

# Symantec Mobile Management User's Guide



# Symantec Mobile Management User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 7.0

## Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014

<http://www.symantec.com>

# Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

## Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

## Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	<a href="mailto:contractsadmin@symantec.com">contractsadmin@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportolutions@symantec.com</a>

## Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

[www.symantec.com](http://www.symantec.com)

Select your country or language from the site index.

# Contents

Technical Support .....	4
Chapter 1	Introducing Mobile Management Solution ..... 11
	About Symantec Mobile Management ..... 11
	Components of Symantec Mobile Management ..... 11
	How Symantec Mobile Management works ..... 12
	What you can do with Symantec Mobile Management ..... 12
Chapter 2	Getting started with Mobile Management Solution ..... 15
	Managing mobile devices ..... 15
	Viewing the Mobile Management Portal page ..... 16
Chapter 3	Installing and configuring Mobile Management ..... 19
	About installing and configuring Symantec Mobile Management ..... 19
	Viewing mobile devices in your resources list ..... 20
	Automatically installing Mobile Management Server software ..... 20
	Installing the Mobile Management Agent ..... 21
	Changing the agent configuration schedule for mobile devices ..... 23
Chapter 4	Securing device communications ..... 25
	About securing device communication ..... 26
	Communication components of Mobile Management Solution ..... 27
	About the device agent ..... 27
	How the device agent and the mobile site service communicate ..... 28
	Securing Mobile Management communications ..... 29
	About obtaining certificates ..... 32
	About using self-signed certificates ..... 32
	Generating self-signed certificates with MakeCert ..... 33
	Installing a server certificate on the mobile site service computer ..... 35
	Configuring IIS to accept SSL connections ..... 36
	Configuring the tunnel service to accept SSL connections ..... 37
	Installing certificates on mobile devices ..... 38

	About the certificate manager tool .....	39
	Certificate manager command-line switches .....	40
	Certificate Manager command-line examples .....	41
	Example for modifying the device agent configuration file for TLS/SSL tunnel connection .....	42
	Modifying device agent configuration files to specify a client certificate .....	42
	Example: modifying each client configuration file .....	43
	About access control .....	45
	User authentication levels .....	45
	Access levels for resources .....	46
	URL Resource Identifiers .....	46
	About RPC Resource Identifiers .....	47
Chapter 5	Gathering inventory data from mobile devices .....	49
	About gathering inventory data from mobile devices .....	49
	Changing the schedule for mobile device inventory .....	50
	About the Heartbeat value for mobile devices .....	51
	Running and viewing reports for mobile devices .....	51
	Battery information fields .....	52
	Battery constants .....	55
	OS version information fields .....	55
	OS version constants .....	56
	System information fields .....	56
	System constants .....	58
	Processor level values .....	59
	Memory information fields .....	60
Chapter 6	Delivering software to mobile devices .....	63
	About delivering software to mobile devices .....	63
	Delivering software to mobile devices .....	64
	Changing software packages for mobile devices .....	65
	Package actions for mobile devices .....	66
	Sample of AppUpdate token for mobile devices .....	71
Chapter 7	Remotely managing mobile devices .....	73
	About remotely managing mobile devices .....	73
	Changing the remote settings for mobile devices .....	74
	Starting a remote session with a mobile device .....	75
	Remote options for mobile devices .....	75
	Function mappings in remote sessions .....	78

Index ..... 79



# Introducing Mobile Management Solution

This chapter includes the following topics:

- [About Symantec Mobile Management](#)
- [Components of Symantec Mobile Management](#)
- [How Symantec Mobile Management works](#)
- [What you can do with Symantec Mobile Management](#)

## About Symantec Mobile Management

Symantec Mobile Management lets you manage, secure, and troubleshoot the mobile devices in your organization. Using Mobile Management, you can automate repetitive tasks to reduce the resources that you spend to control your IT environment. You can also see what mobile devices you have, where each device is located, and what state each device is in. The flexible reporting tools in Mobile Management let you identify any problems in your IT framework. You can then take immediate action to fix those problems from within the reports.

See [“Managing mobile devices”](#) on page 15.

## Components of Symantec Mobile Management

Symantec Mobile Management includes the following key features and benefits:

- Comprehensive mobile inventory. The inventory data gives you a complete view of the mobile devices in your organization.  
See [“About gathering inventory data from mobile devices”](#) on page 49.

- Intelligent software management. You can optimize licenses and detect, analyze, install, and update software. You can also take advantage of policies within Symantec Management Platform to target and schedule the devices that need software management.  
See [“About delivering software to mobile devices”](#) on page 63.
- Flexible remote assistance. Mobile Management lets you troubleshoot and fix mobile devices in any location. Using remote control sessions, you can take control of a mobile device to rapidly fix any problems that users experience.  
See [“About remotely managing mobile devices”](#) on page 73.

## How Symantec Mobile Management works

Using Symantec Installation Manager, you can quickly install Symantec Mobile Management. You can then quickly install and configure the Mobile Management server software and the Mobile Management Agent. The Mobile Management Server lets Notification Server communicate with the agent and with each mobile device.

See [“About installing and configuring Symantec Mobile Management”](#) on page 19.

After you configure Mobile Management, you can then choose from several options. For example, you can collect inventory data, take remote control of specific devices, or manage the software on each device. These features are installed on Symantec Management Platform and included with Mobile Management.

See [“Managing mobile devices”](#) on page 15.

## What you can do with Symantec Mobile Management

You can use Symantec Mobile Management to inventory and list your mobile devices. You specify how often and at what times you want to collect inventory data. You can also specify what information to collect. For example, you can choose to list all devices that need recharging soon or that don't have enough memory. You can organize the devices by manufacturer and by platform and operating system.

You can also choose to run reports and determine the status of each mobile device in your organization.

See [“About gathering inventory data from mobile devices”](#) on page 49.

Using the inventory and reporting information that's collected, you can then use remote control features to fix any problems with a specific device.

See [“About remotely managing mobile devices”](#) on page 73.

You can also manage the software on the mobile devices. For example, you can download and install initial applications or choose to update existing software on a specified schedule. You can also copy, move, or delete files, as well as create, delete, or rename folders.

See [“About delivering software to mobile devices”](#) on page 63.

Using Mobile Management, you can control all aspects of the mobile devices in your organization.



# Getting started with Mobile Management Solution

This chapter includes the following topics:

- [Managing mobile devices](#)
- [Viewing the Mobile Management Portal page](#)

## Managing mobile devices

After you install and configure Symantec Mobile Management and the supporting software, you can use it in many ways.

**Table 2-1** Process for managing mobile devices

Step	Action	Description
Step 1	Install and configure Mobile Management.	You can install Mobile Management from within Symantec Installation Manager. Then, you can install its supporting software and configure it.  See <a href="#">“About installing and configuring Symantec Mobile Management”</a> on page 19.
Step 2	(Optional) View the portal page for Mobile Management.	You can view information on the licenses in your environment and a list of all managed mobile devices.  See <a href="#">“Viewing the Mobile Management Portal page”</a> on page 16.

**Table 2-1** Process for managing mobile devices (*continued*)

Step	Action	Description
Step 3	(Optional) Configure the inventory settings and run reports.	You can collect inventory data according to a schedule that you define.  See <a href="#">“About gathering inventory data from mobile devices”</a> on page 49.
Step 4	(Optional) Configure the software schedule settings and manage software packages.	You can create mobile software packages and schedule their installation. You can also configure several package actions, such as running or stopping a process or copying, moving, deleting, or renaming files and folders.  See <a href="#">“About delivering software to mobile devices”</a> on page 63.
Step 5	(Optional) Configure the remote control settings and directly control mobile devices.	You can directly manage a remote device and access several of its subsystems, which includes the <b>File</b> , <b>System</b> , <b>Registry</b> , and <b>Processes</b> menus.  See <a href="#">“About remotely managing mobile devices”</a> on page 73.

## Viewing the Mobile Management Portal page

The **Mobile Management Portal** page contains a quick summary of how Mobile Management is used in your environment.

For example, the license status includes the status of any Mobile Management licenses. It also contains information on the license type, expiration date, total number of licenses, and how many licenses are currently in use.

From the links in the left pane of the portal page, you can also view other Mobile Management pages and reports.

See [“Managing mobile devices”](#) on page 15.

For more information, view topics on portal pages and Web parts in the *Symantec Management Platform Help*.

**To view the Mobile Management Portal page**

- ◆ In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.

From the **Mobile Management Portal** page, you can review the information that is contained in each Web part.



# Installing and configuring Mobile Management

This chapter includes the following topics:

- [About installing and configuring Symantec Mobile Management](#)
- [Viewing mobile devices in your resources list](#)
- [Automatically installing Mobile Management Server software](#)
- [Installing the Mobile Management Agent](#)
- [Changing the agent configuration schedule for mobile devices](#)

## About installing and configuring Symantec Mobile Management

You install Symantec Mobile Management from Symantec Installation Manager. For complete instructions and prerequisites, see the [Release Notes article](#).

After Mobile Management is installed, you can configure your mobile resources so that you can view them. You also need to install and configure the Mobile Management server software and the Mobile Management Agent.

See [“Viewing mobile devices in your resources list”](#) on page 20.

See [“Automatically installing Mobile Management Server software”](#) on page 20.

See [“Installing the Mobile Management Agent”](#) on page 21.

See [“Managing mobile devices”](#) on page 15.

See [“Changing the agent configuration schedule for mobile devices”](#) on page 23.

## Viewing mobile devices in your resources list

You need to configure your mobile resources so that you can properly view them and select them to install the server software on them.

See [“About installing and configuring Symantec Mobile Management”](#) on page 19.

For more information on resources, see the *Symantec Management Platform Help*.

### To view mobile resources in your resource list

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, click **Default**.
- 3 In the right pane, in the right corner, click **Filter**.
- 4 On the **Filter Visible Groups** page, expand the **All Resources** group.
- 5 Expand the **Asset > Network Resource** group.
- 6 Check **Mobile**.
- 7 Click **OK** to save your changes.

## Automatically installing Mobile Management Server software

You install the Mobile Management Server software to create a Mobile Management Server. This server lets Notification Server communicate with the Mobile Management Agent. The Mobile Management Servers page then lists all of your Mobile Management servers.

By default, the Mobile Management Server software installs on all Notification Server computers that have Microsoft Message Queue Service installed on them. These computers include the Notification Server computer that Mobile Management is installed on. The Mobile Management Server is installed on the next configuration update from the computers it is targeted to. By default, this process happens once an hour.

You can run install the server software on a remote server or you can run the installation on the Notification Server computer.

You must have the following software installed before you install the server software:

- IIS
- ASP.NET

- Microsoft Message Queuing

See “[About installing and configuring Symantec Mobile Management](#)” on page 19.

For more information, view topics about policies and schedules in the *Symantec Management Platform Help*.

#### To automatically install Mobile Management Server software and create a Mobile Management Server

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
  - 2 In the left pane, ensure that the **Settings > Mobile Management > Mobile Management Service > Policies** folders are expanded.
  - 3 Click **Mobile Management Service Install (x86)**.
  - 4 Click **Apply to** to specify the resources to install the software on.
    - The **Quick Apply** option lets you target an entire group of resources for the installation.
    - The **Computers** option lets you target specific resources for the installation.
- By default, the install policy targets all of the site servers that are listed in the **Site Servers Requiring Mobile Management Service Install** policy.
- 5 Specify when the installation update and the configuration update runs.
  - 6 Specify any other scheduling options.
  - 7 Click **Save changes**.

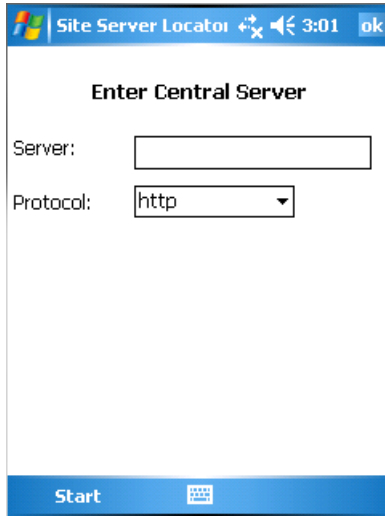
## Installing the Mobile Management Agent

After a Mobile Management Server is created, you can install the Mobile Management Agent on the mobile devices in your environment. The agent lets your mobile devices communicate back to the Mobile Management Server and Notification Server. You can install the agent from any Mobile Management Server and choose whether authentication is required to remotely control any mobile device.

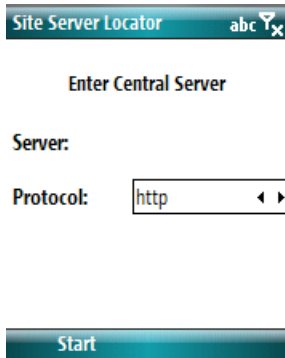
On the Mobile Management Server, ensure that IIS is configured to run on the default port. If IIS is configured to run on a non-default port, the administrator needs to manually enter the port on the Agent Install Page. This process ensures that you receive the proper URL to bootstrap the device or export the configuration file.

You are prompted to enter the location of the site server in the **Site Server Locator** screen on the device if Mobile Management cannot automatically detect it. .

**Figure 3-1** Pocket PC server location screen



**Figure 3-2** Smartphone server location screen



For a Windows CE mobile device, if the .NET Compact Framework is not already installed, you need to install it. This framework can be downloaded from the Mobile Management Server by using the following URL:

`http://MobileManagementServerName/MobileManagement/cf/`

See “[Changing the agent configuration schedule for mobile devices](#)” on page 23.

See “[About installing and configuring Symantec Mobile Management](#)” on page 19.

### To install the Mobile Management Agent

- 1 In your browser, go to the following URL:

`http://MobileManagementServer/MobileManagement`

This URL is listed in the Symantec Management Console, under **Settings > All Settings > Mobile Management > Mobile Agent Settings**, in the **Mobile Agent Install** page.

- 2 Enter the credentials if required.
- 3 Click **Open** to download the `locatesiteserver.cab` file.  
On older mobile devices (wince 4), this file might be the `locatesiteserver-wince4.cab` file.
- 4 Complete the rest of the installation process.

## Changing the agent configuration schedule for mobile devices

You can choose how often agent configuration updates are requested.

By default, agent configuration update requests happen every hour.

See [“Installing the Mobile Management Agent”](#) on page 21.

See [“About installing and configuring Symantec Mobile Management”](#) on page 19.

### To change the agent configuration schedule for mobile devices

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, ensure that the **Settings > Mobile Management > Mobile Agent Settings** folders are expanded.
- 3 Click **Agent Configuration Update Schedule**.
- 4 In the right pane, specify the configuration schedule information:
  - Number of units. For example, 6.
  - Type of unit. Either minutes, hours, or days.
- 5 Click **Save changes**.



# Securing device communications

This chapter includes the following topics:

- [About securing device communication](#)
- [Communication components of Mobile Management Solution](#)
- [About the device agent](#)
- [How the device agent and the mobile site service communicate](#)
- [Securing Mobile Management communications](#)
- [About obtaining certificates](#)
- [About using self-signed certificates](#)
- [Generating self-signed certificates with MakeCert](#)
- [Installing a server certificate on the mobile site service computer](#)
- [Configuring IIS to accept SSL connections](#)
- [Configuring the tunnel service to accept SSL connections](#)
- [Installing certificates on mobile devices](#)
- [About the certificate manager tool](#)
- [Certificate manager command-line switches](#)
- [Certificate Manager command-line examples](#)
- [Example for modifying the device agent configuration file for TLS/SSL tunnel connection](#)

- [Modifying device agent configuration files to specify a client certificate](#)
- [Example: modifying each client configuration file](#)
- [About access control](#)
- [User authentication levels](#)
- [Access levels for resources](#)
- [URL Resource Identifiers](#)
- [About RPC Resource Identifiers](#)

## About securing device communication

Symantec Mobile Management Solution enables organizations of all sizes to easily manage and support mobile devices in the field, or in the four walls. You can secure device communications for Symantec Mobile Management Solution.

The solution implements a multiple-layer approach to security that lets you take advantage of your existing web and Internet infrastructure. It lets you safely deploy the mobile devices that connect to, and are accessed from, corporate networks.

The device agent communicates with the mobile site service to perform tasks. It can provision devices software and settings, transmit hardware and software inventory, and establish a remote support tunnel connection. You can secure communications between the device agent and the mobile site service.

See [“Communication components of Mobile Management Solution”](#) on page 27.

Securing device communications involves the securing the following:

- **Data privacy**  
Involves enabling the 128-bit TLS/SSL connections and use of hypertext transfer protocol over TLS/SSL (HTTPS). This task secures data transmission between devices running the device agent and the mobile site service. It prevents unauthorized monitoring of the data that is transferred over the network.  
See [“How the device agent and the mobile site service communicate”](#) on page 28.
- **Authentication**  
Involves validating the certificates or validating the credentials that are used to establish connections between the device agent and mobile site service.  
See [“How the device agent and the mobile site service communicate”](#) on page 28.

- Access control configuration  
Involves restricting the access rights to resources based upon identity.  
See [“About access control”](#) on page 45.

## Communication components of Mobile Management Solution

The communication components of Mobile Management Solution include the following:

- Notification Server  
Notification Server includes the mobile management console Web interface and the mobile management web services.  
See [“How Symantec Mobile Management works”](#) on page 12.
- Device agent  
The device agent provides all of the essential elements for effective device management  
See [“About the device agent”](#) on page 27.
- Mobile site service  
The mobile site service communicates with the device agent to perform tasks. You can install the mobile site service on the same computer as Notification Server or on another computer.  
See [“Automatically installing Mobile Management Server software”](#) on page 20.

## About the device agent

Mobile Management Solution includes a modular device agent. The agent includes an integrated Web server and Web services engine. These parts are available for all the devices that run Microsoft Windows Mobile/CE software.

The agent is designed around open Internet standards and protocols such as HTTP/S, TLS/SSL, HTML, and SOAP. It is extensible through the use of services and plug-ins.

The agent provides all of the essential elements for effective device management, such as the following elements:

- Service discovery
- Hardware and software inventory collection
- Software and settings provisioning
- Online interactive support tools in real time, such as remote control.

See [“Communication components of Mobile Management Solution”](#) on page 27.

## How the device agent and the mobile site service communicate

The device agent initiates all connections between itself and the mobile site service. The mobile site service accepts these connections and coordinates various functions between the device agent and Notification Server. To establish secure communications, the device agent must be configured to use TLS/SSL for all of the connections.

TLS/SSL connections use an encrypted communications channel. All of the data that is transmitted over the channel is secure. In addition, you can perform authentication to verify the identity of the server or the client.

TLS/SSL connections include two levels of authentication: one-way authentication (server authentication) and mutual TLS/SSL authentication (client and server authentication). The Mobile Management device agent supports both levels of authentication. The most secure way to establish connections between the agent and the site service is by using certificates and mutual TLS/SSL authentication.

See [“Securing Mobile Management communications”](#) on page 29.

### One-way TLS/SSL authentication

One-way TLS/SSL authentication requires the server to pass its certificate and its certificate authority chain to the device agent. If the device agent trusts the certificate authority that issued the server certificate then a connection is made. If the certificate’s issuer on the server is trusted, the device agent can establish a TLS/SSL link between the device and the server. Only the server certificate passes from the server to the client. Therefore, only the server is authenticated and trusted. The user names and the passwords must be configured and transmitted to the server to approve the device agent to set up one-way TLS/SSL authentication.

**Mutual TLS/SSL authentication**

Mutual TLS/SSL authentication is the most secure way for the device agent to communicate with a server. It requires both the server and the device to authenticate by exchanging and validating certificates in each direction. When both sides pass certificates to each other to establish a TLS/SSL link, mutual certificate-based authentication by two-way TLS/SSL is established. Both the server and the device trust the identity of the other from their respective certificates.

Mutual TLS/SSL authentication assures that software updates, device settings, data files, multimedia files, and sensitive corporate data are not distributed to an untrustworthy recipient. The server cannot be configured to recognize an untrustworthy recipient as valid. If a device is stolen, you can revoke the device's client certificate on the server. The the device (and only that device) is immediately denied access to the server.

## Securing Mobile Management communications

The following process outlines how to configure data privacy between the mobile device agent and the mobile site service.

**Table 4-1** Process for securing Mobile Management communications

Step	Action	Description
Step 1	Obtain certificates for the mobile site service computer.	You must obtain SSL certificates from either a trusted issuer, such as VeriSign, or from your site infrastructure's existing SSL chain.  See <a href="#">"About obtaining certificates"</a> on page 32.

**Table 4-1** Process for securing Mobile Management communications  
*(continued)*

Step	Action	Description
Step 2	Obtain certificates for the mobile devices (mutual TLS/SSL authentication only).	<p>You must obtain SSL certificates from either a trusted issuer, such as VeriSign, or from your site infrastructure’s existing SSL chain.</p> <p>See <a href="#">“About obtaining certificates”</a> on page 32.</p> <p>This step is required for mutual TLS/SSL authentication only. If you plan to set up one-way TLS/SSL authentication, then this step is not necessary.</p> <p>See <a href="#">“How the device agent and the mobile site service communicate”</a> on page 28.</p>
Step 3	(Optional) Generate your own self-signed certificates.	<p>You can use a utility from the Windows SDK to generate your self-signed certificate.</p> <p>See <a href="#">“About using self-signed certificates”</a> on page 32.</p> <p>See <a href="#">“Generating self-signed certificates with MakeCert”</a> on page 33.</p>
Step 4	Install a server certificate on the mobile site service computer	<p>You must install a server certificate on the mobile site service computer.</p> <p>See <a href="#">“Installing a server certificate on the mobile site service computer”</a> on page 35.</p>
Step 5	Configure IIS to accept TLS/SSL connections.	<p>To secure mobile management communications, you must configure IIS to accept SSL connections</p> <p>See <a href="#">“Configuring IIS to accept SSL connections”</a> on page 36.</p>

**Table 4-1** Process for securing Mobile Management communications  
*(continued)*

Step	Action	Description
Step 6	Configure the tunnel service to accept TLS/SSL connections.	<p>You must configure the site service computer tunnel service to accept TLS/SSL connections.</p> <p>See <a href="#">“Configuring the tunnel service to accept SSL connections”</a> on page 37.</p>
Step 7	(Optional) Install the certificates on the mobile devices.	<p>You must install certificates on your mobile devices if you plan to use self-signed certificates, or if you plan to enable mutual TLS/SSL authentication.</p> <p>See <a href="#">“Installing certificates on mobile devices”</a> on page 38.</p> <p>This step is required for mutual TLS/SSL authentication. If you plan to set up one-way TLS/SSL authentication, step is not necessary.</p> <p>See <a href="#">“How the device agent and the mobile site service communicate”</a> on page 28.</p>
Step 8	Modify the device agent configuration file for a TLS/SSL tunnel connection.	<p>When using TLS/SSL, you must modify the device agent tunnel client configuration file to match that of the tunnel server configuration.</p> <p>See <a href="#">“Example for modifying the device agent configuration file for TLS/SSL tunnel connection ”</a> on page 42.</p>

**Table 4-1** Process for securing Mobile Management communications  
*(continued)*

Step	Action	Description
Step 9	Modify the device agent configuration files to specify the client certificate (mutual TLS/SSL authentication only).	<p>You must modify the agent configuration files to specify a client certificate.</p> <p>See <a href="#">“Modifying device agent configuration files to specify a client certificate”</a> on page 42.</p> <p>This step is required for mutual TLS/SSL authentication only. If you plan to set up one-way TLS/SSL authentication, this step is not necessary.</p> <p>See <a href="#">“How the device agent and the mobile site service communicate”</a> on page 28.</p>

## About obtaining certificates

You must obtain SSL certificates from either a trusted issuer, such as VeriSign, or from your site infrastructure’s existing SSL chain.

You must obtain SSL certificates for the following certificate authority (CA) certificates:

- A certificate authority (CA) certificate if using self-signed certificates. See [“About using self-signed certificates”](#) on page 32.
- A server certificate to install on the mobile site service computer. The agent uses this certificate to validate the site service's identity.
- A client certificate to install on the mobile device. The site service uses this certificate to validate the agent’s identity. This certificate is required only if you plan to set up Mutual TLS/SSL authentication.

See [“Securing Mobile Management communications”](#) on page 29.

## About using self-signed certificates

If you cannot obtain the SSL certificates from a trusted issuer, you should contact your company’s infrastructure security team to request the required certificates. As an alternative, you can use Microsoft Certificate Services to create certificates.

See “[About obtaining certificates](#)” on page 32.

See “[Securing Mobile Management communications](#)” on page 29.

Microsoft provides the following command-line certificate creation tools with the Microsoft Windows SDK:

**MakeCert**      MakeCert (MakeCert.exe) is a certificate creation tool that generates X.509 certificates. The tool creates a public and private key pair for digital signatures and stores it in a certificate file. This tool also associates the key pair with a specified publisher's name. The tool creates an X.509 certificate that binds a user-specified name to the public part of the key pair. MakeCert includes standard and extended options. Standard options are those that are most commonly used to create a certificate. Extended options provide more flexibility.

For information about MakeCert see:

[http://msdn.microsoft.com/en-us/library/bfskty3\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/bfskty3(VS.71).aspx).

See “[Generating self-signed certificates with MakeCert](#)” on page 33.

**Pvk2Pfx**      Pvk2Pfx (Pvk2Pfx.exe) is a command-line tool that copies public key and private key to a Personal Information Exchange (.PFX) file. This format is needed to import the server certificate. The keys are contained in .SPC, .CER, and .PVK files.

For information about Pvk2Pfx see:

<http://msdn.microsoft.com/en-us/library/dd434714.aspx>.

For information about Microsoft Certificate Services see:

[http://msdn.microsoft.com/en-us/library/aa376539\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa376539(VS.85).aspx) .

See “[Generating self-signed certificates with MakeCert](#)” on page 33.

See “[Installing a server certificate on the mobile site service computer](#)” on page 35.

## Generating self-signed certificates with MakeCert

The following instructions outline how to generate self-signed certificates using MakeCert on a desktop PC that has the Microsoft Windows SDK installed on it. The MakeCert tool is typically found in the following folder:

```
C:\Program Files\Microsoft SDKs\Windows\v6.0A\bin
```

See “[About using self-signed certificates](#)” on page 32.

See “[Securing Mobile Management communications](#)” on page 29.

## To generate a self-signed certificate with MakeCert

- 1 Open a command prompt and enter the following:

```
makecert -r -pe -n "CN= MyCompany" -sky signature -sv ca.pvk  
ca.cer
```

The command creates the following files:

ca.cer        The DER-encoded X.509 certificate.  
ca.pvk        The private key in Microsoft's proprietary PVK format.

This step creates a trusted certificate authority named *MyCompany*. The certificate authority can be used for signing and validation purposes on both the server and the client.

If the devices reach the server using the URL:

<https://mobiles.MyCompany.com>, the trusted authority name can be: "*MyCompany*".

- 2 Enter the following command:

```
makecert -pe -n "CN= mobiles/MyCompany.com" -sky exchange -eku  
1.3.6.1.5.5.7.3.1 -ic ca.cer -iv ca.pvk -sv server.pvk server.cer
```

The command creates the following files for the server certificate:

server.cer    The DER-encoded X.509 certificate.  
server.pvk    The private key in Microsoft's proprietary PVK format.

---

**Note:** You should change "*mobiles/MyCompany.com*" to match the host name and domain of your mobile site service computer.

---

**3** Enter the following command:

```
pvk2pfx -pvk server.pvk -spc server.cer -pfx server.pfx -f
```

The command creates the following file:

```
server.pfx
```

X.509 certificate in Microsoft's proprietary PFX format containing public and private keys.

This step creates a server certificate that the mobile device agent can use to validate your mobile site service computer's identity. The new trusted certificate authority that you created in the previous steps signed the server certificate.

---

**Note:** If the client reaches the server with the URL: `https://mobiles.MyCompany.com` then the common name is: `mobiles/MyCompany.com`.

If the client reaches the server with the URL: `https://mobiles/MyVirtual` the common name is `mobiles`.

---

**4** Enter the following command:

```
makecert -pe -n "CN=!Client1" -sky exchange -ic ca.cer -iv ca.pvk  
-sv client1.pvk client1.cer
```

The command creates the following files:

```
client1.cer
```

The DER-encoded X.509 certificate.

```
client1.pvk
```

The private key in Microsoft's proprietary PVK format.

This step creates a client certificate named `!Client1`. The Web server can use the certificate to validate the device agent's identity. The trusted certificate authority signed the client certificate.

## Installing a server certificate on the mobile site service computer

The following instructions explain how to install a certificate on the mobile site service computer.

See [“Securing Mobile Management communications”](#) on page 29.

#### To install a server certificate on the mobile site service computer

- 1 In windows, click **Start > run**, then enter `mmc`.
- 2 Click **Computer account**.
- 3 Click **Local computer**.
- 4 Right-click the **Personal** folder then click **All Tasks > Import**.
- 5 Follow the wizard to import the server certificate into the **Personal** store.

When using self-signed certificates, you must also import the certificate authority certificate. If you followed the example for creating self-signed certificates with `MakeCert.exe`, click **server.pfx**.

See [“Generating self-signed certificates with MakeCert”](#) on page 33.

- 6 Right-click the **Trusted Root Authorities** folder, then click **All Tasks > Import**.
- 7 Follow the wizard to import the certificate authority into the **Trusted Root Authorities** store.

If you followed the example for creating self-signed certificates with `MakeCert.exe`, click **ca.cerif**.

See [“Generating self-signed certificates with MakeCert”](#) on page 33.

## Configuring IIS to accept SSL connections

The following procedure explains how to configure Internet Information Server (IIS) to accept SSL connections.

See [“Securing Mobile Management communications”](#) on page 29.

To configure Internet Information Server (IIS) to accept SSL connections:

- 1 Click **Start > Administrative Tools > Internet Information Services**.
- 2 Right-click **Default Web Site**, then click **Properties**.
- 3 Click the **Directory Security** tab.
- 4 Under **Secure Communications**, click **Server Certificate**.
- 5 Click **Assign an Existing Certificate**.
- 6 Follow the rest of the wizard steps to assign the server certificate.
- 7 Click **OK**.
- 8 In the treeview pane, click **Web Sites > Default Web Site > MobileManagement**.
- 9 Right-click **MobileManagement** and then click **Properties**.

- 10 Under **Secure Communications**, click **Edit**.
- 11 Click **Require Secure Channel (SSL)**.
- 12 If you plan to validate client certificates, click **Require Client Certificates**.

---

**Note:** This step is required for mutual TLS/SSL authentication only. If you plan to set up one-way TLS/SSL authentication, then this step is not necessary.

---

See [“How the device agent and the mobile site service communicate”](#) on page 28.

- 13 Click **OK**.
- 14 Click **Web Sites > Default Web Site > SymantecMobileServices** in the treeview pane.
- 15 Right-click **SymantecMobileServices** and then click **Properties**.
- 16 Under **Secure Communications**, click **Edit**.
- 17 Click **Require Secure Channel (SSL)**.
- 18 If you plan to validate client certificates, click **Require Client Certificates**.

---

**Note:** This step is required for mutual TLS/SSL authentication only. If you plan to set up one-way TLS/SSL authentication, this step is not necessary.

---

See [“How the device agent and the mobile site service communicate”](#) on page 28.

- 19 Click **OK**.

## Configuring the tunnel service to accept SSL connections

You must configure the site service computer tunnel service to accept SSL connections to secure mobile management communications.

See [“Securing Mobile Management communications”](#) on page 29.

To configure the tunnel service to accept SSL connections:

- 1 Gather the following information:
  - Server certificate issuer.
  - Server certificate subject substring.

- Client certificate issuer (required only for mutual TLS/SSL authentication). See “How the device agent and the mobile site service communicate” on page 28.
  - Client certificate subject substring (required only for mutual TLS/SSL authentication). See “How the device agent and the mobile site service communicate” on page 28.
- 2 Modify the tunnel service configuration file (`TunnelServer.exe.config`). This file is typically located in the following folder on the mobile site service computer:
- ```
C:\Program Files\Symantec\Mobile Management\TunnelServer
```
- 3 Perform one of the following changes to the `Port=7780` binding in the `<Bindings>` section of the tunnel service configuration file:
- For one-way TLS/SSL, you must remove the `<ClientCertificates>` section within the binding. For example:

```
<Add Port="7780" Address="0.0.0.0" AllowInternal="true"
AllowExternal="false" CertificateIssuer="MyCompany"
CertificateSubject="mobiles">
</Add>
```
  - For mutual TLS/SSL authentication, add a `<ClientCertificates>` section within the binding, and then add items to this section for the required client certificate validation. For example:

```
<Add Port="7780" Address="0.0.0.0" AllowInternal="true" AllowExternal="f
<ClientCertificates>
<Add Issuer="MyCompany" Subject="!Client" Username="" Password="" Authen
</ClientCertificates>
</Add>
```
- 4 Restart the tunnel service for the new binding to take effect.

## Installing certificates on mobile devices

You must install certificates on your mobile devices if either of the following conditions are true:

- You use self-signed certificates.
- You enable mutual TLS/SSL authentication.

If you obtain a server certificate from a trusted authority and use one-way TLS/SSL, you do not need to install certificates on your devices.

See [“How the device agent and the mobile site service communicate”](#) on page 28.

See [“Securing Mobile Management communications”](#) on page 29.

#### To install certificates on mobile devices

- 1 Copy (or distribute) the client certificates to a folder on your mobile device. If you use self-signed certificates, you must also include the certificate authority certificate.

If you followed the example for creating self-signed certificates with `MakeCert.exe`, the following files are included:

- `ca.cer`
- `client1.cer`
- `client1.pvk`

- 2 Run **Certificate Manager** (`CertMan.exe`) on the device.

See [“About the certificate manager tool”](#) on page 39.

- 3 Import the client certificate into the **User Certificates/Personal** store.

If you followed the example for creating self-signed certificates with `MakeCert.exe`, click `client1.cer`.

- 4 If you use self-signed certificates, import the certificate authority certificate.

- 5 Import the certificate authority certificate into the **System Certificates/Trusted Root Certification Authorities** store.

If you followed the example for creating self-signed certificates with `MakeCert.exe`, click `ca.cer`.

## About the certificate manager tool

You can use the certificate manager tool (`CertMan.exe`) to install or remove certificates on a device. The device agent installation includes this tool. You can usually find it on the device in the **Start > Programs** menu.

The certificate manager tool provides PKI certificate Management Services on Windows Mobile/CE devices. The Windows Mobile version is designed to run on any device, including any Professional and Standard edition devices. The tool lets you browse the system certificate stores, and import and delete certificates.

The import functionality is limited to DER-encoded X.509 (.CER) files. However, it can also import private keys in Microsoft's proprietary .PVK format. When you

import a .cer file, a matching .PVK file is also imported. The .PVK file is associated with the certificate. If no .PVK file is found, only the certificate is imported.

The certificate manager tool supports a variety of command line switches. You can use the switches to automate the installation and removal of certificates on mobile devices.

See “[Certificate manager command-line switches](#)” on page 40.

## Certificate manager command-line switches

Certificate manager supports the following command line switches:

See “[About the certificate manager tool](#)” on page 39.

**Table 4-2** Certificate Manager command-line switches

| Command-line switch                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/hidden</code>                           | Causes the application to run invisibly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>/action:&lt;import   delete&gt;</code>   | <p>Specifies the action to perform.</p> <p>The import action imports the certificate into the store where <code>/import-file</code> specifies the certificate and <code>/store-type</code> and <code>/store-name</code> identify the store.</p> <p>The delete action deletes one or more certificates from the store where <code>/store-type</code> and <code>/store-name</code> identify the store and <code>/delete-issuer</code>, <code>/delete-subject</code>, and <code>/delete-expired</code> criteria options determine the certificates to delete. The certificate must match all of the given criteria to be deleted.</p> |
| <code>/store-type:&lt;user   system&gt;</code> | Specifies the location of the certificate store. The only valid types are user and system. Required by <code>/action:import</code> and <code>/action:delete</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>/store-name:&lt;name&gt;</code>          | Specifies the name of the certificate store. Typical names include MY, CA, and ROOT. Required by <code>/action:import</code> and <code>/action:delete</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 4-2** Certificate Manager command-line switches (*continued*)

| Command-line switch                          | Description                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/import-file:&lt;file&gt;</code>       | The <code>/action:import</code> command requires this switch. The <code>&lt;file&gt;</code> specification must be the path to a DER-encoded X.509 file with a <code>.cer</code> extension. Relative paths are relative to the location of the executable. If a matching <code>.PVK</code> file exists, the private key is imported. |
| <code>/delete-issuer:&lt;issuer&gt;</code>   | Causes <code>/action:delete</code> to delete certificates only where the <code>Issuer</code> fields contain the <code>&lt;issuer&gt;</code> substring. The substring search is case-insensitive.                                                                                                                                    |
| <code>/delete-subject:&lt;subject&gt;</code> | Causes <code>/action:delete</code> to only delete certificates where the <code>Subject</code> fields contain the <code>&lt;subject&gt;</code> substring. The substring search is case-insensitive.                                                                                                                                  |
| <code>/delete-expired</code>                 | Causes <code>/action:delete</code> to delete only expired certificates.                                                                                                                                                                                                                                                             |

## Certificate Manager command-line examples

You can use the following Certificate Manager command-line examples:

See [“About the certificate manager tool”](#) on page 39.

See [“Certificate manager command-line switches”](#) on page 40.

- Import `ca.cer` into the user root store:

```
/action:import /store-type:user /store-name:ROOT /import-file:"ca.cer"
```

- Import `client1.CER` and `client1.PVK` into the user personal store:

```
/action:import /store-type:user /store-name:MY /import-file:"client1.cer"
```

- Delete all expired certificates from the user personal store:

```
/action:delete /store-type:user /store-name:MY /delete-expired
```

- Delete all certificates from the user personal store that `"MyCompany"` issued:

```
/action:delete /store-type:user /store-name:MY /delete-issuer:"MyCompany"
```

## Example for modifying the device agent configuration file for TLS/SSL tunnel connection

When you use TLS/SSL, you must modify the device agent tunnel client configuration file (`Tclient.CFG`) to match the tunnel server configuration. The device agent configuration files are typically located in the following folder:

`C:\Program Files\Altiris\MobileManagement\Packages\athena\config`

See [“Securing Mobile Management communications”](#) on page 29.

The following is an example of how to modify the device agent tunnel client configuration file to enable one-way TLS/SSL connections.

This example assumes that you followed the example for creating self-signed certificates with `MakeCert.exe`.

See [“Generating self-signed certificates with MakeCert”](#) on page 33.

### Tclient.cfg

```
#
# Define the list of servers.
#
# At least one entry is required.
#
# Each entry consists of 2 to 5 arguments:
#
# <host> <port> [flags] [issuer] [subject]
#
# <host>      Host Name or IP Address
# <port>      Port Number (1 to 65535)
# [flags]     The sum of the following integers:
#             1 - Use SSL
#             2 - Ignore SSL Certificate Errors
# [issuer]    Client Certificate Issuer Substring
# [subject]   Client Certificate Subject Substring
#
SERVER {SERVERNAME} 7780 1
```

## Modifying device agent configuration files to specify a client certificate

You must modify the agent configuration files and specify a client certificate to set up mutual TLS/SSL authentication.

This step is required for mutual TLS/SSL authentication only. If you plan to set up one-way TLS/SSL authentication, then this step is not necessary.

See [“How the device agent and the mobile site service communicate”](#) on page 28.

See [“Securing Mobile Management communications”](#) on page 29.

The following modules are the four device agent modules that establish connections with the mobile site service:

- **Tracker**  
Performs the registration tasks for the device.
- **LogManager**  
Performs the hardware inventory tasks and software inventory tasks.
- **AppUpdate**  
Performs the software delivery tasks.
- **TunnelClient**  
Establishes a remote support tunnel connection.

Each module has a supporting configuration file that defines the client certificate to use for SSL communications, along with other relevant settings, for example `Athena-Tracker.CFG`, `Athena-LogManager.CFG`, `AppUpdate.XML`, and `Tclient.CFG`.

The device agent configuration files are typically located in the following folder:

```
C:\Program Files\Altiris\MobileManagement\Packages\athena\config
```

#### **To modify the device agent configuration files to specify a client certificate**

- ◆ Set the client certificate directive on each of the configuration file.  
Do this step if you require mutual TLS/SSL authentication and have also configured IIS and the Tunnel Server for client authentication.  
See [“Example: modifying each client configuration file”](#) on page 43.

## **Example: modifying each client configuration file**

The following is an example of how to modify each configuration file.

See [“Modifying device agent configuration files to specify a client certificate”](#) on page 42.

This example assumes that you followed the example for creating self-signed certificates with `MakeCert.exe`.

See [“Generating self-signed certificates with MakeCert”](#) on page 33.

**Athena-Tracker.cfg**

**Example: modifying each client configuration file**

```
#
# Define the SSL certificate to use for client authentication.
#
# The default value is an empty string, which means no client
# authentication is performed. Setting a valid certificate
# subject substring causes the client to authenticate itself to the
# server when required. The certificate must exist in the "My" store
# under HKEY_CURRENT_USER.
#
CLIENT_CERT !Client
```

**Athena-LogManager.cfg**

```
#
# Define the SSL certificate to use for client authentication.
#
# The default value is an empty string, which means no client
# authentication is performed. Setting a valid certificate
# subject substring causes the client to authenticate itself to the
# server when required. The certificate must exist in the "My" store
# under HKEY_CURRENT_USER.
#
MACRO $$RpcCertificate !Client
```

**AppUpdate.xml**

```
<!--
=====
Define the SSL certificate to use for client authentication.
When client authentication is requested, the personal store is searched for
a certificate with an issuer containing this value. If that fails, a search
on certificate subject is performed. Both searches are case-insensitive.
Default Value: (None)
=====
-->
<value name="Certificate">!Client</value>
```

**Tclient.cfg**

```
#
# Define the list of servers.
#
# At least one entry is required.
#
# Each entry consists of 2 to 5 arguments:
```

```
#  
# <host> <port> [flags] [issuer] [subject]  
#  
# <host>      Host Name or IP Address  
# <port>      Port Number (1 to 65535)  
# [flags]     The sum of the following integers:  
#             1 - Use SSL  
#             2 - Ignore SSL Certificate Errors  
# [issuer]    Client Certificate Issuer Substring  
# [subject]   Client Certificate Subject Substring  
#  
SERVER {SERVERNAME} 7780 1 "MyCompany" "!Client"
```

## About access control

The main configuration file of the mobile device, which is `Athena.CFG`, contains two sections that define access control. The `USER` section of the file is used to define authentication (user names, access levels, and password digests). The `LEVEL` section is used to define access control (access levels for resources).

See [“User authentication levels”](#) on page 45.

See [“Access levels for resources”](#) on page 46.

See [“URL Resource Identifiers”](#) on page 46.

See [“URL Resource Identifiers”](#) on page 46.

See [“About RPC Resource Identifiers”](#) on page 47.

## User authentication levels

The `USER` keyword is used to define an authorized device agent user. The first argument is the user name. The second argument is a 32-bit integer that defines the user access level (defaults to zero). The third argument is a password digest (defaults to empty).

The following is an example of how to define users:

```
USER user 1 {SMD5}uOo1ZcS3waDbExjq2hcIG/1NaftyzS3s  
USER admin 9 {SMD5}PUaJo8NDqpXo5MP7DO5c6hIawCXcnPNB
```

The access level that is assigned to a user name is an integer value ranging from 0 to `N`. Zero represents the lowest access level, and `N` represents the highest access level. You can design your own security scheme or access profile with a custom

access level range to fit. For example, 0-4, 0-10, 0-100, etc. Consider using a scheme where each value is equivalent to a security role or group.

The following is an example that defines a range of 0-4:

- 1 = Tier one Help Desk users
- 2 = Tier two Help Desk users
- 3 = Tier three Help Desk users
- 4 = Super Administrator users

The access levels would then be assigned to each device agent resource identifier.

See [“Access levels for resources”](#) on page 46.

See [“About access control”](#) on page 45.

## Access levels for resources

The LEVEL keyword is used to assign access levels to resource identifiers.

The first argument following the LEVEL keyword is a URL or RPC resource identifier.

The second argument is the required user access level. URL and RPC resource identifiers can contain wildcards. The default level for any unlisted resource is zero.

The following is an example of how to define access levels for resources:

```
LEVEL URL:* 1
LEVEL RPC:FileManager.CreateFolder 2
```

See [“About access control”](#) on page 45.

## URL Resource Identifiers

A URL resource identifier is used to control access to any device agent Web (HTML) page (or any URL GET request by the browser).

The first entry in the example defines that the user must have access level 1 or higher to access any (\*) device agent web (HTML) page. The minimum level of access control for the device agent is enabled.

The second entry defines that the user must have access level 3 or higher to access the FileManager/upload.html page.

The following is an example of URL resource identifiers:

```
LEVEL URL:* 1
LEVEL URL:FileManager/upload.html 3
```

See “[About access control](#)” on page 45.

## About RPC Resource Identifiers

The LEVEL keyword can define access to specific RPC (SOAP) functions that the device agent services expose.

The first entry defines that the user must have access level 2 or higher to access any function provided by the Configuration service.

The second and third entries define the minimum access level to perform the FileManager.ListFiles and FileManager.DeleteFile functions. It works the same for all of the device agent services. For a full list of RPC functions, see the device agent configuration file (Athena.CFG).

The following is an example of RPC resource identifiers:

```
LEVEL RPC:Configuration.* 2
LEVEL RPC:FileManager.ListFiles 1
LEVEL RPC:FileManager.DeleteFile 2
```

A special case is the authorization for the remote control service. It is handled through a combination of URL resource identifiers and special logic. The special logic is between the Athena service host, the remote control service, and the Java client applet.

The Java client applet connects using TCP/SSL to the remote control service on a different port. By default the port is 7777, but it can be configured to use any port. This case prevents anyone from directly running the Java client and successfully establishing a remote control session without authenticating through the Athena service host. This example works like the email servers that authenticate through a POP account within a time window before you can use SMTP. The remote control security works the same way. You must authenticate through the Athena service host (HTTP/S) within a certain time window. You must authenticate before the Java client can establish a remote control session with the remote control service over TCP/SSL.

The agent validates the credentials against the USER section. It grants or denies access. Access is based on the minimum access level for the requested resource identifier versus the access level that is assigned to the user. The minimum access level is defined in the LEVEL section.

See “[About access control](#)” on page 45.



# Gathering inventory data from mobile devices

This chapter includes the following topics:

- [About gathering inventory data from mobile devices](#)
- [Changing the schedule for mobile device inventory](#)
- [About the Heartbeat value for mobile devices](#)
- [Running and viewing reports for mobile devices](#)
- [Battery information fields](#)
- [Battery constants](#)
- [OS version information fields](#)
- [OS version constants](#)
- [System information fields](#)
- [System constants](#)
- [Processor level values](#)
- [Memory information fields](#)

## About gathering inventory data from mobile devices

You can set how often inventory data is collected. You can also choose how often and at what time the information is then sent to Mobile Management Server and then to Notification Server.

The **Reports** feature in Symantec Management Platform lets you view inventory data for all of the mobile devices in your environment. You can also view inventory data for a specific device from that device's **Resource Manager** page, on the **View** menu, under **Inventory**.

The standard reports in Mobile Management contain some audit reports. These reports are updated whenever a reportable action occurs on a mobile device. Depending on the load on the system, it might take a moment for the report to receive the updated information.

See [“Changing the schedule for mobile device inventory”](#) on page 50.

See [“Running and viewing reports for mobile devices”](#) on page 51.

See [“Managing mobile devices”](#) on page 15.

For more information, view topics on reports and inventory in the *Symantec Management Platform Help*.

## Changing the schedule for mobile device inventory

You can set the schedule for how often inventory data is collected and sent to Notification Server.

The sample schedule specifies when data is collected from a mobile device. The transmit schedule specifies when the collected data is sent to the Mobile Management Server and then to Notification Server. You can reduce your network load by collecting several data samples from a mobile device before sending it. By default, Mobile Management collects data every six hours and transmits that data once a day. If you use the default schedule, Mobile Management collects four inventories in a day, and then transmits the data one time as a compressed transmission.

The times that you select to collect and transmit data coordinate with the time on the specific mobile device, not the Mobile Management Server computer.

If you select days as the type of unit, you can also specify the time when the inventory data is collected and sent.

See [“About gathering inventory data from mobile devices”](#) on page 49.

### To change the schedule for mobile device inventory

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, ensure that the **Settings > Mobile Management > Mobile Agent Settings** folders are expanded.
- 3 Click **Inventory Schedule**.

- 4 Specify the **Sample** schedule information:
  - Number of units. For example, 6.
  - Type of unit. Either hours or days.
  - Hour and minutes. For example, 20:30.
- 5 Specify the **Transmit** schedule information:
  - Number of units. For example, 2.
  - Type of unit. Either hours or days.
  - Hours and minutes. For example, 22:00.
- 6 Specify the **Heartbeat** schedule in minutes.  
See [“About the Heartbeat value for mobile devices”](#) on page 51.
- 7 Click **Save changes**.

## About the Heartbeat value for mobile devices

You can set the **Heartbeat** value on the Inventory Schedule page.

See [“Changing the schedule for mobile device inventory”](#) on page 50.

The first time this value is used it specifies when the mobile device is created as a resource.

Subsequently, this value indicates when the mobile device checks into the Mobile Management Server and updates networking information. For example, where the mobile device is and how to connect to it.

On the mobile device side, the **Heartbeat** checks hardly affects the CPU load. The bandwidth it consumes is also minimal. Basically, the **Heartbeat** process is an HTTP get command with some query string parameters. The exact amount of bandwidth that it consumes is variable and depends on the number of network interfaces that Mobile Management discovers.

## Running and viewing reports for mobile devices

You can choose from a long list of standard Mobile Management reports that provide information about each mobile device in your organization. The reports contain summary information, such as lists of devices by manufacturer or platform and operating system. For example, you can also choose to run and view the reports that list the devices that are running out of memory or battery power.

Each report runs when you select it and automatically updates with the latest information that you can review.

Most reports contain the information that you can customize. This information includes options such as whether you want the latest information or information from the last report that was saved. In some reports, you can also choose the timeframe that the information is collected from.

See [“About gathering inventory data from mobile devices”](#) on page 49.

Inventory data is collected and sent to Notification Server according to the schedule you set.

See [“Changing the schedule for mobile device inventory”](#) on page 50.

#### To run and view reports for mobile devices

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, ensure that the **Reports > Mobile Management** folders are expanded.
- 3 Click one of the standard reports that are listed.

In the right pane, the report runs and then displays the gathered data.

See [“Battery information fields”](#) on page 52.

See [“OS version information fields”](#) on page 55.

See [“System information fields”](#) on page 56.

See [“Memory information fields”](#) on page 60.

## Battery information fields

The **Devices with Low Battery** report contains information about the health of the battery in each mobile device.

See [“Running and viewing reports for mobile devices”](#) on page 51.

**Table 5-1** Battery information fields

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACLineStatus</b>             | <p>The AC power status.</p> <p>The following values are defined for this field. All other values are reserved.</p> <ul style="list-style-type: none"> <li>■ 0 Offline</li> <li>■ 1 Online</li> <li>■ 255 Unknown status</li> </ul>                                                                                                                                                         |
| <b>BatteryFlag</b>              | <p>The battery charge status.</p> <p>Contains a combination of the following values:</p> <ul style="list-style-type: none"> <li>■ BATTERY_FLAG_HIGH</li> <li>■ BATTERY_FLAG_CRITICAL</li> <li>■ BATTERY_FLAG_CHARGING</li> <li>■ BATTERY_FLAG_NO_BATTERY</li> <li>■ BATTERY_FLAG_UNKNOWN</li> <li>■ BATTERY_FLAG_LOW</li> </ul> <p>See “<a href="#">Battery constants</a>” on page 55.</p> |
| <b>BatteryLifePercent</b>       | <p>The percentage of a full battery charge that is left. This number can be a value in the range of 0 to 100, or it is 255 if the status is unknown. All other values are reserved.</p>                                                                                                                                                                                                    |
| <b>Reserved1</b>                | <p>Reserved. Set to zero.</p>                                                                                                                                                                                                                                                                                                                                                              |
| <b>BatteryLifeTime</b>          | <p>The number of seconds of battery life that is left. 0xFFFFFFFF if the remaining number of seconds are unknown.</p>                                                                                                                                                                                                                                                                      |
| <b>Reserved2</b>                | <p>Reserved. Set to zero.</p>                                                                                                                                                                                                                                                                                                                                                              |
| <b>BackupBatteryFlag</b>        | <p>The backup battery charge status. Contains a combination of the values that are listed in this table as the description for <b>BatteryFlag</b>.</p> <p>See “<a href="#">Battery constants</a>” on page 55.</p>                                                                                                                                                                          |
| <b>BackupBatteryLifePercent</b> | <p>The percentage of the full backup battery charge that is left. This number must be in the range of 0 to 100, or BATTERY_PERCENTAGE_UNKNOWN.</p>                                                                                                                                                                                                                                         |
| <b>Reserved3</b>                | <p>Reserved. Set to zero.</p>                                                                                                                                                                                                                                                                                                                                                              |

**Table 5-1** Battery information fields (*continued*)

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BackupBatteryLifeTime</b>     | The number of seconds of battery life that is left. BATTERY_LIFE_UNKNOWN if the remaining number of second are unknown.                                                                                                                                                                                                                                                                                                                                        |
| <b>BackupBatteryFullLifeTime</b> | The number of seconds of backup battery life when the battery is fully charged. BATTERY_LIFE_UNKNOWN if the fully charged time is unknown.                                                                                                                                                                                                                                                                                                                     |
| <b>BatteryVoltage</b>            | The amount of battery voltage in millivolts (mV). This number is in the range of 0 to 65,535.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>BatteryCurrent</b>            | The amount of instant current drain in milliamperes (mA). This number is in the range of 0 to 32,767 for charge, or 0 to -32,768 for discharge.                                                                                                                                                                                                                                                                                                                |
| <b>BatteryAverageCurrent</b>     | The short-term average of device current drain in milliamperes (mA). This number is in the range of 0 to 32,767 for charge, or 0 to -32,768 for discharge.                                                                                                                                                                                                                                                                                                     |
| <b>BatteryAverageInterval</b>    | The time constant in milliseconds that is used in reporting the <b>BatteryAverageCurrent</b> field.                                                                                                                                                                                                                                                                                                                                                            |
| <b>BatterymAHourConsumed</b>     | The long-term average discharge in milliamperes per hour. This number is in the range of 0 to -32,768. The number can be reset by charging or changing the batteries.                                                                                                                                                                                                                                                                                          |
| <b>BatteryTemperature</b>        | The battery temperature in degrees Celsius (C). This number is i the range of -3,276.8 to 3,276.7, in increments of 0.1 C degree.                                                                                                                                                                                                                                                                                                                              |
| <b>BackupBatteryVoltage</b>      | The backup battery voltage in millivolts (mV).                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Battery Chemistry</b>         | The type of battery.<br>The following values are defined for this field: <ul style="list-style-type: none"> <li>■ Alkaline BATTERY_CHEMISTRY_ALKALINE</li> <li>■ Cadmium BATTERY_CHEMISTRY_NICD</li> <li>■ Nickel metal hydride BATTERY_CHEMISTRY_NIMH</li> <li>■ Lithium ion BATTERY_CHEMISTRY_LION</li> <li>■ Lithium polymer BATTERY_CHEMISTRY_LIPOLY</li> <li>■ Zinc air BATTERY_CHEMISTRY_ZINCAIR</li> <li>■ Unknown BATTERY_CHEMISTRY_UNKNOWN</li> </ul> |

## Battery constants

The following constants are defined for battery information:

- 0x01 BATTERY\_FLAG\_HIGH
- 0x02 BATTERY\_FLAG\_LOW
- 0x04 BATTERY\_FLAG\_CRITICAL
- 0x08 BATTERY\_FLAG\_CHARGING
- 0x80 BATTERY\_FLAG\_NO\_BATTERY
- 0xFF BATTERY\_FLAG\_UNKNOWN

See [“Battery information fields”](#) on page 52.

## OS version information fields

Mobile Management collects the information in this section so that you can view it in various reports.

See [“Running and viewing reports for mobile devices”](#) on page 51.

**Table 5-2** OS version information fields

| Field               | Description                                                                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MajorVersion</b> | The major version number of the OS. For example, the major version number is 2 for Windows CE 2.10.                                                                                                                                                                                                                             |
| <b>MinorVersion</b> | The minor version number of the OS. For example, the minor version number is 1 for Windows CE 2.10.                                                                                                                                                                                                                             |
| <b>BuildNumber</b>  | The build number of the OS, or zero.                                                                                                                                                                                                                                                                                            |
| <b>PlatformId</b>   | The value that identifies the OS.<br>The following constants are defined for this value: <ul style="list-style-type: none"> <li>■ VER_PLATFORM_WIN32s</li> <li>■ VER_PLATFORM_WIN32_WINDOWS</li> <li>■ VER_PLATFORM_WIN32_NT</li> <li>■ VER_PLATFORM_WIN32_CE</li> </ul> See <a href="#">“OS version constants”</a> on page 56. |
| <b>CSDVersion</b>   | A null-terminated string that provides additional, arbitrary information about the OS.                                                                                                                                                                                                                                          |

## OS version constants

The following constants are defined for OS version information:

- 0 VER\_PLATFORM\_WIN32s for Windows 3.1 OS
- 1 VER\_PLATFORM\_WIN32\_WINDOWS for Windows 95 or 98  
 For Windows 95, **dwMinorVersion** is zero.  
 For Windows 98, **dwMinorVersion** is greater than zero.
- 2 VER\_PLATFORM\_WIN32\_NT
- 3 VER\_PLATFORM\_WIN32\_HH
- 3 VER\_PLATFORM\_WIN32\_CE

See “[OS version information fields](#)” on page 55.

## System information fields

Mobile Management collects the information in this section so that you can view it in various reports.

See “[Running and viewing reports for mobile devices](#)” on page 51.

**Table 5-3** System information fields

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OemId</b>                 | A string that identifies the OEM.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>ProcessorArchitecture</b> | <p>The architecture for the system’s processor.</p> <p>The following values are defined for this field:</p> <ul style="list-style-type: none"> <li>■ PROCESSOR_ARCHITECTURE_INTEL</li> <li>■ PROCESSOR_ARCHITECTURE_MIPS</li> <li>■ PROCESSOR_ARCHITECTURE_UNKNOWN</li> <li>■ PROCESSOR_ARCHITECTURE_SHX</li> <li>■ PROCESSOR_ARCHITECTURE_ARM</li> </ul> <p>See “<a href="#">System constants</a>” on page 58.</p> |
| <b>Reserved</b>              | Reserved for future use.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>PageSize</b>              | The size of the page and the granularity of page protection and commitment. This number is the same page size that the <b>VirtualAlloc</b> function uses.                                                                                                                                                                                                                                                           |

**Table 5-3** System information fields (*continued*)

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ActiveProcessorMask</b>   | A bit mask that represents the set of processors that are configured into the system. Bit 0 is processor 0; bit 31 is processor 31.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>NumberOfProcessors</b>    | The number of processors that are in the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>ProcessorType</b>         | <p>The type of each processor that is in the system. This field is no longer relevant. Instead, use the <b>wProcessorArchitecture</b>, <b>wProcessorLevel</b>, and <b>wProcessorRevision</b> fields to determine the type of each processor.</p> <p>The following values are defined for this flag:</p> <ul style="list-style-type: none"> <li>■ PROCESSOR_INTEL_386</li> <li>■ PROCESSOR_INTEL_486</li> <li>■ PROCESSOR_INTEL_PENTIUM</li> <li>■ PROCESSOR_INTEL_PENTIUMII</li> <li>■ PROCESSOR_MIPS_R4000</li> <li>■ PROCESSOR_HITACHI_SH3</li> <li>■ PROCESSOR_HITACHI_SH4</li> <li>■ PROCESSOR_STRONGARM</li> <li>■ PROCESSOR_ARM720</li> <li>■ PROCESSOR_MIPS_R5000</li> <li>■ PROCESSOR_SHxSH3DSP</li> </ul> <p>See “<a href="#">System constants</a>” on page 58.</p> |
| <b>AllocationGranularity</b> | The granularity with which virtual memory is allocated. For example, a <b>VirtualAlloc</b> request to allocate a byte reserves an address space of <b>dwAllocationGranularity</b> . This value was hard coded as 64 KB in length, but other hardware architectures might require different values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>ProcessorLevel</b>        | The architecture-dependent processor level for the system.<br>See “ <a href="#">Processor level values</a> ” on page 59.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 5-3** System information fields (*continued*)

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ProcessorRevision</b> | <p>The revision of the architecture-dependent processor.</p> <p>The following values are defined for each type of processor architecture:</p> <ul style="list-style-type: none"> <li>■ Intel 80386 or 80486. In the form <i>xyz</i>.<br/>                     If <i>xx</i> is equal to 0xFF, <i>y-0xA</i> is the model number, and <i>z</i> is the stepping identifier. For example, an Intel 80486-DD system returns 0xFFD0.<br/>                     If <i>xx</i> is not equal to 0xFF, <i>xx+A</i> is the stepping letter, and <i>yz</i> is the minor stepping identifier.</li> <li>■ Intel Pentium, Cyrix, or NextGen 586. In the form <i>xyy</i>, where <i>xx</i> is the model number and <i>yy</i> is the stepping identifier.</li> <li>■ MIPS. In the form 00xx, where <i>xx</i> is the 8-bit revision number of the processor (or the low-order 8 bits of the PRId register).</li> <li>■ SHx. The <b>wProcessorRevision</b> is always zero.</li> <li>■ ARM. A value from 1 to 16. Consult your ARM CPU manual.</li> </ul> |

## System constants

The following constants are defined for system information:

- 0 PROCESSOR\_ARCHITECTURE\_INTEL
- 1 PROCESSOR\_ARCHITECTURE\_MIPS
- 2 PROCESSOR\_ARCHITECTURE\_ALPHA
- 3 PROCESSOR\_ARCHITECTURE\_PPC
- 4 PROCESSOR\_ARCHITECTURE\_SHX
- 5 PROCESSOR\_ARCHITECTURE\_ARM
- 6 PROCESSOR\_ARCHITECTURE\_IA64
- 7 PROCESSOR\_ARCHITECTURE\_ALPHA64
- 0xFFFF PROCESSOR\_ARCHITECTURE\_UNKNOWN
- 386 PROCESSOR\_INTEL\_386
- 486 PROCESSOR\_INTEL\_486

- 586 PROCESSOR\_INTEL\_PENTIUM
- 686 PROCESSOR\_INTEL\_PENTIUMII
- 4000 PROCESSOR\_MIPS\_R4000 (includes R4101 & R3910 for Windows CE)
- 5000 PROCESSOR\_MIPS\_R5000 (includes R5432 for Windows CE)
- 21064 PROCESSOR\_ALPHA\_21064
- 403 PROCESSOR\_PPC\_403
- 601 PROCESSOR\_PPC\_601
- 603 PROCESSOR\_PPC\_603
- 604 PROCESSOR\_PPC\_604
- 620 PROCESSOR\_PPC\_620
- 10003 PROCESSOR\_HITACHI\_SH3 (Windows CE)
- 10004 PROCESSOR\_HITACHI\_SH3E (Windows CE)
- 10005 PROCESSOR\_HITACHI\_SH4 (Windows CE)
- 821 PROCESSOR\_MOTROLA\_821 (Windows CE)
- 103 PROCESSOR\_SHx\_SH3 103 (Windows CE)
- 104 PROCESSOR\_SHx\_SH4 (Windows CE)
- 105 PROCESSOR\_SHx\_SH3DSP (Windows CE)
- 2577 PROCESSOR\_STRONGARM (Windows CE - 0xA11)
- 1824 PROCESSOR\_ARM720 (Windows CE - 0x720)
- 2080 PROCESSOR\_ARM820 (Windows CE - 0x820)
- 2336 PROCESSOR\_ARM920 (Windows CE - 0x920)
- 70001 PROCESSOR\_ARM\_7TDMI (Windows CE)

See “[System information fields](#)” on page 56.

## Processor level values

If **wProcessorArchitecture** is PROCESSOR\_ARCHITECTURE\_INTEL, **wProcessorLevel** is one of the following values.

See “[System information fields](#)” on page 56.

5          Pentium

If **wProcessorArchitecture** is PROCESSOR\_ARCHITECTURE\_ARM, **wProcessorLevel** is one of the following values:

4          ARM version 4

If **wProcessorArchitecture** is PROCESSOR\_ARCHITECTURE\_MIPS, **wProcessorLevel** is one of the following values:

3          MIPS R3000

4          MIPS R4000

5          MIPS R5000

If **wProcessorArchitecture** is PROCESSOR\_ARCHITECTURE\_SHX, **wProcessorLevel** is one of the following values:

3          SH3 or SH3-DSP

4          SH4

## Memory information fields

Mobile Management collects the information in this section so that you can view it in various reports.

See [“Running and viewing reports for mobile devices”](#) on page 51.

**Table 5-4**          Memory information fields

| Field                          | Description                                                                                                                                                                            |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MemoryLoad</b>              | A number that gives a general idea of the current memory use. This number is in the range of 0 - 100. Zero indicates no memory is in use and 100 indicates that full memory is in use. |
| <b>TotalPhysicalMemory</b>     | The total number of bytes of physical memory.                                                                                                                                          |
| <b>AvailablePhysicalMemory</b> | The available number of bytes of physical memory.                                                                                                                                      |
| <b>TotalPageFile</b>           | The total number of bytes that can be stored in the paging file. This number does not represent the actual physical size of the paging file that is on disk.                           |

**Table 5-4** Memory information fields (*continued*)

| Field                         | Description                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>AvailablePageFile</b>      | The number of bytes that are available in the paging file.                                                                              |
| <b>TotalVirtualMemory</b>     | The total number of bytes that are in the user mode portion of the virtual address space for the calling process.                       |
| <b>AvailableVirtualMemory</b> | The number of bytes of unreserved and uncommitted memory in the user mode portion of the virtual address space for the calling process. |
| <b>TotalStorageMemory</b>     | The total number of bytes of storage memory.                                                                                            |
| <b>AvailableStorageMemory</b> | The available number of bytes of storage memory.                                                                                        |
| <b>TotalMemory</b>            | The total number of bytes of physical and storage memory.                                                                               |



# Delivering software to mobile devices

This chapter includes the following topics:

- [About delivering software to mobile devices](#)
- [Delivering software to mobile devices](#)
- [Changing software packages for mobile devices](#)
- [Package actions for mobile devices](#)
- [Sample of AppUpdate token for mobile devices](#)

## About delivering software to mobile devices

You can manage many details regarding software for the mobile devices in your organization.

Using inventory and reports, you can detect what software versions are currently installed on any device. You can download and install initial applications with Mobile Management. You can then use policies to schedule the jobs and the tasks that update the software with the latest versions and patches. These features help ensure that all software is up-to-date and in compliance with your organization's IT guidelines.

You can also copy, move, or delete files, as well as create, delete, or rename folders on each mobile device.

See [“Delivering software to mobile devices”](#) on page 64.

See [“Changing software packages for mobile devices”](#) on page 65.

See [“Managing mobile devices”](#) on page 15.

For more information on software delivery, see the *Symantec Management Platform Help*.

## Delivering software to mobile devices

You can create the software policies that contain the specific pieces of software. The software is then delivered according to the schedule that the maintenance windows set.

See [“About delivering software to mobile devices”](#) on page 63.

The integrity of the software is checked and repaired when the software delivery or configuration policy runs.

See [“Changing the agent configuration schedule for mobile devices”](#) on page 23.

For more information, view topics on policies and schedules in the *Symantec Management Platform Help*.

### To deliver software to mobile devices

- 1 In the Symantec Management Console, on the **Actions** menu, click **Mobile > Mobile Software Management**.
- 2 In the left pane, ensure that the **Policies > Mobile Management** folders are expanded.
- 3 Right-click the **Software Management** folder.
- 4 Click **New > Mobile Device Software Delivery**.
- 5 In the right pane, click the **New Mobile Device Software Delivery** title, and then enter a name for your software management package.
- 6 Click **Select Software**.
- 7 On the **Select Software** page, select the software that you want to include in your package.
- 8 Click the appropriate arrow icons to move your selections to the **Selected software** box.
- 9 Click **OK**.
- 10 Click the down arrow next to **Applied To**.
- 11 Select the computers (targets) that you want to deliver the software to.
- 12 At the upper right corner of the page, click the colored circle, and then click **On** to turn on the policy.
- 13 Click **Save changes**.

# Changing software packages for mobile devices

You can create new software packages and change the standard Mobile Management software packages. Software packages let you define the software, the actions to perform on each piece of software, and the metrics to report.

You can add packages or edit the actions on each package from the **Package** tab. From the **Actions** tab, you can choose the actions to perform on software resources and the order in which the actions are performed. The **Health** tab lets you choose the data that is checked to ensure that the software correctly installs.

See [“About delivering software to mobile devices”](#) on page 63.

The integrity of the software is checked and repaired when the software delivery or configuration policy runs.

See [“Changing the agent configuration schedule for mobile devices”](#) on page 23.

## To change software packages for mobile devices

- 1 In the Symantec Management Console, on the **Manage** menu, click **Mobile > Software**.
- 2 In the left pane, ensure that the **Software > Mobile Software** folders are expanded.
- 3 Click one of the defined software packages.
- 4 In the right pane, on the **Properties** tab, choose the version.
- 5 Choose the priority.
  - Automatic. The software automatically installs and no user intervention is required. Use this option most of the time.
  - Manual. The mobile device user has to run the software update manually (using **AppUpdate**) on the device.
- 6 (Optional) Choose the company and the software product.

Click **Browse** to find existing companies or software products or click **New** to add a new company or software product.
- 7 On the **Package** tab, ensure that all of the packages are listed.

You can add and create packages from this tab.

- 8 On the **Actions** tab, click **Auto Generate** to automatically create the steps for downloading and installing the files in each of the packages.

Click the **Add New Action** icon to select other actions to perform on software resources. You can also click the **Edit** icon and select an action to edit a current action.

See “[Package actions for mobile devices](#)” on page 66.

See “[Sample of AppUpdate token for mobile devices](#)” on page 71.

- 9 On the **Health** tab, click **Auto Generate** to automatically create a set of standard statistics.

You can also add your own metrics and choose from the **File Hash**, **Version**, or **Size** statistics.

- 10 Click **Save changes**.

## Package actions for mobile devices

You can specify different actions when you configure packages. These actions are named software delivery actions. This section describes the software delivery actions and their corresponding parameters.

See “[About delivering software to mobile devices](#)” on page 63.

**Table 6-1** Software delivery package actions

| Action        | Description                   | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Download File | Downloads the specified file. | <p><b>Source</b> in the <b>ServerFileName</b> data type. A text value that specifies the directory path of the Web server. If different versions of the file exist, it also includes the file name of the file to download to the mobile device. This string can contain any subdirectories that are not included in the value of &lt;ManifestURL&gt; in the AppUpdate.xml configuration file.</p> <p><b>Target</b> in the <b>DeviceFileName</b> data type. A text value that specifies the directory path of the Web server. If different versions of the file exist, it also includes the file name of the file to download to the mobile device. This string can contain any device subdirectories that prefix the file name.</p> <p><b>AppUpdate Runtime Substitution Token</b> values can be used within the parameters to define the target subdirectories for target files.</p> |

**Table 6-1** Software delivery package actions (*continued*)

| Action       | Description                  | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Install File | Installs the specified file. | <p><b>File</b> in the <b>localfilename</b> data type. A text value that specifies the name of an installable file that resides on the device. The file can be any installable file. For example, <code>.cab</code>, <code>ActiveX.dll</code>, <code>.reg</code>, or <code>.cpf</code> files in OMA format. The format can also include other XML formats that follow the install file guidelines.</p> <p>This action usually requires that you use the optional <b>Critical</b> action setting attribute. Using this setting allows subsequent manifest processing to continue if the install action cannot install the specified file. If the process to be terminated is not running at the time that the <b>Terminate</b> action is called, an error code is issued.</p> <p>To customize a warm boot, place a custom executable file that is named <code>warmboot.exe</code> in the same directory as the <b>AppUpdate</b> executable file. When the <code>warmboot.exe</code> file exists, it runs instead of the default warm boot action.</p> |

**Table 6-1** Software delivery package actions (*continued*)

| Action | Description                                                   | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Run    | Executes the specified program that is locally on the device. | <p><b>Command</b> in the <b>Commandline</b> data type. A text value that specifies the directory path and the file name of the file to run. It also contains any command line parameters that modify the execution options. You can use embedded blanks, and you do not have to use double quotes in the program path to enclose directories with embedded blanks. If you use embedded blanks, test the command as a shortcut first before you use it in this context.</p> <p><b>AppUpdate Runtime Substitution Token</b> values can be used within a value to define the subdirectories for executable files and command line parameters.</p> <p>See <a href="#">“Sample of AppUpdate token for mobile devices”</a> on page 71.</p> <p><b>Timeout</b> in the <b>Timeout value</b> data type. A numeric integer value that specifies how long the device should wait before it continues the subsequent manifest processing.</p> <p>You can use the following values:</p> <ul style="list-style-type: none"> <li>■ Less than zero (default). For example, -1. The device manifest processing waits indefinitely for the action to finish before it continues with any subsequent steps.</li> <li>■ 0. The device manifest processing does not wait for the action to finish before it continues with any subsequent steps.</li> <li>■ Greater than zero. For example, 10. The device manifest processing waits the specified number of milliseconds for the action to finish before it continues with any subsequent steps.</li> </ul> |

**Table 6-1** Software delivery package actions (*continued*)

| Action       | Description                                                                                 | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Terminate    | Stops the specified module process.                                                         | <p><b>Modules</b> in the <b>ModuleName</b> data type. A text value that specifies an executable file name that is running on the device. For example, <code>cmd.exe</code>. You can use wildcards to specify multiple file names. For example, <code>c*. * *</code> or <code>* * *</code> to specify all processes.</p> <p>This action usually requires that you use the optional <b>Critical</b> action setting attribute. If the process is not running when the <b>Terminate</b> action is called, the removal action attribute issues an error code. Using this setting allows subsequent manifest processing to continue even if the terminate action cannot end a process that is not running.</p> |
| Copy Files   | Copies one or more files from one area (directory or folder) of the device to another area. | <p><b>Source</b> in the <b>localsourcefilespec</b> data type. A string that specifies the path and name of the files on the device to copy during provisioning. You can use wildcard characters.</p> <p><b>Target</b> in the <b>localtargetfoldername</b> data type. A string that specifies where on the device to copy the files during provisioning.</p>                                                                                                                                                                                                                                                                                                                                              |
| Move Files   | Moves one of more files from one area (directory or folder) of the device to another area.  | <p><b>Source</b> in the <b>localsourcefilespec</b> data type. A string that specifies the path and name of the files on the device to move during provisioning. You can use wildcard characters. The files are removed from this location once they are successfully moved to the specified destination.</p> <p><b>Target</b> in the <b>localtargetfoldername</b> data type. A string that specifies where on the device to move the files during provisioning.</p>                                                                                                                                                                                                                                      |
| Delete Files | Deletes one or more local files on the device.                                              | <p><b>Path</b> in the <b>localfilename</b> data type. A string that specifies the name of the files to delete during provisioning. You can use wildcard characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 6-1** Software delivery package actions (*continued*)

| Action        | Description                                       | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rename File   | Renames a specified folder on the device.         | <p><b>Source</b> in the <b>existingfilename</b> data type. A string that specifies the path and name of a file that exists on the device. The file is renamed during provisioning.</p> <p><b>Target</b> in the <b>newfilename</b> data type. A string that specifies the new name of the file. The new name cannot already exist in the path that is specified in <b>Source</b>. Do not prefix the file name with the path specification. Use the raw file name.</p> |
| Create Folder | Creates a local folder (directory) on the device. | <b>Path</b> in the <b>localfoldername</b> data type. A string that specifies the name of the folder on the device to create during provisioning.                                                                                                                                                                                                                                                                                                                     |
| Remove Folder | Deletes a local folder (directory) on the device. | <b>Path</b> in the <b>localfoldername</b> data type. A string that specifies the name of the folder on the device to delete during provisioning. All files in the specified folder are also deleted.                                                                                                                                                                                                                                                                 |
| Rename Folder | Renames a local folder (directory) on the device. | <p><b>Source</b> in the <b>existingfoldername</b> data type. A string that specifies the path on the device to rename during provisioning.</p> <p><b>Target</b> in the <b>newfoldername</b> data type. A string that specifies the new name of the folder. The new name cannot already exist in the path that is specified in <b>Source</b>.</p>                                                                                                                     |
| Uninstall     | Uninstalls a previously installed .cab file.      | <b>Name</b> in the <b>applicationname</b> data type. Text that specifies the name of an application that was previously installed on the device. You can locate the application name by navigating on the device to <b>Start &gt; Settings &gt; System &gt; Remove Programs</b> . Any applications that appear in the list can be uninstalled.                                                                                                                       |

## Sample of AppUpdate token for mobile devices

The following code is an example of the token for **AppUpdate**:

See “[Package actions for mobile devices](#)” on page 66.

```
{TEMP}="\Application Data\Volatile\  
{WINDOWS}="\Windows\  
{SYSTEM}="\Windows\  
{STARTUP}="\Windows\StartUp\  
{PROGRAMS}="\Program Files\  
{DOCUMENTS}="\My Documents\  
{START_MENU}="\Windows\Start Menu\  
{PROGRAMS_MENU}="\Windows\Start Menu\Programs\  
{DEVICE_ID}="76F447353E7CD16B31EE3531A5340274"  
{DEVICE_CPU}="ARMV4I"  
{DEVICE_OEM}="SYMBOL MC9090G"  
{MAC_ADDRESS}="112233445566"  
{OS_MAJOR}="5"  
{OS_MINOR}="1"  
{OS_BUILD}="478"  
{OS_PLATFORM}="WinCE"  
{OS_SHELL}="PocketPC"  
{SCREEN_CX}="240"  
{SCREEN_CY}="320"  
{NLS_LCID}="00000409"  
{NLS_OEMCP}="000001B5"  
{NLS_ANSICP}="000004E4"  
{APP_MAJOR}="2"  
{APP_MINOR}="0"  
{APP_BUILD}="3232"
```

# Remotely managing mobile devices

This chapter includes the following topics:

- [About remotely managing mobile devices](#)
- [Changing the remote settings for mobile devices](#)
- [Starting a remote session with a mobile device](#)
- [Remote options for mobile devices](#)
- [Function mappings in remote sessions](#)

## About remotely managing mobile devices

Symantec Mobile Management lets you control any of the mobile devices in your environment that have the Mobile Management agent installed on them.

See [“Installing the Mobile Management Agent”](#) on page 21.

You can specify if each remote session is automatically accepted or if the user has to approve the session request. You can also specify options and choose how each session looks, such as the color depth and size of a session.

See [“Changing the remote settings for mobile devices”](#) on page 74.

During a remote session, you can view and fix any problems a user experiences with their device. You can also choose from several options that provide access to the File System, Registry, and Processes subsystems of the managed mobile device.

See [“Starting a remote session with a mobile device”](#) on page 75.

See [“Managing mobile devices”](#) on page 15.

# Changing the remote settings for mobile devices

You can determine how each remote session looks and behaves.

The **Request behavior** determines how the remote session request is handled. The **Control behavior** determines how the remote session handles keyboard and mouse interactions. You can also set the color depth of each session and how the device is sized in the console.

See [“About remotely managing mobile devices”](#) on page 73.

## To change the remote settings for mobile devices

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, ensure that the **Settings > Mobile Management > Mobile Agent Settings** folders are expanded.
- 3 Click **Remote Control Policy**.
- 4 In the right pane, choose one of the following options for the **Request behavior**:
  - **Always allow Remote Control request**
  - **Prompt user to allow Remote Control request**
  - **Always deny Remote Control request**
- 5 Choose one of the following options for the **Control behavior**:
  - **Always allow keyboard and mouse interaction**
  - **Prompt user to allow keyboard and mouse interaction**
  - **Always deny keyboard and mouse interaction**
- 6 Select a color depth for the remote session.

The larger color depths can negatively affect your network load. You can select either 2-bit, 4-bit, 8-bit, or 16-bit color depth. If you use a wide-area device, we recommend that you use the 4-bit option. However, you can experiment and see what setting works best in your environment.
- 7 Select the size scale for the session.

You can select either the same size (1x) or twice the size (2x).
- 8 Click **Save changes**.

## Starting a remote session with a mobile device

You can control any managed device in your organization and directly interact with that device. For example, you can stop a process that is running on the mobile device or start another process.

See [“About remotely managing mobile devices”](#) on page 73.

For the issues that require UI access, the remote link uses the remote settings that you defined.

See [“Changing the remote settings for mobile devices”](#) on page 74.

If you press a function key on your computer, it performs an action on your mobile device during a remote session. The effect that each function key has on your mobile device might be different than the effect that it usually has on your computer.

See [“Function mappings in remote sessions”](#) on page 78.

### To start a remote session

- 1 In the Symantec Management Console, on the **Actions** menu, click **Mobile > Remote Management**.
- 2 On the **Remote Management** page, click the mobile device that you want to connect to.
- 3 Click **Connect**.

See [“Remote options for mobile devices”](#) on page 75.

## Remote options for mobile devices

After you connect to a mobile device, you can choose from several options that provide access to the mobile device. For example, you can manage the File System, Registry, and Processes subsystems of the mobile device.

The right pane of the device name page contains the static information that was last captured in the inventory scan.

If you click an option in the left pane, the mobile device is called. The information might take a few seconds to load because it is dynamically collected and then displays in the right pane.

See [“Starting a remote session with a mobile device”](#) on page 75.

**Table 7-1** Remote options for mobile devices

| Option                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Device name</i>      | Lists the static information about the mobile device that was collected during the last inventory scan. For example, the date that the inventory was last collected and the name and the IP address of the device.                                                                                                                                                                                                                                                                                         |
| <b>Remote Control</b>   | <p>Lets you remotely control and view the mobile device. You can start processes and explore the device by double-clicking this option.</p> <p>In the <b>Remote Control</b> window, you can also choose the color and the zoom options for the session.</p> <p>If you click the camera icon in the <b>Remote Control</b> window, you can take a picture from the mobile device. Even if you select the 2-bit color option, your picture is in color because it is taken from the mobile device's view.</p> |
| Identification          | Lists the identifying information for the specific mobile device. For example, the name, ID, and OEM ID of the device.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Operating System</b> | Lists the information about the operating system that is currently running on the mobile device. For example, the type, ID, and version number of the platform that is on the device.                                                                                                                                                                                                                                                                                                                      |
| <b>Processor</b>        | Lists the information about the processor on the mobile device. For example, the architecture, core, clock speed, and name of the processor on the device.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Power</b>            | Lists the information about the battery and the power for the mobile device. For example, the voltage, temperature, and chemistry of the battery in the device.                                                                                                                                                                                                                                                                                                                                            |
| <b>Memory</b>           | Lists the information about the memory for the mobile device. For example, the percentage load, total and available physical and virtual memory, and storage memory for the device.                                                                                                                                                                                                                                                                                                                        |
| <b>Display</b>          | Lists the horizontal and the vertical resolution and the display colors of the mobile device.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Processes</b>        | Lists the information about the processes that are running on the mobile device. For example, the name and ID of the process, the thread count, and the CPU time for each process.                                                                                                                                                                                                                                                                                                                         |

**Table 7-1** Remote options for mobile devices (*continued*)

| Option                   | Description                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Certificates</b>      | Lists the information about the certificates that are currently issues on the mobile device. For example, the issuer name, issued and expiration date, and public and private key information for each certificate. |
| <b>Adapters</b>          | Lists the information about the adapters that are on the mobile device. For example, the name, IP address, mask, and gateway for each adapter.                                                                      |
| <b>Connections</b>       | Lists the connection information for the mobile device. For example, the status, local address and remote address, and local and remote port of each connection.                                                    |
| <b>IP Routing Table</b>  | Lists the IP routing information for the mobile device. For example, the destination IP address, adapter name, protocol, and age (in seconds) for each connection.                                                  |
| <b>ARP Table</b>         | Lists the Address Resolution Protocol (ARP) information for the mobile device. For example, the name and index of the adapter, Mac and IP address, and type.                                                        |
| <b>TCP/IP Statistics</b> | Lists the information about the TCP/IP connections for the mobile device. For example, the minimum timeout and maximum timeout values, number of open connections, and segments received.                           |
| <b>Wi-Fi</b>             | Lists the Wi-Fi information for the mobile device.                                                                                                                                                                  |
| <b>Applications</b>      | Lists the applications that are currently installed on the mobile device. You can also remove applications from the device through this page.                                                                       |
| <b>Program Files</b>     | Lists the program files that are on the mobile device. For example, the name, size, version, and date modified.                                                                                                     |
| <b>File Explorer</b>     | Lets you manipulate the directories and files on the mobile device. You cannot delete a folder if it contains any files. You can also search for a specific string in the current folder.                           |
| <b>Registry Explorer</b> | Lets you manipulate the registry entries on the mobile device. You can search for a specific string in the node that is currently highlighted.                                                                      |

## Function mappings in remote sessions

You can press a function key on your computer to perform an action on your mobile device during a remote session. However, the effect that each function key has on your mobile device might be different than the effect that it usually has on your computer.

See [“Starting a remote session with a mobile device”](#) on page 75.

**Table 7-2** Function mappings in remote sessions

| Computer function key | Smartphone action        |
|-----------------------|--------------------------|
| F1                    | Soft key 1 (left)        |
| F2                    | Soft key 2 (right)       |
| F3                    | Talk                     |
| F4                    | End                      |
| F6                    | Volume Increases         |
| F7                    | Volume Decreases         |
| F8                    | Dial pad *               |
| F9                    | Dial pad #               |
| F10                   | Voice notes or Record    |
| F11                   | Symbol list              |
| Backspace             | Backspace                |
| Enter                 | Action                   |
| Arrow keys            | Left, Right, Up, or Down |
| Esc                   | Back                     |

# Index

## A

- about
  - delivering software to mobile devices 63
  - gathering inventory data from mobile devices 49
  - managing mobile devices 73
  - Mobile Management 11
  - remote management of mobile devices 73
  - reports from mobile devices 49
- action
  - remote session for mobile devices 75
- actions
  - software packages for mobile devices 66
- agent
  - installing Mobile Management 21
- agent configuration
  - changing schedules for mobile devices 23
- AppUpdate token
  - sample for mobile devices 71

## B

- battery
  - constants for mobile devices 55
- battery information
  - fields for mobile devices 52

## C

- changing
  - agent configuration for mobile devices 23
  - remote settings for mobile devices 74
  - schedule for mobile device inventory 50
  - software data for mobile devices 65
  - software packages for mobile devices 65
  - software statistics for mobile devices 65
- configuring
  - Mobile Management 19
- constants
  - battery flags for mobile devices 55
  - OS version flags for mobile devices 56
  - system flags for mobile devices 58

## creating

- software packages for mobile devices 65

## customizing

- remote settings for mobile devices 74
- software data for mobile devices 65
- software statistics for mobile devices 65

## D

### data

- about viewing for mobile devices 49
- battery constants for mobile devices 55
- battery for mobile devices 52
- changing schedule for mobile device 50
- editing for mobile device software 65
- memory for mobile devices 60
- OS version constants for mobile devices 56
- OS Version for mobile devices 55
- processor level values for mobile devices 59
- running and viewing for mobile devices 51
- system constants for mobile devices 58
- system for mobile devices 56

### delivering

- software packages for mobile devices 65
- software to mobile devices with a policy 64

### delivering software

- to mobile devices
  - about 63

## E

### editing

- software packages for mobile devices 65

## F

### features of

- Mobile Management 11

### fields

- battery constants for mobile devices 55
- battery for mobile devices 52
- memory for mobile devices 60
- OS version constants for mobile devices 56

fields *(continued)*

- OS version for mobile devices 55
- system constants for mobile devices 58
- system for mobile devices 56

## file

- actions for mobile device 66

## flags

- battery constants for mobile devices 55
- OS version constants for mobile devices 56
- system constants for mobile devices 58

## folder

- actions for mobile device 66

## function

- mappings in remote sessions 78

**H**

## health

- editing statistics for mobile devices 65

## heartbeat

- value for mobile devices 50

## home page

- Mobile Management 16

**I**

## installing

- Mobile Management 19
- Mobile Management Agent 21
- Mobile Management server software
  - automatically 20
- Mobile Management Service 20

## inventory

- about gathering from mobile devices 49
- battery constants for mobile devices data 55
- battery for mobile devices data 52
- changing schedule for mobile device 50
- memory for mobile devices data 60
- OS version constants for mobile devices data 56
- OS version for mobile devices data 55
- processor level values for mobile devices data 59
- running and viewing mobile device data 51
- system constants for mobile devices data 58
- system for mobile devices data 56

**M**

## managing

- mobile devices remotely 75

## managing mobile devices

- process for 15

## mapping

- functions for remote sessions 78

## memory information

- fields for mobile devices 60

## metrics

- editing for mobile devices 65

## mobile device

- about delivering software 63
- about gathering data 49
- about managing 73
- about reports 49
- battery constants 55
- battery fields 52
- changing settings for remote session 74
- changing software data 65
- changing software statistics 65
- changing the agent configuration schedule 23
- changing the inventory schedule 50
- creating software package 65
- delivering software 64
- functions for remote sessions 78
- managing remotely 75
- memory fields 60
- OS version constants 56
- OS version fields 55
- package actions for 66
- process for managing 15
- processor level values 59
- running and viewing data 51
- running and viewing inventory 51
- running and viewing reports 51
- sample of AppUpdate token 71
- settings for remote management 75
- system constants 58
- system fields 56

## mobile devices

- viewing as resources 20

## Mobile Management

- about 11
- configuring 19
- features of 11
- how it works 12
- installing 19
- overview process 15
- portal page 16
- token sample 71
- what you can do with 12

## Mobile Management Agent

- installing 21

- Mobile Management Server
  - installing automatically 20
- Mobile Management server software
  - automatically installing 20
- Mobile Management Service
  - installing automatically 20
- Mobile Management service
  - installing 20

## O

- option
  - remote for mobile devices 75
- OS version
  - constants for mobile devices 56
- OS version information
  - fields for mobile devices 55
- overview
  - Mobile Management 15

## P

- package
  - editing software for mobile devices 65
- policy
  - creating new software delivery for mobile devices 64
- portal page
  - Mobile Management 16
- process for
  - managing mobile devices 15
- processor level
  - values for mobile devices 59

## R

- remote
  - actions for mobile devices 75
  - settings for mobile devices 75
- remote management
  - about mobile device 73
- remote session
  - changing settings for mobile devices 74
  - functions for mobile devices 78
  - starting with mobile devices 75
- reports
  - about mobile device 49
  - battery information for mobile devices 52
  - changing the schedule for mobile device 50
  - Devices with Low Battery for mobile devices 52
  - memory for mobile devices 60

- reports *(continued)*
  - OS version for mobile devices 55
  - runing and viewing for mobile devices 51
  - system for mobile devices 56
- resources
  - viewing mobile devices 20
- running
  - reports and inventory data for mobile devices 51

## S

- sample
  - AppUpdate token for mobile devices 71
  - Mobile Management 71
- schedule
  - changing agent configuration for mobile devices 23
  - changing inventory for mobile device 50
  - creating new software delivery for mobile devices 64
- session
  - remote with mobile devices 75
- setting
  - customizing remote session for mobile devices 74
- smartphone
  - functions for remote sessions 78
- software delivery
  - actions for mobile device 66
  - creating new software policies for mobile devices 64
  - editing packages for mobile devices 65
- software delivery to mobile devices
  - about 63
- software package
  - actions for mobile device 66
  - actions for mobile devices 66
  - customizing for mobile devices 65
- software policy
  - creating new for mobile devices 64
- system
  - constants for mobile devices 58
- system information
  - fields for mobile devices 56

## T

- token sample
  - AppUpdate for mobile devices 71

## **V**

### values

- processor level for mobile devices 59

### viewing

- mobile devices as resources 20

- reports and inventory data for mobile devices 51