as a result of a forgotten or lost PIN, PIN Reset gets the user back up and running in a fast and predictable manner. While easing pressure on the IT helpdesk, this also helps prevent potential loss of data with a device wipe or a hindering of user productivity with a device swap.
- Performance and scalability capabilities in Mobile Device Manager 2008 SP1 increase system/server capacity to 40,000 users from Mobile Device Manager 2008 levels.
- Virtualization capabilities in Mobile Device Manager 2008 SP1 provide Hyper-V™ support using hosted Windows Server 2003 for testing purposes.

IT Professional Scenarios

How do I manage mobile devices like PCs on the corporate network?

Mobile Device Manager 2008 SP1 is the only mobile management solution that works well with Active Directory/Group Policy, the enterprise directory network most companies already use for desktop management, allowing IT professionals to set and control policies in a single environment. With the Active Directory/Group Policy Targeting feature found in Mobile Device Manager 2008 SP1, you can

configure ActiveSync® settings or enable a "password required" policy, and create additional policies beyond those included with the product. A Windows Mobile device with the Mobile Device Manager client conforms to group policy settings just like a standard Windows®-based desktop or laptop computer. Using the updated Group Policy management tools, you can assign specific Group Policy Objects to Organizational Units and security groups, or, if required, block specific devices from receiving policies.

How do I manage software distribution to multiple groups of users?

Mobile Device Manager 2008 SP1 includes OTA Software Distribution based on WSUS 3.0. Mobile Device Manager 2008 SP1 uses WSUS to distribute applications to managed devices, and works with WSUS to

check for and push application updates to managed devices. Device Management server regularly checks with WSUS for newly published software packages, evaluating all the managed devices against the applicability rules of the packages and approval information. Using this information, the Device Management server determines which packages are applicable to each device and creates the required OMA-DM commands in the database. When a device connects, it will download and install the software packages approved for installation, all without user intervention or action.



How do I provision mobile devices without physically touching them?

Mobile Device Manager 2008 SP1 offers full OTA provisioning and bootstrapping, enabling you to provision multiple mobile devices simultaneously without physically touching them. Mobile Device Manager 2008 SP1 delivers a simple and seamless experience to users to enroll and connect Windows Mobile devices to the company network server. The user simply enters his/her e-mail address on the Windows Mobile device. The e-mail address is used to find the Mobile Device Manager Enrollment Server to connect to; the user then enters a PIN (which is provided separately to the user by the organization or via the Self Service Portal) to authenticate the enrollment and push down the machine certificate. When the authentication and enrollment are complete, the device can connect to the Mobile Device Manager Gateway server through the Mobile VPN IPSec-encrypted tunnel. Upon first connect, Mobile Device Manager 2008 SP1 can push the global policies, configuration settings, and software packages set by the IT administrator directly to the device, provisioning the device quickly.

How do I allow more secure connectivity with single-point network access control?

Mobile Device Manager 2008 SP1 helps deliver a single point for security-enhanced, behind-the-firewall access to corporate data and LOB applications for Windows Mobile devices through a cutting-edge Mobile VPN optimized for the mobile environment. With the help of Mobile VPN, Mobile Device Manager 2008 SP1 ensures that Windows Mobile device users access their corporate network (via a cellular network or Wi-Fi connection) through an encrypted IPsec tunnel that encapsulates an encrypted SSL communication channel. As a result, Windows Mobile device users gain security-enhanced, behind-the-firewall access to corporate data and LOB applications as well as gateway-monitored access to the public Internet. With Mobile Device Manager 2008 SP1, you can allow or deny a network access connection between a Windows Mobile device and your organization's network, e-mail, or mobile LOB application servers. A managed, connected Windows Mobile device then becomes a trusted machine on the network the same way PCs and laptops are trusted machines on the network.

How do I allow specific business units individual control over the devices in their unit?

Mobile Device Manager 2008 SP1 now offers Multiple Instance, which enables organizations to deploy more than one instance of Mobile Device Manager 2008 SP1 within the same Active Directory forest. Multiple Instance gives organizations flexibility, enabling multiple divisions within the same organization, with different geographies and administrative policies, to share the same Mobile Device Manager 2008 SP1 infrastructure. Multiple Instance provides greater mobile device management flexibility for you by enabling IT staff from one geographical location to set up an instance and manage the devices associated with that instance completely independently of any other instance in the domain. Multiple Instance also helps support enterprises managing more than 30,000 mobile devices within a single forest.

Additional Information

For more information on Mobile Device Manager 2008 SP1, see

<http://www.microsoft.com/windowsmobile/en-us/default.mspx>

For more information on Windows Mobile devices for business, see

<http://www.windowsmobile.com/business>