Symantec™ Mobile Management 7.1 Implementation Guide

Symantec™ Mobile Management 7.1 Implementation Guide

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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 support 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/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/

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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support 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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Technical Support 4

Chapter 1 Introducing Symantec Mobile Management 13

About Mobile Management 13
How Mobile Management works 14
Components of Mobile Management 14
Mobile device features 17
What's new in Mobile Management 7.1 19

Chapter 2 Setting up Mobile Management 23

Mobile Management requirements 23
Network ports used by Mobile Management 25
Supported devices and device operating systems 26
Setting up Mobile Management 27
Mobile Management certificate distribution 29

Chapter 3 Setting up a Mobile Device Management Certificate 31

About the Mobile Device Management (MDM) Certificate 31
Setting up an MDM Certificate 32
MDM Certificate requirements 34
Creating an App ID using Mac OS X 35
Exporting an MDM Certificate using Mac OS X 36
Generating a certificate request 36
Creating an App ID using a Windows Server 2003 or 2008 37
Exporting an MDM Certificate using a Windows Server 2003 or 2008 38
Installing an MDM Certificate 39

Chapter 4 Installing Mobile Management 41

About installing Mobile Management 41
Installing Mobile Management 42
Installing Mobile Management on an existing Symantec Management Platform server 42

Installing Mobile Management on a new server 43
Deploying Mobile Management to the site server 43

Chapter 5 Configuring Mobile Management 45

About configuring Mobile Management 45
Configuring Mobile Management 45
Configuring the site server to communicate with iOS devices 47
Configuring profile security settings 48
Configuring iOS device MDM enrollment 49
Adding additional configuration profiles 50

Chapter 6 Setting up Exchange ActiveSync 53

About using Exchange ActiveSync with Mobile Management 53
Setting up Exchange ActiveSync 54
Enabling the Exchange ActiveSync functionality 56
Configuring the SymantecEASService NT 56
Selecting the Exchange ActiveSync server 57
Restarting the Mobile Management Service Agent 57
Verifying the SymantecEASService configuration 58
About connecting iOS devices to Exchange ActiveSync 58

Chapter 7 Setting up the Mobile Management Agent application on iOS devices 61

About the Mobile Management Agent application on iOS devices 61
Setting up the Mobile Management Agent application on iOS devices 62
Downloading the Mobile Management Agent application from the Apple App Store 63
Enrolling iOS devices 64
Changing the enrollment URL to an email address for iOS devices 65
Enabling and creating the End User License Agreement for iOS devices 65
About the differences between the app store and the in-house Mobile Management Agent applications 66

Chapter 8 Setting up the Mobile Management Agent on Windows Mobile and BlackBerry devices 67

About the Mobile Management Agent on Windows Mobile and BlackBerry devices 67
Setting up the Mobile Management Agent on Windows Mobile devices 68
Setting up the Mobile Management Agent on BlackBerry devices 69
Setting the Mobile Management Agent configuration schedule for mobile devices 70

Chapter 9 Managing the Mobile Library for iOS devices 71

About the Mobile Library 71
Setting up Mobile Library feeds 72
Creating Mobile Library feeds 72
Adding items to Mobile Library feeds 73
Publishing an existing feed or item 75

Chapter 10 Using actions, policies, and configuration profiles 77

About actions 78
Performing actions on mobile devices 78
About policies 78
Creating policies 79
Assigning policies 79
Supported policies for specific devices 80
About configuration profiles on iOS devices 80
Devices that support configuration profiles 81
Setting up configuration profiles for iOS devices 82
Creating configuration profiles 82
Adding configuration profiles to a policy 83
Assigning configuration profile policies 84
About available configuration profile settings for iOS devices 85
About AutoLock settings on iOS devices 86

Chapter 11 Using inventory data, reports, and the event log 89

About inventory data 89
Viewing inventory data 90
Setting the inventory schedule for Windows Mobile devices 90
Setting the inventory schedule for iOS devices 91

About reports 92
Running reports 93
Available reports by device 93
About event logs 95
Viewing the event log 95

Chapter 12 Remotely managing devices 97

About remotely managing devices 97
Creating remote settings for devices 98
Starting a remote session with a device 99
Remote options for Windows Mobile devices 99
Remote options for BlackBerry devices 102
Function key mapping during remote sessions with Windows Mobile devices 103
Function key mapping during remote sessions with BlackBerry devices 104
Options for remotely wiping devices 105

Chapter 13 Managing software on Windows Mobile devices 109

About software management on Windows Mobile devices 109
Creating software packages for Windows Mobile devices 110
Delivering software packages to Windows Mobile devices 111
Configuring the software maintenance windows 112
Software package actions 113
Software package health actions 127
Sample AppUpdate runtime substitution tokens 130

Appendix A Creating the in-house Mobile Management Agent application for iOS devices 133

About the in-house Mobile Management Agent application 134
Creating the in-house Mobile Management Agent application 134
Requirements for creating the in-house Mobile Management Agent application 138
Downloading a WWDR Intermediate Certificate 138
Creating a Developer Certificate 139
Registering an iOS device for testing 139
Setting up an App ID 139
Downloading the project 140
Preparing the iOS device for testing 140
Loading the project 141

Creating and installing a Development Provisioning Profile 141
Customizing the Bundle identifier 142
Customizing the localized string files 143
Customizing the Target settings 143
Building and testing the application 144
Building and distributing the application 144

Appendix B Troubleshooting 147

Troubleshooting configuration policy distribution problems 147
Troubleshooting iOS device agent enrollment 148
Troubleshooting Mobile Management Server configurations 149
About troubleshooting errors with the SymantecEASService configuration 150
Verifying that the Push Certificate Subject matches the App ID's Bundle identifier 150
Configuring Mobile Management to work with a development APNS certificate 151

Appendix C Third-Party Attributions 153

Third-Party Legal Notices 153
ZLib v 1.2.2 153
Z.4.7 - Zlib v1.2.5 (G) 154
SQlite v 3.7.4 and SQlite NET.Wrapper v 1.0.66.0: 154
Expat v 1.2: 154

Index 157

Chapter 1

Introducing Symantec Mobile Management

This chapter includes the following topics:

- About Mobile Management
- How Mobile Management works
- Components of Mobile Management
- Mobile device features
- What's new in Mobile Management 7.1

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 Symantec Management Platform to simplify the management of and communication with the devices in your environment.

See "How Mobile Management works" on page 14.

See "Components of Mobile Management" on page 14.

See "Mobile device features" on page 17.

See "What's new in Mobile Management 7.1" on page 19.

How Mobile Management works

Mobile Management works with the management components and the security components in your environment to manage and secure all of your enterprise devices. When a user receives a corporate device, Mobile Management can control the device's capabilities and settings. The user of the device can use their enterprise credentials to enroll to receive recommended content from administrators. This content can include software and applications, documents, media, or Web links.

After users enroll, they can also receive customizable contact information for the IT department in their organization. If the user has a problem with a device, an administrator can remotely control the device to troubleshoot the problem. Because all of the devices communicate back to Mobile Management, the administrator can also collect inventory data and reports from the devices in the environment. In this way, administrators can determine the status of devices in the environment. Through the inventory, reporting, and policy features, administrators can target and schedule the devices that need management or assistance.

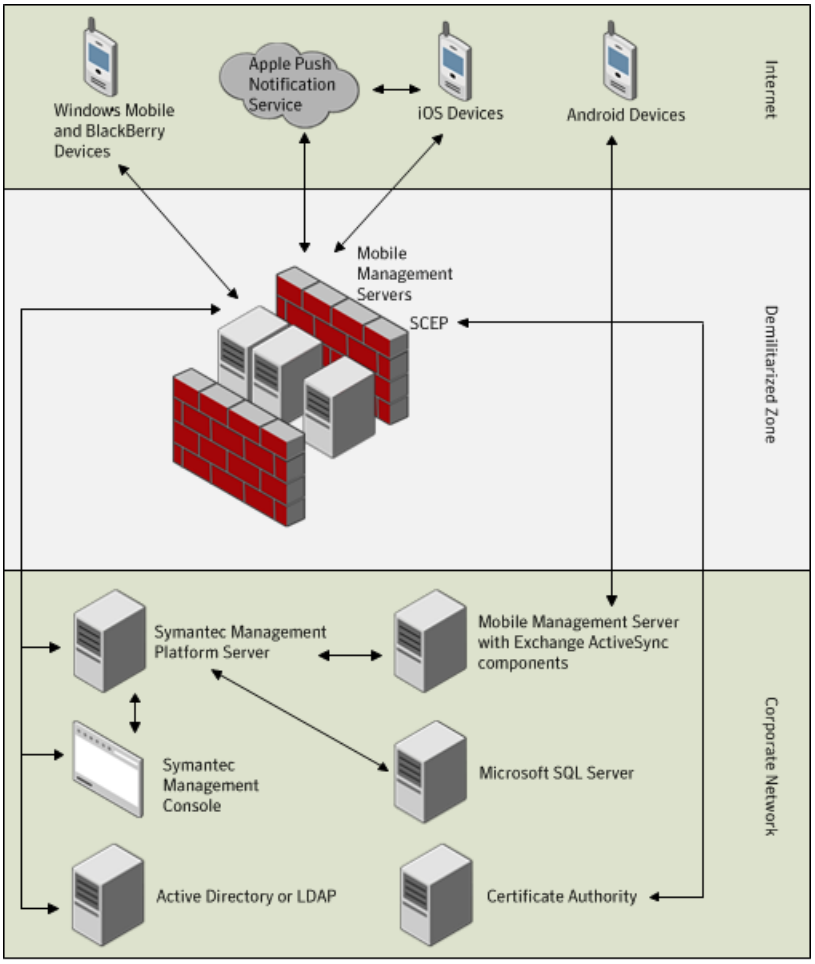
All of these capabilities are executed over the air by administrators through Mobile Management and the Symantec Management Platform.

See "About Mobile Management" on page 13.

See "Components of Mobile Management" on page 14.

Components of Mobile Management

The following diagram contains an overview of the possible Mobile Management components:



The following table contains descriptions of the Mobile Management components:

Table 1-1 Mobile Management components

Component	Description
Mobile Management Servers	You can have one or more Mobile Management Servers in your environment. All device communications pass through the Mobile Management Server(s).

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

Component	Description
Symantec Management Console	The Symantec Management Console is a Web-based administration utility that is part of the Symantec Management Platform. After you install Mobile Management, a Mobile Management portion of the console is added on. All of the management tasks that are associated with Mobile Management are accomplished in the console.
Mobile Management Agent	The Mobile Management Agent is the portion of Mobile Management that is on the device. The agent communicates directly with the Mobile Management Server during remote control. All other times, the agent either communicates with Exchange ActiveSync or the Apple Push Notification Service which communicates with the Mobile Management Server.

The following table contains descriptions of the additional components that the Mobile Management system uses:

Table 1-2 Mobile Management system components

Component	Description	Required or optional
Symantec Management Platform Server	The Symantec Management Platform Server is where all of the device information is stored. The Symantec Management Platform Server communicates with the Mobile Management Server to collect information or push notifications, software, or alerts down to the devices.	Required
Microsoft SQL Server	The Microsoft SQL Server hosts the Mobile Management and Symantec Management Platform Server databases.	Required
Active Directory or LDAP	Users, groups, and workstations are imported from Active Directory or LDAP.	Required

Table 1-2 Mobile Management system components *(continued)*

Component	Description	Required or optional
Certificate Authority	The Certificate Authority manages security credentials and public and private keys for secure communication. Symantec highly recomends a Certificate Authority for a secure environment.	Optional but strongly recommended
SCEP	The Simple Certificate Enrollment Protocol (SCEP) works with the Certificate Authority to issue certificates in large enterprises. It handles the issuing and revocation of digital certificates. The SCEP and Certificate Authority can be located on the same server.	Required if you use a Certificate Authority
Microsoft Exchange ActiveSync	Microsoft Exchange ActiveSync synchronizes the email, contacts, calendar, tasks, and notes that are associated with mailboxes on the Mobile Management Server with devices.	Optional
Apple Push Notification Service	The Mobile Management Server communicates through the Apple Push Notification Service to iOS devices.	Required if you want to manage iOS devices

See "About Mobile Management" on page 13.

See "How Mobile Management works" on page 14.

Mobile device features

Different devices support different Mobile Management features, depending on the device's limitations. The following table outlines the devices that are supported and the available features.

Table 1-3 Mobile device features

Device type	Available features
iOS	■ Customizable Mobile Management Agent ■ Mobile Library ■ Exchange ActiveSync ■ Configuration profiles ■ Actions ■ Policies ■ Reports ■ Remote wipe ■ Inventory data ■ Event log
Windows Mobile and CE	■ Mobile Management Agent ■ Exchange ActiveSync (except Windows Phone 7) ■ Actions ■ Policies ■ Reports ■ Inventory data ■ Remote control ■ Software management
BlackBerry	■ Mobile Management Agent ■ Actions ■ Policies ■ Reports ■ Inventory data ■ Remote control ■ Inventory data
Palm (hpWebOS) and Symbian (Nokia)	■ Exchange ActiveSync ■ Actions ■ Policies ■ Reports ■ Inventory data ■ Remote wipe ■ Inventory data

See "About Mobile Management" on page 13.

What's new in Mobile Management 7.1

The following table contains information on the new features that were released as part of Mobile Management 7.1.

See "About Mobile Management" on page 13.

Table 1-4 New features in Mobile Management 7.1

Feature	Description
Automated device provisioning	The automated device provisioning feature on iOS devices provides an easy, automated provisioning process to connect iOS devices to corporate email and other services in a secure way. The following are the features and benefits of automated device provisioning: ■ An iOS agent that streamlines the automated provisioning process. See "About the Mobile Management Agent application on iOS devices" on page 61. ■ Automatic provisioning of a certificate on the device by the standard SCEP protocol. ■ Automatic configuration of corporate email, VPN, APN, IMAP/POP email, LDAP, and WiFi settings. The automatic configuration enables mobile users to be even more productive within the enterprise environment. ■ Automatic provisioning of the certificate enables the use of authenticated email, secure WiFi, and VPN. This automatic provisioning prevents unauthorized users from connecting directly to corporate email and other corporate resources. ■ The ability to display a custom EULA that the end user must accept before they connect to corporate resources. See "Enabling and creating the End User License Agreement for iOS devices" on page 65.
Minimum requirements check	The advanced network access control capabilities let the administrator define minimum compliance and security requirements on iOS devices. These requirements are checked before Mobile Management allows devices to connect to enterprise assets. In addition, Mobile Management periodically re-verifies the compliance checks to ensure that the device continues to meet the minimum security requirements. The administrator can also block groups of devices from connecting to company assets based on device type, model, OS version, and user group. See "About policies" on page 78. See "About configuration profiles on iOS devices" on page 80.

Table 1-4 New features in Mobile Management 7.1 *(continued)*

Feature	Description
Advanced security and management settings	Advanced security and management settings allow support for the native Mobile Device Management (MDM) features in iOS 4. This support includes the ability to set, deploy, and update the security settings and the management settings for iOS devices. This ability does not require the iPhone Configuration Utility or any action from the end user. The advanced security and management settings also lets the administrator perform the following tasks: ■ Remotely lock devices. See "About actions" on page 78. ■ Selectively wipe corporate email, contacts, and calendars. See "Options for remotely wiping devices" on page 105. ■ Complete a full wipe of all data on the device, resetting it to factory condition. See "Options for remotely wiping devices" on page 105. ■ Define and enforce passcode policies for different groups of users or different users. See "About policies" on page 78. ■ Clear and reset passcodes. See "About policies" on page 78. See "About configuration profiles on iOS devices" on page 80. ■ Apply application restrictions such as screen capture, application installation, and voice dialing when locked. See "About policies" on page 78. See "About configuration profiles on iOS devices" on page 80. ■ Control whether email is automatically synchronized when the phone is roaming. See "About policies" on page 78. See "About configuration profiles on iOS devices" on page 80. ■ Control configuration profile removal by the user. See "About policies" on page 78. See "About configuration profiles on iOS devices" on page 80.
Updated device reporting	■ Collect advanced device network asset information. See "About reports" on page 92. ■ Collect reports for provisioning profiles, restrictions, and certificates. See "About reports" on page 92.
Mobile Library content management	In Mobile Management 7.1 the ability to manage applications, documents, links, and media on iOS devices was added. The Mobile Library enables this functionality. The Mobile Library enables enterprises to publish sets of applications, documents, links, and media to different groups of users in their environment. The content in the Mobile Library can be updated in real time by the administrator. See "About the Mobile Library" on page 71.

Table 1-4 New features in Mobile Management 7.1 *(continued)*

Feature	Description
Simplified deployment	Previously, device management was restricted to Microsoft Exchange ActiveSync. Now, Mobile Management can manage iOS devices using a native iOS application. See "About the Mobile Management Agent application on iOS devices" on page 61.
Expanded support	Mobile Management now supports Windows Phone 7 devices through Microsoft Exchange ActiveSync. Support for the 64-bit Symantec Management Platform 7.1.

Chapter 2

Setting up Mobile Management

This chapter includes the following topics:

- Mobile Management requirements
- Network ports used by Mobile Management
- Supported devices and device operating systems
- Setting up Mobile Management
- Mobile Management certificate distribution

Mobile Management requirements

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

Table 2-1 Mobile Management requirements

Component	Requirement and description
Mobile Management Server	■ Symantec Management Agent. ■ Web Server (IIS) that corresponds with your operating system. IIS must also have the role defaults and Role Service IIS 6 Management compatibility. ■ .NET Framework that corresponds with your operating system and IIS. ■ Microsoft Message Queuing Service. ■ ASP.NET. ■ APNS certificate.
Symantec Management Platform	See *Symantec Management Platform Help*.
Symantec Management Console	■ Internet Explorer 7.1 ■ Java Runtime Environment ■ See *Symantec Management Platform Help* for additional requirements.
Mobile Management Agent	■ iPhone 3G, 3GS, and 4 running iOS 4.1 or later ■ iPod Touch 2nd generation, 3rd generation, and 4th generation running iOS 4.1 or later ■ iPad running iOS 4.2 or later ■ Windows Mobile 2003, 5, 6.1, and 6.5 ■ Windows CE 4.2 to 6.0 ■ Blackberry OS 4.3 to 5.0
Symantec Management Platform server	■ Windows Server 2008 R2 64-bit ■ SQL Server 2005 or 2008 ■ IIS 6.0 ■ .NET Framework 3.0 ■ Microsoft Message Queuing ■ Symantec Management Platform 7.1 ■ See *Symantec Management Platform Help* for additional requirements.
Microsoft SQL Server	See SQL Server documentation.
Active Directory	See Active Directory documentation.
LDAP	See LDAP documentation.

Table 2-1 Mobile Management requirements *(continued)*

Component	Requirement and description
Certificate Authority	See Certificate Authority documentation.
SCEP	See SCEP documentation.
Microsoft Exchange ActiveSync	Exchange ActiveSync integration software requirements: ■ Microsoft Exchange 2007 SP1 or SP2 with Exchange Server 2007 Management Tools or Microsoft Exchange 2010 with Exchange Server 2010 Management Tools ■ 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.

See "Setting up Mobile Management" on page 27.

Network ports used by Mobile Management

The following table describes the ports that Mobile Management uses:

Table 2-2 Network ports used by Mobile Management

Port	From	To	Description
80, 443	Agent	Mobile Management Server	IIS HTTP for agent communication, IIS HTTPS for agent communication (optional)
7780	Agent	Mobile Management Server	Remote control connection

Table 2-2 Network ports used by Mobile Management *(continued)*

Port	From	To	Description
5223	Agent	Apple Push Notification Service	APNS communications to Apple by APNS servers
2195, 2196, 5223	Mobile Management Server	Apple Push Notification Service	APNS communications to agent by APNS servers
7778	Symantec Management Platform Server	Mobile Management Server	Remote control connection
80	Mobile Management Server	Symantec Management Platform Server	IIS HTTP
80	Symantec Management Console browser	Symantec Management Platform Server	Console
7778	Symantec Management Console browser	Mobile Management Server	Remote control connection
Standard SQL ports	Symantec Management Platform Server	Microsoft SQL Server	Database

See "Setting up Mobile Management" on page 27.

Supported devices and device operating systems

The following table describes the devices and device operating systems that the Mobile Management components support:

Table 2-3 Supported devices and device operating systems

Component	Requirement and description
Exchange ActiveSync	■ Apple iOS running iOS 2.x, 3.x, and 4.x ■ Android 2.2 and higher ■ Windows Mobile 6.1 and 6.5 ■ Windows Phone 7 ■ Palm WebOS 1.4.5 ■ Nokia (running Mail for Exchange v3.0.50)
Mobile Management Agent	■ Apple iPhone 3G, 3GS, and 4 running iOS 4.1 or later ■ Apple iPad running iOS 4.2 ■ iPod Touch 2nd generation, 3rd generation, and 4th generation running 4.1 or later ■ Windows Mobile 2003, 5, 6.1, and 6.5 ■ Windows CE 4.2 to 6.0 ■ Blackberry OS 4.3 to 5.0

See "Setting up Mobile Management" on page 27.

Setting up Mobile Management

The process for setting up Mobile Management includes the steps you need to take to set up your environment before you install Mobile Management. It also includes the steps you need to take to configure your environment to work with Mobile Management and install the Mobile Management software.

See "Mobile Management requirements" on page 23.

Table 2-4 Process for setting up Mobile Management

Step	Action	Description
Step 1	Secure your environment.	To secure your environment, you need to set up a Certificate Authority. You can either purchase a commercial Certificate Authority or set up a Certificate Authority yourself. If your environment is already secure, you can skip this step. See "Mobile Management certificate distribution" on page 29.
Step 2	Set up Simple Certificate Enrollment Protocol (SCEP).	Set up SCEP in your environment. If you already have SCEP setup in your environment, you can skip this step.
Step 3	(Optional) Setup a Mobile Device Management Certificate.	If you want to manage iOS devices in your environment, this step is mandatory. See "Setting up an MDM Certificate" on page 32.
Step 4	Install Mobile Management.	Install the Mobile Management components. See "Installing Mobile Management" on page 42.
Step 5	(Optional) Setup additional security in your environment.	For additional security, you can set up profile security in your Mobile Management environment. Profile security lets you encrypt and sign data. To set up profile security, add signing certificates and encryption certificates to your Certificate Authority. See "Mobile Management certificate distribution" on page 29.
Step 6	Configure Mobile Management in the Symantec Management Console.	Configure and customize the components of your Mobile Management environment in the Symantec Management Console. See "Configuring Mobile Management" on page 45.

Table 2-4 Process for setting up Mobile Management *(continued)*

Step	Action	Description
Step 7	(Optional) Setup Exchange ActiveSync.	Set up and configure Exchange ActiveSync to work with Mobile Management. See "Setting up Exchange ActiveSync" on page 54.

See "About Mobile Management" on page 13.

See "Components of Mobile Management" on page 14.

Mobile Management certificate distribution

The following table contains a list of Mobile Management components and the certificates that should be installed on each of them.

Root Certificates are only required when you use a non-commercial certificate authority. Root Certificates are also not needed if you use your own certificate authority for SCEP but an external certificate authority for Server Authentication Certificates.

SSL is not required for SCEP. If you choose to use SSL, you must have the Server Authentication Certificate or Root Certificate installed.

Table 2-5 Mobile Management certificate distribution

Component	Certificates
Mobile Management server	Certificate authority: ■ Server Authentication (SSL) Certificate ■ Root Certificate Profile Security: ■ Signing Certificate with public and private keys ■ Encryption Certificate with public key
Symantec Management Platform Server	Certificate authority: ■ Root Certificate

Table 2-5 Mobile Management certificate distribution *(continued)*

Component	Certificates
iOS device	Certificate authority: ■ Server Authentication (SSL) Certificate ■ Root Certificate Profile Security: ■ Encryption Certificate with public and private keys

See "Setting up Mobile Management" on page 27.

Chapter 3

Setting up a Mobile Device Management Certificate

This chapter includes the following topics:

- About the Mobile Device Management (MDM) Certificate
- Setting up an MDM Certificate
- MDM Certificate requirements
- Creating an App ID using Mac OS X
- Exporting an MDM Certificate using Mac OS X
- Generating a certificate request
- Creating an App ID using a Windows Server 2003 or 2008
- Exporting an MDM Certificate using a Windows Server 2003 or 2008
- Installing an MDM Certificate

About the Mobile Device Management (MDM) Certificate

The Mobile Device Management (MDM) Certificate allows the Mobile Management Server to push commands through the Apple Push Notification Service to iOS devices in your environment. The MDM Certificate creates a trust relationship with Apple and functions as a sort of credential for the Apple Push Notification Service servers. All Apple customers who want to communicate with iOS devices have to set up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

Setting up an MDM Certificate

You can set up an MDM Certificate on Mac OS X or Windows Server 2003 or 2008. Symantec recommends creating the MDM Certificate on Mac OS X.

This task is a step in the process for setting up Mobile Management.

See "Setting up Mobile Management" on page 27.

Table 3-1 Process for setting up a Mobile Device Management Certificate on Mac OS X

Step	Task	Description
Step 1	Make sure that you meet the MDM Certificate requirements.	Make sure that you meet the Apple Developer Membership, Agreement, and hardware and software requirements. See "MDM Certificate requirements" on page 34.
Step 2	Log on to your iOS Developer Enterprise Program account.	Log on to your iOS Developer Enterprise Program account as your Team Agent entity at the following location: https://developer.apple.com/membercenter/index.action#iPhoneDev
Step 3	Create an App ID.	To create an MDM Certificate, you must create an App ID through Apple. After you create the App ID, you create the MDM Certificate, which is saved in your key chain. See "Creating an App ID using Mac OS X" on page 35.

Table 3-1 Process for setting up a Mobile Device Management Certificate on Mac OS X *(continued)*

Step	Task	Description
Step 4	Create and export an MDM certificate.	After you create the MDM Certificate, you need to export it so you can transfer it to your Mobile Management server. See "Exporting an MDM Certificate using Mac OS X" on page 36.
Step 5	Install the certificate.	You must install the MDM Certificate on all the Mobile Management servers in your environment. See "Installing an MDM Certificate" on page 39.

Table 3-2 Process for setting up a Mobile Device Management Certificate on a Windows server 2003 or 2008

Step	Task	Description
Step 1	Make sure that you meet the MDM Certificate requirements.	Make sure that you meet the Apple Developer Membership, Agreement, and hardware and software requirements. See "MDM Certificate requirements" on page 34.
Step 2	Log on to your iOS Developer Enterprise Program account.	Log on to your iOS Developer Enterprise Program account as your Team Agent entity at the following location: https://developer.apple.com/membercenter/index.action#iPhoneDev

Table 3-2 Process for setting up a Mobile Device Management Certificate on a Windows server 2003 or 2008 *(continued)*

Step	Task	Description
Step 3	Generate a certificate request.	To create an MDM Certificate on a Windows Server 2003 or 2008, you must first generate a certificate request. See "Generating a certificate request" on page 36.
Step 4	Set up an App ID and download an APN certificate.	To create an MDM Certificate, you must create an App ID through Apple. After you create the App ID, you create the MDM Certificate, which is saved on your computer. See "Creating an App ID using a Windows Server 2003 or 2008" on page 37.
Step 5	Install the certificate.	You must install the MDM Certificate on all the Mobile Management servers in your environment. See "Installing an MDM Certificate" on page 39.

See "About the Mobile Device Management (MDM) Certificate" on page 31.

MDM Certificate requirements

Ensure that your environment meets the requirements for setting up an MDM Certificate.

This topic is part of the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

Table 3-3 MDM Certificate requirements

Requirement	Description
Hardware and software requirements	■ One or more server(s) running the current version of Windows Server 2003 or 2008. ■ Apple Safari, Mozilla Firefox, or Google Chrome Web. ■ (Optional but recommended) Mac computer running the current version of Mac OS X.
iOS Developer Enterprise Program membership	You can sign up for the iOS Developer Enterprise Program membership at the following Web site: http://developer.apple.com /programs/ios /enterprise/
MDM Agreement	You must contact Apple directly to acquire the MDM Agreement.

Creating an App ID using Mac OS X

To create an MDM Certificate, you must create an App ID through Apple. After you create the App ID, you create the MDM Certificate, which is saved in your key chain.

This task is a step in the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

To create an App ID using Mac OS X

1 Go to the following URL:

https://developer.apple.com/ios/manage/bundles/howto.action

2 Complete the instructions for the following tasks:

- **Generating an App ID**
  To use MDM commands, the App ID's Bundle Identifier must be in the following form: com.apple.mgmt.*<SuffixOfYourChoice>*. For example, `com.apple.mgmt.symantec`.
- Steps 1 to 6 of **Registering an App ID for Apple Push Notification service**
  Choose **Configure Development Push SSL Certificate** if you set up the Mobile Management server for development and testing purposes.

Choose **Configure Production Push SSL Certificate** if you set up the Mobile Management server for production use.

3 You should now have an Apple Development Push Services or an Apple Production Push Services Certificate and the private key associated with it in your key chain.

Exporting an MDM Certificate using Mac OS X

After you create the MDM Certificate, you need to export it so you can transfer it to your Mobile Management server.

This task is a step in the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

To create and export an MDM Certificate using Mac OS X

1 Open **Keychain Access**.

2 Under **Keychains** in the left pane, select **login**.

3 Under **Categories**, select **Certificates**.

4 Select your Apple Development Push Services or Apple Production Push Services Certificate.

5 Choose **File > Export Items...**.

6 Select Personal Information Exchange as the file format and click **Save**.

7 Enter a password to lock the MDM Certificate and click **OK**.

8 Enter your logon key chain password. This password is your Apple computer account password.

9 Click **Allow**.

10 Transfer the MDM Certificate that you created to the computer running the Mobile Management server.

Generating a certificate request

To create an MDM Certificate on a Windows Server 2003 or 2008, you must first generate a certificate request.

This task is a step in the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

To generate a certificate request

1. Select **Start > Control Panel > Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.
3. Select the server, and then double-click **Server Certificates**.
4. On the **Actions** menu, click **Create Certificate Request**. Enter the following information:
   - **Common Name** - The name that is attached to your certificate request.
   - **Organization** - The name of your organization.
   - **Organizational unit** - The name of the group or department within your organization
   - **City/locality** - The city or locality where your organization is located.
   - **State/province** - The state or province where your organization is located.
   - **Country/region** - The country or region where your organization is located.
5. Click **Next**.
6. In the **Cryptographic Service Provider Properties** window, select **Microsoft RSA SChannel Cryptographic Provider** for the **Cryptographic service provider**. Select **2048** for the **Bit length**.
7. Click **Next**. In the **File Name** window, type a file path and name or click the ellipsis button to browse.
8. Click **Finish** to generate and save the certificate request.

Creating an App ID using a Windows Server 2003 or 2008

To create an MDM Certificate, you must create an App ID through Apple. After you create the App ID, you create the MDM Certificate, which is saved on your computer.

This task is a step in the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

To create an App ID using a Windows Server 2003 or 2008

1. Navigate to the following URL:

   https://developer.apple.com/ios/manage/bundles/howto.action
2. Complete the instructions for the following tasks:

- **Generating an App ID**
  To use MDM commands, the App ID's Bundle Identifier must be in the following form: com.apple.mgmt.*<SuffixOfYourChoice>*. For example, `com.apple.mgmt.symantec`.
- Steps 1 to 6 of **Registering an App ID for Apple Push Notification service**
  Choose **Configure Development Push SSL Certificate** if you set up the Mobile Management server for development and testing purposes.
  Choose **Configure Production Push SSL Certificate** if you set up the Mobile Management server for production use.

3 Click **Download** to download the SSL certificate, and then click **Done**. An Apple Push Notification Service SSL certificate is now available in your browser's download location.

Exporting an MDM Certificate using a Windows Server 2003 or 2008

After you create the MDM Certificate, you need to export it so you can transfer it to your Mobile Management server.

This task is a step in the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

To create and export an MDM certificate using a Windows Server 2003 or 2008

1 Select **Start > Control Panel > Administrative Tools**.

2 Select **Internet Information Services (IIS) Manager**.

3 Select the server, and then double-click **Server Certificates**.

4 In the **Actions** menu, click **Complete Certificate Request**.

5 In the **Specify Certificate Authority Response** window, click the ellipsis button and browse to the Apple Push Notification Service SSL certificate that you downloaded previously. In the **Friendly name** field, enter a friendly name.

6 Click **OK**.

7 Select the Server Certificate with the friendly name that you entered in step 5.

8 In the **Actions** menu, click **Export**.

9 In the **Export Certificate** window, click the ellipsis button and browse to the location where you want to export the MDM Certificate. In the **Password** field, enter a password to secure the MDM Certificate.

10 Click **OK**.

Transfer the MDM Certificate that you created to the computer running the Mobile Management server.

Installing an MDM Certificate

You must install the MDM Certificate on all the Mobile Management servers in your environment.

This task is a step in the process for setting up an MDM Certificate.

See "Setting up an MDM Certificate" on page 32.

To install an MDM Certificate on Windows Server 2003

1 Download and install the Windows HTTP Services Certificate Configuration Tool (WinHttpCertCfg.exe) from the following Web site:

http://www.microsoft.com/downloads/en/detials.aspx?familyid=c42e27ac-3409-40e9-8667-c748e422833f&displaylang=en

2 Open a command prompt window and navigate to the install directory of the Windows HTTP Services Certificate Configuration Tool.

3 Execute the following command:

```
winhttpcertcfg -i <PathToMDMCertificate> -c LOCAL_MACHINE\My -a
"NETWORK SERVICE" -p <Password>
```

To install an MDM Certificate on Windows Server 2008

1 Click **Start** and then click **Run**.

2 In the command prompt, type **mmc** and then click **OK** to open the Microsoft Management Console.

3 In the Microsoft Management Console, click **File > Add/Remove Snap-in...**.

4 Click **Certificates** in the **Available snap-ins** box and then click **Add**.

5 In the **Certificates snap-in** window, select **Computer account**, and then click **Next**.

6 Click **Finish** and then click **OK**.

7 Expand **Certificates**, right-click the **Personal** tree node, and select **All Tasks > Import**.

8. In the wizard, point to the MDM Certificate and provide the password you entered to secure it. Complete the steps in the wizard.
9. Expand **Personal** and double-click the **Certificates** folder.
10. Right-click the MDM Certificate you installed and select **All Tasks > Manage Private Keys**.
11. In the **Security** tab, add the Network Service account and provide Read access.

Chapter 4

Installing Mobile Management

This chapter includes the following topics:

- About installing Mobile Management
- Installing Mobile Management
- Installing Mobile Management on an existing Symantec Management Platform server
- Installing Mobile Management on a new server
- Deploying Mobile Management to the site server

About installing Mobile Management

Mobile Management is installed as a plug-in to the Symantec Management Platform. Installing Mobile Management adds the Mobile Management section to the Symantec Management Console. It also adds the Mobile Management software components to the Symantec Management Platform server.

Once you have installed Symantec Management Platform and Mobile Management Solution, you can deploy Mobile Management server components to additional servers. You can have one or more Mobile Management site servers in your environment. The Mobile Management server components allow devices to talk to the site servers and thus to the Symantec Management Platform server.

See "Installing Mobile Management" on page 42.

Installing Mobile Management

The following table outlines the steps to install Mobile Management.

This task is a step in the process for setting up Mobile Management.

See "Setting up Mobile Management" on page 27.

Table 4-1 Process for installing Mobile Management

Step	Task	Description
Step 1	Install Mobile Management on the Symantec Management Platform server.	See "Installing Mobile Management on an existing Symantec Management Platform server" on page 42.
		See "Installing Mobile Management on a new server" on page 43.
Step 2	Deploy Mobile Management on the site servers in your environment.	See "Deploying Mobile Management to the site server" on page 43.

See "About installing Mobile Management" on page 41.

Installing Mobile Management on an existing Symantec Management Platform server

If you already have the Symantec Management Platform server in place, you can install Mobile Management. It adds the Mobile Management section to the Symantec Management Console and the Mobile Management software components to the Symantec Management Platform server.

This task is a step in the process for installing Mobile Management.

See "Installing Mobile Management" on page 42.

To install Mobile Management on an existing Symantec Management Platform server

1. Make sure that your Symantec Management Platform server meets the minimum requirements.

   See "Mobile Management requirements" on page 23.

2. On the Symantec Management Platform server, run the Symantec Installation Manager.

3 Select to install Mobile Management Solution.

4 Follow the prompts in the installation wizard to install Mobile Management.

See "About installing Mobile Management" on page 41.

Installing Mobile Management on a new server

If you do not have the Symantec Management Platform installed, you need to install it before you install Mobile Management. After you install the Symantec Management Platform, you can install Mobile Management.

This task is a step in the process for installing Mobile Management.

See "Installing Mobile Management" on page 42.

To install Mobile Management on a new server

1 Make sure that your Symantec Management Platform server meets the minimum requirements.

See "Mobile Management requirements" on page 23.

2 Install the Symantec Management Platform.

For instructions, see the *Symantec Management Platform Help*.

3 On the Symantec Management Platform server, run Symantec Installation Manager.

4 Select to install Mobile Management Solution.

5 Follow the prompts in the installation wizard to install Mobile Management.

See "About installing Mobile Management" on page 41.

Deploying Mobile Management to the site server

To install Mobile Management on the site servers in your environment, you must deploy it through the Symantec Management Console.

This task is a step in the process for installing Mobile Management.

See "Installing Mobile Management" on page 42.

To deploy Mobile Management to the site server

1 Open the Symantec Management Console.

2 Select **Settings > All Settings**.

3 Expand **Settings > Mobile Management > Mobile Management Service**.

4 Click **Mobile Management Servers**.

5 In the **Mobile Management Servers** pane, click **New** and choose a computer to add as the Mobile Management site server.

6 Click **OK**.

Chapter 5

Configuring Mobile Management

This chapter includes the following topics:

- About configuring Mobile Management
- Configuring Mobile Management
- Configuring the site server to communicate with iOS devices
- Configuring profile security settings
- Configuring iOS device MDM enrollment
- Adding additional configuration profiles

About configuring Mobile Management

After all of the components of your Mobile Management environment are set up, you need to configure them to work with Mobile Management.

See "Configuring Mobile Management" on page 45.

Configuring Mobile Management

You can configure and customize the components of your Mobile Management environment in the Symantec Management Console.

This task is a step in the process for setting up Mobile Management.

See "Setting up Mobile Management" on page 27.

Table 5-1 Process for configuring Mobile Management

Step	Task	Description
Step 1	(Optional) Integrate the MDM Certificate.	If you set up an MDM Certificate previously, this step is required. After you install the MDM Certificate on your Mobile Management servers, you must configure Mobile Management to use the MDM Certificates.
Step 2	(Optional) Configure the site server to communicate with iOS devices.	If you want to manage iOS devices in your environment, this step is required. See "Configuring the site server to communicate with iOS devices" on page 47.
Step 3	(Optional) Configure profile security settings.	If profile security is set up in your environment, you can complete this step. See "Configuring profile security settings" on page 48.
Step 4	(Optional) Configure iOS device MDM enrollment.	If you set up the MDM Certificate to manage iOS devices, this step is required. See "Configuring iOS device MDM enrollment" on page 49.
Step 5	(Optional) Add additional configuration profiles.	If you want to send configuration profiles to all iOS devices on enrollment, you can add configuration profiles during setup. See "Adding additional configuration profiles" on page 50.

See "About configuring Mobile Management" on page 45.

Configuring the site server to communicate with iOS devices

If you have iOS devices in your environment, you need to configure each site server's settings. The settings determine the rules for how the devices communicate with Mobile Management.

This task is a step in the process for configuring Mobile Management.

See "Configuring Mobile Management" on page 45.

To configure the site server

1. Open the Symantec Management Console.
2. Click **Home**.
3. Expand **Configuration**.
4. Click **Mobile Management Server Settings**.
5. In the **Mobile Management Server Settings** pane, click the **Enrollment** tab.
6. On the **Enrollment** tab, configure the following settings:
   - **Enable Authentication Check** - If you check this option, you must enter your server information. The server information is used to validate the user name and password from the agent's enrollment page. If you do not check this option, users without credentials can enroll a device and access content and information in the Mobile Management Agent.
     You can also enter a list of **Allowed Groups**. The allowed groups are AD or LDAP groups. If you enter a list of groups in this field, only users in those groups can enroll. Enter the groups with a pipe character between them. For example, Sales|Engineering|Marketing.
   - **Allow Jailbroken Devices** - If you check this option, any device that fails the jailbreak test during enrollment is not managed. Jailbroken devices can enroll, but they cannot see content in the Mobile Library.
   - **Require EULA acceptance** - If you check this option, any user who does not accept the End User Licensing Agreement (EULA) is not enrolled. Therefore, the server does not manage that user.
   - **Minimum OS Version** - If you enter a value in this field, devices with operating system versions that are earlier than the value in the field are not allowed to enroll. This field defaults to 4.1 since that is the minimum supported OS version by Mobile Management. You can only set a single value for all iOS devices connecting to the system. You cannot have minimum OS versions set for different types of iOS devices.

- **Non-approved Platforms** - If you enter values in this field, the device platforms that you enter are blocked from registering.

7 Click the **Agent** tab.

8 In the **Agent** tab, configure the following settings:

- **Report Frequency (seconds)** - Enter the polling interval in seconds. This polling interval determines how often the Mobile Management Agent on iOS devices checks in to the server.
- **Support Company** - This information appears on the Mobile Management Agent's **About** page.
- **Support Phone** - This information appears on the Mobile Management Agent's **About** page.
- **Support URL** - This information appears on the Mobile Management Agent's **About** page.

9 Click the **APNS** tab.

10 On the **APNS** tab, add the Certificate Thumbprint for your company-specific Apple Push Notification Certificate.

11 Click **Save Changes** to save all of your settings.

12 (Optional) To change the site server from using FQDN to an IP address, select the server in the **Site Server Settings** section. Click the edit button. Check **Override server connection info** and in the **Server name override** field, enter the IP address. In the **Port** field, enter **80** and click **Save changes**.

- Check **Manual Settings** if you want to edit web.config files manually. If you check **Manual Settings** the Mobile Management Server files and configuration files are not automatically updated.
- Check **Https** to force iOS device communication over https instead of http.

It can take up to 15 minutes for the settings to be applied to the site server.

Configuring profile security settings

If you set up profile security in your Mobile Management environment, you can configure the security settings of the profile security to work with Mobile Management.

This task is a step in the process for configuring Mobile Management.

See “Configuring Mobile Management” on page 45.

To configure profile security settings

1. In the Symantec Management Console, click **Home**.
2. Expand **Configuration** and click **Mobile Management Server settings**.
3. In the **Mobile Management Server Settings** pane, click **Profile Security**.
4. (Optional) Enter any of the following settings:
   - **Profile Signing Cert Thumbprint** - The thumbprint of the certificate that is used for signing the Mobile Management server personal store.
   - **Profile Encryption Cert Thumbprint** - The thumbprint of the certificate that is used for encryption on the Mobile Management server personal store.
   - **Device Decryption Cert Config** - The credential payload that contains a certificate that is placed on devices for decryption.
   - **Device Signing Validation Cert Config** - The credential payload that contains a certificate that is placed on devices to validate signing.
   - **Device Signing/Encryption Root Cert Config** - The credential payload that contains a root certificate that is placed on devices to complete the certificate chain for the decryption and signing validation certificates.
5. Click **Save changes**.

Configuring iOS device MDM enrollment

If you set up the MDM Certificate to manage iOS devices, you must set up iOS device MDM enrollment. The Mobile Management server settings must be configured to include a cryptographic credential that is created during MDM Credential setup. The settings that you configure control how enrollment occurs and where iOS device users can get help. The settings also define how messages are sent to the Apple Push Notification Service. In addition, they define how the configuration profiles that are sent to iOS devices are secured against tampering or viewing by third parties.

This task is a step in the process for configuring Mobile Management.

See "Configuring Mobile Management" on page 45.

To configure iOS device MDM enrollment

1. In the Symantec Management Console, click **Home**.
2. Expand **Configuration** and click **iOS MDM Enrollment Configuration**.

3 In the **Push Certificate Subject** field, enter the subject of the Apple Push Notification Service certificate that is used for MDM.

For more information, see the *MDM Certificate Guide for iOS*.

If you use a development MDM Certificate and not a production certificate, select the **Use Development APNS Server**.

Warning: The state of the checkbox must match the state of the checkbox for **Use Development APNS** on the **APNS** tab of the Mobile Management server settings.

See "Configuring the site server to communicate with iOS devices" on page 47.

---

4 In the **Cryptographic credential used for authentication** field, choose the credential for Mobile Management to use for iOS device identification purposes.

5 Click **Save changes**.

Adding additional configuration profiles

If you want to send configuration profiles to all iOS devices on enrollment, you can add configuration profiles during setup. Adding configuration profiles at this point adds a point of failure. Therefore, if any configuration profiles do not successfully install on the iOS devices, the entire enrollment fails and rolls back.

Symantec recommends that you only send credentials profiles during enrollment. Symantec also recommends that you do not send policies that contain passcodes or restrictions during setup.

This task is a step in the process for configuring Mobile Management.

See "Configuring Mobile Management" on page 45.

To add additional configuration profiles

1 In the Symantec Management Console, click **Home**.

2 Expand **Configuration** and click **iOS MDM Enrollment Configuration**.

3 Under **Additional Configuration Profiles to include**, click the yellow star button.

4 In the **Symantec Management Console** window, select the configuration profile to include, and click **OK**.

See "Creating configuration profiles" on page 82.

5 Click **Save changes**.

See “About configuration profiles on iOS devices” on page 80.

Chapter 6

Setting up Exchange ActiveSync

This chapter includes the following topics:

- About using Exchange ActiveSync with Mobile Management
- Setting up Exchange ActiveSync
- Enabling the Exchange ActiveSync functionality
- Configuring the SymantecEASService NT
- Selecting the Exchange ActiveSync server
- Restarting the Mobile Management Service Agent
- Verifying the SymantecEASService configuration
- About connecting iOS devices to Exchange ActiveSync

About using Exchange ActiveSync with Mobile Management

Mobile Management has the capability to manage iPhone, Palm, and Android devices through the use of Exchange ActiveSync. Exchange ActiveSync is a protocol that synchronizes a mobile device with Microsoft Exchange. Exchange ActiveSync enables management, role-based access policies, and viewing details on individual devices or groups. It also lets you perform a range of administrative tasks.

Exchange ActiveSync supports the following device operating systems:

- Apple iOS 2.x, 3.x, and 4.x

- Windows Mobile 6.1 and 6.5
- Windows Phone 7
- Palm (hpWebOS) 1.4.5
- Nokia (running Mail for Exchange v3.0.50)

See "About connecting iOS devices to Exchange ActiveSync" on page 58.

See "Setting up Exchange ActiveSync" on page 54.

Setting up Exchange ActiveSync

You can set up Exchange ActiveSync to work with Mobile Management.

Table 6-1 Setting up Exchange ActiveSync

Step	Action	Description
Step 1	Set up an Exchange Administrator account.	Microsoft requires an Exchange Administrator account to secure communications and access Exchange ActiveSync. For more information and to sign up for an account, visit the following URL: http://technet.microsoft.com/en-us/exchange/default.aspx
Step 2	Enable Exchange ActiveSync functionality.	The Exchange ActiveSync functionality is not set up by default. You need to enable the Exchange ActiveSync functionality in the Symantec Management Console. See "Enabling the Exchange ActiveSync functionality" on page 56.
Step 3	Configure SymantecEASService NT Service.	For Mobile Management to communicate with Exchange ActiveSync, you need to configure the SymantecEASService NT. See "Configuring the SymantecEASService NT" on page 56.

Table 6-1 Setting up Exchange ActiveSync *(continued)*

Step	Action	Description
Step 4	Set access rights for the Exchange Administrator account.	See Microsoft Exchange ActiveSync documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558.aspx
Step 5	Secure the IIS Application Pool.	See Microsoft Exchange ActiveSync documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558.aspx
Step 6	Set up the Exchange Administrator account as a member of the correct groups.	Set up the Exchange Administrator account as a member of the local IIS_WPG group in Windows Server 2003 (IIS6) or as a member of the IIS_IUSRS group in Windows Server 2008 (IIS7). See Microsoft Exchange ActiveSync documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558.aspx
Step 7	Set up the Exchange Administrator account read and write access rights.	See Microsoft Exchange ActiveSync documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558.aspx
Step 8	(Optional) Give the Exchange ActiveSync Inventory and Service Policy Web Service domain admin privileges.	If you use Exchange ActiveSync 2010 the Exchange ActiveSync Inventory and Service Policy Web Service must have domain admin privileges.
Step 9	Restart the Application Pool.	See Microsoft Exchange ActiveSync documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558.aspx
Step 10	Select the Exchange ActiveSync server.	In the Symantec Management Console, select the server on which you want Exchange ActiveSync to be installed. See "Selecting the Exchange ActiveSync server" on page 57.

Table 6-1 Setting up Exchange ActiveSync *(continued)*

Step	Action	Description
Step 11	Restart the Mobile Management Service Agent.	Restart the Mobile Management Service Agent to refresh the settings. See "Restarting the Mobile Management Service Agent" on page 57.
Step 12	(Optional) Verify that the SymantecEASService configuration is correct.	After the Exchange ActiveSync setup is complete, you should verify that the SymantecEASService configuration and the EAS folders' security permissions are correct. See "Verifying the SymantecEASService configuration" on page 58.

See "About using Exchange ActiveSync with Mobile Management" on page 53.

Enabling the Exchange ActiveSync functionality

The Exchange ActiveSync functionality is not set up by default. You need to enable the Exchange ActiveSync functionality in the Symantec Management Console.

This task is a step in the process for setting up Exchange ActiveSync.

See "Setting up Exchange ActiveSync" on page 54.

To enable Exchange ActiveSync functionality

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**, and then click **Solution settings**.
3. In the right pane, check **Enable Exchange ActiveSync Functionality**.
4. Click **Save changes**.

Configuring the SymantecEASService NT

For Mobile Management to communicate with Exchange ActiveSync, you need to configure the SymantecEASService NT.

This task is a step in the process for setting up Exchange ActiveSync.

See "Setting up Exchange ActiveSync" on page 54.

To configure the SymantecEASService NT Service

1. On the **Start** menu, click **Administrative Tools > Services**.
2. Right-click **SymantecEASService**, and click **Properties**.
3. In the **Properties** dialog box, click the **Log On** tab.
4. Click **This Account** and click **Browse** to navigate to your Exchange Administrator account.
5. Click the Exchange Administrator account and enter the account password.
6. Click **Apply**.
7. (Optional) If a dialog box is displayed, click **OK** to allow the account to log on as a service.
8. Click **OK**.

Selecting the Exchange ActiveSync server

In the Symantec Management Console, select the server on which you want Exchange ActiveSync to be installed. The server hosting Exchange ActiveSync needs to be able to communicate with the Symantec Management Platform server.

This task is a step in the process for setting up Exchange ActiveSync.

See "Setting up Exchange ActiveSync" on page 54.

To select the Exchange ActiveSync server

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**, and then click **Solution settings**.
3. Under **Mobile Management Solution Settings**, check **Enable Exchange ActiveSync functionality**.
4. Under **Exchange ActiveSync Settings**, in the drop-down list, click the server that you configured with the Exchange Administrator Security and Permissions.
5. Click **Save changes**.

Restarting the Mobile Management Service Agent

Restart the Mobile Management Service Agent to refresh the settings.

This task is a step in the process for setting up Exchange ActiveSync.

See "Setting up Exchange ActiveSync" on page 54.

To restart the Mobile Management Service Agent

1. On the **Start** menu, click **Administrative Tools > Services**.
2. In the **Services** dialog box, click **Symantec Mobile Management Service Agent**.
3. Click **Restart the service**.
4. (Optional) On the toolbar, click **Action > Refresh** to see the current status of the SymantecEASService.

Verifying the SymantecEASService configuration

After the Exchange ActiveSync setup is complete, you should verify that the SymantecEASService configuration and the EAS folders' security permissions are correct.

This task is a step in the process for setting up Exchange ActiveSync.

See "Setting up Exchange ActiveSync" on page 54.

To verify the SymantecEASService configuration

1. On the **Start** menu, click **Administrative Tools > Event Viewer**.
2. In the **Event Viewer** window, click **Application**.
3. In the right pane, click **AthenaEASService**.

   Depending on the results of the setup and configuration, you see the following entries in the event log for the AthenaEASService source:

Service successfully transmitted a total of (6) ActiveSync device partnerships is displayed	The SymantecEASService configuration is correct.
An error message is displayed.	The SymantecEASService configuration is not correct.
An access denied error message is displayed.	The EAS folders' security permissions are not correct.

About connecting iOS devices to Exchange ActiveSync

You can find information about how to connect iOS devices to Exchange ActiveSync at the following locations:

- http://images.apple.com/iphone/business/docs/iPhone_EAS.pdf
- http://support.apple.com/kb/ht2480
- http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

See "About using Exchange ActiveSync with Mobile Management" on page 53.

Chapter 7

Setting up the Mobile Management Agent application on iOS devices

This chapter includes the following topics:

- About the Mobile Management Agent application on iOS devices
- Setting up the Mobile Management Agent application on iOS devices
- Downloading the Mobile Management Agent application from the Apple App Store
- Enrolling iOS devices
- Changing the enrollment URL to an email address for iOS devices
- Enabling and creating the End User License Agreement for iOS devices
- About the differences between the app store and the in-house Mobile Management Agent applications

About the Mobile Management Agent application on iOS devices

The Mobile Management Agent should be installed on all of the iOS devices in your environment. This agent lets Symantec Management Platform monitor and manage the devices.

After a Mobile Management server is created, you can install the Mobile Management Agent on the mobile devices in your environment. The agent lets

the mobile devices communicate with the Mobile Management server and Symantec Management Platform.

The agent also enables you to use Mobile Management to do the following:

- Automatically configure the device's access to corporate email and VPN.
- Publish a set of recommended applications, files, and links through the Mobile Library to the device.
- Automatically apply a set of policies to the device, such as security and passcode policies.
- Perform remote actions such as remote wipe, remote lock, and passcode reset.
- Get centralized reporting on the device.

See "Setting up the Mobile Management Agent application on iOS devices" on page 62.

See "Changing the enrollment URL to an email address for iOS devices" on page 65.

See "Enabling and creating the End User License Agreement for iOS devices" on page 65.

Setting up the Mobile Management Agent application on iOS devices

You can set up the Mobile Management Agent on iOS devices.

See "About the Mobile Management Agent application on iOS devices" on page 61.

Table 7-1 To set up the Mobile Management Agent application on iOS devices

Step	Task	Description
Step 1	There are two different ways to install the Mobile Management Agent, depending on how you want to distribute it to the device. One way is to have users download the Mobile Management Agent from the Apple App Store. Another way is to have users download the Mobile Management Agent from an internal Web site. See "About the differences between the app store and the in-house Mobile Management Agent applications" on page 66.	You can have users download the Mobile Management Agent from the Apple App Store. See "Downloading the Mobile Management Agent application from the Apple App Store" on page 63.
		You can create the Mobile Management Agent application for internal deployment and upload it to an internal site for download. After you have created the agent and uploaded it, users can browse to the internal Web site and download and install the agent. See "Creating the in-house Mobile Management Agent application" on page 134.
Step 2	After users have downloaded and installed the agent, they need to enroll their device.	After the Mobile Management Agent is installed on an iOS device, you must enroll it with a Mobile Management server. See "Enrolling iOS devices" on page 64.

Downloading the Mobile Management Agent application from the Apple App Store

Users can download the Mobile Management Agent iOS application from the Apple App Store. They can search for the Symantec Mobile Management app in the Apple App Store and then download it to the device.

This task is a step in the process for setting up the Mobile Management Agent application.

See "Setting up the Mobile Management Agent application on iOS devices" on page 62.

Enrolling iOS devices

After the Mobile Management Agent is installed on an iOS device, you must enroll it with a Mobile Management server.

Once a device is enrolled, the MDM enrollment configuration is set on the device. If you make changes to the MDM configuration the changes are not reflected on the device unless you re-enroll it.

See "About the Mobile Management Agent application on iOS devices" on page 61.

This task is a step in the process for setting up the Mobile Management Agent application.

See "Setting up the Mobile Management Agent application on iOS devices" on page 62.

To enroll the Mobile Management Agent iOS application

1. Tap the Mobile Management Agent iOS application on the iOS device to start it.
2. On the enrollment screen, provide the following information:
   - URL: http://*<Site Server Name or Address>*/MobileEnrollment/Symc-IOSEnroll.aspx
     See "Changing the enrollment URL to an email address for iOS devices" on page 65.
   - Name: Your domain user name.
   - Password: Your domain password.
   - **Note:** Name and password may not be required if authentication is disabled.
3. On the **License** screen, click **Yes**.

   See "Enabling and creating the End User License Agreement for iOS devices" on page 65.
4. Complete the enrollment wizard to enroll your device.

   When you enroll an agent that was downloaded from an internal Web site, you are directed back to the browser after enrollment is complete. To return to the Mobile Management Agent, close the browser and re-open the application.

Changing the enrollment URL to an email address for iOS devices

To make enrollment easier, you can change the Mobile Management Agent to request an email address instead of a URL. Set up a resource record in your domain controller . The resource record takes the domain of the email address and looks for the user's credentials.

See "About the Mobile Management Agent application on iOS devices" on page 61.

To change the enrollment URL to an email address

1. Log in to your domain controller and run DNS.
2. In DNS, navigate to the domain folder.
3. Right-click the folder, and then click **Other New Records...**.
4. In the **Resource record type** window, select **Text (TXT)** and then click **Create Record...**.
5. In the **New Resource Record** window, leave **Record name** blank. Enter the following value in **Text:**, and then click **OK**:

   OSIAGENTREGURL=http://<your-site-server-IP-or-Servername>/MobileEnrollment/Symc-IOSEnroll.ASPX

Enabling and creating the End User License Agreement for iOS devices

You can require users to accept an End User License Agreement (EULA) when they enroll the Mobile Management Agent on their iOS device. The EULA is specific to your company and can be created according to your needs.

See "About the Mobile Management Agent application on iOS devices" on page 61.

To enable the EULA for iOS devices

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**.
3. Click **Mobile Management Server settings**.
4. On the **Mobile Management Server settings** page, click the **Enrollment** tab.
5. Check **Require EULA acceptance**.
6. Click **Save changes**.

To create the EULA for iOS devices

1. On the site server, open the **Symantec > Mobile Management > Enrollment** folders.
2. Double-click `eula-en.html`.
3. Edit the EULA text and save the file. The device automatically replaces the placeholder EULA with your company's EULA.

About the differences between the app store and the in-house Mobile Management Agent applications

The most notable difference between the app store and in-house versions of the Mobile Management Agent application is the presence of the Applications tab. On the app store version of the Mobile Management Agent application, there is no applications tab. Any applications that are delivered to the device appear in the updates tab. These applications remain in the updates tab until a new item is delivered to the updates tab.

See "About the Mobile Management Agent application on iOS devices" on page 61.

Chapter 8

Setting up the Mobile Management Agent on Windows Mobile and BlackBerry devices

This chapter includes the following topics:

- About the Mobile Management Agent on Windows Mobile and BlackBerry devices
- Setting up the Mobile Management Agent on Windows Mobile devices
- Setting up the Mobile Management Agent on BlackBerry devices
- Setting the Mobile Management Agent configuration schedule for mobile devices

About the Mobile Management Agent on Windows Mobile and BlackBerry devices

The Mobile Management Agent should be installed on all of the Windows Mobile and BlackBerry devices in your environment. The agent enables Symantec Management Platform to monitor and manage them. After the Mobile Management Agent is installed, the device becomes a managed device.

After a Mobile Management server is created, you can install the Mobile Management Agent on the mobile devices in your environment. The agent lets

the mobile devices communicate with the Mobile Management server and Symantec Management Platform.

The agent also enables you to use Mobile Management to do the following:

- To configure the device's access to corporate email and VPN.
- To apply a set of policies to the device, such as security and passcode policies.
- To perform remote actions such as remote wipe, remote lock, and passcode reset.
- To get centralized reporting on the device.

See "Setting up the Mobile Management Agent on Windows Mobile devices" on page 68.

See "Setting up the Mobile Management Agent on BlackBerry devices" on page 69.

See "Setting the Mobile Management Agent configuration schedule for mobile devices" on page 70.

Setting up the Mobile Management Agent on Windows Mobile devices

After a Mobile Management server is created, you can install the Mobile Management Agent on the Windows Mobile devices in your environment. The Mobile Management Agent should be installed on all of the Windows Mobile and BlackBerry devices in your environment. This agent lets Symantec Management Platform monitor and manage the devices.

Note: Before you complete this procedure, make sure that Internet Information Services (IIS) is configured to run on the default port on the Mobile Management server. If IIS is configured to run on a non-default port, you must manually enter the port on the **Mobile Agent Install** page. By providing the appropriate port number, you ensure that you receive the proper URL to bootstrap the device or export the configuration file.

See "About the Mobile Management Agent on Windows Mobile and BlackBerry devices" on page 67.

See "Setting the Mobile Management Agent configuration schedule for mobile devices" on page 70.

To set up the Mobile Management Agent on Windows Mobile devices

1. On the Internet, go to http://<*MobileManagementServer*>/mobilemanagement to access the local site server Web page.

   Your **Mobile Agent download URL** can be found in the Symantec Management Platform. On the **Home** menu, click **Mobile Management**. Expand **Configuration** and then click **Agent installation**. On the **Mobile Agent Install** page, the **Mobile Agent download URL** is listed.
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 named `locatesiteserver-wince4.cab`.
4. Complete the rest of the installation process.

Setting up the Mobile Management Agent on BlackBerry devices

After a Mobile Management server is created, you can install the Mobile Management Agent on the BlackBerry devices in your environment. The Mobile Management Agent should be installed on all of the Windows Mobile and BlackBerry devices in your environment. The agent enables Symantec Management Platform to monitor and manage them.

See "About the Mobile Management Agent on Windows Mobile and BlackBerry devices" on page 67.

See "Setting the Mobile Management Agent configuration schedule for mobile devices" on page 70.

To set up the Mobile Management Agent on BlackBerry devices

1. In your browser, go to http://<*Site-Server name or IP adress*>/mobilemangement to access the local site server Web page.

   The **Mobile Agent download URL** can be found in the Symantec Management Platform. On the **Home** menu, click **Mobile Management**. Expand **Configuration** and then click **Agent installation**. On the **Mobile Agent Install** page, the **Mobile Agent download URL** is listed.
2. On the **Download Agent** screen, click **Download**.
3. In the **Application was sucessfully installed** dialog box, click **OK**.

Setting the Mobile Management Agent configuration schedule for mobile devices

You can choose how often agent configuration updates are requested on Windows Mobile and BlackBerry devices.

By default, agent configuration update requests occur every hour.

See "Setting up the Mobile Management Agent on Windows Mobile devices" on page 68.

See "About the Mobile Management Agent on Windows Mobile and BlackBerry devices" on page 67.

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, expand **Settings** > **Mobile Management** > **Mobile Agent Settings**.
3. Click **Agent Configuration Update Schedule**.
4. In the right pane, specify the configuration schedule information:
   - Number of units.
   - Type of unit. Either minutes, hours, or days.
5. Click **Save changes**.

Chapter 9

Managing the Mobile Library for iOS devices

This chapter includes the following topics:

- About the Mobile Library
- Setting up Mobile Library feeds
- Creating Mobile Library feeds
- Adding items to Mobile Library feeds
- Publishing an existing feed or item

About the Mobile Library

The Mobile Library enables you to publish sets of content to the managed iOS devices in your environment.

The Mobile Management Agent supports three types of content that you can publish:

- Applications – Commercial and in-house applications
- Documents – Documents, PDFs, presentations, and spreadsheets
- Media – YouTube video links, Web links, MP4 videos, images, graphics, MP3s, podcasts, and eBooks

Mobile Library content can be hosted on public application stores, Web sites, or private servers. The Mobile Library is delivered to the Mobile Management Agent as a set of RSS feeds. All feeds that match the Mobile Management Agent language selection on the device are delivered to the device. These feeds provide organizations with employees in multiple countries or with multiple languages

the content that is tailored to the language preference of the users. If there are multiple feeds for a language, all of the feeds are delivered to the device. If items in feeds are changed, the Mobile Management Agent updates the content in the Mobile Library. The items in the feeds are available on the device even when the device is offline.

The device to which you deliver the content determines the file size that is allowed.

Warning: Due to Apple restrictions, any applications that are installed from the Mobile Library are not remotely removable. Applications can only be removed by the end user. Also, any files that are sent to a device through the Mobile Library that are opened and saved in another application are not remotely removable.

See "Setting up Mobile Library feeds" on page 72.

Setting up Mobile Library feeds

This section explains the process for setting up Mobile Library feeds. Mobile Library feeds deliver sets of content to the managed iOS devices in your environment. This content can include applications, documents, and media.

See "About the Mobile Library" on page 71.

Table 9-1 Process for setting up Mobile Library feeds

Step	Action	Description
Step 1	Create the Mobile Library feed.	Create a Mobile Library feed that will contain the items you want to send to the devices. See "Creating Mobile Library feeds" on page 72.
Step 2	Add items to the Mobile Library feed.	Add the items of your choice to the feed. See "Adding items to Mobile Library feeds" on page 73.

Creating Mobile Library feeds

The Mobile Library feed contains the items that are sent when you publish sets of content to the managed iOS devices in your environment.

All feeds that match the Mobile Management Agent language selection on the device are delivered to the device. These feeds provide organizations with

employees in multiple countries or with multiple languages the content that is tailored to the language preference of the users. If there are multiple feeds for a language, all of the feeds are delivered to the device. If items in feeds are changed, the Mobile Management Agent updates the content in the Mobile Library. The items in the feeds are available on the device even when the device is offline.

See "About the Mobile Library" on page 71.

This task is a step in the process for setting up Mobile Library feeds.

See "Setting up Mobile Library feeds" on page 72.

To create a Mobile Library feed

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**, and then click **Mobile Library Editor**.
3. On the **Mobile Library** page, click **Feeds**.
4. On the **Feeds** page, click **New Feed**.
5. In the **Create New Feed** dialog box, specify the information.

   If you do not have a feed for every language, you can check **Feed Is Language Default**. The feed that has this checked is delivered to any devices whose set language does not have a corresponding feed.

   Check **Feed Is Published** if you want to publish the feed. If the feed is not published, it is not sent to the devices. If you want to configure the feed and add items to it before it is published, you may choose not to publish the feed immediately.

   See "Publishing an existing feed or item" on page 75.
6. Click **OK**.

Adding items to Mobile Library feeds

After you create a Mobile Library feed, you can add items to it. Items can include applications, documents, links, and media. The items in the feeds are available on the device even when the device is offline.

See "About the Mobile Library" on page 71.

This task is a step in the process for setting up Mobile Library feeds.

See "Setting up Mobile Library feeds" on page 72.

To add items to a Mobile Library feed

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**, and then click **Mobile Library Editor**.
3. On the **Mobile Library** page, click **Items**.
4. Under **Items**, select the feed to which you want to add items from the drop-down menu.
5. Click **New Item**.
6. In the **Create New Feed Item** dialog box, specify the information and upload the files.

Note: Files in items can be up to 25 MB.

- Check **Item Is Published** if you want to publish the item in the feed. If the item is not published, it is not sent to the devices. If you want to configure the item before it is published, you may choose not to publish the item immediately.
  See "Publishing an existing feed or item" on page 75.

- **Note:** Under **Platform Type**, unsupported platforms are listed. You must choose **iOS (iPhone/iPad/iPod Touch)** to deliver your item to the Mobile Library.

- **Item Priority** is used to sort the items in the feed on the agent. The following are the different options for the **Item Priority**:
  - **Optional** – The lowest priority items. Items appear toward the bottom of the list.
  - **Recommended** – Medium priority items. Items are displayed in the middle of the list.
  - **Required** – The highest priority items. Items are displayed at the top of the list. Required items also have a pop-up warning that appears to the user, informing them that there is a required item available. This warning appears even if the agent is in the background.
- Only upload one file per document item.
- When you select an application item, set the **Item Type** to **Commercial** or **In-house**.

- If you want to add a commercial application, you need to add the link to the application's App Store page in the field labeled **Item Link**. The App Store link is found on the application's App Store page.

  Warning: Do not edit the **Item Link** field when you create a commercial application. If you do so, the user who attempts to download the application item receives multiple error messages.

- If you want to add an in-house application, you must upload the `.ipa`, the `.plist`, and all image files that are referenced in the `.plist`. These files must be selected and uploaded in the following order: Image files, `.ipa` file, `.plist` file. The `.plist` and the `.ipa` files are generated after you archive the agent framework in Xcode and go through the sharing wizard. The Mobile Management server modifies the `.plist` file so that the file links automatically point to the application files on the Mobile Management server. Before saving the item in the library, you must upload the `.ipa`, the `.plist`, and the image files. For library items to appear with a custom icon, you must upload a `.png` file that is 57x57 pixels. Otherwise, a generic icon appears next to the item.

7 Click **OK**.

Publishing an existing feed or item

If you did not check **Item Is Published** when you created a feed or an item, you can publish the feed or item after you saved it.

See "About the Mobile Library" on page 71.

See "Setting up Mobile Library feeds" on page 72.

To publish an existing feed or item

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

2 In the left pane, expand **Configuration**, and then click **Mobile Library Editor**.

3 On the **Mobile Library** page, click the **Feeds** or **Items** tab.

4 On the **Feeds** or **Items** tab, select the green edit icon next to the feed or item you want to edit.

5 In the **Edit Feed** or **Edit Item** window, select **Feed Is Published** or **Item is Published**.

6 Click **OK**.

Chapter 10

Using actions, policies, and configuration profiles

This chapter includes the following topics:

- About actions
- Performing actions on mobile devices
- About policies
- Creating policies
- Assigning policies
- Supported policies for specific devices
- About configuration profiles on iOS devices
- Devices that support configuration profiles
- Setting up configuration profiles for iOS devices
- Creating configuration profiles
- Adding configuration profiles to a policy
- Assigning configuration profile policies
- About available configuration profile settings for iOS devices
- About AutoLock settings on iOS devices

About actions

Actions are the features available for devices based on the solutions that are installed in your environment. Depending on the device, the actions that are listed are different. Actions are available for all the devices in your environment.

See "Performing actions on mobile devices" on page 78.

Performing actions on mobile devices

This section explains how to perform actions on mobile devices. Actions are the features available for devices based on the solutions that are installed in your environment.

See "About actions" on page 78.

To perform actions on mobile devices

1. In the Symantec Management Console, on the **Manage** menu, click **Mobile > Devices**.
2. On the **Mobile** page, under **Name**, right-click the device name, and then click **Resource Manager**.
3. On the **Resource Manager** page, choose the actions for the mobile device.

About policies

Policies are collections of settings that Exchange ActiveSync enforces to ensure that devices are in compliance. Policies can include password, sync, and device settings. They can also include instructions to uninstall, install, or upgrade applications.

Policies are distributed and assigned through Exchange ActiveSync. Because of the way Microsoft licenses Exchange ActiveSync, each device manufacturer can choose what policy functionalities their devices support. It means that three devices with the same operating system could work completely differently even if they have the same policies assigned to them. Symantec recommends testing the devices in your environment to see how they react to the policies.

See "Creating policies" on page 79.

See "Assigning policies" on page 79.

See "Supported policies for specific devices" on page 80.

See "About configuration profiles on iOS devices" on page 80.

Creating policies

This section explains how to create policies. Policies are collections of settings that Exchange ActiveSync enforces to ensure that devices are in compliance. Policies can include password, sync, and device settings. They can also include instructions to uninstall, install, or upgrade applications.

See "About policies" on page 78.

See "Assigning policies" on page 79.

See "Supported policies for specific devices" on page 80.

To create a new policy for mobile devices

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Exchange ActiveSync**, and click **Manage policies...**.
3. In the **EAS Policy Editor** window, click the **Create New Policy** icon.
4. In the **Explorer User Prompt** dialog box, enter the name of the policy, and click **OK**.
5. In the right pane, configure the options and settings for the policy.
6. Click **Save changes**.

Assigning policies

Policies are assigned through Exchange ActiveSync. In the Symantec Management Console, you assign policies by device. However, the policy is assigned to the mailbox that is associated with the device. If there are multiple devices associated with the mailbox, all of the devices receive the policy that you assigned.

For more information, see the topics on assigning policies and targets in the *Symantec Management Platform Help*.

See "About policies" on page 78.

See "Creating policies" on page 79.

See "Supported policies for specific devices" on page 80.

To assign a policy

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Exchange ActiveSync**, and click **Assign Policy to devices...**.

3 In the **Assign EAS Policy** window, in the left pane, click the policy that you want to assign to the devices.

In the right pane, under **Applied To**, specify to which devices you want to apply the policy, and then click **Save Changes**.

The set policy is automatically applied to all new devices that match the settings you specify by using **Filters**, **Groups**, or by excluding specific resources. If you want to target a specific device or list of devices, then you should specifically pick those devices. Use the **Resource List** filtering criteria to select the desired devices. Right-click the specific devices to exclude them from the filtered lists. Click **Update Results** to verify what devices are targeted.

4 On the upper right corner of the page, click the colored circle and then click **On** to turn on the policy.

5 Click **Save Changes**.

Note: When you assign the Mobile Management Service Install (x86) policy, you must first have added a Mobile Management Server. If you have not added a Mobile Management Server, no computers are listed for this policy. To add a Mobile Management Server, navigate to the Mobile Management Server. Once servers are added on the page they show up in the policy.

Supported policies for specific devices

For a list of devices and the policies they support, see the following article on the Symantec knowledge base .

BlackBerry devices are not listed in the article because Mobile Management policies are not supported on BlackBerry devices. Any policies you want to enforce on BlackBerry devices must be created through the BlackBerry Enterprise Server (BES).

http://www.symantec.com/docs/HOWTO35972

See "About policies" on page 78.

About configuration profiles on iOS devices

Configuration profiles are the XML files that are used to configure sets of preferences and configurations. They can contain security policies and restrictions, VPN information, WiFi settings, email and calendar accounts, and authentication credentials.

With Mobile Management, configuration profiles let you set how often inventory data is collected from the managed iOS devices in your environment. Through configuration profiles, you can also choose how often and at what time the payload information is sent to the Mobile Management server and Symantec Management Platform. Configuration profiles are delivered through policies to selected devices.

See "Setting up configuration profiles for iOS devices" on page 82.

See "Devices that support configuration profiles" on page 81.

See "About policies" on page 78.

Devices that support configuration profiles

The following table contains the iOS devices that support configuration profiles.

See "About configuration profiles on iOS devices" on page 80.

Table 10-1

Device	Supported version
iPhone	Minimum iOS version ■ 4.1 Models supported ■ 3G ■ 3GS ■ 4
iPod Touch	Minimum iOS version ■ 4.1 Models supported ■ 2nd generation ■ 3rd generation ■ 4th generation
iPad	Minimum iOS version ■ 4.2 Models supported ■ All models

Setting up configuration profiles for iOS devices

The following table contains the process to set up configuration profiles for iOS devices. Configuration profiles contain device security policies and restrictions, VPN configuration information, WiFi settings, email and calendar accounts, and authentication credentials. Configuration profiles allow iOS devices to work with your enterprise systems.

See "About configuration profiles on iOS devices" on page 80.

See "Devices that support configuration profiles" on page 81.

Table 10-2 Process for setting up configuration profiles for iOS devices

Step	Task	Description
Step 1	Create the configuration profiles.	Create a configuration profile that contains the settings of your choice. See "Creating configuration profiles" on page 82.
Step 2	Add the configuration profiles to a policy.	When you have created the configuration profile, you need to add it to a policy. See "Adding configuration profiles to a policy" on page 83.
Step 3	Assign the policy.	Apply the policy to the devices you want to target. See "Assigning configuration profile policies" on page 84.

Creating configuration profiles

Configuration profiles are the files that configure the settings on iOS devices. Configuration profiles contain one or more configuration payloads.

Configuration payloads are individual collections of settings within a configuration profile. For example, VPN settings.

This task is a step in the process for setting up configuration profiles with iOS devices.

See "Setting up configuration profiles for iOS devices" on page 82.

To create a configuration profile

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**, and then click **iOS Configuration Editor**.
3. On the **iOS Configuration Editor** page, in the left pane, under **iOS Configuration Profiles**, click the type of payload that you want to add to the configuration profile.
4. In the right pane, click the yellow star button to create a new payload and then specify the payload options.
   - You must enter a value in the **Host** field for every payload.
   - You must enter a value in the **Mail Server**, **Port**, and **Email Address** fields for the email payload.
   - **Warning:** Do not enter a number greater than 65535 in the CalDAV and CardDAV port fields.
   - Some of the payload settings include specific values you should enter. For example, in the Exchange ActiveSync payload, enter values for **Account Name**, Exchange ActiveSync **Host**, **Use SSL**, and **Past Days of Mail to Sync**. However, it is best to leave **User**, **Email Address**, and **Password** blank. See "About available configuration profile settings for iOS devices" on page 85.
   - If CalDAV **Account Username**, CardDAV **Account Username**, Exchange ActiveSync **User**, **User Name** on the **Incoming Mail** tab, **User Name** on the **Outgoing Mail** tab, LDAP **Account Username**, Subscribed Calendars **Username** are left blank, the validated user name is substituted. The validated user name is also added to the **Email address domain name**. For example, *validatedusername@domainname*.com.
5. Click **Save Changes**.

Adding configuration profiles to a policy

After you have created the configuration profiles you need to add them to a policy. Most configuration profiles are distributed to the devices in your environment through policies. Some configuration profiles can also be distributed on enrollment.

This task is a step in the process for setting up configuration profiles with iOS devices.

See "Setting up configuration profiles for iOS devices" on page 82.

Unlike the policies that are enforced through Exchange ActiveSync, policies on iOS devices always act the same way.

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

See "About policies" on page 78.

See "Adding additional configuration profiles" on page 50.

To add configuration profiles to a policy

1. In the Symantec Management Console, on the **Manage** menu, click **Policies**.
2. Expand **Policies > Mobile Management**, and right-click **Mobile Configuration Policies**.
3. Click **New > Mobile Device Configuration Policy**.
4. In the right pane, click the **New Mobile Device Configuration Policy** title, and then enter a name for your configuration profile policy.

   If you want to rename the policy, either do it before you edit the policy or after you have saved it. If you edit the policy and then change the name before you save it, your settings and edits are lost.
5. Under **Profile settings**, specify the settings.

   You can sign and encrypt profiles and allow end users to remove the profiles that are included in the policy. This removal can be done without having to remove the full MDM profile. You can also specify whether a password is required for user removal of the policy set. These settings are applied to all of the profiles that are included in this policy.
6. Under **Configuration settings**, click the yellow star button.
7. In the **Symantec Management Console** dialog box, select the preconfigured profiles that you want to add to the policy, and then click **OK**.
8. Click **Save Changes**.

Assigning configuration profile policies

After you have created the configuration profiles you need to distribute them to the devices in your environment. The distribution is done by using policies.

This task is a step in the process for setting up configuration profiles with iOS devices.

See "Setting up configuration profiles for iOS devices" on page 82.

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

To assign a configuration profile policy

1. In the Symantec Management Console, on the **Manage** menu, click **Policies**.
2. Expand **Policies > Mobile Management > Mobile Configuration Policies**.
3. Click the policy that you want to assign.
4. Under **Applied To**, specify to which devices you want to apply the policy, and then click **Ok**.

   The set policy is automatically applied to all new devices that match the settings you specify by using **Filters** and **Groups** or by excluding specific resources. If you want to target a specific device or list of devices, then you should specifically pick those devices. Use the **Resource List** filtering criteria to select the desired devices. Right-click the specific devices to exclude them from the filtered lists. Click **Update Results** to verify which devices are targeted.
5. On the upper right corner of the page, click the colored circle and then click **On** to turn on the policy. When the policy is turned on, it is delivered to the devices.
6. Click **Save Changes**.

About available configuration profile settings for iOS devices

The available configuration profile settings specify the details of the configuration settings you can apply to the devices. The settings define device security policies and restrictions, VPN configuration information, WiFi settings, email and calendar accounts, and authentication credentials.

For more details about the different profiles, see the topics about creating configuration profiles in Apple's *iPhone Configuration Utility* guide. You can find the guide at the following URL:

developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility

Though most of the profiles available with Mobile Management are the same as Apple's, there are a few differences. The following table outlines the differences between Symantec's and Apple's configuration profiles.

Table 10-3 Configuration profile differences with Mobile Management

Profile	Notes
Web Clip	When you use Mobile Management, web clip URLs must contain http:// or https://. Also, the **Item Icon** for web links may change after the user clicks the link for the first time. The **Item Icon** changes to the web link's default icon if the creator of the Web page set a default icon. The **Item Icon** of web links to video pages does not change.
Credentials	**View Certificate** shows different information in the Symantec Management Console than in the Apple Configuration Utility.
Passcode	The AutoLock options in the Symantec console are different than in the Apple Configuration Utility. See "About AutoLock settings on iOS devices" on page 86.
Email	You can add the user's email address in two different formats in the Symantec Management Console. In the Apple Configuration Utility only one format is accepted.
Mobile Device Management	This profile is removed in the Symantec Management Console.

See "About configuration profiles on iOS devices" on page 80.

About AutoLock settings on iOS devices

AutoLock settings are settings sent to iOS devices through passcode configuration profiles. However, the AutoLock setting can react differently depending on the iOS device it is sent to. If the iOS device changes the AutoLock setting, it opts for a stricter setting than the one that is in the configuration profile. For example, a configuration profile specifying a 3-minute AutoLock was sent to an iPad and an iPhone. The iPad automatically rounds up the AutoLock to 2 minutes, the strictest setting on the iPad. The iPhone leaves the AutoLock setting at 3 minutes.

Unless the configuration profile sends down the strictest AutoLock setting, the user of the device can reset the AutoLock setting to a stricter setting.

The following chart shows the relationship between possible AutoLock settings and how they are interpreted on different iOS devices:

Table 10-4 iOS Passcode configuration profile AutoLock behavior

AutoLock setting	Result on iPhone/iPod Touch	Result on iPad
1 minute	1 minute	2 minutes
2 minutes	2 minutes	2 minutes
3 minutes	3 minutes	2 minutes
4 minutes	4 minutes	2 minutes
5 minutes	5 minutes	5 minutes
10 minutes	5 minutes	10 minutes
15 minutes	5 minutes	15 minutes
--	Never	Never

See "About available configuration profile settings for iOS devices" on page 85.

Chapter 11

Using inventory data, reports, and the event log

This chapter includes the following topics:

- About inventory data
- Viewing inventory data
- Setting the inventory schedule for Windows Mobile devices
- Setting the inventory schedule for iOS devices
- About reports
- Running reports
- Available reports by device
- About event logs
- Viewing the event log

About inventory data

Inventory data is detailed data viewable per device in Symantec Management Platform. Inventory data is collected from all of the devices in your environment.

A full inventory scan runs once a day through Exchange ActiveSync. Incremental inventory scans through Exchange ActiveSync run every five minutes to check for new devices.

The Mobile Management Agent also runs an inventory scan. The inventory schedule of the agent is configurable on Windows Mobile and iOS devices.

See "Setting the inventory schedule for Windows Mobile devices" on page 90.

See "Setting the inventory schedule for iOS devices" on page 91.

See "Viewing inventory data" on page 90.

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

Viewing inventory data

After the inventory scan you can view the inventory data that is collected.

See "About inventory data" on page 89.

See "Setting the inventory schedule for Windows Mobile devices" on page 90.

See "Setting the inventory schedule for iOS devices" on page 91.

To view inventory data

1. In the Symantec Management Console, on the **Manage** menu, click **Mobile > Devices**.
2. On the **Mobile** page, under **Name**, right-click the device name, and then click **Resource Manager**.
3. On the **Resource Manager** page, on the **View** menu, click **Inventory**.
4. In the center pane, expand **Data Classes > Inventory > Mobile Inventory**, and click the inventory that you want to view.

   You can also switch between the **Current** and **History** tabs in the right pane to view current and past inventory data.

Setting the inventory schedule for Windows Mobile devices

You can set the schedule for how often inventory data is collected and sent to Symantec Management Platform for Windows Mobile devices.

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. 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.

See "About inventory data" on page 89.

Setting the inventory schedule for Windows Mobile devices

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Settings > Mobile Management > Mobile Agent Settings**.
3. Click **Inventory Schedule**.
4. In the right pane, specify the **Sample** schedule information:
   - Number of units.
   - Type of unit. Either hours or days.
   - Hour and minutes.

   The **Sample** schedule specifies when data is collected from a mobile device.
5. Specify the **Transmit** schedule information:
   - Number of units.
   - Type of unit. Either hours or days.
   - Hours and minutes.

   The **Transmit** schedule specifies when the collected data is sent to the Mobile Management server and then to Symantec Management Platform.
6. Specify the **Heartbeat** schedule in minutes.

   The **Heartbeat** schedule specifies when the device sends a short message to the Mobile Management server to let it know that it is still connected.
7. Click **Save changes**.

Setting the inventory schedule for iOS devices

You can set the schedule for the inventory that the Mobile Management Agent collects on iOS devices. Two types of inventory are collected on iOS devices. One type is through the MDM certificate. The other type is through the Mobile Management Agent.

By default, the inventory data that the MDM certificate collects is transmitted once a day. This inventory schedule is not configurable through the Symantec Management Console. The MDM certificate collects the following inventories:

See "About inventory data" on page 89.

- Mobile_Certificate_iOS
- Mobile_Device_iOS_MDM

- Mobile_GlobalRestrictions_iOS
- Mobile_Profile_iOS
- Mobile_ProfileContent_iOS
- Mobile_ProfileRestrictions_iOS
- Mobile_Program_iOS
- Mobile_Provisioning_Profile_iOS
- Mobile_SecurityInfo_iOS

By default, the inventory data that the Mobile Management Agent collects is transmitted once a day. You can change this iOS agent inventory transmit schedule. The Mobile Management Agent collects the following inventories:

- Mobile_Device
- Mobile_Device_iOS
- Mobile_Device_Site_Server
- Mobile_Identification
- Mobile_Memory
- Mobile_Operating_System
- Mobile_Power

To set the agent inventory schedule for iOS devices

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**.
3. Click **Mobile Management Server settings**.
4. On the **Agent** tab, set the **Report Frequency (seconds)**.

   Note: The minimum reporting frequency is 600 seconds.

5. Click **Save changes**.

About reports

Mobile Management lets you run reports on all of the devices in your environment. In the Symantec Management Console, you can choose from a list of pre-made reports that collect and provide data from the devices in your environment in real

time. The reports can contain summary information, such as lists of devices by manufacturer, platform, or operating system. The reports can also list the devices that are running out of memory or battery power.

Most of the reports contain customizable parameters. These parameters may include options such as whether you want the latest information or information from the last report that was saved. In some reports, you can also enter the timeframe from which the information is collected.

See "Running reports" on page 93.

See "Available reports by device" on page 93.

Running reports

Most of the reports contain customizable parameters. These parameters may include options such as whether you want the latest information or information from the last report that was saved. In some reports, you can also enter the timeframe from which the information is collected.

See "About reports" on page 92.

See "Available reports by device" on page 93.

To run reports

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Reports > Mobile Management**.
3. Click one of the standard reports that are listed. After the report runs, the data appears in the right pane.

Available reports by device

The following table lists the possible devices in your environment and the reports that are available on them.

See "About reports" on page 92.

See "Running reports" on page 93.

Table 11-1 Available reports by device

Device	Supported reports
iOS	■ **Detailed iOS Device Status** ■ **Devices by Manufacturer** ■ **Devices by Platform and Operating System** ■ **Devices with Low Battery** ■ **Devices with Low Program Memory** ■ **Devices with Outdated Inventory** ■ **Jailbroken iOS Devices** ■ **Mobile Device Summary** ■ **Remote Management Activity Audit** ■ **Remote Management Usage Summary By Action** ■ **Remote Management Usage Summary By Device** ■ **Software Compliance Remediation Summary** ■ **Software Compliance Status** ■ **Software Installation Summary**
BlackBerry and Windows Mobile	■ **Devices by Manufacturer** ■ **Devices by Platform and Operating System** ■ **Devices with Low Battery** ■ **Devices with Low Program Memory** ■ **Devices with Outdated Inventory** ■ **Mobile Device Summary** ■ **Remote Management Activity Audit** ■ **Remote Management Usage Summary By Action** ■ **Remote Management Usage Summary By Device** ■ **Software Compliance Remediation Summary** ■ **Software Compliance Status** ■ **Software Installation Summary**

Table 11-1 Available reports by device *(continued)*

Device	Supported reports
Palm/hpWebOS and Symbian/Nokia	■ **Exchange ActiveSync Devices by Policy** ■ **Exchange ActiveSync Devices with Pending Wipe** ■ **Non-Synced Exchange ActiveSync Devices** ■ **Wiped Exchange ActiveSync Devices**

About event logs

Mobile Management provides a history of important events for managed devices in your environment through the event log. For example, if someone tries to break into the device, it is recorded in the event log. This feature allows the administrator to detect and monitor security risks on each device. The event log is available for the devices on which the Mobile Management Agent is installed.

See "Viewing the event log" on page 95.

Viewing the event log

Events on managed devices are automatically recorded. You can view the event logs for your managed devices through the Symantec Management Console.

See "About event logs" on page 95.

To view the event log

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Inventory**, and click **Devices by Operating System**.
3. On the **Mobile Management Portal** page, under **Devices by Operating System**, click the part of the graph that represents the operating system of the device that you want to view.
4. Under **Device Name**, right-click the device name, and then click **Resource Manager**.
5. On the **Resource Manager** page, on the **View** menu, click **Events**.
6. Expand **Data Classes > Mobile Events > Inventory**, and then click **Mobile _Log**.

Chapter 12

Remotely managing devices

This chapter includes the following topics:

- About remotely managing devices
- Creating remote settings for devices
- Starting a remote session with a device
- Remote options for Windows Mobile devices
- Remote options for BlackBerry devices
- Function key mapping during remote sessions with Windows Mobile devices
- Function key mapping during remote sessions with BlackBerry devices
- Options for remotely wiping devices

About remotely managing devices

Mobile Management lets you remotely access the Windows Mobile and BlackBerry devices in your environment on which the Mobile Management Agent is installed.

During a remote session, you can view and fix any problems a user experiences on their device. Mobile Management allows access to the file system, registry, and processes subsystems of the managed mobile device.

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 "Creating remote settings for devices" on page 98.

See "Starting a remote session with a device" on page 99.

Creating remote settings for devices

In Symantec Management Platform, you can determine how every remote session looks and behaves.

On Windows Mobile devices, you can set the Request behavior, Control behavior, and color depth and size of remote sessions. The Request behavior determines how the remote session request is handled. The Control behavior determines how the remote session handles keyboard and mouse interactions.

On BlackBerry devices, you can set the color depth and size of remote sessions.

See "About remotely managing devices" on page 97.

See "Starting a remote session with a device" on page 99.

To create the remote settings for mobile devices

1. In the Symantec Management Console, on the **Home** menu, click **Mobile Management**.
2. In the left pane, expand **Configuration**, and then click **Remote Control settings**.
3. (Windows Mobile only) On the **Remote Control Policy** page, under **Remote Control Session Settings**, 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**
4. (Windows Mobile only) 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**
5. 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.

6 Select the size scale for the session.

You can select either the same size (1x) or twice the size (2x).

7 Click **Save changes** to save your remote settings.

Starting a remote session with a device

Through a remote session, you can control any managed device in your organization.

The remote session uses the remote settings that you can define in the Symantec Management Console.

If you press a function key on your computer, it performs an action on the 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 "Creating remote settings for devices" on page 98.

See "Function key mapping during remote sessions with Windows Mobile devices" on page 103.

See "Function key mapping during remote sessions with BlackBerry devices" on page 104.

See "Remote options for Windows Mobile devices" on page 99.

See "Remote options for BlackBerry devices" on page 102.

To start a remote session with a device

1 In the Symantec Management Console, on the **Actions** menu, click **Mobile > Remote Management**.

2 On the **Remote Management** page, click the mobile device to which you want to connect.

3 Click **Connect**.

Remote options for Windows Mobile devices

After connecting to a Windows Mobile device, you can choose from several options that provide access to the device. For example, you can remotely control the device and manage its file system, registry, and processes subsystems.

The right pane of the device page contains the static information that was last captured in the inventory scan. If you click an option in the left pane, data appears

in the right pane. The information might take a few seconds to load because it is collected in real time.

See "Starting a remote session with a device" on page 99.

Table 12-1 Remote options for Windows Mobile devices

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

Table 12-1 Remote options for Windows Mobile devices *(continued)*

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

Remote options for BlackBerry devices

After connecting to a BlackBerry device, you can choose from several options that provide access to the device.

The right pane of the device page contains the static information that was last captured in the inventory scan. If you click an option in the left pane, data appears in the right pane. The information might take a few seconds to load because it is collected in real time.

See "Starting a remote session with a device" on page 99.

Table 12-2 Remote options for BlackBerry devices

Option	Description
Device name	Lists the static information about the device that was collected during the last inventory scan. For example, the date that the inventory was last collected, the name, and the IP address of the device.
Remote Control	Lets you remotely control and view the mobile device. You can start processes and explore the device by double-clicking this option. In the **Remote Control** window, you can also choose the color and the zoom options for the session. If you click the camera symbol in the **Remote Control** window, you can take a screen shot of the mobile device. However, even if you select the 2-bit color option in your remote settings, the screen shot reflects the device's color settings.
Identification	Lists the identifying information for the device. For example, the name, ID, and OEM ID of the device.
Operating System	Lists the information about the operating system that is currently running on the device. For example, the type, ID, and version number of the platform that is on the device.
Power	Lists the information about the battery and the power for the device. For example, the voltage, temperature, and chemistry of the battery in the device.
Memory	Lists the information about the memory for the device. For example, the percentage load, total and available physical and virtual memory, and storage memory for the device.
Display	Lists the horizontal and the vertical resolution and the display colors of the device.

Table 12-2 Remote options for BlackBerry devices *(continued)*

Option	Description
General Statistics	Lists the number of bytes Sent and Received.
GSM	Lists the information about the GSM Network adapter configuration.
CDMA	Lists the information about the CDMA Network adapter configuration.
WLAN	Lists the information about the WLAN Network adapter configuration.
Applications	Lists the applications that are currently installed on the device. You can remove applications from the device through this page.
Modules	Lets you list and search the modules for the installed applications on the Blackberry Smartphone.

Function key mapping during remote sessions with Windows Mobile devices

To remotely control the devices that do not have a touch screen, you can use your computer keyboard to perform remote actions on the device. However, the effect that each function key has on the mobile device may be different than the effect that it usually has on your computer.

See "Starting a remote session with a device" on page 99.

Table 12-3 Function key mapping during remote sessions with Windows Mobile devices

Computer function key	Remote control action on device
Arrow keys	Navigate to the left, right, up, or down.
Backspace	Backspace.
Insert	Open the menu.
End	End.
Enter	Run the action.
Esc	Go back.

Table 12-3 Function key mapping during remote sessions with Windows Mobile devices *(continued)*

Computer function key	Remote control action on device
F1	Use the soft key 1 (left).
F2	Use the soft key 2 (right).
F3	Talk.
F4	End, or lock.
F6	Mute the sound volume.
F7	Decrease the sound volume.
F8	Use the dial pad * symbol, or increase the sound volume.
F9	Navigation click, or use the Dial pad # symbol.
F10	Create voice notes or record audio.
F11	Open the symbol list.
Home	Send.
Page Up	Use the left convenience key.
Page Down	Use the right convenience key.

Function key mapping during remote sessions with BlackBerry devices

To remote control the devices that do not have a touch screen, you can use your computer keyboard to perform remote actions on the device. However, the effect that each function key has on the mobile device may be different than the effect that it usually has on your computer.

See "Starting a remote session with a device" on page 99.

Table 12-4 Function key mapping during remote sessions with BlackBerry devices

Computer function key	Remote control action on device
Arrow keys	Navigate to the left, right, up, or down.

Table 12-4 Function key mapping during remote sessions with BlackBerry devices *(continued)*

Computer function key	Remote control action on device
Insert	Open the menu.
Esc	Go back.
Home	Send.
End	End.
F4	Lock.
F6	Mute the sound volume.
F7	Decrease the sound volume.
F8	Increase the sound volume.
F9	Navigation click.
Page Up	Use the left convenience key.
Page Down	Use the right convenience key.

Options for remotely wiping devices

This table describes the different ways you can remotely wipe devices. Devices can be wiped in multiple ways through actions, policies, and the Mobile Management Agent.

Table 12-5 Options to remotely wipe devices

Option	Description
Wipe Device	This action can be performed through Exchange ActiveSync. It performs a complete wipe of the device. Personal data and other information is removed from the device, and the device is completely reset. This action can also be performed on iOS devices through the Apple Push Notification Service. The functionality is the same as when the action is performed through Exchange ActiveSync. See "About actions" on page 78.
Delete Partnership	This action can be performed through Exchange ActiveSync. It removes the device's partnership in Exchange. The device can reestablish the partnership in Exchange by attempting to sync and thus reenable the trust connection between the server and the device. To remove the device's partnership so that it cannot reestablish it, you must complete this action and remove the partnership on the device. See "About actions" on page 78.
Clear Wipe	This action can be performed through Exchange ActiveSync. It lets you cancel the Wipe Device action. See "About actions" on page 78.

Table 12-5 Options to remotely wipe devices *(continued)*

Option	Description
Remove MDM and Reset Agent	This action performs a full wipe of all of the Mobile Management components on iOS devices through the Apple Push Notification Service. This wipe includes all of the corporate settings and the Mobile Library. When the corporate email settings are removed, all the email content, contacts, and calendar information that is associated with the profile is wiped. However, the Mobile Management Agent is not removed. The user can re-enroll the device after it has been wiped. See "About actions" on page 78.
Selective wipe	This action lets you selectively wipe devices by deleting or turning off individual policies. If you delete or turn off an individual policy, the policy privileges are revoked. See "About policies" on page 78.

Chapter 13

Managing software on Windows Mobile devices

This chapter includes the following topics:

- About software management on Windows Mobile devices
- Creating software packages for Windows Mobile devices
- Delivering software packages to Windows Mobile devices
- Configuring the software maintenance windows
- Software package actions
- Software package health actions
- Sample AppUpdate runtime substitution tokens

About software management on Windows Mobile devices

Mobile Management lets you manage software and software settings on the Windows Mobile devices in your environment. Software packages can contain single pieces of software, multiple pieces of software, or actions that run on the devices. You can also create upgrade packages and packages to remove other software packages.

Through the Symantec Management Console, you can create, change, and deliver software packages.

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

See "Creating software packages for Windows Mobile devices" on page 110.

See "Delivering software packages to Windows Mobile devices" on page 111.

Creating software packages for Windows Mobile devices

Software packages can contain single pieces of software, multiple pieces of software, or actions that run on the devices. You can also create upgrade packages and packages to remove other software packages.

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

See "About software management on Windows Mobile devices" on page 109.

See "Delivering software packages to Windows Mobile devices" on page 111.

To create software packages for Windows Mobile devices

1. In the Symantec Management Console, on the **Manage** menu, click **Mobile > Software**.
2. In the left pane, expand **Software > Mobile Software**.
3. Right-click the **Mobile Software** folder and then click **New > Mobile Software**.
4. In the right pane, click the **New Mobile Software** title and enter a name for your software package.
5. On the **Properties** tab, enter the version of the software.
6. 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 must run the software update manually (using AppUpdate) on the device.
7. 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.
8. On the **Package** tab, click **Add package** to add software to the package.

   You can add packages or edit the actions on each package from the **Package** tab.
9. In the **Add or Edit Package** dialog box on the **Details** page, specify the details of your package. The **Name** field is the only one that is required.

10 Click **Add** and browse to the file you want to include in your package.

11 On the **Package Server** tab, specify the **Package Destination Location**. In the **Assign package to** menu, select a server. Click **OK** to add the software to the package.

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

- On the **Actions** tab, you can choose the actions to perform on software resources and the order in which the actions are performed.
  See "Software package actions" on page 113.
- Click the **Add New Action** symbol to select other actions to perform on software resources. You can use the AppUpdate runtime substitution tokens when you define the actions.
  See "Sample AppUpdate runtime substitution tokens" on page 130.
- You can click the **Edit** symbol and select an action to edit a current action.

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

- The **Health** tab lets you choose the data that is checked to ensure that the software installs correctly.
- You can add your own metrics and choose from the **File Hash**, **Version**, or **Size** statistics.
  See "Software package health actions" on page 127.

14 Click **Save changes**.

Delivering software packages to Windows Mobile devices

Mobile Management lets you deliver the software packages that you have created to managed Windows Mobile devices through policies.

Software packages are delivered according to the schedule that the maintenance windows set. By default, there are no maintenance windows policies enabled. A maintenance windows policy must be enabled to allow for the scheduled delivery of software. The integrity of the software is checked and repaired when the software delivery or configuration policy runs.

See "About software management on Windows Mobile devices" on page 109.

See "Creating software packages for Windows Mobile devices" on page 110.

See "Configuring the software maintenance windows" on page 112.

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

To deliver software to Windows Mobile devices

1. In the Symantec Management Console, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Policies > Mobile Management**.
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 enter a name for your software delivery policy.
6. Click **Select Software** in the right pane.
7. On the **Select Software** page, select the package that you want to include in your policy.
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 **Resources** to choose the devices to which to deliver the software and click **Ok**.

    The set policy is automatically applied to all new devices that match the settings you specify by using **Filters**, **Groups**, or by excluding specific resources. If you want to target a specific device or list of devices, then you should specifically pick those devices. Use the **Resource List** filtering criteria to select the desired devices. Right-click the specific devices to exclude them from the filtered lists. Click **Update Results** to verify what devices are targeted.
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** to deliver your software packages to the selected devices.

Configuring the software maintenance windows

Software maintenance windows configure the Mobile Management Agent and tell it when to perform software update checks.

See "Delivering software packages to Windows Mobile devices" on page 111.

To configure software maintenance windows

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Mobile Management > Mobile Software Maintenance Windows**.
3. Right-click the **Mobile Software Maintenance Windows** folder.
4. Click **New > Mobile Maintenance Window**.
5. In the right pane, click the **New Mobile Maintenance Window** title and enter a name for your software maintenance window.
6. Configure your software maintenance window.
7. Click the down arrow next to **Applied To**.

   The set policy is automatically applied to all new devices that match the settings you specify by using **Filters**, **Groups**, or by excluding specific resources. If you want to target a specific device or list of devices, then you should specifically pick those devices. Use the **Resource List** filtering criteria to select the desired devices. Right-click the specific devices to exclude them from the filtered lists. Click **Update Results** to verify what devices are targeted.
8. At the upper right corner of the page, click the colored circle, and then click **On** to turn on the policy.
9. Click **Apply** to apply your software maintenance window to the selected devices.

Software package actions

The following table describes the install actions, settings, and parameters that can be entered when you configure software package actions.

Table 13-1 Software package actions

Action	Description
Download	Specifies an Install Action that executes a file download for the following settings: Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Download Actions Settings ■ Source - contains the Web server directory path and file name of the file to be downloaded to the device if required by versioning. ■ Target - {DeviceFileName} data type. Text value that specifies the Web server directory path and file name of the file to be downloaded to the device if versioning indicates it is required. This string can contain any device subdirectories prefixing the file name. Note that the AppUpdate Runtime Substitution Token values can be used within the value to define target subdirectories for target files. See "Sample AppUpdate runtime substitution tokens" on page 130. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
Install	Specifies an Install Action that installs an installable file such as a CAB. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Install Action Settings The following parameters specify the name of the installable file: ■ Command - {command value} data type. Optional text value that specifies an installation command. ■ File - {localfilename} data type. Text value which specifies a file name of an installable file residing on the device. Installable files include CAB files, ActiveX DLL files, REG import files, CPF files in OMA format and other XML formats which follow install file guidelines. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
Uninstall	Specifies an Install Action that uninstalls an installed CAB file. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Uninstall Action Settings The application to uninstall, specified by the following: ■ Name - {applicationname} data type. Text that specifies the name of an application that is installed on a device. The application name can be located by navigating on the device to **Start > Settings > System > Remove Programs**. Any applications appearing in the list can be specified for Uninstall. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
Process>WarmBoot	Specifies an Install Action that soft/warm resets the device when all actions for the specified package are completed (not at the time the WarmBoot Action is encountered or after the last action of all packages). The WarmBoot Install Action does not require parameters. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device. To customize the warm boot logic, place a custom executable (which must be named `warmboot.exe`) in the same directory as the AppUpdate executable. When the file warmboot.exe is found it is executed instead of the default warm boot Install Action.

Table 13-1 Software package actions *(continued)*

Action	Description
Process > Run	

Table 13-1 Software package actions *(continued)*

Action	Description
	Specifies an Install Action that executes a program locally on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Run Action Settings This command execution is specified by the following: ■ Command - {Commandline} data type. Text value that specifies a directory path and file name on the device of the file to be run and any command line arguments to modify the run. Embedded blanks are allowed and double quotes are not required in the program path to enclose directories with embedded blanks. Command line arguments with embedded blanks should be tested as shortcuts before using here. Note that the AppUpdate Runtime Substitution Token values can be used within a value to define subdirectories for executable files and command line arguments as needed. See "Sample AppUpdate runtime substitution tokens" on page 130. ■ Timeout - {Timeout value} data type. Integer value that specifies how long the device should wait when it executes the Run Action before it continues to process. The following are the allowable values: {value less than zero, ex. -1} - (default) specifies that device processing waits indefinitely for the action to finish before it continues with subsequent steps. {"0"} - Device processing does not wait for the action to finish before it continues with subsequent steps. {value greater than zero, ex. 10} - device processing waits (value that is specified in milliseconds) for the action to finish before it continues with subsequent steps. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
	■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.
Process>Terminate	Specifies an Install Action that terminates a module process running on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. ■ Note that the Terminate Install Action issues an error return code if the process to be terminated was not running at the time the call was made. Changing the default Critical continue only on success Action Setting to Critical continue allows subsequent Install Action processing to continue if the Install Action cannot install a specified file or stop a process that is not running. Terminate Action Settings The name of the process(es), specified by the following: ■ Modules - {ModuleName} data type. Text value that specifies an executable name (cmd.exe) or wildcard inclusion of multiple executable names running on the device (ex c*.* or * for all processes). Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System>Copy Files	Specifies an Install Action that copies one or more files from one area (directory or folder) of the device to another. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Copy Files Action Settings The name of the source folder and file name and the target folder that is specified by the following: ■ Source - {localsourcefilespec} data type. Path and file name(s) existing on the device to copy from during provisioning. Using wildcard characters is allowed. ■ Target - {localtargetfoldername} data type. Path existing on the device to receive files during provisioning. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System > Move Files	Specifies an Install Action that moves one or more files from one area (directory or folder) of the device to another. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Move Files Action Settings The name of the source folder and file name and the target folder that is specified by the following: ■ Source - {localsourcefilespec} data type. Path and file name(s) existing on the device to move from during provisioning. Using wildcard characters is allowed. Files are removed from this location upon successful move to target. ■ Target- {localtargetfoldername} data type. Path existing on the device to receive the moved files during provisioning. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System > Delete Files	Specifies an Install Action that deletes a local file on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Delete Files Action Settings The name of the file to be deleted, specified by the following: ■ Path - {localfilename} data type. File name(s) on the device to delete during provisioning. Using wildcard characters is allowed. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System > Rename File	Specifies an Install Action that renames a file in a specified folder on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Rename File Action Settings The name of the source file (existing file name) and the target file name (new file name), specified by the following: ■ Source - {existingfilename} data type. Path and file name existing on the device to be renamed during provisioning. ■ Target - {newfilename} data type. New file name not yet existing in the path that is specified in source. Note: Do not prefix with the path/folder specification. Use the raw file name. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System > Create Folder	Specifies an Install Action that creates a local folder (directory) on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Create Folder Action Settings The name of the folder (directory) to be created, specified by the following: ■ Path - {localfoldername} data type. Folder name on the device to be created during provisioning. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System > Remove Folder	Specifies an Install Action that deletes a local folder (directory) on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Remove Folder Action Settings The name of the folder (directory) to be deleted, specified by the following: ■ Path - {localfoldername} data type. Folder name on the device to delete during provisioning. All files in this folder are also deleted. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Table 13-1 Software package actions *(continued)*

Action	Description
File System > Rename Folder	Specifies an Install Action that renames a folder on the device. Actions Settings ■ Critical, continue only on success - (default) specifies that subsequent action steps in the package are only run if this step completes successfully. ■ Critical, continue - specifies that subsequent action steps in the package are run regardless of the success or failure of this step. ■ Critical, continue only on error - specifies that subsequent action steps in this package are only run if this step fails. Rename Folder Action Settings The name of the source folder name (existing folder or directory on the device) and the target folder name (new folder or directory on the device), specified by the following: ■ Source - {existingfoldername} data type. Path existing on the device to be renamed during provisioning. ■ Target - {newfoldername} data type. New folder name not yet existing on device. Targeted Device Type Used to provision specific devices by processor, major version, and platform: ■ CPU - contains the processor type of the device. ■ OS Major - {osmajor value} data type. Integer that specifies the major version number of the device operating system. ■ OS Platform - contains the mobile operating system of the device.

Software package health actions

The following table describes the metrics and statistics that can be entered when you configure the health reporting packages.

Table 13-2 Software package health actions

Action	Description and parameters
File Hash	Specifies a file hash to compare and determine whether provisioning needs to be performed. File Hash Metric Settings ■ File- device file name and the path that is used for comparing the hash value. ■ Hash- MD5 hash value of specified file (Read Only). Metric Generation Settings ■ Metric Source- file name and path of the server repository source file that is used to derive the file version for comparing to the device file. The device file version must match this file version. The Metric source cannot be manually entered. ■ Folder- path for Metric source file. ■ CAB File- CAB file containing Metric source file. ■ Virtual File- Metric source file that is contained in the CAB file. Targeted Device Type ■ CPU- specifies the processor type of a device. ■ OS Major- specifies the major version number of a device OS. ■ OS Platform- mobile operating system of a device.

Table 13-2 Software package health actions *(continued)*

Action	Description and parameters
File Version	Specifies a file version to compare and determine whether package provisioning actions need to be run to update a device. File Version Metric Settings ■ Field- file version field that is used as the file version definition. Values are File or Product. The literal file version or a field in the file version set should be used. If the application has an embedded assembly, a sub class of File (file version) or Product (product version) may be specified. ■ File- device file name and the path that is used for comparing the hash value. ■ Operator- comparison operator for file version. Values are equal to (EQ), not equal to (NE), greater than (GT), greater than or equal to (GE), less than (LT), and less than or equal to (LE). ■ Value- file version of specified file (Read Only). Metric Generation Settings ■ Metric Source- file name and path of the server repository source file that is used to derive the file version for comparing to the device file. The device file version must match this file version. ■ Folder- path for Metric source file. ■ CAB File- file containing Metric source file. ■ Virtual File- metric source file that is contained in the CAB file. Targeted Device Type ■ CPU- specifies the processor type of a device. ■ OS Major- specifies the major version number of a device OS. ■ OS Platform- mobile operating system of a device.

Table 13-2 Software package health actions *(continued)*

Action	Description and parameters
File Size	Specifies the file size to compare and determine whether package provisioning actions need to be run to update a device. File Size Metric Settings ■ Metric Type- file content properties that are used to indicate whether package provisioning actions are run to update or align a parent product. ■ File- device file name and the path that is used for comparison. ■ Operator- comparison operator for file size. Values are equal to (EQ), not equal to (NE), greater than (GT), greater than or equal to (GE), less than (LT), and less than or equal to (LE). Size- size value in bytes (Read Only). Metric Generation Settings ■ Metric Source- file name and path of the server repository source file that is used to derive the file version for comparing to the device file. The device file version must match this file version. The Metric source cannot be manually entered. Targeted Device Type ■ CPU- specifies the processor type of a device. ■ OS Major- specifies the major version number of a device OS. ■ OS Platform- mobile operating system of a device.

Sample AppUpdate runtime substitution tokens

The following runtime substitution tokens can be used when you define actions while you create software packages:

```
{TEMP} - temporary directory on the device.
{WINDOWS} - Windows directory on the device.
{SYSTEM} - Windows system directory on the device (same as {WINDOWS} on Windows CE).
```

{STARTUP} - startup shortcuts directory on the device.
{PROGRAMS} - program files on the device.
{DOCUMENTS} - personal documents on the device.
{START_MENU} - root start menu on the device.
{PROGRAMS_MENU} - programs menu on start menu (same as {START_MENU} on Smartphone)
on the device.
{DEVICE_ID} - hex device ID (MD5 hash).
{DEVICE_ID2} - unique ID algorithm.
{DEVICE_ID3} - unique ID algorithm for older devices
(pre-Windows Mobile 5).
{DEVICE_ID4} - unique ID algorithm that indicates the platform.
{DEVICE_CPU} - instruction set (ARMV4, ARMV4I, etc).
{DEVICE_OEM} - OEM info string (Windows CE only).
{OS_MAJOR} - major OS version (e.g. 4).
{OS_MINOR} - minor OS version (e.g. 20).
{OS_BUILD} - OS build number.
{OS_PLATFORM} - WinCE or Win32.
{OS_SHELL} - Standard, PocketPC, or Smartphone.
{PRODUCT} - name attribute ({PRODUCT}) of the current package being processed in the
Manifest (server-side and device-side).
{VERSION} - version attribute ({VERSION}) of the current package being processed in the
Manifest (Server-side and Device-side).
{SCREEN_CX} - device horizontal resolution.
{SCREEN_CY} - device vertical resolution.
{Hxxx\yyyy\zzzz...\} - Registry entry value. The first segment of the specification
either be a long name or short name of one of the following Root key values:
HKEY_CLASSES_ROOT or HKCR
HKEY_CURRENT_USER or HKCU
HKCU and HKEY_LOCAL_MACHINE or HKLM - Supported value types that can be returned are
REG_SZ (string), REG_DWORD (hexadecimal value, preceded with 0x) and REG_BINARY
(block of 2-digit hexadecimal values).
{MAC_ADDRESS} - device Network Interface Card (NIC) Media Access Layer (MAC)
address of the NIC used to retrieve the host’s Manifest XML payload.
{APP_MAJOR} - major release number.
{APP_MINOR} - minor release number.
{APP_BUILD} - build number.
{NLS_LCID} - National Language Support table device location identifier.
{NLS_OEMCP} - National Language Support table OEM code page.
{NLS_ANSICP} - National Language Support table ANSI code page.
{BATTERY_LEVEL} - percent of battery charge level on the device.
{DEVICE_NAME} - device name.
{DEVICE_PHONE} - device phone number.
{FREE_SPACE} - available free space on the device.

See “Creating software packages for Windows Mobile devices” on page 110.

Appendix A

Creating the in-house Mobile Management Agent application for iOS devices

This appendix includes the following topics:

- About the in-house Mobile Management Agent application
- Creating the in-house Mobile Management Agent application
- Requirements for creating the in-house Mobile Management Agent application
- Downloading a WWDR Intermediate Certificate
- Creating a Developer Certificate
- Registering an iOS device for testing
- Setting up an App ID
- Downloading the project
- Preparing the iOS device for testing
- Loading the project
- Creating and installing a Development Provisioning Profile
- Customizing the Bundle identifier
- Customizing the localized string files
- Customizing the Target settings
- Building and testing the application

- Building and distributing the application

About the in-house Mobile Management Agent application

You can create the Mobile Management Agent application for internal deployment and upload it to an internal site for download. After you have created the Agent and uploaded it, users can browse to the internal Web site and download and install the Agent.

See "About the Mobile Management Agent application on iOS devices" on page 61.

Creating the in-house Mobile Management Agent application

You can build and set up the Mobile Management Agent for internal download. The process includes instructions for acquiring certificates and the other resources that are required to build and deploy an application.

The first time you build the Mobile Management Agent iOS application, you must complete all of the steps in table Table A-1 and table Table A-2.

After you create the application for the first time, you can create another application by completing the steps in table Table A-2.

See "About the in-house Mobile Management Agent application" on page 134.

Table A-1 Process for preparing to create the in-house Mobile Management Agent application

Step	Action	Description
Step 1	Make sure that you meet all of the requirements for building and distributing an in-house application.	You must ensure that your environment meets the requirements for creating the in-house Mobile Management Agent application. See "Requirements for creating the in-house Mobile Management Agent application" on page 138.

Table A-1 Process for preparing to create the in-house Mobile Management Agent application *(continued)*

Step	Action	Description
Step 2	Log on to your iOS Developer Enterprise Program account.	Log on to your iOS Developer Enterprise Program account as the Team Agent entity at the following Web site: https://developer.apple.com/membercenter/index.action#iPhoneDev
Step 3	Download a WWDR Intermediate certificate.	The WWDR Intermediate Certificate tests the authenticity of your other certificates. See "Downloading a WWDR Intermediate Certificate" on page 138.
Step 4	Create a Developer Certificate.	The Developer Certificate identifies you as the owner of the applications you build. See "Creating a Developer Certificate" on page 139.
Step 5	Register an iOS device for testing.	iOS devices must be registered with Apple before they can be used for testing. See "Registering an iOS device for testing" on page 139.
Step 6	Set up an App ID.	The App ID is an identifier for any project that is made through Apple. See "Setting up an App ID" on page 139.

Table A-1 Process for preparing to create the in-house Mobile Management Agent application *(continued)*

Step	Action	Description
Step 7	Download the project.	Symantec provides a pre-compiled project to use to develop the agent application. When you install Mobile Management, this template is placed in your Symantec Management Platform Server directory. See "Downloading the project" on page 140.
Step 8	Prepare an iOS device for testing.	You need to prepare your registered Apple testing device for testing. See "Preparing the iOS device for testing" on page 140.

Table A-2 Process for creating the in-house Mobile Management Agent application

Step	Action	Description
Step 1	Load the project in Xcode.	Symantec provides a pre-compiled project to use to develop the agent application. Symantec recommends that you make a copy of the provided project template and make modifications to the copy. See "Loading the project" on page 141.
Step 2	Create and install a Development Provisioning Profile to build and test your application.	Apple uses the Development Provisioning Profile to determine who works on which projects, and on which devices they can test. See "Creating and installing a Development Provisioning Profile" on page 141.

Table A-2 Process for creating the in-house Mobile Management Agent application *(continued)*

Step	Action	Description
Step 3	Customize the Bundle identifier value.	The Bundle identifier is built into the application and attaches to certifications. It allows the device to receive notifications from the Apple Push Notification Service. See "Customizing the Bundle identifier" on page 142.
Step 4	Customize the localized string files.	The string files contain the information that appears in the settings of the application on the device. See "Customizing the localized string files" on page 143.
Step 5	Customize the Target settings.	The Target settings are the various settings that are set to determine to which devices the agent is delivered. See "Customizing the Target settings" on page 143.
Step 6	Build the application for testing and test it.	To test the application, build it for testing and test it in your device. See "Building and testing the application" on page 144.
Step 7	Build the application for distribution and set up the download URL.	After you build and test your application, it should install and launch on your testing device. After the application installs and launches successfully on your testing device, you can build the application for internal deployment. See "Building and distributing the application" on page 144.

See "About the in-house Mobile Management Agent application" on page 134.

Requirements for creating the in-house Mobile Management Agent application

You must ensure that your environment meets the requirements for creating the in-house Mobile Management Agent application.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

Table A-3 Requirements for creating the application

Requirement	Description
Hardware and software requirements	■ Mac computer running the current version of Mac OS X ■ Current version of Xcode and iOS SDK ■ At least one iOS device for testing
Membership requirements	iOS Developer Enterprise Program membership You can sign up at the following Web site: http://developer.apple.com/programs/ios/enterprise/

Downloading a WWDR Intermediate Certificate

The WWDR Intermediate Certificate tests the authenticity of your other certificates.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To download a WWDR Intermediate Certificate

1. Go to the following URL:

   https://developer.apple.com/ios/manage/certificates/team/index.action
2. Click **Click here to download now**.
3. After the certificate has downloaded, double-click the certificate to add it to your key chain.

Creating a Developer Certificate

The Developer Certificate identifies you as the owner of the applications you build. The Developer Certificate and the Development Provisioning Profile work together so that you have profiles for development and distribution.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To create a Developer Certificate

1. Go to the following URL:

   https://developer.apple.com/ios/manage/certificates/team/howto.action

2. Follow the instructions for the following:
   - **Generating a Certificate Signing Request**
   - **Submitting a Certificate Signing Request for Approval**
   - **Approving Certificate Signing Requests**
   - **Downloading and Installing Development Certificates**

Registering an iOS device for testing

iOS devices must be registered with Apple before they can be used for testing.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To register an iOS device for testing

1. Go to the following URL:

   https://developer.apple.com/ios/manage/devices/howto.action

2. Follow the instructions for the following:
   - **Locating a Unique Device ID**
   - **Adding Individual Devices**

Setting up an App ID

The App ID is an identifier for any project that is made through Apple.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To set up an App ID

1 Go to the following URL:

https://developer.apple.com/ios/manage/bundles/howto.action

2 Follow the instructions for the following:

- **Generating an App ID**
  Since the App ID needs to be enabled for APNs, it cannot be a wildcard. Symantec recommends that you use a name like com.*<YourCompany>*.*<YourAppName>*. This name is also used in the `AthenaFramework-Info.plist` file.
- **Registering an App ID for Apple Push Notification Service**
- **Configure Development Push SSL certificate**

Note: Anytime you change your App ID settings, you must regenerate and replace any existing provisioning profiles that use the App ID.

Downloading the project

Symantec provides a pre-compiled project to use to develop the agent application. When you install Mobile Management, this template is placed in your Symantec Management Platform Server directory.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To download the project

1 Browse to the following location:

C:\Program Files\Altiris\MobileManagement\Agents\iOSAgentFramework

2 Copy `iOSAgentFramework.zip` to your desktop.

Preparing the iOS device for testing

You need to prepare your registered Apple testing device for testing.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To prepare an iOS device for testing

1. Open Xcode.
2. In the **Windows** menu, click **Organizer**.
3. On the **Organizer** page, in the left pane, expand **iPhone Development**, and click **Provisioning Profiles**.
4. Connect your registered iOS device to your Mac computer using a USB cable.
5. In the left pane, expand **Devices**, and click the registered iOS device.
6. Click **Use for Development**.
7. Enter your iOS Developer Enterprise Program credentials.

Loading the project

Symantec provides a pre-compiled project to use to develop the agent application. Symantec recommends that you make a copy of the provided project template and make modifications to the copy.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To load the project

1. Open Xcode and click **Open Other**.
2. Browse to the Athena Framework project folder and select `iOSAgentFramework.zip`.
3. Click **Open**.

Creating and installing a Development Provisioning Profile

Apple uses the Development Provisioning Profile to determine who works on which projects, and on which devices they can test.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To create and install a Development Provisioning Profile

1 Go to the following URL:

https://developer.apple.com/ios/manage/provisioningprofiles/howto.action

2 Follow the instructions for the following:

- **Creating a Development Provisioning Profile**
- **Installing a Development Provisioning Profile**
- **Building and installing your Development Application**
  In step 2, your device will be available from the drop-down menu in the upper-left hand corner.
  Perform step 5 before step 4. Complete all other steps in order.
  The Build and Go button that is referenced in step 6 is instead labeled **Build and Run**.

Warning: Do not attempt to use the Xcode Simulator to test your build. You must perform the tests on an actual device. If you use the Mobile Management Agent template to build applications, they do not load in the simulator. The simulator lacks required functionality, such as the Apple Push Notification Service.

Customizing the Bundle identifier

The Bundle identifier is built into the application and attaches to certifications. It allows the device to receive notifications from the Apple Push Notification Service.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To customize the Bundle identifier

1 Open your project in Xcode.

2 In the left pane, under **Groups & Files**, expand **athenaFramework-template > Resources > plists**, and click **AthenaFramework-Info.plist**.

3 In the **Bundle identifier** field, enter the same value as your App ID.

Customizing the localized string files

The string files contain the information that appears in the settings of the application on the device.

Warning: When you edit `LocalizableStrings-en.plist` or localize it to a new language, do not change the names of the keys on the left. Change only the string values on the right.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To customize the localized string files

1. Open your project in Xcode.
2. In the left pane, under **Groups & Files**, expand **AthenaFramework-template > Resources > plists**, and click **LocalizableStrings-en.plist**.
3. In the right pane, modify the content of **AboutView**, **EnrollView**, **HomeView**, **Preferences**, and **StatusView**.
4. (Optional) If you change the name of the Mobile Management Agent, you need to change the name in the agent in the string files. In **HomeView**, change the **Agent Title** field to the name of your agent. In **AboutView**, change the **Name** field to match the name of your agent.

Customizing the Target settings

The Target settings are the various settings that are set to determine to which devices the agent is delivered.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To customize the Target settings

1. Open your project in Xcode.
2. Click **Project** in the left pane.
3. In the middle pane, click the project under **Targets**.
4. Click **Build Settings**.
5. Under **Architectures**, make the following changes:

- Set **Base SDK** according to the target for your application. The minimum value is iOS Device 4.2. You can select newer SDK versions, but not older versions.
- Under **Code Signing**, select the previously created provisioning profile.
- Under **Deployment**, choose the desired **Targeted Device Family**. iOS 4.1 is the minimum supported version.

6 (Optional) If you change the name of the Mobile Management Agent, you need to change the name of the agent in the Target settings. Under **Packaging**, change **Product Name** to match the name of your agent.

Building and testing the application

To test the application, build it for testing and test it in your device. If the application installs and launches on your testing device, the application is complete and the project is correct.

Warning: Do not to use the Xcode Simulator to test your build. You must perform the tests on an actual device. If you use the Mobile Management Agent template to build applications, they do not load in the simulator. The simulator lacks required functionality, such as the Apple Push Notification Service.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To build and test your application

1 Open your project in Xcode.

2 Connect your registered iOS testing device to your Mac computer.

3 In the field in the upper left of the screen, make sure that your testing device is selected.

4 Click the **Run** button in the top left corner. If the application installs and launches on your testing device, the application is complete and the project is correct.

Building and distributing the application

After you build and test your application, it should install and launch on your testing device. After the application installs and launches successfully on your

testing device, you can build the application for internal deployment. The following steps outline the process of building your application and setting up the distribution URL.

This task is a step in the process for preparing to create the in-house Mobile Management Agent application.

See "Creating the in-house Mobile Management Agent application" on page 134.

To build and distribute your application

1. Log in to your iOS Developer Enterprise Program account as the Team Agent entity at the following Web site:

   https://developer.apple.com/membercenter/index.action#iPhoneDev

2. Go to the following URL:

   https://developer.apple.com/ios/manage/distribution/index.action

3. Follow the instructions for the following:

   - **Building your Application with Xcode for Distribution**
   - **Verifying a Successful Distribution Build**
   - **Updating your Application**

Appendix B

Troubleshooting

This appendix includes the following topics:

- Troubleshooting configuration policy distribution problems
- Troubleshooting iOS device agent enrollment
- Troubleshooting Mobile Management Server configurations
- About troubleshooting errors with the SymantecEASService configuration
- Verifying that the Push Certificate Subject matches the App ID's Bundle identifier
- Configuring Mobile Management to work with a development APNS certificate

Troubleshooting configuration policy distribution problems

This section outlines troubleshooting steps to go through if the iOS devices in your environment do not receive configuration policies.

See "About configuration profiles on iOS devices" on page 80.

To troubleshoot configuration policy distribution problems

1. Make sure that you turned on the policy.

   See "Assigning policies" on page 79.

2. Make sure that you properly targeted your device.

   See "Assigning policies" on page 79.

3. Run the **Update Policies** action on the device.

4. Make sure that policies are delivered. Check for delivery by sending the **Lock Device** action to a device you have and see if it locks within a few minutes.

5 Make sure that the APNS ports are open in your environment.

6 Check your MDM Certificate configuration.

See "Setting up an MDM Certificate" on page 32.

7 Make sure that you have an MDM profile on your device. Check for this profile by going to **Settings > General > Profiles** on the device.

8 Make sure that you apply the policies from the correct Mobile Management Server.

Troubleshooting iOS device agent enrollment

You can ensure that the Mobile Management Agent is correctly enrolled by verifying the following things:

- You can see the Mobile Library content in the Mobile Management Agent.
- You can see the MDM profile on the device.
  You can check this item by going to **Settings > General > Profiles** on the device.
- The agent appears on the desktop of the device.
- The **Agent** and **MDM Enrollment** status in the Symantec Management Console are listed as true.
  You can check this status in the Symantec Management Console. Click the **Reports** tab and then click **All Reports**. In the left pane, expand Mobile Management and click **Detailed iOS Device Status**. Find the device you want to have enrolled and make sure that **Agent Enrolled** and **MDM Enrolled** are both True.
- The Push Certificate Subject matches the App ID's Bundle identifier that is found in the APNS certificate.
- The device receives notifications from the Symantec Management Platform through APNS.

If one of the preceding items was unverifiable, the Mobile Management Agent was not enrolled correctly.

To try to fix the agent enrollment, you can do the following:

- Remove the agent and then re-download and re-enroll it.
  If you are not able to enroll the Mobile Management Agent on an iOS device, you may need to remove any old MDM profiles. The existence of old MDM profiles on the device can cause the installation of the Mobile Management Agent to fail. Remove the Mobile Management Agent and any old MDM profiles. After you have completely removed the agent, re-download and re-enroll it.

See "About the Mobile Management Agent application on iOS devices" on page 61.
See "Enrolling iOS devices" on page 64.

- Troubleshoot the Mobile Management Server installation.
  If you get an MDM enrollment error when you attempt to enroll a device your Mobile Management Server configuration may be wrong.
  See "Troubleshooting Mobile Management Server configurations" on page 149.
- After you install the APNS certificate on your Mobile Management Server, you can verify that the Push Certificate Subject matches the App ID's Bundle identifier.
  See "Verifying that the Push Certificate Subject matches the App ID's Bundle identifier" on page 150.
- If your APNS certificate was created for development and not production, you need to make sure that you configure Mobile Management accordingly.
  See "Configuring Mobile Management to work with a development APNS certificate" on page 151.

Troubleshooting Mobile Management Server configurations

If you suspect that your Mobile Management configuration is incorrect, you can take steps to troubleshoot the problem. You also may need to troubleshoot your Mobile Management Server installation if you receive error messages relating to your Mobile Management Server.

See "Configuring the site server to communicate with iOS devices" on page 47.

To troubleshoot Mobile Management Server installations

1. Make sure that the APNS certificate is installed on the site server.
2. Make sure that the Mobile Management Server settings are correct. For example, make sure that the server IP or name is properly entered in **Site Server Settings**.
3. Make sure that the APNS thumbprint matches the APNS certificate.
4. Make sure that the type of APNS certificate is properly selected.
5. Make sure that the SCEP information is properly entered. For example, verify the URL, Subject, and Challenge phase.
6. Make sure that the SCEP service is properly set up.
7. Make sure the Push Certificate Subject matches the APNS certificate.

About troubleshooting errors with the SymantecEASService configuration

If you get errors with the SymantecEASService, you may need to check your security permissions. The following permissions should be set on the Mobile Management Server:

- The eadmin account is a member of the Exchange Organization Administrators tab.
- The SymantecEASService is running as Exchange Admin.
- The eadmin has read and write access to %ProgramFiles%\Symantec\Mobile Management\eas\.
- The SymantecEASPolicyAppPool has a configurable identity.
- SYMMOBILE\eadmin is a member of the local IIS_WPG group.
- The eadmin has read and write access to %SystemRoot%\Temp.

See "Setting up Exchange ActiveSync" on page 54.

Verifying that the Push Certificate Subject matches the App ID's Bundle identifier

After you install the APNS certificate on your Mobile Management Server, you can verify that the Push Certificate Subject matches the App ID's Bundle identifier.

To verify that the Push Certificate Subject matches the App ID's Bundle identifier

1. Click Start. In the search box, type mmc.
2. Click the mmc.exe.
3. In the MMC console, navigate to **File > Add/Remove Snap-in**.
4. Select **Certificates** from the left pane.
5. Click **Add** and select **Computer Account**.
6. Click **Next**, **Finish**, and then click **OK**.
7. Next, navigate to **Certificates (Local Computer) > Personal > Certificates**.
8. Find the certificate you created in the right pane and double-click the certificate.
9. Click on the **Details** tab and select **Subject**.

10 Look in the bottom box of the window and locate the Bundle Identifier. For example, = com.apple.mgmt.<*yourstring*>. Record the Bundle Identifier so you can compare it with the one in the Symantec Management Console.

11 Open the Symantec Management Console.

12 Navigate to **Home > Mobile Management > iOS MDM Enrollment Configuration**.

13 The Push Certificate Subject field on the iOS MDM Enrollment page should match the Bundle Identifier that is recorded from the APNS certificate.

Configuring Mobile Management to work with a development APNS certificate

If your APNS certificate was created for development and not production, you need to configure Mobile Management accordingly.

See "Configuring the site server to communicate with iOS devices" on page 47.

To configure Mobile Management to work with a development APNS certificate

1 Open the Symantec Management Console and click the **Home** tab.

2 Expand **Mobile Management** and click **Mobile Management Server Settings**.

3 Click the **APNS** tab, and then check **Use Development APNS**.

4 Click **Save changes**.

5 Next, navigate to **Home > Mobile Management > iOS MDM Enrollment Configuration**.

6 On the **iOS MDM Enrollment** page, check **Use Development APNS**.

7 Click **Save changes**.

Appendix C

Third-Party Attributions

This appendix includes the following topics:

- Third-Party Legal Notices
- ZLib v 1.2.2
- Z.4.7 - Zlib v1.2.5 (G)
- SQlite v 3.7.4 and SQlite NET.Wrapper v 1.0.66.0:
- Expat v 1.2:

Third-Party Legal Notices

This Symantec product may contain third party software for which Symantec is required to provide attribution ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. This appendix contains proprietary notices for the Third Party Programs and the licenses for the Third Party Programs, where applicable.

See "About Mobile Management" on page 13.

ZLib v 1.2.2

URL to license agreement: http://www.jclark.com/xml/expat.html

See "Third-Party Legal Notices" on page 153.

Z.4.7 - Zlib v1.2.5 (G)

Jean-loup Gailly and Mark Adler Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

- 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
- 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
- 3. This notice may not be removed or altered from any source distribution.

See “Third-Party Legal Notices” on page 153.

SQlite v 3.7.4 and SQlite NET.Wrapper v 1.0.66.0:

This code may be accessed at: http://www.sqlite.org/copyright.html

See “Third-Party Legal Notices” on page 153.

Expat v 1.2:

Thai Open Source Software Center Ltd

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

License Agreement URL: http://www.jclark.com/xml/copying.txt

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

See “Third-Party Legal Notices” on page 153.

Expat v 1.2:

Index

A

about
- actions 78
- AutoLock settings on iOS devices 86
- available configuration profile settings 85
- configuration profiles 80
- configuring Mobile Management 45
- connecting iOS devices to Exchange ActiveSync 58
- event logs 95
- Exchange ActiveSync 53
- in-house Mobile Management Agent application 134
- installing Mobile Management 41
- inventory data 89
- MDM Certificate 31
- Mobile Library 71
- Mobile Management 13
- Mobile Management Agent
  - on BlackBerry devices 67
  - on iOS devices 61
  - on Windows Mobile devices 67
- policies 78
- remotely managing devices 97
- reports 92
- software management on Windows Mobile devices 109

actions
- about 78
- performing 78

Active Directory, requirements 23

adding
- additional configuration profiles 50
- configuration profiles to a policy 83

agent. *See* Mobile Management Agent

APNS certificate 151

App ID
- creating using a Windows Server 37
- creating using Mac OS X 35
- setting up 139

Apple devices. *See* iOS devices

Apple Push Notification Service
- network ports used 25
- requirements 23

AppUpdate, sample runtime subtitution tokens 130

assigning
- configuration profile policies 84
- policies 79

AutoLock settings, about 86

B

BlackBerry devices
- available features 17
- available reports 93
- function key mapping during remote sessions 104
- remote options 102
- setting up Mobile Management Agent on 69
- supported policies 80

building and distributing the in-house Mobile Management Agent application 144

building and testing the in-house Mobile Management Agent application 144

Bundle identifier, customizing 142

C

Certificate Authority
- requirements 23
- setting up 27

certificate request, generating 36

certificates 29

changing, enrollment URL to an email address 65

components, Mobile Management 14

configuration policies, troubleshooting 147

configuration profiles
- about 80
- adding additional 50
- adding to a policy 83
- assigning 84
- available settings 85
- creating 82
- setting up 82

configuration profiles *(continued)*
supported devices 81
configuration schedule, setting 70
configuring
iOS device MDM enrollment 49
Mobile Management 45
Mobile Management to work with a development APNS certificate 151
policy security settings 48
software maintenance windows 112
SymantecEASService NT 56
creating
App ID using a Windows Server 37
App ID using Mac OS X 35
configuration profiles 82
Developer Certificate 139
Development Provisioning Profile 141
EULA 65
in-house Mobile Management Agent application 134
Mobile Library feeds 72
policies 79
remote settings for devices 98
software packages 110
customizing
Bundle identifier 142
localized string files 143
Target settings 143

D

delivering, software packages 111
Developer Certificate, creating 139
Development Provisioning Profile
creating 141
installing 141
downloading
Mobile Management Agent from the Apple App Store 63
project 140
WWDR Intermediate certificate 138

E

enabling
EULA 65
Exchange ActiveSync functionality 56
Encryption Certificate 29
End User License Agreement. *See* EULA
enrolling, iOS devices 64
enrollment URL, changing to an email address 65
EULA
creating 65
enabling 65
event logs
about 95
viewing 95
Exchange ActiveSync
about 53
about connecting iOS devices 58
enabling functionality of 56
requirements 23
setting up 54
supported device operating systems 53
supported devices 26
Exchange ActiveSync server, selecting 57
exporting
MDM Certificate using a Windows Server 38
MDM Certificate using Mac OS X 36

F

feeds
adding items to 73
creating 72
publishing existing 75
setting up 72
function key mapping during remote sessions
BlackBerry devices 104
Windows Mobile devices 103

G

generating, certificate request 36

H

hpWebOS devices. *See* Palm devices

I

in-house agent application. *See* Mobile Management Agent
installing
Development Provisioning Profile 141
MDM Certificate 39
Mobile Management 42
Mobile Management on a new server 43
Mobile Management on an existing Symantec Management Platform Server 42
inventory data
about 89

inventory data *(continued)*
setting the inventory sechedule
iOS devices 91
Windows Mobile devices 90
viewing 90
inventory schedule, setting
iOS devices 91
Windows Mobile devices 90
iOS Developer Enterprise Program membership 34
iOS devices
available features 17
available reports 93
configuring MDM enrollment of 49
configuring the site server to communicate with 47
enrolling 64
preparing for testing 140
registering for testing 139
setting up Mobile Management Agent on 62
supported configuration profiles 81
supported policies 80
troubleshooting agent enrollment 148
items
adding to feeds 73
publishing existing 75

L

LDAP, requirements 23
loading, project 141
localized string files, customizing 143

M

MDM Agreement 34
MDM Certificate
about 31
exporting using a Windows Server 38
exporting using Mac OS X 36
installing 39
requirements 34
setting up 32
Microsoft Exchange ActiveSync. *See* Exchange ActiveSync
Microsoft SQL Server. *See* SQL Server
Mobile Device Management Certificate. *See* MDM Certificate
mobile devices
available features 17
remotely wiping 105
Mobile Library
about 71
adding items to feeds 73
creating feeds 72
publishing an existing feed or item 75
setting up feeds 72
Mobile Management
about 13
about configuring 45
about installing 41
certificates 29
components 14
configuring 45
deploying to the site server 43
how it works 14
installing 42
installing on a new server 43
installing on an existing Symantec Management Platform Server 42
network ports used 25
requirements 23
setting up 27
what's new in 7.1 19
Mobile Management Agent
about
on BlackBerry devices 67
on iOS devices 61
on Windows Mobile devices 67
about the in-house application 134
building and distributing the in-house application 144
building and testing the in-house application 144
creating the in-house application 134
differences between versions 66
downloading from the Apple App Store 63
enrolling 64
in-house application requirements 138
requirements 23
setting the configuration schedule 70
setting up
BlackBerry devices 69
iOS devices 62
Windows Mobile devices 68
supported devices 26
Mobile Management Server
network ports used 25
requirements 23
troubleshooting configuration of 149

Mobile Management Service Agent, restarting 57
Mobile Management site server. *See* site server

N

network ports used by Mobile Management 25
Nokia devices. *See* Symbian devices

P

Palm devices
    available features 17
    available reports 93
    supported policies 80
policies
    about 78
    assigning 79
    creating 79
    supported 80
policy security, configuring settings of 48
preparing, iOS devices for testing 140
Profile security 27
project
    downloading 140
    loading 141
Push Certificate Subject, verifying 150

R

registering, iOS devices for testing 139
remote options
    BlackBerry devices 102
    Windows Mobile devices 99
remote sessions
    function key mapping
        BlackBerry devices 104
        Windows Mobile devices 103
    starting 99
remote settings for devices
    creating 98
remotely managing devices
    about 97
    creating remote settings 98
    function key mapping
        BlackBerry devices 104
        Windows Mobile devices 103
    remote options
        BlackBerry devices 102
        Windows Mobile devices 99
    remotely wiping devices 105
    starting remote sessions 99
remotely wiping, mobile devices 105
reports
    about 92
    available by device 93
    running 93
requirements
    in-house Mobile Management Agent application 138
    MDM Certificate 34
    Mobile Management 23
restarting, Mobile Management Service Agent 57
Root Certificate 29
running, reports 93

S

sample AppUpdate runtime substitution tokens 130
SCEP
    requirements 23
    setting up 27
selecting, Exchange ActiveSync server 57
Server Authentication Certificate 29
setting
    inventory schedule
        iOS devices 91
        Windows Mobile devices 90
    Mobile Management Agent configuration schedule 70
setting up
    App ID 139
    Certificate Authority 27
    configuration profiles 82
    Exchange ActiveSync 54
    MDM Certificate 32
    Mobile Library feeds 72
    Mobile Management 27
    Mobile Management Agent
        BlackBerry devices 69
        iOS devices 62
        Windows Mobile devices 68
    SCEP 27
Signing Certificate 29
site server
    about deploying 41
    configuring to communicate with iOS devices 47
    deploying 43
software maintenance windows, configuring 112
software package actions 113
software package health actions 127

software packages
actions 113
creating 110
delivering 111
health actions 127
SQL Server
network ports used 25
requirements 23
SSL Certificate. *See* Server Authentication Certificate
starting, remote sessions 99
Symantec Agent. *See* Mobile Management Agent
Symantec Management Console, Mobile Management section 41
Symantec Management Console, requirements 23
Symantec Management Platform
installing 43
requirements 23
Symantec Management Platform Server
network ports used 25
requirements 23
SymantecEASService
troubleshooting errors with 150
verifying configuration of 58
SymantecEASService NT, configuring 56
Symbian devices
available features 17
available reports 93
supported policies 80

T

Target settings, customizing 143
Third-Party Attributions 153
troubleshooting
configuration policy distribution problems 147
errors with the SymantecEASService configuration 150
iOS device agent enrollment 148
Mobile Management Server configurations 149

V

verifying
Push Certificate Subject 150
SymantecEASService configuration 58
viewing
event logs 95
inventory data 90

W

Windows Mobile and CE devices
available features 17
available reports 93
supported policies 80
Windows Mobile devices
about software management 109
function key mapping during remote sessions 103
remote options 99
setting up Mobile Management Agent on 68
wiping devices, remotely 105
WWDR Intermediate certificate, downloading 138