Symantec™ Mobile Management 7.2 MR1 Release Notes

Symantec™ Mobile Management 7.2 Release Notes

This document includes the following topics:

About Mobile Management

Symantec Mobile Management lets you manage, secure, and troubleshoot the mobile devices in your organization. Using Mobile Management, you can automate IT tasks and control your IT environment more effectively. By becoming more effective, you can reduce the effort and costs of managing, securing, and troubleshooting mobile devices. Mobile Management works with the Symantec Management Platform to simplify the management of and communication with the devices in your environment.

What's new in Mobile Management 7.2

The 7.2 release of Symantec Mobile Management features several enhancements and new features, including support for Nitrodesk TouchDown™. For a complete listing of new features and enhancements, see the Symantec Knowledge Base article, *What's new in Symantec Mobile Management 7.2* at http://www.symantec.com/docs/TECH191144.

The updates include the enhancements, changes, or deprecations in the features that existed in Symantec Mobile Management 7.1 SP1.

Note: The MR1 release of Symantec Mobile Management replaces the now-deprecated Google Cloud-to-Device Messaging with Google Cloud Messaging (GCM).

Symantec Mobile Management 7.2 documentation

The most recent versions of the Mobile Management documentation are at the following URLS:

- Mobile Management Implementation Guide: http://www.symantec.com/docs/DOC5662
- Mobile Management Quick-start Guide: http://www.symantec.com/docs/DOC5665
- Mobile Management Release Notes: http://www.symantec.com/docs/DOC5666

Mobile Management requirements

The following table describes the requirements of each Mobile Management component:

Table 1-1 Mobile Management requirements

Component	Requirement and description
Mobile Management Server	■ Symantec Management Agent. See Symantec Management Platform 7.1 SP2 Installation Guide for more information about the Symantec Management Agent ■ IIS 7.5 (IIS 6 compatibility) ■ .NET Framework 3.5 SP1 ■ Microsoft Message Queuing Service. ■ ASP.NET. ■ APNS certificate.
Symantec Management Console	■ Internet Explorer 7.1, or later ■ Java Runtime Environment ■ See Symantec Management Platform 7.1 SP2 Installation Guide for additional requirements.
	■ iPhone 3G, 3GS, 4, and 4S running iOS 4.1 or later Symantec Mobile Management 7.2 supports policy settings on iOS 5 ■ iPod Touch 2nd generation, 3rd generation, and 4th generation running iOS 4.1 or later ■ iPad running iOS 4.2 or later ■ Android 2.2 or later. ■ Windows Mobile 6.0, 6.1, and 6.5-Professional and Standard ■ Windows CE 4.2 to 6.0 ■ Windows Phone 7.5 ■ Blackberry OS 4.3 - 6.x

Table 1-1 Mobile Management requirements *(continued)*

Component	Requirement and description
Symantec Management Platform server	■ Windows Server 2008 R2 & R2 SP1, 64-bit only- Enterprise, Standard, and Datacenter editions. Core Edition is not supported. ■ SQL Server 2005 SP2, SP3, SP4 or SQL Server 2008 SP1, SP2, R2, R2 SP1 ■ IIS 7.5 (IIS 6 compatibility) ■ .NET Framework 3.5 SP1 **Note:** The Windows Communication Foundation subcomponent is required on the Symantec Management Platform server. See the Symantec Management Platform system requirements for more information. ■ Microsoft Message Queuing ■ Microsoft Silverlight 3.x, 4.x, 5.x ■ Symantec Management Platform 7.1 SP1/SP2 See Symantec Management Platform 7.1 SP2 Installation Guide for additional requirements.
Microsoft SQL Server	See SQL Server documentation.
Active Directory	See Active Directory documentation.
LDAP	See LDAP documentation.
Certificate Authority	See Certificate Authority documentation.
SCEP	See SCEP documentation.

Table 1-1 Mobile Management requirements *(continued)*

Component	Requirement and description
Microsoft Exchange ActiveSync	Exchange ActiveSync integration software requirements: ■ Microsoft Exchange 2007 SP1 or SP2 with Exchange Server 2007 Management Tools or Microsoft Exchange 2010 ■ Microsoft Windows Management Framework, specifically Windows PowerShell 2.0 See Microsoft Exchange ActiveSync documentation for Exchange ActiveSync requirements.
Apple Push Notification Service	See Apple Push Notification Service documentation.
Google Cloud Messaging (GCM)	GCM allows you to push data to Android devices. There are no specific system requirements for GCM but you must obtain a Project ID number and API server key from Google. See Google GCM documentation

Installing Mobile Management

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *IT Management Suite Implementation Guide* at http://www.symantec.com/docs/DOC4827.

For detailed information about installing and setting up Mobile Management 7.2, see the *Mobile Management Implementaion Guide* at: http://www.symantec.com/docs/DOC5662.

Upgrading Mobile Management

Use the following procedure to update to latest version of Symantec Mobile Management:

To upgrade Symantec Mobile Management

1. You upgrade Mobile Management through the Symantec Installation Manager. Go to **Start > All Programs > Symantec > Symantec Installation Manager**.
2. On the **Installed Products** page, click **View and install updates**.
3. Select *Symantec Mobile Management 7.2* and click **Next**.
4. On the Optional Installations page, click Next
5. Accept the EULA and click **Next**.
6. On the **Contact Information** page, click **Next**.
7. Verify the installation details and click .
8. On the **Installation Complete** page, click **Finish**.

After you install Mobile Management 7.2, you must upgrade Mobile Management servers manually in the Symantec Management Console to complete the upgrade. Use this procedure to upgrade Symantec Mobile Management Server.

Upgrading the Mobile Management Server manually

1. In the Symantec Management Console, click **Home > Mobile Management > Settings > Mobile Management Server Settings**
2. Under **Site Server Rollout and Settings**, highlight the site server and then on the toolbar, click **Upgrade**.
3. Repeat Step 2 for each server.
4. Click **Save changes**

For more information about upgrading the products that use the Symantec Management Platform, see Symantec Knowledge-base article HOWTO 44338, *Installing an update or an additional product.*

Ugrading the Symantec Mobile Management device Agent.

Device owners can download the new version of the Symantec Mobile Management 7.2 Agent app from the app venue that is appropriate for their device operating system. The process to upgrade the agent is the same as when you download and install a new agent.

Fixed issues

The following are fixed issues for this release.

- Fixed an issue that allowed users to turn on the tablet DLP feature even if the VPN On Demand functionality was disabled in the **DLP VPN Assignment Policy**.
- Mobile Management now uses Google GCM for pushing data to Android devices. C2DM has been deprecated by Google and is no longer used.
- Fixed an issue that caused the scrollbar on the **Additional Configuration Profiles** page to not appear.
- Fixed an issue that sometimes caused the DLP inventory to disappear after inventory is sent.
- Fixed an issue that allowed unmanaged devices to access content from the Mobile Library by a direct link.
- Fixed an issue that caused the **Mobile Management Service Upgrade** policy to not work if the user's Mobile Management system had been upgraded before.
- Fixed an issue that caused the Mobile Management Agent to crash when the user clicked Install on the **Updates** page.
- Fixed an issue that caused payloads to not use the user name that the user provided to the agent during enrollment.
- Fixed an issue that caused the Symantec Management Platform installation to fail when the database name was not [Symantec_DMDB].
- Fixed an issue that caused the product to not warn the user when it checked **Sign configuration profile to device** if the proper certificates were not set up in **Mobile Management Server Settings > Profile Security**.
- Fixed an issue that caused the platform and manufacturer to be listed as unknown on the inventory page for Motorola Atrix 4G devices.
- Fixed an issue that caused Exchange Active Sync email addresses to show up twice on the **Devices by Operating System** page if the email address was configured and working before it was enrolled.
- Fixed an issue that caused Advanced iOS Configuration Payloads containing APN settings to be delivered to managed devices as empty payloads.
- Fixed an issue that made using the override settings to set the protocol to SSL for SMP > MMS communications to not work properly because it pulled the protocol information from the wrong place.
- Fixed an issue that caused the EAS profile to have an unusable email address if the user authenticated using domain/username or username@domain.com. Now the email address for the EAS profile is username@domain.com as long as the user fills in the following fields: Exchange server, domain, user, and email address.

See the following example for more information:

Exchange server:10.200.120.35 (or use FQDN: v120-35.newtest.com)
Domain: newtest
User: Account
Email Address:{user}@newtest.com

Note: {user} is not replicable.

- Fixed an issue that caused managed devices with a DLP policy to get a "-500" error message when they attempted to access a .com Web site.
- Fixed an error in the Symantec™ Mobile Management 7.2 documentation. In the topic *Enrolling a mobile device*, the enrollment URLs incorrectly show "SYMS" instead of "SYMC." The documents have been updated to correct this error.

Known issues

The following are known issues for this release.

Table 1-2 Known issues

Issue	Work around
If trailing or leading whitespaces are used in the subject of the SCEP settings, the settings can have problems registering.	Do not use trailing or leading whitespaces.
If the AD/LDAP server is set with the IP address instead of the host name during authentication check setup, user authentication does not work on iOS devices.	Always set the AD/LDAP server with host name.
The Enroll button is still displayed on devices that are already enrolled.	
If you stay on the EAS policy editor for more than 20 minutes without any action you receive a server error when you attempt to save any changes.	Complete any changes on this page within 20 minutes or save your changes periodically.
The Print button is not available on documents that are published to iOS5 devices.	To make the button appear, close the agent and reopen it. You can also follow links in the document and then return to the document.
When you use an older version of the agent with a 7.2 server, the About page shows Mobile Library items rather than about information.	Upgrade to the 7.2 agent.

Table 1-2 Known issues *(continued)*

Issue	Work around
The XML file with telemetry information does not contain statistic data when you run the schedule task manually, except the first time you run it.	
On the Inventory page you receive the following error message when you double-click Default Folder, Infrastructure, Notification Server Events, Software Delivery Summary, or user data : “Error loading callback data.”	Ignore this error message.
After you delete a document on the server console, the document is not removed from the Mobile Library on Android and Windows phone devices.	To make the document disappear for Windows phone users, have the user re-enroll. No workaround for Android users.
On iOS and Android devices, the Remove MDM and Reset Agent action does not work after you delete a device on the server console. On iOS devices: After the device is deleted, the device information reappears on the server after the user clicks agent update. The device is then unable to enter the enrollment interface. On Android devices: After the device is deleted, the device information does not reappear on the server. However, the device is unable to enter the enrollment interface.	Use the Remove MDM and Reset Agent action before you delete a device on the server console.
When you create an EAS policy with French characters in the title you receive an error.	Do not use French characters in the titles of EAS policies.
When you create an EAS policy with Simplified Chinese characters in the title the characters are truncated.	Do not use Simplified Chinese characters in the titles of EAS policies.
When dynamic_enrollment is set to YES, user login fails if anything was set in the URL field.	The only valid configurations for dynamic_enrollment are as follows: dynamic_enrollment = YES URL = empty dynamic_enrollment = NO URL = hard-coded or URL = empty