

HP Enterprise Mobility Suite

Device Management Functional Whitepaper



Table of Contents

Introduction.....	3
Features.....	3
Benefits	4
Mobile Service Configuration.....	5
Application Management	5
Upload of applications	5
Lifecycle Management	6
Firmware Over-the-Air (FOTA) Management	7
Group-Based Policy Management.....	8
Managing Mobile Devices.....	11
Self-Care Console	11
Setup My Device	12
Diagnose My Device	12
Update Software	12
Device Lock/Wipe	12
IT Help Desk Console	13
User Summary.....	13
Device Details.....	14
Device History.....	15
Device Policy	15
Bulk Campaign Jobs	15
Selecting Target Devices	15
Defining Bulk Job Parameters.....	16
Monitoring Bulk Jobs	16
Inventory Management.....	18
Summary	20

Introduction

The HP Enterprise Mobility Suite (EMS) provides enterprises comprehensive tools for effective device management, including over-the-air (OTA) mobile device initial setup, configuration, diagnostics and security. This software suite allows enterprise IT to simplify wireless device deployments and management, and launch advanced mobile services that are secure and reliable.

The HP Enterprise Mobility Suite extends device management to mobile devices, giving IT the control and security typically available for desktops, servers, and notebooks. Additionally, it brings over-the-air (OTA) device management to the enterprise, with standards developed and endorsed by the top handset manufacturers worldwide. EMS enables IT to gain insight into deployed mobile device settings and configurations as well as resident software and applications. IT will also be able to remotely diagnose device issues, deliver software and feature updates, configure service settings, or lock and wipe devices to protect sensitive corporate data.

The Suite includes server and client software; the HP Enterprise Mobility Manager and the HP Enterprise Mobility Agent. Since it leverages industry standard protocols – Open Mobile Alliance (OMA) Device Management and Download specifications – it also supports leading handset manufacturers’ native device management clients.

Features

Seamless Out-of-the- Box Experience

Automated OTA Delivery Without Cradle. The HP Enterprise Mobility Suite provisions and sets up devices using OTA data networks to help ensure a superior user-experience. Users are not required to install PC software or configure the device to communicate with the PC. The entire process is handled seamlessly OTA.

Simple One Click Trigger for Configuring New Devices. IT managers can setup a new device with a single click trigger from a web browser. HP Enterprise Mobility Suite automates the configuration of settings, software, and firmware within a single transaction.

Out-of-Box to Fully Configured, Ready-to-Use Device. Getting the mobile workforce up and running is now quick and painless using HP’s Enterprise Mobility Suite. Users can simply let the system handle the configuration and be ready for use in just minutes.

Security

Remotely Lock Compromised Devices. Remotely push lock commands to lost or stolen devices to restrict access to data and device functionality. Locking a device immediately enacts security safeguards to protect data until the device has been recovered or wiped.

Unlock Recovered Devices. Return your mobile users to productivity quickly with remote unlock of recovered devices. User data remains intact and access is returned to the user for continued usage.

Wipe Device Data OTA. Immediately kill data and applications and restore the device to a factory state with remote wipe. Any sensitive data will be cleaned from the device, allowing you to maintain corporate security even in the field.

Application Management

Collect Software Inventory of Device Fleet. Gather a precise record of all software installed on each mobile device. Audited software inventory can be used to detect problem software as well as identify missing software for the user.

OTA Push New Applications and Updates. Keep mobile workers up-to-date with the latest applications and updates. Setup large scale campaigns to quickly distribute new applications or updates OTA.

Detect and Remove Unauthorized Software. Mitigate security risks and safeguard mission critical networks with remote detection and removal of unauthorized software. Ensure adherence to IT security policies and prevent software conflicts OTA.

Diagnostics

Instantly Validate All Device Settings. Profile the device OTA to quickly gather the full set of device settings. View and compare these settings to validate and correct device configuration without requiring users to punch through menus.

Automatically Detect Device Faults. Identify device faults using the rules engine which parses the profiled device data and summarizes all issues discovered along with recommended fixes. Develop and grow the rules over time to provide even more effective diagnostics and repair.

OTA Push Fixes to Address Root Causes. Precisely target the problem rather than guessing at solutions. The HP Enterprise Mobility Suite presents a detailed view of the device along with found problems and recommended solutions that can be pushed with a single click of a button.

Group Policy Management

Define specific settings for different groups. Apply unique management policies to different enterprise user groups, with settings and applications that best suit their business needs.

Comprehensive definition of device settings. Include policies for all settings including mobile service parameters, applications, and ROM update packages.

Device independent policy management. Meta-data contained in software updates combined with HP EMS device interoperability framework provides a device agnostic approach to policy management.

Benefits

Reduce Support Costs With Automated Fault Detection.

Using the end-user to help diagnose problems is time consuming and ineffective. With the Enterprise Mobility Suite, IT managers can directly query the device, view a summary of found issues, and administer fixes in a fraction of the time and cost.

Reduce Number of Support Calls with Self-Service Portal.

Empower end-users with self-service facilities available from any standard web browser. End-users can self-diagnose, setup, and secure their devices, eliminating the need to contact IT, thus reducing costs.

Improve Mobile Work Force Productivity.

Reduce the downtime of mobile device services and ensure workers have the mobile services operational that keep them productive.

Enhance Security of Sensitive Corporate Data.

Mitigate the risks of compromised corporate data with remote lock and wipe of lost or stolen devices. Extend your corporate security policy enforcement to the mobile device and reduce security vulnerabilities with OTA access to the entire fleet of devices.

Unified Mobility Solution.

Support multiple device types across multiple wireless networks and service providers with HP's Enterprise Mobility Suite. Leverage standards-based protocols to ensure a wide array of device support. The device agnostic architecture provides for flexibility to easily add new device types as they are approved for the network. In addition, HP Enterprise Mobility Suite services operate seamlessly across worldwide wireless networks providing global support regardless of service provider.

Mobile Service Configuration

HP EMS is capable of configuring a broad set of mobile services as well as applications over the air. HP EMS leverages the OMA-DM protocol to issue a series of commands to the device which detail the specific parameters to be written to the devices. Configuration includes provisioning the following services on the device:

- Cellular Connectivity (network access points and proxies)
- Email
- Active Sync (Exchange Server)
- SIP/VoIP
- VPN
- Wi-Fi
- Bluetooth Mode

Application Management

In addition to configuration of key mobile services, HP EMS provides content management and deployment capabilities for mobile applications. HP EMS lifecycle management allows IT administrators to upload, test, and release mobile applications. HP EMS also supports application entitlement to different user groups of users within an enterprise.

Certificate Management:

Certificates may be distributed OTA to Windows Mobile devices using the HP EMS application management feature. Certificates can be pushed using a CSP file imbedded within a CAB file and delivered as if it were an application.

Security Software Distribution:

HP EMS application management can be used to distribute security software to devices to support advanced security features such as device data encryption and virus protection. The security software is distributed as part of the device setup process based on policies set within HP EMS.

Upload of applications

HP EMS provides a web interface for uploading new applications into the server. Along with the actual installable application, dependency information such as the associated platform is included to ensure that the particular application is appropriate for the device requesting it. Additional relevant information is stored along with the application such as download time, version, and description.

Figure 1: Uploading New Mobile Application into HP EMS

Create Device Application

* **Application Name:** **Please make sure this name is the same as the actual application name.**

* **Platform:**

* **Life Cycle State:**

* **Application File:**

* **Application Version:**

Type: **Application**

Download Time(secs):

Descripton:

Lifecycle Management

Content including both firmware updates and software installs are managed through the HP EMS lifecycle framework. This framework allows enterprises to setup different lifecycle states for each application to test within an internal lab environment prior to releasing the application to the end-users. HP EMS enables IT to define:

- The number of lifecycle states
- The access control of the application at each state
- The allowed transitions between lifecycle states
- The email notification list when a particular application has changed states.

Figure 2: Lifecycle states for management of mobile applications and firmware updates

Lifecycle States Definition

Lifecycle State >> State Transition

Lifecycle states define the workflow for the test cycle.

The DELIMITER between 2 email addresses should be semicolon ";".

Priority	State	Device User Groups	Email Notification	Action
1	Testing	<input type="text" value="DEFAULT"/>	<input type="text"/>	<input type="button" value="X"/>
2	New	<input type="text" value="Disable download for all"/>	<input type="text"/>	<input type="button" value="X"/>
3	Approved	<input type="text" value="Disable download for all"/>	<input type="text"/>	<input type="button" value="X"/>
4	Released		<input type="text"/>	
5	Inactive	<input type="text" value="Disable download for all"/>	<input type="text"/>	<input type="button" value="X"/>
7	Discarded	<input type="text" value="Disable download for all"/>	<input type="text"/>	<input type="button" value="X"/>

As an application goes through the lifecycle states from New to Testing to Approved and Released, the application downloads are restricted to the designated end-users listed in the Device User Groups

associated with that state. In the released state, the application entitlement occurs through HP EMS policy management.

Firmware Over-the-Air (FOTA) Management ¹

For devices that support embedded FOTA technology, HP EMS supports management and deployment of OTA ROM updates in a fashion similar to software applications. FOTA updates are based on binary differencing between an existing ROM version and the new ROM version. Because of this dependency, it is important for HP EMS to understand the existing ROM version of a target device to select the appropriate update package for that device.

Note:

FOTA requires special binary update packages based on bit-level delta compression algorithms. They are typically only available for maintenance type releases and can only be created by the handset manufacturer. In addition, release of these update packages typically rely on approval of the operator for locked devices. Consult with your handset manufacturer and operator as to the availability of FOTA update packages for devices in your network.

The management screen for an individual firmware update includes additional dependency information for managing these packages.

¹ FOTA requires a device that supports the Open Mobile Alliance Device Management (OMA-DM) Firmware Management Object (FUMO) specification. Consult with your handset manufacturer as to whether the handsets in your network have been tested and conform to this standard.

Figure 3: Firmware Package Details

Modify Update Package

To make a package downloadable, change the state. The fields below Update Time will be used in the Download Descriptor.

Package Id:	15899
Upload Date:	Fri Jun 08 02:48:19 CST 2007
Size:	183139
Manufacturer:	Manufacturer A
Phone Model:	Model A
Source Version:	1.04
Target Version:	1.05
Current State:	actual
Change state to:	<input type="text" value="actual"/>
* Update Time (secs):	<input type="text" value="120"/>
* Download Time (secs):	<input type="text" value="45"/>
Severity:	<input type="text" value="High"/>
Description:	<input type="text"/>
Type:	firmware
Additional Parameters:	
DD_TYPE:	application/octet-stream
Release Notes:	<div style="border: 1px solid #ccc; height: 100px;"></div>

For the instance of the update package shown above, the specific manufacturer and model are identified along with the source and target versions of the update package. The global standard for interfacing with FOTA-capable devices is defined by the Open Mobile Alliance and products supporting this standard are identified as being OMA-DM FUMO 1.0 compliant.

Group-Based Policy Management

HP EMS policy management enables IT to configure each group within an enterprise with the specific set of settings, applications, and ROM versions in accordance with the policies set for that Device User Group. The Device User Group consists of device user members and the policies are enforced to the user for any devices that the user has registered.

The Device User Group lists all settings, applications, and firmware updates that are available and assigned to the members of the group. During any setup process, configuration information is pulled from the Device User Group and applied to the target device. During any diagnostics process, information currently on the target device is compared to the policies defined in the Device User Group and all out-of-compliance issues are flagged with appropriate remedies that may be applied.

Figure 4: Define Device User Group Members

* User Group Name:	DEFAULT
Description:	DEFAULT DESCRIPTION
Parent User Group:	none
Service Type:	none
Last Modified Date:	May 30, 2007 04:07 AM HKT
Last Modified By:	catty
Import Device Users:	<input type="text"/> Browse...
Eligible for Upgrade:	<input checked="" type="checkbox"/> View Device Users
* SMSC Routing:	Actual
Provider:	<input type="text"/>

Each Device User Group is defined with a name, description and members as well as the selected short message service for that group for push transactions. Device User Groups may also inherit properties of a Parent User Group which may represent more global settings consistent across multiple groups.

Figure 5: Define Group Settings for Mobile Services

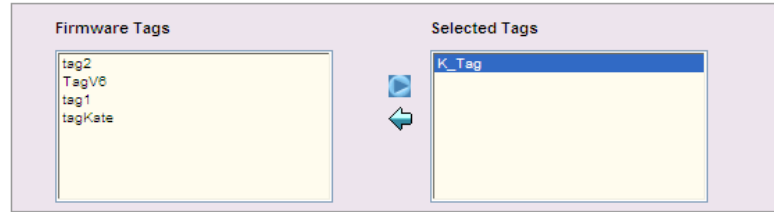
■ Provisioning Settings

Setting Name	Input Field
AS_CALENDAR_ENABLED	
AS_CONNECTION_DOMAIN	
AS_CONNECTION_SERVER	
AS_CONNECTION_USER	
AS_CONTACTS_ENABLED	
AS_MAIL_ENABLED	
AS_SETTINGS_ALLOW_SSL_OPTION	
AS_SETTINGS_BODY_TRUNCATION	
AS_SETTINGS_CALENDAR_AGE_FILTER	
AS_SETTINGS_DEVICE	
AS_SETTINGS_EMAIL_AGE_FILTER	
AS_SETTINGS_ENABLE_NONLOCAL_CROSS_POLLINATION	
AS_SETTINGS_MAIL_BODY_TRUNCATION	
AS_SETTINGS_MAIL_FILE_ATTACHMENTS	
AS_SETTINGS_MIME_TRUNCATION	
AS_SETTINGS_OFF_PEAK_FREQUENCY	
AS_SETTINGS_OUT_BOUND_MAIL_DELAY	
AS_SETTINGS_PEAKDAYS_FRI	
AS_SETTINGS_PEAKDAYS_MON	
AS_SETTINGS_PEAKDAYS_SAT	
AS_SETTINGS_PEAKDAYS_SUN	
AS_SETTINGS_PEAKDAYS_THR	
AS_SETTINGS_PEAKDAYS_TUE	
AS_SETTINGS_PEAKDAYS_WED	
AS_SETTINGS_PEAK_END_TIME	
AS_SETTINGS_PEAK_FREQUENCY	
AS_SETTINGS_PEAK_START_TIME	
AS_SETTINGS_RADIO_ENABLED_DEVICE	
AS_SETTINGS_SAVE_SENT_ITEMS	
AS_SETTINGS_SEND_MAIL_ITEMS_IMMEDIATELY	
AS_SETTINGS_SYNC_AFTER_TIME_WHEN_CRADLED	
AS_SETTINGS_SYNC_WHEN_ROAMING	
AS_SETTINGS_VERSION_MAJOR	
AS_SETTINGS_VERSION_MINOR	

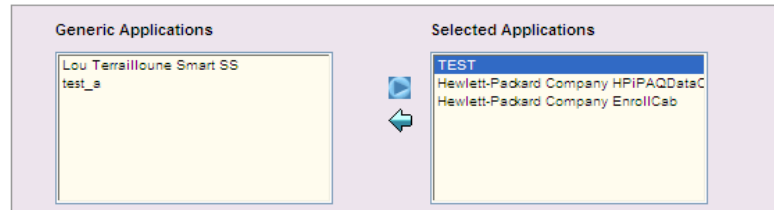
The configuration settings for each mobile service are defined under its corresponding tab. Detailed parameters are defined within the Device User Group and are enforced during device setup and flagged during diagnostics.

Figure 6: Select approved mobile applications and firmware updates

■ Firmware Tags



■ Generic Applications



Selected applications will be sent to the device in accordance with the Device User Group as well as the platform of the particular device. Any available firmware update will also be deployed to members of the group as long as the target device meets the dependency criteria with regards to particular manufacturer, model, and current firmware version. It should be noted that only applications and firmware update packages that have been put into the 'Released' lifecycle state will be available here for adding to the Device User Group.

Managing Mobile Devices

HP EMS supports use-cases for managing devices by single device transactions as well as bulk job transactions that target multiple devices. Single transactions may be initiated by IT personnel through the IT Help Desk console or by end-users themselves through the Self-Care console. Bulk transactions may only be initiated by IT personnel through the IT Help Desk Console.

Any transaction can be lumped into one of 4 types:

1. Device Setup
2. Diagnostics
3. Application Management
4. Device Lock/Wipe

Self-Care Console

The Self-Care console shows the simplest rendition of initiating these transactions.

Figure 7: Self-Care Console Screenshot



Setup My Device

Clicking Setup My Device will send a notification to the device which will start a session. During the initial portion of the session, HP EMS gathers basic device information to understand the current manufacturer, model, platform, and firmware revision information. It will then compile the appropriate changes to the device based on the Device User Group to which the user is assigned. Finally, it will issue a set of commands to the device to configure the appropriate values.

Diagnose My Device

Diagnostics transactions are nearly identical to the Setup Device scenario except that in this case, HP EMS will flag all non-compliant issues rather than setting them up from scratch. During a diagnostics session, HP EMS will gather the complete set of device information including inventory of all settings, operating parameters, software inventory, and hardware specific information. This information is compared against the rules defined for each Device User Group and any non-compliant items are flagged for action. By checking each flagged item and selecting 'Apply,' HP EMS issues the commands to the device to resolve the found issues.

Update Software

For managing software on the device, HP EMS will first query the device to check for installed inventory. Similar to diagnostics, HP EMS will check the device platform and current inventory and compare that against the applications that have been approved for the Device User Group to which the user belongs. Once the user selects the applications from the approved list, HP EMS delivers and installs those applications to the user's device.

Device Lock/Wipe

Remote lock and wipe can be applied by selecting the appropriate option from the Lock & Wipe screens. For lock, HP EMS issues the lock command which will apply the native lock mechanism on

the device which protects the device from access. Because the locking mechanism itself is native to the device, it will maintain the lock even after replacing the battery and SIM card.

For devices with an existing lock code, HP EMS will not change the lock code but simply trigger the locking mechanism. The user is required to enter the lock code on the device to unlock devices in this scenario. For devices without an existing lock code, HP EMS will apply its own lock code which will need to be applied by the user on the device or by HP EMS to unlock the device.

HP EMS can also send a wipe command which will clear all device data and data stored on external storage cards such as SD cards (does not clear SIM cards) restoring the device to a cleared factory state. In addition, for devices that are in the locked state, HP EMS will provision an allowable number of tries to enter the lock code before the device is completely wiped.

IT Help Desk Console

The IT Help Desk Console is designed for IT personnel to remotely manage end-user devices and includes an extensive set of data for each device viewable by IT. In addition to the operations shown in the Self-Care console, the IT Help Desk provides all parameters collected during any of the transactions. IT can search for an individual user through a set of filters and for that user, IT is shown a complete set of device data collected during the last transaction with the user. The information is split into the following categories:

- **User Summary:** Shows overview information about subscriber and device including additional tabs for each mobile service.
- **Device Details:** Shows in-depth information regarding hardware and network information.
- **Device History:** Shows all historic transactions allowing IT to compare previously collected data for understanding changes in device and operating environment.
- **User Policy:** Shows the values of the policies assigned to the particular user through their membership in a specific Device User Group.

User Summary

For details about any specific service settings on a user's device, the IT personnel can select the appropriate tab and click on details for a complete listing of the device settings as of the last device profile.

Figure 8: User and Device Summary Screenshot

The screenshot displays the 'User Summary' page for a user named Glenn Hamasaki. The page is divided into several sections:

- User Information:** Name (Glenn Hamasaki), Email Address (glenn.hamasaki@hp.com), Mobile Number (949) 555-1236, Device ID (358534000011078 (IMEI)), Manufacturer (HP), Model (iPAQ 510 Voice Messenger), and Device State (Unlocked).
- Network and Device Settings:** Operator (Cingular), Device User Group (DEFAULT), Firmware Version (1.1), Last Known Action (Profile), Network Type (GSM), Home Network (Network 1), Roaming (false), SMSC Routing (Cingular), Platform Name (Pocket PC Phone Edition), Platform Version (4.0), DM Version (1.1), and Available Memory (30 MB).
- Cell Connections Table:**

Connection Name	Connection Type	Access Point	Authentication Type	Username	Primary DNS	Secondary DNS	IP Address
ATT MMS	GPRS	wap.cingular	n/a	WAP@CINGULARGPRS.COM	0.0.0.0	n/a	n/a
ATT GPRS WAP	GPRS	wap.cingular	n/a	WAP@CINGULARGPRS.COM	0.0.0.0	n/a	n/a
ATT GPRS	GPRS	wap.cingular	n/a	WAP@CINGULARGPRS.COM	0.0.0.0	n/a	n/a

At the bottom of the page, there are buttons for 'Device Setup', 'Device Diagnosis', 'Software Updates', and 'Lock and Wipe'.

Details for the device's configuration and software inventory are viewable through the appropriate tab. The data presented is collected directly from the device during the previous session.

Figure 9: ActiveSync Service Settings

ActiveSync Details		Device ID	358534000011078 (IMEI)	Last Known Action Profile		Platform Version	4.0
AllowSSL/UseSSL	Yes/	Autosync	n/a	Auto Sync When Cradled	n/a	Conflict Resolution	n/a
Domain		Carrier Age Filter	n/a	Carrier Connector	n/a	Carrier Connector List	n/a
Password	n/a	Client Negotiated	n/a	Client Protocol/Version	n/a	Device Addressing Method	n/a
URI	n/a	Device Phone Ready Only	n/a	Device SMS Address	n/a	Enable Non Local Cross Pollination	No
User		Enable Non Local Cross Pollination	No	MIME Truncation	5120	Notifications Supported	n/a
Server		MIME Truncation	5120	Off Peak Frequency	-1	Radio Enabled Device	Yes
Calendar Enabled	No	Off Peak Frequency	-1	Sync After Count	n/a	Sync After Time	n/a
Calendar Age Filter	4	Radio Enabled Device	Yes	Sync After Time	n/a	Sync After Time When Cradled	5
Contacts Enabled	No	Sync After Count	n/a	Sync After Time When Cradled	5	Version Major	1
Folder Type	n/a	Sync When Roaming	No	Version Major	1	Version Minor	1
Folder Sync Enabled	n/a	Sync After Time	n/a				
Email Enabled	No	Sync After Time When Cradled	5				
Email Age Filter	2						
Email Body Truncation	512						
Email File Attachments	No						
Send Email	Immediately						
Save Sent Items	Yes						
Sync Switch Purge	n/a						
Peak Days (Sun-Sat)	Mon,Tue,Wed,Fri						
Peak End Time	1800						
Peak Start Time	0800						
Peak Frequency	-1						

Device Details

For detailed information about the hardware and operating environments, the IT personnel can select Device Details. A complete set of information is provided showing device and network related operating parameters. The Device Details presents more in depth information as memory usage, battery strength, platform versioning, and signal strength.

Figure 10: Device Details View

Search Customer Details

User Summary Device Details Device History User Policy

Manufacturer	HP	Device State	n/a
Model	iPAQ 510 Voice Messenger	PLMN	n/a
Mobile Number	(949)555-1236	Registered	n/a
Device ID	358534000011078 (IMEI)	Network	n/a
Platform (Major Version)	4.0	Roaming	false
Platform (Minor Version)	n/a	System ID	n/a
Platform (Build Number)	n/a	Network ID	n/a
Processor (Architecture)	n/a	Cell ID	n/a
Processor (Model)	n/a	Location Area Code	n/a
Processor (Level)	n/a	Country Code	n/a
Battery Level	n/a	Signal Strength	n/a
AC Power	false	SMS Address	n/a

Memory ROM		
Type	Available	Total
Internal	n/a	n/a
Virtual	n/a	n/a
External	n/a	n/a

Device Setup Device Diagnosis Software Updates Lock and Wipe

Device History

HP EMS maintains a record of each transaction and Device History allows IT personnel look at any historic device profiles as well as any configuration activities. Each transaction is date and time stamped and shows the person who carried out the transactions. Any type of transaction will be listed including those done by other IT personnel, those done by the end-user in self-care, and any that were carried out during bulk job transactions.

IT can then take a closer look at any of the transactions to see the diagnostics results found during the previous transaction. In addition, IT can select two or more historic transactions and compare results. Any differences are displayed. IT can use this information to detect any changes that might have impacted service and performance of the device.

Device Policy

For easy reference, the Device Policy shows the policies associated with the Device User Group to which the user belongs. This is the same information contained in the Device User Group and is available within the user record so that IT can reference the information quickly.

Bulk Campaign Jobs

For initiating a management transaction to a number of target users and devices, HP EMS provides an interface through the IT Help Desk Console to specify the devices and job parameters. In addition, the console enables IT to monitor and track progress of the overall campaign as well as any individual transactions.

Selecting Target Devices

HP EMS begins a new bulk job with identification of the target devices for which the campaign will apply. The target list may be built from the system's internal list of known devices which can be filtered by:

- Customer ID Range
- Device User Group
- Manufacturer

- Model
- Email Address Range
- Mobile Number Range
- Device ID Range

The filter can be applied multiple times to develop an aggregate target list with multiple filter criteria. Alternatively, a pre-compiled comma separate value (CSV) list can be imported to define the target list of devices for the bulk campaign.

Defining Bulk Job Parameters

For each bulk job, HP EMS allows for behavior to be customized for the tasks within the campaign. The following parameters will characterize the tasks that are included in a particular job:

- Start date and time: The scheduled date and time when the first transaction will start.
- Bulk job name: The identifying name to which all tasks within the job will be associated.
- Rate plan: The selected throttling rate schedule for tasks within the job. Rate plans control how many transactions are allowed per hour during each hour of a day.
- Priority: The priority relative to other pending tasks in the bulk queue
- Job action: The transaction type that is being created for each device in the job.
- Number of retries: The number of retries allowed for each device until the state is concluded as failed.
- Retry expiration: The total number of minutes allowed before a task is concluded as failed.
- Time between retries: The number of minutes to pause between each retry attempt.
- Send Courtesy SMS: Determines whether or not to send an informational message prior to initiating the actual transaction. In addition, the job allows for definition of this informational message and the time before the transaction at which to send the courtesy message.

Monitoring Bulk Jobs

HP EMS tracks bulk jobs through their completion and provides an interface for IT to monitor each job at a summary level as well as at a detailed level. For each bulk job, the summary level report shows the number of tasks:

- Waiting to start (pending)
- Running
- Succeeded
- Failed

At the bulk queue summary level, the bulk job list may be filtered by the following parameters:

- Begin and end dates
- Job status
- Job action

Figure 11: Bulk Job Summary Report

Single
Bulk

↳ Bulk Queue

New Bulk Job

Bulk Queue Filter

Date Range Begin

Date Range End

Job Status

Name

Job Action

Filter

Bulk Queue

<input type="checkbox"/>	Start Date	Name	Job Action	Amount	Job Status
<input type="checkbox"/>	06/03/2007 06:00 PM	Moto Q Fix 2/20	Diagnose	53	53 Cancelled
<input type="checkbox"/>	03/15/2007 08:00 AM	Moto Q Fix 2/15	Diagnose	2	2 Failed
<input type="checkbox"/>	03/10/2007 08:00 AM	Verizon Fix 2/10	Diagnose	60	60 Failed
<input type="checkbox"/>	03/05/2007 03:00 PM	Verizon Fix Again 2/5	Diagnose	5	5 Succeeded
<input type="checkbox"/>	03/02/2007 01:00 PM	Verizon Fix 1/30	Diagnose	45	45 Succeeded
<input type="checkbox"/>	02/25/2007 12:00 PM	Verizon Fix 1/25	Diagnose	37	37 Succeeded
<input type="checkbox"/>	02/20/2007 11:00 AM	Moto Setup 1/20	Set Up	450	450 Succeeded
<input type="checkbox"/>	02/15/2007 09:00 AM	GM Setup 1/15	Set Up	153	30 Succeeded 50 Running 50 Waiting To Start 23 Failed
<input type="checkbox"/>	02/10/2007 10:00 AM	Moto Q Fix 1/10	Diagnose	35	35 Running
<input type="checkbox"/>	02/05/2007 06:00 PM	Moto Q Fix 1/5	Diagnose	25	25 Failed

0 of 18 selected
Page 1 of 2

Pause
Resume
Cancel

For additional insight into any of the bulk jobs, HP EMS provides detailed information about each task within the bulk campaign. In addition, information about the operating parameters of the particular bulk job are maintained for reference. The export button allows IT to extract the information in CSV format for offline analysis.

Figure 12: Bulk Job Details Report

Single
Bulk

[Bulk Queue](#) ▶ Bulk Job Details

Bulk Job Details

Start On	06/03/2007 06:00 PM	Number Of Retries	18
Bulk Job Name	Moto Q Fix 2/20	Retry Expiration (min)	06/03/2007 06:00 PM
Rate Plan	Rate Plan 2	Time Between Retries	3 Min
Priority	1	Send Courtesy SMS	sms
Job Action	Diagnose	SMS Pause Time (min)	1

Refresh

Bulk Job Target Group

<input type="checkbox"/>	Device User Group	Manufacturer Model	Mobile Number	Email Address	Details	Status
<input type="checkbox"/>	Group A	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-6456	joe.user@hp.com	Details	Activated
<input type="checkbox"/>	Group B	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-7367	fred.user@hp.com	Details	Activated
<input type="checkbox"/>	Group A	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-3567	ellen.user@hp.com	Details	Device Discovered
<input type="checkbox"/>	Group C	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-7435	john.user@hp.com	Details	Notification Sent
<input type="checkbox"/>	Group C	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-2243	george.user@hp.com	Details	Successfully Completed
<input type="checkbox"/>	Group B	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-3445	sarah.user@hp.com	Details	Failed
<input type="checkbox"/>	Group A	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-2224	bill.user@hp.com	Details	Successfully Completed
<input type="checkbox"/>	Group A	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-7473	angela.user@hp.com	Details	Failed
<input type="checkbox"/>	Group A	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-9824	sean.user@hp.com	Details	Successfully Completed
<input type="checkbox"/>	Group A	hp iPAQ hw6945 Microsoft Windows Mobile Version 5.0	(913) 555-0876	jason.user@hp.com	Details	Successfully Completed

0 of 11 selected
Page 1 of 2

Export
Cancel

Back To Bulk Queue

Inventory Management

With each transaction, HP EMS collects a broad array of device information including key operating parameters. In addition to the configurable settings identified in this paper, HP EMS also collects the following information for each device providing valuable information to IT about their mobile fleet:

Hardware Info

OEMInfo	Manufacturer unique model identification
Platform	Platform information
Name	Software platform (Symbian, MS Smart phone, etc.)
MajorVer	Major version
MinorVer	Minor version

BuildNbr	Build Number
Processor	Processor information
Architecture	INTEL, MIPS, SHX, ARM, IA64, etc.
Model	ARM720, STRONGARM, HITACHI SH4, etc.
Level	Processor revision level
BatteryLevel	Percentage, 0 to 100%
ACPower	Boolean, true if connected to AC outlet
Memory	Memory information
ROM	Internal ROM memory size in KB
Internal	Internal physical RAM memory information
Total	Total memory installed in KB
Available	Available memory in KB
Virtual	Virtual memory information
Total	Total memory installed in KB
Available	Available memory in KB
External	External physical RAM memory information
Total	Total memory installed in KB
Available	Available memory in KB

Network Info

PLMN	PLMN ID from the SIM card
Registered	Boolean, true if registered
NetShort	User readable short network name
NetLong	User readable long network name
Roaming	Boolean, true if roaming
SID	Current System ID
NID	Current Network ID
CellID	Cell ID
LAC	Location area code
CC	Country code
Signal	Signal strength, 0% to 100%
SMSCAddr	Service center address (phone number) from SIM
PhoneID	IMSI for GSM, MIN for CDMA

PhoneNum	MSISDN for GSM, MDN for CDMA
----------	------------------------------

Application Info

AppsInstalled	Number of applications installed
AppsRunning	Number of applications currently running
<AppList>	Unique application ID
Name	User readable name of the application
Version	Application version
Size	Application storage size
Running	Boolean, true if the application is running
Memory	Application memory usage if running, else 0
Threads	Thread count if running, else 0
ProcessID	Process ID if running, else 0

Summary

The HP Enterprise Mobility Suite delivers a number of unique features for enterprise device management which leverage industry standard protocols for multi-platform support across the fragmented mobile environment.

- True push capabilities using short messaging service
 - Instant remote lock/wipe and remote device wakeup
- End-User Self-Service
 - Accessible via web-based browser based self-care portal
- Cross Platform Support
 - Supports industry standard OMA-DM
 - Supported by all major device manufacturers
- Diagnostics Engine for precision troubleshooting
 - Single interface regardless of device type
- Highly scalable standard web server
 - Pure Java web server stack
 - Supports normal and reverse proxy

HP Enterprise Mobility Suite eases the pain of mobile deployments by helping to:

- Lowering IT Support Costs
- Improving Workforce Productivity
- Protecting Corporate Data

For more information

www.hp.com/go/bitfone

© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Itanium is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

4AA0-XXXXENW, May 2006

