Symantec™ Mobile Security 7.2 MR1 Implementation Guide
Symantec™ Mobile Security 7.2 MR1 Implementation Guide

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

Documentation version: 7.2.1

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("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. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

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

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific and Japan</td>
<td><a href="mailto:customercare_apac@symantec.com">customercare_apac@symantec.com</a></td>
</tr>
<tr>
<td>Europe, Middle-East, and Africa</td>
<td><a href="mailto:semea@symantec.com">semea@symantec.com</a></td>
</tr>
<tr>
<td>North America and Latin America</td>
<td><a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a></td>
</tr>
</tbody>
</table>
Contents

Technical Support ........................................................................................................................................ 4

Section 1  Setting up Symantec Mobile Security 7.2 .............................................................................. 11

Chapter 1  Introducing Symantec Mobile Security 7.2 ............................................................... 13

What's new in Symantec Mobile Security 7.2 ........................................................................... 13
Getting started ................................................................................................................................. 13
Terms and component names to know ........................................................................................ 14
Using the Symantec Management Console .............................................................................. 15

Chapter 2  Installing Symantec Mobile Security 7.2 ................................................................. 17

Downloading and installing Symantec Mobile Security 7.2 ...................................................... 17
Accessing the Symantec Mobile Security user interface ........................................................ 19

Chapter 3  Distributing the Symantec Mobile Security 7.2 Agent app ........................................ 21

About distributing the Agent app to device owners ........................................................................ 21
Distributing the Agent app to Android device owners .............................................................. 22
Distributing the Agent app to Windows Mobile device owners .............................................. 22
Installing the Mobile Security Agent app on mobile devices ............................................. 23

Chapter 4  Server Configuration ................................................................................................................. 25

Configuring the Symantec Mobile Security server .................................................................. 25
Configuring Symantec Mobile Security Gateway server .................................................... 28
Setting up Google Cloud Messaging (GCM) ........................................................................... 31
Securing the management console ............................................................................................. 33
Configuring Microsoft Active Directory for enrolling mobile devices .................................. 33
Contents

Chapter 14  Database maintenance ................................................................. 97

Purging Android mobile device data from the database ................................. 97

Appendix A  Symantec Mobile Security 7.2 System
Requirements and Port Usage ................................................................. 99

Server requirements .................................................................................. 99
Mobile device requirements ...................................................................... 100
Port Usage ............................................................................................... 100

Appendix B  Mobile Security Implementation Architectures .............. 103

Mobile Security implementation architectures .................................... 103
Single-box implementation ..................................................................... 104
Typical implementation ........................................................................... 105
Reverse proxy implementation ............................................................... 106

Appendix C  Third-party Attributions ....................................................... 107

Third-Party Legal Notices ........................................................................ 107
Bouncy Castle Crypto C# ......................................................................... 107
Iquery ........................................................................................................ 108
Log4Net ..................................................................................................... 108

Index ......................................................................................................... 113
Setting up Symantec Mobile Security 7.2

- Chapter 1. Introducing Symantec Mobile Security 7.2
- Chapter 2. Installing Symantec Mobile Security 7.2
- Chapter 3. Distributing the Symantec Mobile Security 7.2 Agent app
- Chapter 4. Server Configuration
- Chapter 5. Adding additional Gateway servers
Introducing Symantec Mobile Security 7.2

This chapter includes the following topics:

- What's new in Symantec Mobile Security 7.2
- Getting started
- Terms and component names to know
- Using the Symantec Management Console

What's new in Symantec Mobile Security 7.2

The 7.2 release of Symantec Mobile Security features significant enhancements and several new features, including support for Android devices. For a complete listing of new features and enhancements, see the Symantec Knowledge Base article, What's new in Symantec Mobile Security 7.2 at http://www.symantec.com/docs/TECH190323


Getting started

Symantec Mobile Security 7.2 is a multi-component solution for securing mobile devices in an enterprise environment. The Symantec Mobile Security server is installed on the Symantec Management Platform. The Symantec Management Platform provides centralized administration, product download and installation, and content update services for a variety of Symantec enterprise software.
solutions. A client (also called an agent) resides on the mobile device and receives administrative requests to perform security actions, and report status and security events.

You can set up the Mobile Security components in several ways, as your needs dictate. Three architectural scenarios that can serve as starting points for your implementation are provided in the appendices.

See “Mobile Security implementation architectures” on page 103.

You use Symantec Installation Manager to install Symantec Management Platform and Symantec Mobile Security. Once the products are installed, you access the mobile security components and perform administrative tasks through the Symantec Management Platform console.

After you install the server-side components, you can distribute the Symantec Mobile Security Agent to the device owners.

See “About distributing the Agent app to device owners” on page 21.

You begin by installing the server-side components which include the Symantec Management Platform and Symantec Mobile Security software. Before you proceed, verify that your environment meets the minimum requirements.

See “Server requirements” on page 99.

---

**Note:** An Install Readiness Check utility runs as part of the installation process. The utility prevents an installation on any systems that do not meet the minimum requirements.

---

**Terms and component names to know**

The following list provides descriptions for terms and component names related to Symantec Mobile Security and security policies:

- **Symantec Installation Manager** - A stand-alone utility that you use to download and install certain Symantec products.

- **Symantec Management Platform** - A set of components based on the Altiris ITMS management system that provides centralized management capabilities for certain Symantec products.

- **Symantec Management Console, Management Console or ‘console’** - The HTML-based UI that you use to interact with the Symantec Management Platform. You conduct all management, configuration, and update activities through the management console. You access the console through Internet Explorer 7 or later. Open an instance of the browser and go to...
http://[hostname]/Altiris/Console, where [hostname] is the name of the computer that hosts the installation.

- **Symantec Mobile Security** - The component-set that provides the security functions to Symantec Management Platform that allow it to secure mobile devices.

- **Gateway Server or Gateway** - The Gateway isolates the enterprise network from the public Internet. By default, the host instance of Symantec Management Platform is configured as a Gateway. Additional Gateways can be configured to improve performance in large networks. See “Configuring Symantec Mobile Security Gateway server” on page 28.

- **Agent or Agent app** - A small mobile device application that communicates with the Mobile Security infrastructure and allows security actions to be executed on the mobile device. See “About distributing the Agent app to device owners” on page 21.

- **GCM** - Google Cloud Messaging (GCM), a Google service that allows messages to be quickly sent from a server to an Android mobile device. GCM replaces Google C2DM service which has been deprecated. For information about GCM see the Google GCM Web site at http://developer.android.com/guide/google/gcm/index.html See “Setting up Google Cloud Messaging (GCM)” on page 31.

# Using the Symantec Management Console

The Symantec Mobile Security user interfaces (UI) are standardized around the Symantec Management Console layout and navigation scheme. The management console is part of Symantec Management Platform, the framework that supports Symantec Mobile Security. The following conventions apply:

- The main Symantec Management Platform section tabs are always available in the main UI. The **Home** tab provides access to most of the configuration options, management tools, and reporting functions.

- You select key functionality in the left pane. The right pane displays the granular details for the selected key functionality.

- The left pane is divided into collapsing sections based on the nature of the functions they contain. Click the reveal button to expand or collapse a section.

- Double-clicking on a listed device opens a detailed report of activity for the chosen device.
Right-clicking on a listed device displays a menu that provides access to several commonly used functions that you can apply to the chosen device. This menu and its options are available from any screen that lists individual devices.

Configuration screens feature a toolbar with a standardized set of icons to invoke a set of common functions:

- Yellow star icon- Opens a new configuration template.
- Pencil icon- Opens an existing configuration that you first select from a list.
- X icon- Used to delete a configuration.
- Green check-mark icon- Verifies configuration settings.

Reports and device detail screens open in a new browser window.

For more information about navigating the UI, see the Symantec Management Platform User Guide. The Symantec Management Platform documentation is available on the Help tab of the platform console and at http://www.symantec.com/business/support/index?page=content&key=55274&channel=DOCUMENTATION

See “Accessing the Symantec Mobile Security user interface” on page 19.
Installing Symantec Mobile Security 7.2

This chapter includes the following topics:

- Downloading and installing Symantec Mobile Security 7.2
- Accessing the Symantec Mobile Security user interface

**Downloading and installing Symantec Mobile Security 7.2**

If you do not have Symantec Management Platform installed, you first download and install Symantec Installation Manager. Be sure that your environment meets the system requirements.

See “Server requirements” on page 99.

If Symantec Management Platform 7.1 SP2 is already installed, on the Symantec Management Platform computer, go to Start > All programs > Symantec > Symantec Installation Manager. Start the application and then follow the steps in the procedure, Installing Symantec Management Platform and Symantec Mobile Security 7.2, omitting Symantec Management Platform from the item selection in Step 1.
**Downloading and installing Symantec Installation Manager**

1. Go to go.symantec.com/Get_Mobile_Security, and log into your Symantec account. If you do not have an account, a registration link is provided on the Web page.

2. On the Software Download page for Symantec Mobile Security, click **Download Now**.

   _Note:_ The download includes Symantec Installation Manager and Symantec Management Platform.

3. Follow the on-screen instructions to set up Symantec Installation Manager. At the end of the installation, check **Automatically launch Symantec Installation Manager**, and then click **Finish**.

   _Note:_ If an update to Symantec Installation Manager is available, you are prompted to download and install the update.

**Installing Symantec Management Platform and Symantec Mobile Security 7.2**

1. In Symantec Installation Manager, on the **Install New Products** page, in the **Available products** list, select the following items:

   ■ Symantec Management Platform 7.1 SP2
   ■ Symantec Mobile Security 7.2

   _Note:_ To quickly locate the software, set the left filter option to **Filter by Product Type** and the right filter option to **Filter: None** and then enter the word *mobile* into the search field.

2. Click **Review selected products**, verify that the correct products are selected, and then click **Next**.

3. On the End User License Agreement page, accept the terms of the license and click **Next**.

   _Note:_ A 30 day trial license is provided with Symantec Mobile Security. To use the trial license, skip the option to add a license.
4 On the **Install Readiness Check** page, verify that the computer meets the minimum requirements and then click **Next**.

5 The installer prompts you to configure the server and the database:

- For maximum security, select **Require SSL**

  **Note:** If you chose to require SSL, you must also install a trust certificate that is issued from a commercial certificate authority (CA).

- Test setups can use an on-box instance of SQL Express. SQL Express is included with the product installation software. Production installations with more than 500 devices should use an off-box instance of SQL Server. See the system requirements for supported versions of SQL Server. See “**Server requirements**” on page 99.

After you configure the components, click **Next**.

6 Skip the page, **Computers to Manage** and then click **Begin install**.

7 Wait for the installer to complete and then click **Finish**.

**Verifying the installation**

1 Open an instance of Internet Explorer 7 or later and go to http://<hostname>/Altiris/Console (where <hostname> is the name of the computer that hosts the installation).

2 On the toolbar, click **Home > Mobile Security** and then in the left pane, select **Settings**.

3 Select **Mobile Security Gateway** and in the right pane, check that the status condition is **Active** for the listed gateway.

  **Note:** The listed gateway is the computer that hosts the installation. Additional gateways can be added as needed.

  See “**Configuring Symantec Mobile Security Gateway server**” on page 28.

---

**Accessing the Symantec Mobile Security user interface**

You access the Symantec Mobile Security user interface on the Symantec Management Console. You access the console through Internet Explorer (version 7 or later).
**Note:** Throughout this guide and other related documentation, the console is also referred to as Symantec Management Console, or "management console".

To open the console, open an instance of Internet Explorer and go to **http://[hostname]/Altiris/Console**, where [hostname] is the name of the computer that hosts the installation.

Use the credentials you established during installation to open the console.

**Note:** You may access the console from any network connected computer that has Internet Explorer 7 or later installed. You can also open more than one instance of the console.

See “**Using the Symantec Management Console**” on page 15.
Distributing the Symantec Mobile Security 7.2 Agent app

This chapter includes the following topics:

- About distributing the Agent app to device owners
- Distributing the Agent app to Android device owners
- Distributing the Agent app to Windows Mobile device owners
- Installing the Mobile Security Agent app on mobile devices

About distributing the Agent app to device owners

You distribute the Symantec Mobile Security 7.2 Agent app by either:

- Pulling the app down from a download host.
- By pushing the app down with a mobile device management system.

Before you distribute the Agent app, you configure the Agent app enrollment and management settings. See “Configuring Android enrollment and management settings” on page 53.

To have users pull the app down to their devices, you send a notification that provides a URL to the download host location. The device owner retrieves the Agent app and installs it themselves. When you push the Agent app down to devices, the installation method depends on how the device is managed. You may have the device owner perform the installation, or you may configure a management policy to install the Agent app automatically.
Distributing the Agent app to Android device owners

Use the following procedure to distribute the Agent app to Android device owners:

Distributing the Agent app to Android device owners

1. On the **Home > Mobile Security > Settings > Mobile Security Gateways** screen, highlight the Mobile Security Gateway, and then on the toolbar, click the email template icon.

   **Note:** If you have configured more than one Gateway Server, select the server that the device owner is assigned to.

2. Copy the message from the **Enrollment e-mail message** panel to a new email message,

3. Send the message to the appropriate mobile device users.

   **Note:** If you modify the message to device users, leave the URL and file location information unmodified.

The device owner uses their device to first browse to the location for the file, and then download the file to their device. The app is installed using the customary method for Android app installation.

Distributing the Agent app to Windows Mobile device owners

The Agent app for Windows Mobile devices is available on the Symantec Mobile Security 7.2 Trialware Web site. Go to [http://go.symantec.com/Get_Mobile_Security](http://go.symantec.com/Get_Mobile_Security) to download the Windows Mobile Agent file. You provision this file from a location that is available to Windows Mobile device owners in your organization. Typically, you provision the file on a Web site and provide the URL to the file location to the device owners.

The device owner uses their device to first browse to the location for the file, and then download the file to their device. The file is installed using the customary installation method for Windows Mobile app installation.
Installing the Mobile Security Agent app on mobile devices

The installation procedure you use depends on the mobile device operating system. Use the procedure appropriate for your mobile device operating system.
Distributing the Symantec Mobile Security 7.2 Agent app

Installing the Mobile Security Agent app on mobile devices
Server Configuration

This chapter includes the following topics:

- Configuring the Symantec Mobile Security server
- Configuring Symantec Mobile Security Gateway server
- Setting up Google Cloud Messaging (GCM)
- Securing the management console
- Configuring Microsoft Active Directory for enrolling mobile devices

Configuring the Symantec Mobile Security server

Symantec Mobile Security can be used immediately after installation. However, additional functionality and performance tuning is available through the configuration options. Table 4-1 provides a list of the available configuration options, and suggestions for using them.
### Table 4-1 Mobile Security management server settings options

<table>
<thead>
<tr>
<th>Option</th>
<th>Location</th>
<th>Suggested use</th>
</tr>
</thead>
</table>
| Thresholds and Alerting: Threats | **Home > Mobile Security > Settings > Management Server Settings** | ■ **Warning threshold** - based on the percentage of all devices that are at risk for any reason.  
■ **Critical threshold** - based on the total number of threats that are found on all managed devices, combined.  
■ **Send email for threat alerts** - If you enable this option, configure the email address for the administrator who is responsible for threat oversight.  
Use these settings to control when warnings appear on the status overview page and when alert emails are sent. The default values are selected to provide reasonable advanced warnings for most users. If your needs include a high level of vigilance you may want to lower these thresholds. If you find that you are alerted more often than necessary, you can increase the thresholds to reduce the number of alerts. |
### Table 4-1  Mobile Security management server settings options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Location</th>
<th>Suggested use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thresholds and Alerting: Licensing</td>
<td>Home &gt; Mobile Security &gt; Settings &gt; Management Server Settings</td>
<td>You license this product according to the number of managed devices. These alerts warn you when you approach your licensing limits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Available licenses warning</strong> - based on percentage of total available licenses. If you add new devices often or expect several new devices to be added at once, increase this value to give you more advance warning. In environments where managed devices remain relatively constant, you can set the value lower.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Send email for available-license warning</strong> - If you enable this option, configure the email address for the administrator who is responsible for licensing oversight.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>License expiration warning</strong> - based on time remaining before license expiry. Depending on your license procurement process, you may require more or less advanced warning of license expiry. For instance, if your procurement process requires a longer lead-time than the default, increase the value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Send email for license-expiry warning</strong> - If you enable this option, configure the email address for the administrator who is responsible for license oversight or for license procurement.</td>
</tr>
</tbody>
</table>
Table 4-1  Mobile Security management server settings options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Location</th>
<th>Suggested use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thresholds and Alerting:</td>
<td><strong>Home &gt; Mobile Security &gt; Settings &gt;</strong></td>
<td>In most cases, you target a single policy to each managed device. However, it is possible that a device becomes unintentionally targeted by more than one policy. In this case, a conflict may arise that results in mis-applied security settings.</td>
</tr>
<tr>
<td>Policy Targeting</td>
<td><strong>Management Server Settings</strong></td>
<td><em>Send email for multiple-policy-target alert</em>- If you enable this option, configure the email address for the administrator who is responsible for mobile device security policy oversight.</td>
</tr>
<tr>
<td>Miscellaneous Settings</td>
<td><strong>Home &gt; Mobile Security &gt; Settings &gt;</strong></td>
<td>Symantec uses statistical data about product use to improve product quality. Enable this option to anonymously send statistical data to Symantec.</td>
</tr>
<tr>
<td></td>
<td><strong>Management Server Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Symantec Mobile Security Gateway server

Android devices communicate with a Gateway server that is connected virtually to the Management Server. Gateway servers add a layer of protection against the mobile device applications that may attempt to circumvent standard network security. A Gateway server is created by default during installation on the host computer, and additional Gateway servers can be added as needed.

See “Adding additional Gateway servers” on page 35.

To edit the settings for the Gateway, on the management console, go to **Home > Mobile Security > Settings > Mobile Security Gateway**. On the toolbar, click the **Edit** (pencil) icon.

Table 4-2 provides a list of configuration settings for the Gateway Server.
<table>
<thead>
<tr>
<th><strong>Setting</strong></th>
<th><strong>Use</strong></th>
</tr>
</thead>
</table>
| Server:                   | If more than one Gateway Server is configured, you select the server you want to configure in the drop-down menu. If only one Gateway server is configured, no selection is available.  
**Note:** By default, the initial Gateway server is established on the Symantec Management Platform that hosts Symantec Mobile Security.                                                                                      |
| External host address     | This setting lets you override the default address that is used to provision the Agent app. Devices communicate through this address.  
See “Distributing the Agent app to Android device owners” on page 22.                                                                                                                                                                                                         |
| Binding IP address:       | The binding IP address and port are also used to configure IIS for new Gateway servers. You can also use this setting to set the IP address when more than one NIC is used. For instance, a NIC dedicated to external network connectivity can be selected. If you set an address in IIS and verified the connection using the Verify option, the IIS address appears in this field.  
See “Adding additional Gateway servers” on page 35.                                                                                                                                                                                                                       |
| Binding IP port           | If you need to use a non-default port, you change it here. The default port is 443. The binding port is used to configure IIS when you install a new Gateway server.  
**Note:** The Gateway install fails when there is a port conflict. Use the Verify button (green check-mark) to test the Gateway to Security server connection.                                                                                       |
Table 4-2  Gateway server configuration settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment package</td>
<td>The drop-down menu shows the available Android Agent packages. The package that is displayed by default is the most recent version. For the 7.2 release of Symantec Mobile Security, there is one available package. Additional packages become available in subsequent releases. See “Distributing the Agent app to Android device owners” on page 22.</td>
</tr>
</tbody>
</table>

Table 4-3 describes how to use the controls available on the Gateway server configuration page.

Table 4-3  Gateway server configuration toolbar

<table>
<thead>
<tr>
<th>Control</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Click this icon to add a new Gateway Server. See “Adding additional Gateway servers” on page 35.</td>
</tr>
<tr>
<td>Email (envelope icon)</td>
<td>This icon opens the email template you use to deploy the Android Agent app to device owners. Select a listed Gateway Server first. See “Distributing the Agent app to Android device owners” on page 22. <strong>Note:</strong> The information in the email template is unique to the selected Gateway.</td>
</tr>
<tr>
<td>Verify (check mark)</td>
<td>Click this icon to verify that the Gateway is connected to and communicating with the Symantec Mobile Security server.</td>
</tr>
<tr>
<td>Edit (pencil icon)</td>
<td>Select a listed Gateway and then click this icon to edit the settings for the selected server. See Table 4-2 on page 29.</td>
</tr>
</tbody>
</table>
Table 4-3  Gateway server configuration toolbar (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete ('X' icon)</td>
<td>Select a listed Gateway and then click this icon to delete the selected Gateway Server. Before you can delete a Gateway, be aware of the following:</td>
</tr>
<tr>
<td></td>
<td>■ All of the devices that are enrolled with the Gateway must be reassigned to use an alternate Gateway. To change the Gateway assignment for devices, you provide a new policy to specify the alternate Gateway. See “Configuring the default Android security policy” on page 43.</td>
</tr>
<tr>
<td></td>
<td>■ Before you can delete a Gateway, any policy that references the Gateway must be reconfigured to use a different Gateway.</td>
</tr>
<tr>
<td></td>
<td>See “Assigning Android policies to a specific device or group of devices” on page 50.</td>
</tr>
</tbody>
</table>

Setting up Google Cloud Messaging (GCM)

Google Cloud Messaging (GCM) enables Symantec Mobile Security to quickly communicate with Android mobile devices. GCM lets you push commands to Android devices instead of waiting for the device to check in.

Note: To receive GCM messages, a Google Gmail is required to be set up on the devices running Android 4.04 or older.

You set up GCM in two phases:

■ Create a new project at Google's APIs Web site, obtain the Project ID number, and generate a Google API server key.

■ Configure Symantec Mobile Management to use GCM.
To create a new project and obtain the Project ID number and API server key

1. Go to https://code.google.com/apis/console, sign into your Google account, and then click, Create project...

2. On the left side of the APIs Dashboard page, click the drop-down menu and select Create ...

3. Enter a name for the project and click Create Report. Your browser refreshes and displays a new URL.

4. In the URL, locate the element, #project. Record the number that follows #project. For example, https://console.google.com/apis/console/#project:1066916068160

Note: Note: This number is called the “Google Project ID” and it is required when you configure Symantec Mobile Management to use GCM.

5. Select your project from the API Project drop-down list and then in the left pane, select Services.

6. Scroll down the page to Google Cloud Messaging for Android, and set the ON/OFF widget to ON.

7. On the Google APIs Terms of Service page, agree to and accept the terms of the agreement.

8. Return to the APIs home page and towards the bottom of the page, click Create new Server key.

9. On the Configure Server Key for My Project panel, you can optionally specify a particular server or servers that can use GCM. Enter the IP address of each server on a separate line. Leave the field blank to allow any server IP address. Check the Google documentation for more information.

10. Click Create. The server key is displayed on the API Access page under Key for server apps (with IP locking). Record the server key string for use in the next procedure.

To configure Symantec Mobile Management to use GCM

1. On the Symantec Management Console, go to Home > Mobile Management > Settings > Mobile Management Server Settings and click the GCM tab.

2. Enter the Project ID and Server key you generated in the previous procedure.

3. Click Save changes.

Mobile Management is now configured to send GCM data to Android mobile devices.

Securing the management console

The Symantec Management Platform console should be secured against unauthorized access. You set up console security in Symantec Management Platform. For more information and instructions, see the topic, Accessing the Symantec Management Console in the Symantec Management Platform User Guide.

Note: To access the Symantec Management Platform User Guide, on the console go to Help tab > Documentation.

Configuring Microsoft Active Directory for enrolling mobile devices

The Microsoft Active Directory Import feature of the Symantec Management Platform lets you import Active Directory objects, such as users, computers, sites, and subnets, into the CMDB. This feature lets you leverage the data that already exists in Active Directory without re-creating it.

For instructions to configure Active Directory for enrolling mobile devices, see the topic, About Microsoft Active Directory Import in the Symantec Management Platform User Guide

Note: To access the Symantec Management Platform User Guide, on the console go to Help tab > Documentation.
Configuring Microsoft Active Directory for enrolling mobile devices
Adding additional Gateway servers

This chapter includes the following topics:

- Adding additional Gateway servers
- Gateway server best-practices

Adding additional Gateway servers

You add new Gateway servers to increase the capacity of a Symantec Mobile Security installation, to improve network performance, and to assist the management of security profiles. By default, a Gateway server is installed on the host computer when you install Symantec Mobile Security.

Table 5-1 depicts the basic workflow to install additional Gateway servers.
Table 5-1 Gateway installation workflow

<table>
<thead>
<tr>
<th>Step</th>
<th>Actions to take</th>
</tr>
</thead>
</table>
| Step 1 | Identify the computers to host the additional Gateway servers. Note the following:  
- Gateway servers have specific hardware and software requirements.  
  See “Server requirements” on page 99.  
- The computers that host a Gateway server must have the Symantec Management Agent installed. The Agent provides data and communication integration to the Symantec Management Platform.  
  See the topic, About the Symantec Management Agent in the Symantec Management Platform User Guide.  
  **Note:** You can access the Symantec Management Platform User Guide from the Help tab on the console. |
| Step 2 | Configure the new Gateway server.  
| Step 3 | Configure a new Android security policy to use the new Gateway server.  
  See “Configuring a new Android security policy” on page 48. |
| Step 4 | Distribute the policy.  
  See “Assigning Android policies to a specific device or group of devices” on page 50. |
| Step 5 | Verify that the Android mobile device is able to connect to the new Gateway server.  
  See “Verifying Android device enrollment” on page 52. |

Gateway server best-practices

The Gateway server provides an added layer of security when managing Android devices, and also consolidates Android device network traffic.
Securing Android mobile devices

- Chapter 6. Common Android security tasks
- Chapter 7. Configuring Android security settings and options
Common Android security tasks

This chapter includes the following topics:

■ Locating a lost or stolen Android device
■ Locking a lost or stolen Android device
■ Wiping data from a lost or stolen Android device
■ Triggering an alarm on a lost or stolen Android device
■ Configuring the default Android security policy
■ Configuring a new Android security policy
■ Checking Android mobile device compliance
■ Identifying the Android mobile devices that are at risk
■ Checking Android Web security events
■ Assigning Android policies to a specific device or group of devices
■ Pushing a command to an Android device to initiate a security scan or policy update
■ Verifying Android device enrollment

Locating a lost or stolen Android device

Enrolled Android devices send their location information to the Symantec Mobile Security server at regular intervals. When you view the device information in the console, the device location is shown on a map.
Locating a lost or stolen Android device

1. On the console go to **Home > Mobile Security > Device Management**, and click **Manage Mobile Devices**.
2. In the right pane, select the device you want to locate.

   **Note:** Use the search tool to more quickly find a device within a long list.

3. Right-click on the device you want to locate and from the menu, select **Android Security > View device information**.

When locating a device, be aware of the following:

- The location that is displayed shows the location of the device at the time of its last check-in with the server. By default, location information is sent to the server once an hour. This interval can be adjusted by making a new policy available to the device.
  
  You configure check-in times on the Communication tab of the Android security policy.
  
  See “Configuring the default Android security policy” on page 43.

- If GCM is configured, you can push a command to the device to have it send its current information, including its location.
  
  See “Setting up Google Cloud Messaging (GCM)” on page 31.

- Locating a device requires that location services are enabled on the device.

Locking a lost or stolen Android device

You can remotely lock a managed Android device to prevent unauthorized access.

Locking a lost or stolen Android device

1. On the console, go to **Home > Mobile Security > Device Management** and in the left pane, click **Manage Mobile Devices**.
2. In the right pane, select the device you want to locate.

   **Note:** Use the search tool to more quickly find a device within a long list.

3. Right-click on the device you want to lock and from the menu, select **Android Security > Secure lost/stolen device**.
4. Enable the **Lock device** option. If you only want to lock the device, disable the other options.
5 Enter a new passcode that you issue to the device owner to unlock their device.
6 Optionally, modify the text message that appears when the device is locked.
7 Click OK.

Depending on when the device is set to check in for new security actions, and whether GCM is enabled, it can take 30 minutes or longer to lock the device. By default, the scheduled check-in is set to 30 minutes. This value can be adjusted up or down as desired. GCM allows the lock command to be pushed to the Android device.

See “Setting up Google Cloud Messaging (GCM)” on page 31.

Note: The shorter the check-in interval, the more often the device is active. Battery life, data plan usage, and network traffic is affected by this setting.

You configure check-in times on the Communication tab of the default Android security policy.

See “Configuring the default Android security policy” on page 43.

Wiping data from a lost or stolen Android device

You can remotely wipe the data from a managed Android device to prevent unauthorized access to media, apps, and sensitive information.

Warning: Unless previously synched with a backup system, any data, apps, or media on the device and its SD card are permanently erased. The call history and contacts list on the SIM card is also erased and the device is restored to factory settings.

Wiping data from a lost or stolen Android device

1 On the console, go to Home > Mobile Security > Device Management and in the left pane, click Manage Mobile Devices.
2 In the right pane, select the device you want to locate.

Note: Use the search tool to more quickly find a device within a long list.

3 Right-click on the device you want to lock and from the menu, select Android Security > Secure lost/stolen device.
4 Enable the **Wipe device** option. If you only want to wipe the device, disable the other options.

5 Click **OK**.

Depending on when the device is set to check in for new security actions, and whether GCM is enabled, it can take 30 minutes or longer to lock the device. GCM allows the lock command to be pushed to the Android device. Scheduled check-in is set to 30 minutes by default, and this value can be adjusted up or down as desired. See “Setting up Google Cloud Messaging (GCM)” on page 31.

You configure check-in times on the Communication tab of the default Android security policy. See “Configuring the default Android security policy” on page 43.

**Triggering an alarm on a lost or stolen Android device**

You can remotely trigger an alarm on a managed Android device to draw attention to its presence.

**Triggering an alarm on a lost or stolen device**

1 On the console, go to **Home > Mobile Security > Device Management** and in the left pane, click **Manage Mobile Devices**.

2 In the right pane, select the device you want to locate.

---

**Note:** Use the search tool to more quickly find a device within a long list.

3 Right-click on the device you want to sound the alarm on and from the menu, select **Android Security > Secure lost/stolen device**.

4 Enable the **Turn on alarm** option. If you only want to sound an alarm on the device, disable the other options.

5 Set the duration and number of times to repeat the alarm sound.

6 Click **OK**.

Depending on when the device is set to check in for new security actions, and whether GCM is enabled, it can take 30 minutes or longer to lock the device. By default, the scheduled check-in is set to 30 minutes. This value can be adjusted up or down as desired. GCM allows the lock command to be pushed to the Android device.

See “Setting up Google Cloud Messaging (GCM)” on page 31.
Note: The alarm sounds regardless of volume or mode (vibrate, silent, or ringer) settings on the device.

You configure check-in times on the Communication tab of the default Android security policy.

See “Configuring the default Android security policy” on page 43.

Configuring the default Android security policy

You can modify the default Android security policy to meet the needs of your most common security profile. The default Android policy is also the first policy that is sent to newly enrolled devices.

On the console, go to Home > Mobile Security > Device Management > Default Android Security Policy, and select the tab for the features you want to configure. To retain your changes, click Save changes.

You can also create new policies for lesser-used profiles as you require them.

See “Configuring a new Android security policy” on page 48.

The policy configuration page has four tabs:

- **Security** - configure Anti-Malware Scans, Web protection, and whether to show notifications
  See Table 6-1 on page 43.

- **AppControl** - configure whitelists and blacklists to allow or prevent apps from running, and whether app detection is running.
  See Table 6-2 on page 44.

- **LiveUpdate** - configure how and when the Mobile Security Agent gets program and content updates.
  See Table 6-3 on page 45.

- **Communications** - configure check-in intervals for policies, actions, and inventory; the Gateway that is assigned to the device, the roaming behavior, GCM, and logging options.
  See Table 6-4 on page 46.

Table 6-1 Security tab options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Malware Scans</td>
<td>Allow user to modify the settings on the device</td>
<td>By default, the policy allows the device owner to manage their own settings.</td>
</tr>
</tbody>
</table>
Table 6-1  Security tab options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Anti-Malware Scans    | Enable Anti-Malware scans     | By default, scans are enabled and run at the times that are applied in the settings.  
**Note:** The device owner must be reminded to remove the apps that are not approved.  
You configure which apps are approved on the AppControl tab.  
See Table 6-2 on page 44. |
| Web protection        | Allow user to modify the settings on device | By default, the policy allows the device owner to manage their own settings.  |
| Web protection        | Enable URL protection within browser session | By default, known-malicious Web pages are blocked when using the Android browser. |
| Other                 | Show notifications           | By default, notifications about security events and actions are displayed on the Android device.                                             |

Table 6-2  App Control tab options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable app detection</td>
<td>By default, the policy does not automatically detect apps on the Android device. When this option is enabled, the policy uses the white list or blacklist to determine which apps are allowed.</td>
</tr>
</tbody>
</table>
| Prevent blacklisted apps from running on the device | A blacklist prevents any listed apps from running on the device. To add an app to the list click the plus icon and enter the app information.  
**Note:** **Enable app detection** must be checked to use this feature. |
### Table 6-2  App Control tab options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow only whitelisted apps to run on the device</td>
<td>A whitelist allows the device to only run the listed apps. To add an app to the whitelist, click the plus icon and enter the app information. <strong>Note:</strong> Enable appdetection must be checked to use this feature.</td>
</tr>
<tr>
<td>Importing and exporting lists</td>
<td>For either type of list, you can import and export lists for use with other instances of Symantec Mobile Security and other security policies. Once you have created a list, click the Export icon to open a save dialog. To import a previously saved list, click the Import icon, select the list, and then click Upload. <strong>Note:</strong> The lists are exported as .CSV files.</td>
</tr>
</tbody>
</table>

### Table 6-3  LiveUpdate tab options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to modify the settings on the device</td>
<td>By default, the policy allows the device owner to manage their own settings.</td>
</tr>
<tr>
<td>Enable LiveUpdate</td>
<td>LiveUpdate is enabled by default.</td>
</tr>
<tr>
<td>LiveUpdate scheduling &gt; Automatically check updates:</td>
<td>By default, LiveUpdate runs daily. A drop-down menu provides other intervals. <strong>Note:</strong> Set to Daily, LiveUpdate runs at the approximate time that the device was enrolled.</td>
</tr>
<tr>
<td>LiveUpdate Admin &gt; Use LUA server:</td>
<td>If your organization uses LiveUpdate Administrator (LUA) to provision Symantec updates, you can set the Agent to use LUA. You can also specify which LUA server is used.</td>
</tr>
</tbody>
</table>
### Table 6-4 Communications tab options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Allow user to modify the settings on the device</td>
<td>By default, the policy allows the device owner to manage their own settings.</td>
</tr>
</tbody>
</table>
| **Server Communications**| device check-in frequencies                                | - **Policies** - when the device checks for new policies. Default is each hour.  
- **Actions** - when the device checks for new security actions to execute. Default is 30 minutes.  
- **Inventory** - when the device sends its inventory to the server. Default is every hour.  
**Note:** Set the Inventory check interval to a lower value to get more precise location data. |
| **Server Communications**| inventory to collect                                         | By default, all inventory items are collected.  
**Note:** Regional privacy laws may limit what inventory data you can collect.  |
| **Server Communications**| mobile security gateway that the device communicates with:  | If you have configured more than one Mobile security gateway, you can select which gateway the devices use.  
**Note:** You must preconfigure additional Gateways before assigning them to policies.  
See “Adding additional Gateway servers” on page 35. |
<p>| <strong>Server Communications</strong>| disable LiveUpdate and management communication while roaming | Enabled by default, this option helps to control extra data-plan charges while the device is in a roaming mode. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Server Communications    | Allow untrusted self-signed certificates | By default, the Agent allows the use of un-trusted self-signed certificates. When this option is checked, the Agent does not trust an unsigned server certificate and ceases communication until either:  
- The server starts using a signed certificate  
- The Agent is reinstalled and a new policy is applied. |

GCM Communications         | Enable GCM for Actions      | GCM lets you push commands to perform security actions such as locking or wiping an Android device. Without GCM, security actions must wait for the device to check in. By default, the check-in interval for security actions is 30 minutes.  
See “Configuring the Symantec Mobile Security server” on page 25.  
**Note:** To receive GCM messages, a Google Gmail is required to be set up on the devices running Android 4.04 or older.  
See “Setting up Google Cloud Messaging (GCM)” on page 31. |

Other Communications      | Enable Debug Logging        | Turned off by default, this option can be useful for troubleshooting problems with the Mobile Security Agent app, and communications with the Gateway server. The debug logs are sent to the server at the next Inventory update.  
**Note:** You should disable this option after troubleshooting. |
Configuring a new Android security policy

The default policy may not meet the security needs of certain users. In these cases, you create new policies to meet the needs of individuals and groups for whom the default policy is not appropriate.

Configuring a new Android security policy

1. On the console, go to Home > Mobile Security > Device Management > Add New Policy...

2. A new policy is made by cloning an existing policy. Enter a name for the new policy and then select an existing policy. Select Default Android Security Policy if this policy is your first custom policy.

3. Click OK to begin the configuration process.

4. To configure the settings, use the same procedure you use to configure the default Android policy.

   See “Configuring the default Android security policy” on page 43.

5. The On/Off selector in the upper right corner of the main screen enables or disables the policy. You must enable the policy before it can be deployed.

   See “Assigning Android policies to a specific device or group of devices” on page 50.

Checking Android mobile device compliance

Symantec Mobile Security establishes standards for security compliance through the use of security policies and the Symantec Mobile Security Agent app. When one or more managed devices become non-compliant, they can become security risks. Best practices dictate that you periodically check the compliance status of enrolled mobile devices.

Checking mobile device compliance

1. On the console, go to Home > Mobile Security > Overview and Reports > Device Compliance.

2. The Non-Compliant Devices Details page lists the enrolled devices and their levels of compliance.

   Double-click any of the devices to see more details about its compliance status.

   The column headings refer to the following:

   ■ StatusTime- The last time the device status was logged to the Symantec Mobile Security server.

   ■ Out-of-Date Engine- Whether the malware scan engine is current.
- **Administrator disabled** - Whether the device-administrator permissions on the mobile device have been revoked. The mobile device agent requires administrator permissions on the device to enable the security features such as locking the device and wiping data.

- **Out-of-touch** - The device is turned off or does not have cell service.

- **GCM Registration Failed** - The device is not registered to receive GCM messages. See “Setting up Google Cloud Messaging (GCM)” on page 31.

- **Rooted** - Whether the factory-installed operating system has been circumvented.

### Identifying the Android mobile devices that are at risk

The **At-Risk Devices Details** report provides a list of all enrolled mobile devices that have scanned positive for malware or have attempted to run a blacklisted app. The intent of this report is to give you an indication of the devices that are more likely to become a security risk. Devices that accumulate excessive malware and blacklisted app entries in this report should be considered suspect until more thoroughly investigated.

Go to **Home > Mobile Security > Overview and Reports > At-Risk Devices Details**. To quickly rank the devices by risk, in the right pane, click the column heading to sort by **Malware Count** or **Blacklist Count**. Double-click on a device to see more details about the threats thus far encountered.

### Checking Android Web security events

The mobile devices that visit one or more blocked Web sites appear in the **Web Protection** report. The report lists the name of the device, the date of the visit, and the URL of the blocked site. The main intent of this report is to give you an indication of the devices that are more likely to become a security risk. Devices that accumulate excessive entries in this report should be considered suspect until more thoroughly investigated.

Go to **Home > Mobile Security > Overview and Reports > Web Protection**. To quickly rank the devices by risk, in the right pane, click the column heading to sort by **Device Name**. To rank the Web sites by most visits, click the **Web Site** column header. Double-click on a device to see more details about the threats thus far encountered.
Assigning Android policies to a specific device or group of devices

Symantec Mobile Security installs with a default Android security policy that is sent to each newly enrolled device. To change the policy settings on the Agent, you assign a new policy to the device Agent.

See “Configuring a new Android security policy” on page 48.

You can apply a policy to specific groups of users and devices. These groups are called “resource targets” and you establish them first in Symantec Management Platform. See the Symantec Management Platform User Guide for instructions to create resource targets.

**Note:** The Symantec Management Platform User Guide is available in the Symantec Management Platform Help utility.

You can also push a command to individual mobile devices to download and apply specific policies.

See “Pushing a command to an Android device to initiate a security scan or policy update” on page 51.

**Applying a policy to an individual Android device**

1. On the console, go to Home > Mobile Security > Device Management and in the left pane, select the policy you want to apply.
2. Scroll to the bottom of the pane and in the Applied to section, at the far right, click the reveal button.
3. On the policy page toolbar, set the View: filter to Mobile devices
4. On the Select resources panel, select the device or devices the policy applies to and then click **Apply**.

**Note:** Use the search tool to quickly locate a specific device within a long list.

**Applying a policy to a group of Android devices**

1. On the console, go to Home > Mobile Security > Device Management and in the left pane, select the policy you want to apply.
2. Scroll to the bottom of the pane and in the Applied to section, at the far right, click the reveal button.
3. On the policy page toolbar, set the View: filter selector to Targets
4 On the toolbar, click **Apply to > Quick apply**.

5 In the **Quick apply** dialog, use the dropdown selector to select the group or groups the policy applies to and then click **Apply**.

**Note:** Groups must first be created in Symantec Management Platform before they appear on the list of available groups.

Unless you force an update by pushing a command, the policy is applied the next time the targeted resource checks in with the server. Check-in schedules are configurable on the **Communications** tab of the Android security policy page.

See “**Configuring the default Android security policy**” on page 43.

See “**Pushing a command to an Android device to initiate a security scan or policy update**” on page 51.

### Pushing a command to an Android device to initiate a security scan or policy update

You can push a command to an enrolled Android device to override the scheduled scan or update.

**Note:** To push commands to Android devices, GCM must be configured on the Gateway server and on the device policy.

See “**Setting up Google Cloud Messaging (GCM)**” on page 31.

See “**Configuring the default Android security policy**” on page 43.

**To push a scan or update command to an Android device**

1 On the console, go to **Home > Mobile Security > Device Management > Manage Mobile Devices**.

2 In the right pane, locate the device on which to run the scan or update.

3 Right-click on the device and select **Android Security > Update device protection**.

4 Verify the device name, select the desired actions and then click **OK**.
Verifying Android device enrollment

You can quickly verify the enrollment status of Android mobile devices that run the Symantec Mobile Security Agent app.

On the console, go to Home > Mobile Security > Device Management > Manage Mobile Devices. Search the list by Name and under the Enrollment Status heading, check that the device is enrolled.
Configuring Android security settings and options

This chapter includes the following topics:

- Configuring Android enrollment and management settings
- Configuring how Android devices appear in lists and reports

Configuring Android enrollment and management settings

You configure the type of authentication, the default behavior for security actions, and the GCM Notifications credentials.

To configure these settings, go to Home > Mobile Security > Settings > Android Configuration.

Table 7-1 describes each setting and provides usage suggestions.
### Table 7-1  Android Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Enrollment &gt; Device authentication</strong></td>
<td>Select how the Agent authenticates to the Symantec Mobile Security system.</td>
</tr>
<tr>
<td>- <strong>No authentication</strong></td>
<td>For testing you can choose to not require authentication. You should only use this option for non-critical implementations.</td>
</tr>
<tr>
<td>- <strong>Use Active/LDAP authentication</strong></td>
<td>To use the existing credentials that are associated with Active Directory, you must first import your Active Directory objects into the Symantec Management Platform. For instructions to import Active Directory objects, see the topic <em>About Microsoft Active Directory Import</em> in the <em>Symantec Management Platform User Guide</em>.</td>
</tr>
<tr>
<td><strong>Note:</strong> Go to Help tab &gt; Documentation to access the Symantec Management Platform User Guide from within the Symantec Management Platform console.</td>
<td></td>
</tr>
<tr>
<td>- <strong>Use management server user accounts</strong></td>
<td>If you have created user accounts in Symantec Management Platform, you select <strong>Use management server user accounts</strong>. For information about creating accounts in Symantec Management Platform, see the topic, <em>Creating and configuring Symantec Management Platform user accounts</em> in the <em>Symantec Management Platform User Guide</em>.</td>
</tr>
</tbody>
</table>
### Table 7-1 Android Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Action Defaults</strong></td>
<td>These default settings control the text in the locked-device message and the alarm behavior.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Lock screen text</strong>: The locked-device message appears on the mobile device when it is remotely locked. Use the provided message or create a new message. If you create a new message, keep it short so that it is easily read on a small screen.</td>
</tr>
<tr>
<td></td>
<td>See “Locking a lost or stolen Android device” on page 40.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Alarm duration and repeat interval</strong>: The alarm sounds for the duration that is set, and is silent for the same amount of time.</td>
</tr>
<tr>
<td></td>
<td>Note: The alarm is intentionally loud and annoying. The alarm overrides the device volume level and mode (silent, vibrate, ringer) settings.</td>
</tr>
<tr>
<td></td>
<td>See “Triggering an alarm on a lost or stolen Android device” on page 42.</td>
</tr>
<tr>
<td><strong>GCM Notifications</strong></td>
<td>Enter the GCM Project ID and Server key you generated when you set up GCM.</td>
</tr>
<tr>
<td></td>
<td>See “Setting up Google Cloud Messaging (GCM)” on page 31.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: GCM allows security actions to be pushed down to Android devices instead of devices pulling actions on a scheduled basis.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the default Android security policy” on page 43.</td>
</tr>
</tbody>
</table>
Configuring how Android devices appear in lists and reports

You can configure how Android devices are named in reports, dialogs, and configuration panels.

**Note:** By default, Device ID is used to identify devices when no other fields are specified.

To select and order the fields that appear in the device name, do the following:

**Setting the device name format**

1. Go to Home > Mobile Security > Settings > Android Device Name.
2. In the left panel, select the fields you want to use and then click >> to move them to the right panel.

**Note:** Reverse the procedure to remove one or more fields.

3. To reorder the fields, select a field in the right panel and then click Up or Down.

An example is provided in the user interface that updates in real time to show the result of adding, removing, and reordering fields.

You can also specify the domain of the email account that should be used when a device is associated with more than one email account. Typically, you use the email domain that is common to all device owners, such as your company email domain.
Securing Windows Mobile devices

- Chapter 8. Managing Windows Mobile device protection
- Chapter 9. Configuring the File Access Log policy
Managing Windows Mobile device protection

This chapter includes the following topics:

- Managing Windows Mobile device security
- Creating and applying Windows Mobile security policies
- Managing Windows Mobile antivirus protection
- Excluding files from scans
- Auto-Protect actions
- About managing the firewall
- Creating a custom protection level for the firewall
- Rules for High firewall protection level
- Rules for Medium firewall protection level
- Rules for Low firewall protection level
- Scan automatically after specific actions

Managing Windows Mobile device security

You manage Windows Mobile device security by configuring policies for antivirus protection, the firewall, and security updates. You adjust the settings within the policies to meet the security needs of your organization. You also use policies to manage the software components that enable Windows Mobile device protection.

You also review the status of device protection in your organization by reviewing reports, logs, notifications, and reports.

See “About monitoring device security in Symantec Management Platform” on page 93.

<table>
<thead>
<tr>
<th>Protection component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile antivirus</td>
<td>Protects against virus and spam threats on the device. See “Managing Windows Mobile antivirus protection” on page 61.</td>
</tr>
<tr>
<td>Mobile firewall</td>
<td>Protects against network attacks on the device. See “About managing the firewall” on page 63.</td>
</tr>
<tr>
<td>LiveUpdate Wireless</td>
<td>Provides any available updates to product software and threat definitions files on the device. See “About updating devices” on page 87.</td>
</tr>
</tbody>
</table>

### Creating and applying Windows Mobile security policies

If you manage mobile devices by using the Symantec Management Platform, you create security policies and apply them on the same page of the management console.

If you manage mobile devices by using another mobile device management system, you create security policies in the Symantec Management Platform. You can then export a single policy XML file that contains all your policy settings. You can use any mechanism to push this file to the devices.

**To create security policies**

1. In the Symantec Management Console, go to Manage > Policies > Mobile Security > Windows > name of individual policy.

2. Specify the settings that your organization’s security policies require, and click Save changes.

To create an Agent Installation File

1. In the Symantec Management Console, create the individual security policies that you require.
2. Go to Manage > Policies > Mobile Security > Mobile Security Agent Policy.
3. At the bottom of the policy pane, click Create Agent Installation File.
4. Click Save and save the file to your desired location.
5. Provision the file where device owners can retrieve it.

To apply security policies by using another device management system

1. In the Symantec Management Console, create the individual security policies that you require.
2. Go to Manage > Policies > Mobile Security > Mobile Security Agent Policy.
3. At the bottom of the policy pane, click Export All Policies as Single XML File.
4. In the Select Policy to Export window, check the individual policies that you want to push to your devices, and click Export.
5. Save the XML file to any location.
6. Push the XML file to your devices by using your device management system.

Managing Windows Mobile antivirus protection

To manage Windows Mobile antivirus protection you create one or more antivirus policies and distribute them to the mobile devices.

Symantec Mobile Security antivirus protection includes different types of scans that you can tailor to meet the needs of your organization. Antivirus scans use antivirus definition files that are regularly updated by Symantec. You use LiveUpdate to regularly download the new definition files.

Table 8-2 Types of threat scans

<table>
<thead>
<tr>
<th>Scan type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Protect</td>
<td>As users access files on their devices, Auto-Protect provides real-time threat scanning. See “Auto-Protect actions” on page 63.</td>
</tr>
</tbody>
</table>
Table 8-2  Types of threat scans (continued)

<table>
<thead>
<tr>
<th>Scan type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic scans after specific actions</td>
<td>You can set scans to run automatically after specific actions are performed. These scans are performed on all files on the device. See “Scan automatically after specific actions” on page 68.</td>
</tr>
<tr>
<td>On-demand scans</td>
<td>Users can run one-time scans of all files on the device.</td>
</tr>
</tbody>
</table>

You can also exclude files from scans. File exclusions can help improve performance on the device. You should exclude only the files that do not pose a risk to the security of your network.

See “About updating devices” on page 87.

After you create the policies, you apply them to the devices. You can also export the policy to an XML file for use by a third-party device management system.

See “Creating and applying Windows Mobile security policies” on page 60.

To manage mobile antivirus protection

1. In the Symantec Management Console, go to Manage > Policies > Mobile Security > Windows > Mobile Antivirus Policy.

2. Depending on your organization’s needs, do one of the following:
   - Modify the existing policy.
   - Copy the policy, and modify the settings in the copy. See “Managing Windows Mobile antivirus protection” on page 61.

3. Click Save changes.

Excluding files from scans

You can exclude specific files, file types (extensions), or folders from Auto-Protect scans.
To exclude files from scans

2. In the File Exclusions window, list the specific files, file types, or folders to exclude from scans.
3. Click OK.
4. On the Mobile Antivirus Policy page, click Save changes, and then apply the policy.

Auto-Protect actions

You can specify how Auto-Protect handles the files that contain risks.

Table 8-3  Auto-Protect actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine (default first action)</td>
<td>Tries to move the infected file to the Quarantine on the infected device as soon as it is detected</td>
</tr>
<tr>
<td>Deny access</td>
<td>Tries to prevent any application from opening the infected file.</td>
</tr>
<tr>
<td>Delete</td>
<td>Tries to remove the infected file.</td>
</tr>
<tr>
<td>None (Prompt)</td>
<td>Asks the user to select an action.</td>
</tr>
</tbody>
</table>

About managing the firewall

Symantec Mobile Security includes a firewall to provide a barrier between your organization’s devices and the Internet. The firewall can detect possible hacker attacks, protect personal information, and eliminate unwanted sources of network traffic. All the information that enters or leaves the private network must pass through the firewall.

The firewall examines information packets, and blocks the packets that do not meet the specified security criteria. You control the firewall protection on the devices by creating the firewall policy settings that your organization’s security requires. The firewall policy includes a setting to specify the protection level. The protection level consists of one or more rules that define allowed and blocked network traffic.
The firewall is stateful, which means that incoming traffic that is a response to outgoing traffic from the device is automatically allowed. Only unsolicited incoming traffic is blocked.

The firewall includes four predefined protection levels. You can also define a custom protection level if none of the predefined levels meets your organization’s needs.

See “Creating a custom protection level for the firewall” on page 64.

After you create the policy settings that you require, you can apply the policy to the devices by using the Symantec Management Console. Or you can export the policy to an XML file that you can deploy by using a third-party device management system.

Table 8-4  Predefined firewall protection levels

<table>
<thead>
<tr>
<th>Protection level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Allow standard outgoing traffic, including ActiveSync for Windows Mobile. Block all incoming traffic. See “Rules for High firewall protection level” on page 65.</td>
</tr>
<tr>
<td>Medium</td>
<td>Allow most outgoing traffic. Block all incoming traffic. See “Rules for Medium firewall protection level” on page 67.</td>
</tr>
<tr>
<td>Low</td>
<td>Allow all outgoing traffic. Allow all incoming traffic except IGMP. See “Rules for Low firewall protection level” on page 68.</td>
</tr>
<tr>
<td>None</td>
<td>Turns off the firewall on the device.</td>
</tr>
</tbody>
</table>

Creating a custom protection level for the firewall

The predefined protection levels are sufficient for most organizations. Sometimes, however, you may find that you need to create a custom protection level for a particular group or situation in your organization.

You should be aware of the following issues:

- Rule order is critical. You can adjust rule order after you create individual rules.
To allow passive FTP through port 21, you must allow all outbound TCP traffic. This limitation applies to the Windows Mobile firewall only.

To allow RTSP through port 554, you must allow all outbound UDP traffic. This limitation applies to the Windows Mobile firewall only.

To create a custom protection level

1. In the Symantec Management Console, go to Manage > Policies > Mobile Security > Windows > Mobile Firewall Policy, select Custom, and then click Edit Custom Rules...

2. In the Edit Custom Protection Level window, enter a description for this protection level, and then click the Add icon under Traffic rules.

3. In the Add Firewall Rule window, do one of the following:
   - To create a completely new firewall rule, complete all the fields, and click OK.
   - To work with a predefined rule, click Select predefined rule ..., select the rule to add, change the parameters for the rule as needed, and click OK.

   **Note:** You can edit only some of the parameters for a predefined rule.

4. Repeat step 3 to create as many firewall rules as your protection level requires.

5. In the Edit Custom Protection Level window, move the rules up and down the list until the order meets your needs for this protection level, and click OK.

6. Click Save changes.

**Rules for High firewall protection level**

The High protection level allows standard outgoing traffic, including ActiveSync for Windows Mobile, and blocks all incoming traffic.

See “About managing the firewall” on page 63.

The following parameters are the same for all rules:

- Events are always logged.
- Event severity is always low.
- The IP address range is unrestricted.

The Rule ID is used to associate event log entries with the appropriate rule.
### Table 8-5: High protection level rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Direction</th>
<th>Rule ID</th>
<th>Protocol</th>
<th>Local Port</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow DHCP client</td>
<td>Both</td>
<td>15</td>
<td>UDP</td>
<td>67</td>
<td>68</td>
</tr>
<tr>
<td>Allow DNS query</td>
<td>Both</td>
<td>16</td>
<td>UDP</td>
<td>53</td>
<td>*</td>
</tr>
<tr>
<td>Allow IKE</td>
<td>Both</td>
<td>27</td>
<td>UDP</td>
<td>*</td>
<td>500</td>
</tr>
<tr>
<td>Allow IPSec NAT-T 10000</td>
<td>Both</td>
<td>31</td>
<td>UDP</td>
<td>10000</td>
<td>10000</td>
</tr>
<tr>
<td>Allow IPSec NAT-T 4500</td>
<td>Both</td>
<td>32</td>
<td>UDP</td>
<td>*</td>
<td>4500</td>
</tr>
<tr>
<td>Allow IPSec NAT-T 4502</td>
<td>Both</td>
<td>33</td>
<td>UDP</td>
<td>*</td>
<td>4502</td>
</tr>
<tr>
<td>Allow SMTP</td>
<td>Outbound</td>
<td>57</td>
<td>TCP</td>
<td>*</td>
<td>25</td>
</tr>
<tr>
<td>Allow POP3</td>
<td>Outbound</td>
<td>50</td>
<td>TCP</td>
<td>*</td>
<td>110</td>
</tr>
<tr>
<td>Allow IMAP4</td>
<td>Outbound</td>
<td>28</td>
<td>TCP</td>
<td>*</td>
<td>143</td>
</tr>
<tr>
<td>Allow Telnet</td>
<td>Outbound</td>
<td>64</td>
<td>TCP</td>
<td>*</td>
<td>23</td>
</tr>
<tr>
<td>Allow HTTP</td>
<td>Outbound</td>
<td>20</td>
<td>TCP</td>
<td>*</td>
<td>80</td>
</tr>
<tr>
<td>Allow HTTP alternate 8008</td>
<td>Outbound</td>
<td>21</td>
<td>TCP</td>
<td>*</td>
<td>8008</td>
</tr>
<tr>
<td>Allow HTTP Web proxy 8080</td>
<td>Outbound</td>
<td>22</td>
<td>TCP</td>
<td>*</td>
<td>8080</td>
</tr>
<tr>
<td>Allow HTTPS-TCP</td>
<td>Outbound</td>
<td>23</td>
<td>TCP</td>
<td>*</td>
<td>443</td>
</tr>
<tr>
<td>Allow HTTPS-UDP</td>
<td>Outbound</td>
<td>24</td>
<td>UDP</td>
<td>*</td>
<td>443</td>
</tr>
<tr>
<td>Allow ActiveSync/AirSync</td>
<td>Both</td>
<td>1</td>
<td>TCP</td>
<td>26675</td>
<td>*</td>
</tr>
<tr>
<td>Allow ActiveSync desktop passthrough</td>
<td>Both</td>
<td>2</td>
<td>TCP</td>
<td>5721</td>
<td>*</td>
</tr>
<tr>
<td>Allow ActiveSync heartbeat TCP</td>
<td>Both</td>
<td>3</td>
<td>TCP</td>
<td>5679</td>
<td>*</td>
</tr>
</tbody>
</table>
Table 8-5  High protection level rules (continued)

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Direction</th>
<th>Rule ID</th>
<th>Protocol</th>
<th>Local Port</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow ActiveSync heartbeat UDP</td>
<td>Both</td>
<td>4</td>
<td>UDP</td>
<td>5679</td>
<td>*</td>
</tr>
<tr>
<td>Allow ActiveSync RAPI requests client</td>
<td>Both</td>
<td>5</td>
<td>TCP</td>
<td>990</td>
<td>*</td>
</tr>
<tr>
<td>Allow ActiveSync RAPI requests server</td>
<td>Both</td>
<td>6</td>
<td>TCP</td>
<td>*</td>
<td>990</td>
</tr>
<tr>
<td>Allow ActiveSync RNDIS DHCP server</td>
<td>Both</td>
<td>7</td>
<td>UDP</td>
<td>68</td>
<td>67</td>
</tr>
<tr>
<td>Allow ActiveSync Sync info</td>
<td>Both</td>
<td>8</td>
<td>TCP</td>
<td>5678</td>
<td>*</td>
</tr>
<tr>
<td>Allow ActiveSync time server</td>
<td>Both</td>
<td>9</td>
<td>TCP</td>
<td>999</td>
<td>*</td>
</tr>
<tr>
<td>Allow ActiveSync Wcescomm</td>
<td>Both</td>
<td>10</td>
<td>TCP</td>
<td>7438</td>
<td>*</td>
</tr>
<tr>
<td>Deny all</td>
<td>Both</td>
<td>110</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

Rules for Medium firewall protection level

The Medium protection level allows most outgoing traffic, and blocks all incoming traffic.

It includes the ruleset for the High protection level, plus the following rules. The additional rules are processed after the rules that are included in the High protection level.

Table 8-6  Medium protection level rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Direction</th>
<th>Rule ID</th>
<th>Protocol</th>
<th>Local Port</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow active FTP</td>
<td>Outbound</td>
<td>18</td>
<td>TCP</td>
<td>*</td>
<td>20</td>
</tr>
<tr>
<td>Allow passive FTP</td>
<td>Outbound</td>
<td>17</td>
<td>TCP</td>
<td>21</td>
<td>*</td>
</tr>
<tr>
<td>Allow RTSP UDP</td>
<td>Outbound</td>
<td>56</td>
<td>UDP</td>
<td>*</td>
<td>554</td>
</tr>
</tbody>
</table>
### Table 8-6 Medium protection level rules (continued)

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Direction</th>
<th>Rule ID</th>
<th>Protocol</th>
<th>Local Port</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow RTSP TCP</td>
<td>Outbound</td>
<td>55</td>
<td>TCP</td>
<td>*</td>
<td>554</td>
</tr>
<tr>
<td>Allow TCP</td>
<td>Outbound</td>
<td>63</td>
<td>TCP</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Allow UDP</td>
<td>Outbound</td>
<td>65</td>
<td>UDP</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Block all</td>
<td>Both</td>
<td>110</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

### Rules for Low firewall protection level

The Low protection level allows all outgoing traffic, and all incoming traffic except IGMP.

### Table 8-7 Low protection level rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Direction</th>
<th>Rule ID</th>
<th>Protocol</th>
<th>Local Port</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block IGMP</td>
<td>Both</td>
<td>26/80</td>
<td>IGMP</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Allow all</td>
<td>Both</td>
<td>11</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Block all</td>
<td>Both</td>
<td>110</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

### Scan automatically after specific actions

You can specify that a scan run automatically after a device user performs certain actions.

See “Managing Windows Mobile device security” on page 59.

### Table 8-8 Automatic scans

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUpdate</td>
<td>Scans for threats after LiveUpdate is run.</td>
</tr>
<tr>
<td>Memory card insertion</td>
<td>Scans for threats after the user inserts a memory card into the device.</td>
</tr>
<tr>
<td></td>
<td>(Windows Mobile only)</td>
</tr>
<tr>
<td>Synchronization with computer</td>
<td>Scans for threats after the user synchronizes the device with the desktop computer. (Windows Mobile only)</td>
</tr>
<tr>
<td></td>
<td>You can also specify that a scan run only after the device is synchronized for the first time.</td>
</tr>
</tbody>
</table>
This chapter includes the following topics:

- About the File Access Log
- Configuring the File Access Log policy for Windows Mobile devices
- About managing a lost or stolen Windows device
- Retrieving the Windows Mobile File Access Log
- Decrypting the File Access Log
- How to read the File Access Log

About the File Access Log

The File Access Log provides a record of specified files that are accessed on the device. You can upload it if a device is lost or stolen, or to help monitor activity on the device for any reason.

The File Access Log is different from the Event Log, which provides a record of security-related events on the device. The File Access Log is uploaded to the server only when you specifically request it.

You manage the File Access Log by creating a policy that enables the log and specifies the files and folders to watch.
Configuring the File Access Log policy for Windows Mobile devices

Windows Mobile devices can log their file access activity and upload it to a central location. This feature is useful when you want to monitor access patterns to the sensitive content that is stored on the device. You can also use the logs to verify whether documents have been accessed before you remotely wipe a stolen device.

To enable file-access logging for Windows Mobile devices, you issue a policy that specifies the following:

- The items to be logged
- Maximum log size
- Maximum length of time to keep the logs
- Upload location for the logs

You configure the File Access Log policy on the Manage tab of the Symantec Management Console.

To configure the Windows Mobile File Access Log policy

1. On the console, go to Manage > Policies > Policies > Windows > Mobile File Access Policy
2. In the right pane, select the options, the log file limits, and provide an upload location for the log files.
3. Under Folders to Watch, enter the folders, files, or file types to log or exclude from logging. You use the following syntax:
   - To include an item in the log, precede the folder name, file name, or file type with a plus sign (+). For instance, +Work messages.
   - To exclude an item in the log, precede the folder name, file name, or file type with a minus sign (-). For instance, -My Pictures.
   - Use a semi-colon (;) to separate items. For instance, -My Pictures; +Work messages excludes My Pictures and includes Work Messages.
4. Assign the policy to the Windows Mobile Devices that log their file activity.
   See “Creating and applying Windows Mobile security policies” on page 60.
5. Click Save changes
About managing a lost or stolen Windows device

If a Windows device is lost or stolen, you can examine the Windows Mobile File Access Log and analyze the risks to your organization’s information. The File Access Log provides a record of specified files that are accessed on the device. It can also be useful to help monitor activity on a device for any reason.

The File Access Log is different from the event log, which provides a record of security-related events on the device. The File Access Log is uploaded to the server only when you specifically request it.

You manage the File Access Log by creating a policy that enables the log and specifies the files and folders to watch.

See “Configuring the File Access Log policy for Windows Mobile devices” on page 70.

You upload the log in any of the following ways:

- By specifying the setting to upload the log in the File Access Log policy and then applying the policy
  You use this method if the policy schedule meets your needs for uploading the log file. The schedule is set by using the Mobile Security policy.
  See “Creating and applying Windows Mobile security policies” on page 60.

- By uploading the log file to an FTP server
  You use this method if you manage your devices by using a third-party device management system.
  See “Retrieving the Windows Mobile File Access Log” on page 71.

The uploaded file is encrypted. You decrypt it by running a command-line tool.

See “Decrypting the File Access Log” on page 72.

See “How to read the File Access Log” on page 74.

Retrieving the Windows Mobile File Access Log

How you retrieve the File Access Log from a device depends on how you manage your devices. It also depends on whether the device is connected to your network.

See “About managing a lost or stolen Windows device” on page 71.

After you retrieve the log file, you must decrypt the log before you can read and analyze it.

See “Decrypting the File Access Log” on page 72.

You can apply a new File Access Log policy to the device.
Caution: You must apply a new policy—that is, a policy that includes at least one new setting. This setting should be the option to enable uploading the log file. Do not enable this setting when you apply the policy to your devices for the first time.

To retrieve the File Access Log by applying a new policy

2. Check the Upload File Access Log checkbox, and click Save.
3. Apply the policy to the device that you want to upload the log from.

See “Creating and applying Windows Mobile security policies” on page 60.

If you manage your devices by using a third-party device management system, you can upload the File Access Log to an FTP server.

This procedure is simpler if you have already pushed a policy to the devices that specifies the FTP server. You can add these arguments to the command line, however, if you did not specify them in the policy.

To retrieve the File Access Log by uploading to an FTP server

1. Open a command window, and type the following command:

   FileMonitorMgr.exe /Restart

2. After the log is restarted, type the following command:


where ftp://ftpserver.com, username, and password are not required if you specified them in a policy that you pushed to the device.

The following arguments to FileMonitorMgr.exe are also available:

- /ShutDown
- /Start

Decrypting the File Access Log

You decrypt the File Access Log that you upload to the server by running a command-line tool. The version of the tool that you run depends on the operating environment of the device on which the log was generated.
**Note:** If you manage by using a third-party device management system, you can still run the tools to decrypt the log file. Log file names and locations are different, however, and depend on your particular system.

See “About managing a lost or stolen Windows device” on page 71.

Decryption produces a CSV file that you can analyze in the tool that you choose.

**To decrypt a File Access Log that was created on a Windows Mobile device**

1. On the Notification Server computer, locate the log file that you uploaded to the server.
   
   The file is placed in the following location:
   
   C:\Program Files\Altris\Mobile\FileIOLog\Device ID\n
2. Navigate to the TOOLS folder on the product disc, and double-click CSVConvertTool.exe.

3. Select the file to convert, and click **Convert to CSV**.
   
   You can also run this tool from the command line by using the following command:

   ```
   CSVConvertTool log filename
   ```

4. Review and analyze the log file details.
   
   See “How to read the File Access Log” on page 74.

**To decrypt a File Access Log that was created on a Symbian device**

1. On the Notification Server computer, locate the log file that you uploaded to the server.
   
   The file is placed in the following location:
   
   C:\Program Files\Altris\Mobile\FileIOLog\Device ID\n
2. Open a command window, and type the following commands

   ```
   decryptfileaccesslog log filename
   ```

   The CSV file that these commands produce is placed by default in the same location as the log file.

3. Review and analyze the log file details.
   
   See “How to read the File Access Log” on page 74.
How to read the File Access Log

Each decrypted log file starts with a header that includes the following information:

- The log file size limit
- The folders or files that are watched
- The device IMEI number
- The device serial number

The following example shows a typical header:

Limit file size=1048576
Filter template= (+) \My Documents\*.*
IMEI Number=000
Serial Number= 
2700000140000001200000026000000100000050006F0063006500740050004300000000

Individual log entries include the following information:

- Timestamp
- Event type
- Path to the files and folders that are watched
- The source program that processed the file
- The destination location where the application placed the processed file

The following example shows a typical log entry:

[03/22/07 16:23:12], Category=File Event, Type=File Create, Flags=Flag Sync, 
Path="\My Documents\Test.txt", Source="pword.exe", Destination="(null)",
Access=0x80000000 

This log entry indicates that at 4:23pm, the file \My Documents\Test.txt was opened by the program Pword.exe (Pocket Microsoft Word).

The following event types are logged for Windows Mobile devices:

File Create Indicates that the file was either created or opened.

*Note:* File Create is the internal API used to both create and open files in Microsoft Windows CE.

File Close Indicates that the file was closed
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Move</td>
<td>Indicates that the file was moved from one location to another. The destination value is the location where the file was moved to.</td>
</tr>
<tr>
<td>File Delete</td>
<td>Indicates that the file was deleted</td>
</tr>
<tr>
<td>File Copy</td>
<td>Indicates that the file was copied from one location to another.</td>
</tr>
</tbody>
</table>

The following event types are logged for Symbian devices:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Create</td>
<td>Indicates that the file was created.</td>
</tr>
<tr>
<td>File Open</td>
<td>Indicates the file was opened on the device.</td>
</tr>
<tr>
<td>File Delete</td>
<td>Indicates that the file was deleted</td>
</tr>
<tr>
<td>File Replace</td>
<td>Indicates that the watched file was replaced with a copy from a different location.</td>
</tr>
</tbody>
</table>

The following event types are logged for both device platforms:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Logging</td>
<td>Adds a timestamp when the log begins.</td>
</tr>
<tr>
<td></td>
<td>This event can help determine whether the time range of the log file is valid.</td>
</tr>
<tr>
<td>Stop Logging</td>
<td>Adds a timestamp when the log ends properly.</td>
</tr>
<tr>
<td></td>
<td>If the log file does not include this event, the log was not properly stopped. The time range of the log file may not be valid.</td>
</tr>
</tbody>
</table>

**Note:** The **Start Logging** event can roll off the beginning of the log file. If the first timestamp in the log file is after that start time that you want to review, you may have a compliance issue.
Configuring the File Access Log policy

How to read the File Access Log
Section 4

Maintaining Symantec Mobile Security

- Chapter 10. Licensing Symantec Mobile Security 7.2
- Chapter 11. Migrating to, or updating Symantec Mobile Security 7.2
- Chapter 12. Managing Updates
- Chapter 13. Monitoring and reporting
- Chapter 14. Database maintenance
This chapter includes the following topics:

- Licensing basics
- Using the trial license
- Using a license purchased before installing Symantec Mobile Security
- Adding or updating a Symantec Mobile Security license
- Licensing alerts and reports

**Licensing basics**

For use beyond the trial license period, Symantec Mobile Security requires a paid license. You purchase a license based on the number of mobile devices that are managed by your installation of Symantec Mobile Security. You purchase licenses from your Symantec Sales Partner or sales representative.

---

**Note:** “Mobile devices” or “devices” refers to both physical and emulated forms of the mobile devices that run any of the supported operating systems. The terms of the license apply equally regardless of form or operating system.

Each managed device comprises a single licensing node within the product license. When you purchase a license, you purchase licensing for a specific number of nodes. For instance, to manage 500 devices, you purchase a 500-node license. You purchase licenses from your Symantec Sales Partner or sales representative. For more information about licensing Symantec products, go to [http://www.symantec.com/products/licensing/](http://www.symantec.com/products/licensing/).
Using the trial license

When you install Symantec Mobile Security, you are prompted to install a license. If you have not purchased a license, you skip this step and the trial license is invoked automatically. The trial license is for 25 nodes and expires 30 days after the initial installation of Symantec Mobile Security. The License Report shows the status of your trial license and the number of enrolled devices. Each enrolled device uses one node of the license regardless of form or operating system. For more information, see Licensing alerts and reports.

Using a license purchased before installing Symantec Mobile Security

If you purchased a license before installing the product, you install the license during the installation procedure. The installer prompts you to provide a license file and then proceed with the installation. The license file is sent to you by email when you complete your license purchase.

Note: The license file must be accessible from the computer that hosts the installation of Symantec Mobile Security.

After installation, the License Report and License Overview reflect the paid license, its expiry date, and the number of available license nodes.

See Licensing alerts and reports

Adding or updating a Symantec Mobile Security license

Use the following procedure to add a license after Symantec Mobile Security is already installed, to upgrade from the Trial license or extend an existing paid license, or to add more nodes to an existing license:

Note: The license file must be accessible from the computer that hosts the installation of Symantec Mobile Security.
Adding a license after installing Symantec Mobile Security

1. Open Symantec Installation Manager

   **Note:** Symantec Installation Manager is installed with Symantec Management Platform.

2. Click **Add/Update License**, and then provide the required information.

3. When prompted to install the license, click **Yes**.

# Licensing alerts and reports

The Licensing Report provides details about the number of licensed nodes used, the status of licenses, and license timeframe information. You use this screen to also save and print the reports.

**Note:** In the Licensing overview and reports, licensed nodes are implied by the term, “licenses”.

Alerts can be set to warn you of impending license expiration and when you are about to run out of licenses. Alerts appear in the console and can also be sent by email to the person that is responsible for license administration.

Table 10-1 provides additional details about licensing reports and alerts.

<table>
<thead>
<tr>
<th>Table 10-1 Licensing alerts and reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource</strong></td>
</tr>
<tr>
<td>Licensing Report and License Summary</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Table 10-1  Licensing alerts and reports  (continued)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Overview</td>
<td>On the console, go to <strong>Home &gt; Mobile Security &gt; Overview and Reports &gt; License Overview</strong>&lt;br&gt;The overview displays the same information as the Licensing Report and Licensing Summary, except all on one page.</td>
</tr>
<tr>
<td>Licensing Alerts</td>
<td>You configure the license alerts on the <strong>Home &gt; Mobile Security &gt; Settings &gt; Management Server Settings</strong> page. You can configure:&lt;br&gt;  ■ The threshold for warning about available remaining licenses&lt;br&gt;  ■ The threshold for warning about an impending license expiration&lt;br&gt;  ■ Whether to send email for either threshold condition&lt;br&gt;See Management Server Options for more information</td>
</tr>
</tbody>
</table>
Migrating to, or updating Symantec Mobile Security 7.2

This chapter includes the following topics:

- Migration and upgrade overview
- Migrating Symantec Management Platform and Symantec Mobile Security together

Migration and upgrade overview

Symantec Mobile Security 7.2 installs on and integrates with Symantec Management Platform 7.1 SP2. If you have Symantec Management Platform 7.1 SP2 already installed, you run Symantec Installation Manager to upgrade to Symantec Mobile Security 7.2. If you are currently running an earlier version of Symantec Management Platform, you must first migrate to the 7.1 SP2 version.

See “Migrating Symantec Management Platform and Symantec Mobile Security together” on page 84.

If you must migrate Symantec Management Platform to the 7.1 SP2 version, review the Symantec Knowledge Base article, Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 at http://www.symantec.com/docs/HOWTO54438.

After the upgrade or migration, you may need to perform one or more of the following tasks:

- After the migration or the upgrade process completes, device owners should download and install the new version of the Agent app on their devices.
See “About distributing the Agent app to device owners” on page 21.

- Windows Mobile devices that are enrolled with an earlier version of Symantec Mobile Security may require an updated policy that points to the new Mobile Security server.

- Android devices are supported in Symantec Mobile Security 7.2, and device owners receive a default Android security policy upon enrollment. You can configure the default Android security policy to meet the security requirements that are most often applied to Android devices in your environment. See “Configuring the default Android security policy” on page 43.

## Migrating Symantec Management Platform and Symantec Mobile Security together

Symantec Mobile Security 7.2 installs on the 7.1 SP2 version of Symantec Management Platform. To update to Symantec Mobile Security 7.2, installations currently running an older version of Symantec Management Platform must migrate to Symantec Management Platform 7.1 SP2. You can perform the platform migration and security solution upgrade at the same time.

Before you begin, make sure that the system that hosts Symantec Management Platform 7.1 SP2 and Symantec Mobile Security 7.2 meet the necessary requirements. You also use steps from the Symantec Knowledge Base article *Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1* at [http://www.symantec.com/docs/HOWTO54438](http://www.symantec.com/docs/HOWTO54438)

See “Server requirements” on page 99.

To migrate Symantec Management Platform and Symantec Mobile Security together, you perform the following three procedures in order:

- Migrating Symantec Management Platform and Symantec Mobile Security
- Rolling out the Gateway server after migration
- Changing the default Android policy

**Note:** In the procedures that follow, “Server A” is the old instance of Symantec Management Platform 7.0 with Mobile Security 7.0. “Server B” is the new instance of Symantec Management Platform 7.1 SP2 with Symantec Mobile Security 7.2.
Migrating Symantec Management Platform and Symantec Mobile Security

1. Prepare Server B according to the instructions in Symantec Knowledge Base article, HOWTO54438.

2. Back up the CMDB for Symantec Management Platform 7.0 on Server A. See Symantec Knowledge Base article, HOWTO54438 for instructions.

3. Restore the CMDB for the Server B instance. See Symantec Knowledge Base article, HOWTO54438 for instructions.

4. On Server B, run Symantec Installation Manager (Start > All Programs > Symantec > Symantec Installation Manager) and select the following components:
   - Symantec Mobile Security 7.2
   - The restored CMDB
   - Migration Components

5. Start the installation and allow it to complete. This part of the process can take a considerable amount of time.


   **Note:** Select the "non-silent" version of the file that is appropriate for the operating system on Server A.

7. Copy the NSUpgradeWizard.exe file to a convenient location on Server A and then run the wizard. The wizard creates a .ADB file you use to rebuild the installation on the new server.

8. Copy the .ADB file you created in the previous step to a convenient location on Server B.

9. On server B, go to [Altiris install path]/Upgrade and run the non-silent x-64 version of the Migration Wizard. Select the option to migrate Mobile Security data.

   **Note:** If there are no File Access Log files present on Server A, then the option to migrate Mobile Security data is not displayed.
10 Follow the instructions in the wizard to complete the migration.

11 After migrating, check the device reports to verify that the device data is correct.

See “About mobile security reports” on page 93.

A side effect of migration is that the CMDB contains some references that make Server A appear as a Task server. During the installation of Symantec Mobile Security 7.2 on Server B, an attempt is made to use Server A to roll out the Gateway server. The attempt fails because Server A is not able to execute tasks. Use the following procedure to correct this situation:

**Rolling out the Gateway server after migration**

1 On the Server B Symantec Management Platform console, go to **Settings tab > Site Management > Site Servers** and select Server A. In the right pane, turn off the **Task Service**.

2 On Server B, in the task tray, right-click the Symantec Management Agent icon and select **Symantec Management Agent**.

3 On the **Symantec Management Agent > Task Status** tab, click **Reset Agent**.

4 On Server B, in the Symantec Management Platform console, go to **Home > Symantec Mobile Security > Settings > Mobile Security Gateway**.

5 In the right pane, select Server B and then click **Save changes**.

**Note:** Highlight the new Gateway and click the Verify icon to verify that the Gateway server communicates with the Mobile Security server.


**Changing the Default Android security policy**

1 On the Server B console, go to **Home > Symantec Mobile Security > Device Management > Default Android Security Policy**.

2 In the right pane, on the **Communications** tab under **Server Communications**, select the new Mobile security gateway from the drop-down list.

3 Click **Save changes**.

See “Configuring the default Android security policy” on page 43.
Managing Updates

This chapter includes the following topics:

- About updating devices
- Repackaging LiveUpdate content
- LiveUpdate Repackager command-line syntax

About updating devices

You update devices in two different ways. You can provide content updates and policy updates.

LiveUpdate is the name of the technology that checks for definitions and software updates to devices. LiveUpdate also applies any available updates that it finds. These updates include threat definitions, product updates, and scan engine updates. You can let users run LiveUpdate on their devices, and you can schedule LiveUpdate to run on the devices at specified times.

You can also configure Windows policies and Android policies that include LiveUpdate settings.
Table 12-1: Update types

<table>
<thead>
<tr>
<th>Update type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content updates</td>
<td>Provided by LiveUpdate. You can update content in any of the following ways:</td>
</tr>
<tr>
<td></td>
<td>■ Devices can connect to the Symantec LiveUpdate server.</td>
</tr>
<tr>
<td></td>
<td>■ You can set up an internal LiveUpdate server.</td>
</tr>
<tr>
<td></td>
<td>■ You can download and repackage content updates from the Symantec LiveUpdate server. You decide how and when to distribute the repackaged content to your organization’s devices. See “Repackaging LiveUpdate content” on page 88.</td>
</tr>
<tr>
<td>Policy updates</td>
<td>Provided by applying security policies to the device.</td>
</tr>
<tr>
<td></td>
<td>You use Symantec Mobile Security or a third-party device management system to apply security policies. These policies include a LiveUpdate Policy that configures the settings for content updates. See “Configuring a new Android security policy” on page 48. See “Creating and applying Windows Mobile security policies” on page 60.</td>
</tr>
</tbody>
</table>

Repackaging LiveUpdate content

Symantec Mobile Security provides the LiveUpdate Repackager command-line tool for updating devices manually according to the schedule that you require. LiveUpdate Repackager lets you control the specific content and the schedule of updates. You can package threat definitions updates, protection software updates, or updates to LiveUpdate. Before you run LiveUpdate Repackager, you run LiveUpdate Administrator to obtain the latest updates.

**Note:** To simplify this procedure, place all your tools in the same folder. LiveUpdate Administrator and the LiveUpdate Repackager place their output in this folder by default. You can change the input folder and the output folder if needed, however.

1. Run LiveUpdate Administrator to obtain the latest updates from Symantec.
2. Navigate to the folder that contains the LiveUpdate Repackager executable file, lur.exe.
3. Open a command window, and type the command string to create the update package that you require.

   See “LiveUpdate Repackager command-line syntax” on page 89.

   ■ If updates are found, output similar to the following appears:

     Found update for av_pocketpc, english, target version 4.1.0
     Created package C:\updates\symupdates_ppc.zip
     This file can now be copied to \Symantec Data\Updates on Pocket PC devices.

   ■ If no update is found for a product, no output file is created and a message appears stating that no updates were found.

   ■ If there is an error, no output files are created and no message appears.

4. Use a third-party device management system or any TCP/IP-based network connection to place the symupdates_ppc.zip file on the devices in the following location:

   \Program Files\Symantec\AntiVirus\Symantec Data\Updates

   The updates are automatically detected and applied.

---

**LiveUpdate Repackager command-line syntax**

LiveUpdate Repackager command-line syntax is as follows:

lur [/in file input directory] [/out_pocketpc Pocket PC file output directory] /product {av_pocketpc | av_defs_pocketpc | wlu_pocketpc | fw_pocketpc | fw_smartphone | ma_pocketpc | ma_smartphone | nc_pocketpc | nc_smartphone}... language version_number

---

*Note:* Command-line options are not case sensitive.

The command that you type does not include line breaks.
### Table 12-2  
LiveUpdate Repackager command-line arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/in input directory</td>
<td>The location for the update package that you create by running LiveUpdate Administrator. Optional. The default location is the current folder for LiveUpdate Repackager. Syntax: a mapped drive or UNC. The location must already exist.</td>
</tr>
<tr>
<td>/out_pocketpc output directory</td>
<td>The location for the update package that you create by running LiveUpdate Repackager. Optional The default location is the current folder for LiveUpdate Repackager. Syntax: a mapped drive or UNC. The location must already exist.</td>
</tr>
</tbody>
</table>
### Table 12-2  LiveUpdate Repackager command-line arguments (continued)

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| `/product product_name language version_number` | The details of the products that the content package contains. All arguments are required. `product_name` is repeatable. Specify one or more of the following `product_name` arguments: 
- `av_pocketpc` (Antivirus for all Windows Mobile devices) 
- `av_defs_pocketpc` (Virus definitions for all Windows Mobile devices) 
- `wlu_pocketpc` (LiveUpdate Wireless for all Windows Mobile devices) 
- `fw_pocketpc` (Firewall for Pocket PC/Windows Mobile Professional/Windows Mobile Classic devices) 
- `fw_smartphone` (Firewall for Smartphone/Windows Mobile Standard devices) 
- `ma_pocketpc` (Mobile Security Agent for Pocket PC/Windows Mobile Professional/Windows Mobile Classic devices) 
- `ma_smartphone` (Mobile Security Agent for Smartphone/Windows Mobile Standard devices) 
- `nc_pocketpc` (Network Access Control for Pocket PC/Windows Mobile Professional/Windows Mobile Classic devices) 
- `nc_smartphone` (Network Access Control for Smartphone/Windows Mobile Standard devices) |
|  | `language` is the target language for the update. Specify one `language` argument for each `product_name` argument. The language value is found in the `<tri_file_name>` tag for the related package in the livetri.zip file. This file is produced by LiveUpdate Administrator. |
|  | `version_number` is the two-digit version number of the product that is installed on the devices, not the version of the product to update to. Specify one `version_number` for each `product_name` argument. |
| Caution: | If you include multiple versions of a product in a single update file, make sure that the appropriate target versions are available. You cannot skip versions when you update. |
| `/? /h` | Displays Help. |

See “Repackaging LiveUpdate content” on page 88.
Managing Updates

LiveUpdate Repackager command-line syntax
Monitoring and reporting

This chapter includes the following topics:

- About monitoring device security in Symantec Management Platform
- About mobile security reports
- About Windows Mobile event logging
- About setting up notifications and alerts for mobile security

About monitoring device security in Symantec Management Platform

You can monitor the security of your organization’s devices in the following ways:

- View reports
  See “About mobile security reports” on page 93.
- View logs
  See “About Windows Mobile event logging” on page 95.
- Set up notifications
  See “About setting up notifications and alerts for mobile security” on page 96.

About mobile security reports

Symantec Mobile Security provides several reports and situational overviews to help you quickly assess the state of your environment, manage threats, and troubleshoot problems. To view the main Overview and Reports page, on the console go to Home > Mobile Security > Overview and Reports.

The report pages allow you to filter the results, export and print reports, and depending on the report, perform security related actions on selected devices.
Symantec Mobile Security Solution includes several reports that let you view the security status of devices in your organization. You can create your own reports, if none of the predefined reports meets your needs. For detailed information, see Symantec Management Platform User’s Guide, chapter 20, "Using Reports." Or search for reports in the platform Help.

The mobile security solution includes the following reports:

**Table 13-1**

<table>
<thead>
<tr>
<th>Report name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Overview</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; Threat Overview&lt;br&gt;Provides an at-a-glance view of your current threat posture.</td>
</tr>
<tr>
<td>License Overview</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; License Overview&lt;br&gt;Provides an at-a-glance view of your current licensing status.</td>
</tr>
<tr>
<td>Device Overview</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; Device Overview&lt;br&gt;Provides an at-a-glance view of Android device compliance, recent actions, and enrollment status.</td>
</tr>
<tr>
<td>At-Risk Devices Details</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; At-Risk Devices Details&lt;br&gt;Provides the details about the at-risk devices and the risk conditions present on each device.</td>
</tr>
<tr>
<td>Device Compliance</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; Device Compliance&lt;br&gt;Provides details about the devices that are not compliant with Symantec Mobile Security</td>
</tr>
<tr>
<td>Web Protection Events</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; Web Protection Events&lt;br&gt;Provides details about the devices that have encountered Web Protection incidents.</td>
</tr>
<tr>
<td>All other reports . . .</td>
<td>Home &gt; Mobile Security &gt; Overview and Reports &gt; All other reports . . .&lt;br&gt;Opens the report browser in the left pane of the console. You access the Windows Mobile device reports from this view.</td>
</tr>
</tbody>
</table>
Table 13-1  (continued)

<table>
<thead>
<tr>
<th>Report name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Device Information (Windows)**                | Home > Mobile Security > Overview and Reports > All other reports . . . > Windows > Device Information  
 Provides details about each Windows Mobile device |
| **Highest Severity Events (Windows)**           | Home > Mobile Security > Overview and Reports > All other reports . . . > Windows > Highest Severity Events  
 Reports the events with the highest severity |
| **Infected Status Summary (Windows)**           | Home > Mobile Security > Overview and Reports > All other reports . . . > Windows > Infected Status Summary  
 Provides a summary of the infection rates among the managed Windows Mobile devices. |
| **Linked and Unlinked Mobile Devices (Windows)** | Home > Mobile Security > Overview and Reports > All other reports . . . > Windows > Linked and Unlinked Mobile Devices  
 Reports all devices that have communicated with Notification Server within the time specified |
| **Mobile Security Status Dashboard (Windows)**  | Home > Mobile Security > Overview and Reports > All other reports . . . > Windows > Mobile Security Status Dashboard  
 Reports the security-related health of all client devices in your organization |

Several other reports are available for Android and Windows Mobile devices in the **All other reports** . . . view.

See “About monitoring device security in Symantec Management Platform” on page 93.

**About Windows Mobile event logging**

A history of security-related events is maintained on the Windows Mobile devices in the Activity Log. Firewall events on Windows Mobile devices are displayed in different views of the event log.

You manage event logging by creating a device log policy that lets you control the following settings:

- How often the logs on the device are uploaded to the server
- The definitions of a critical event. If a critical event occurs, the logs are uploaded to the server immediately.
You can view event logs in Symantec Management Platform, or you can upload them from the devices in XML format. You can then view the logs by using any tool that lets you view XML content.

On the Windows Mobile devices, the event logs are placed in \Program Files\Symantec\Antivirus\Symantec Data\Log\symlog.xml.

The Activity Log provides information about antivirus and LiveUpdate events on all devices.

Activity Log events:
- Scans that were started, stopped, or aborted
- Configuration changes
- Threats that were found and the actions that were taken on them
- LiveUpdate events

The event log on Windows Mobile devices contains Event Summary, Event List, and Event Detail views. These views provide information about firewall-related events on Windows Mobile devices.

### About setting up notifications and alerts for mobile security

You can set up notifications and alerts to inform you when a security event occurs on an enrolled mobile device. You can also set up notifications to email reports according to the criteria that you specify. You set up notifications and alerts on the **Home > Mobile Security > Settings > Management Server Settings** page of the console.

See “Configuring the Symantec Mobile Security server” on page 25.
Database maintenance

This chapter includes the following topics:

- Purging Android mobile device data from the database

Purging Android mobile device data from the database

Over time, the Android device activity records accumulate in the Symantec Mobile Security database. You can purge the device data to improve the database performance. Purging the Android database information is enabled by default and the purge is performed weekly.

Note: Your organization may have data-retention polices that affect how you use this feature.

You can enable, disable, and set the schedule for purging Android database records for device logs, events, and actions. You can also purge the devices that have been inactive or unenrolled beyond a chosen length of time.

Go to Home > Mobile Security > Settings > Android Purge Schedule to set the purge options. The settings are self-explanatory.

To immediately purge Android records that meet the purge settings, click Purge Now.
Database maintenance

Purging Android mobile device data from the database
Symantec Mobile Security
7.2 System Requirements and Port Usage

This appendix includes the following topics:

- Server requirements
- Mobile device requirements
- Port Usage

Server requirements

Symantec Mobile Security installs as a part of Symantec Management Platform 7.1 SP2 (formally known as Altiris ITMS). The system runs on Windows Server 2008 (x64). The following table lists the additional requirements for Symantec Mobile Security.

Note: A complete set of requirements for Symantec Management Platform is available in the Management Platform documentation.

<table>
<thead>
<tr>
<th>Table A-1</th>
<th>Server requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Minimum Requirement</td>
</tr>
<tr>
<td>Processor</td>
<td>Pentium 4- x64, 1.8GHz. Faster is recommended for larger systems.</td>
</tr>
</tbody>
</table>
### Table A-1 Server requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>4 GB. More is recommended for larger systems</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>5 GB available space</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows Server 2008 x64 R2</td>
</tr>
<tr>
<td>Management System</td>
<td>Symantec Management Platform 7.1 SP2</td>
</tr>
<tr>
<td>Database</td>
<td>Microsoft SQL Server 2005 (SP2/SP3/SP4) or Microsoft SQL Server 2008 (SP1/SP2/R2/R2,SP1)</td>
</tr>
</tbody>
</table>

**Note:** SQL Server Express is included for testing and for installations serving less than 500 devices.

| Miscellaneous | ■ Microsoft .NET Framework 3.5  
■ Microsoft Silverlight 3.x, 4.x, 5  
■ Microsoft IIS 7.5 (IIS 6.0 compatibility)  
■ Internet Explorer 7,8, or 9  
■ JRE 6 or higher |

---

### Mobile device requirements

The Symantec Mobile Security Agent runs in the following mobile platforms:

- Android 2.x, 3.x, 4.x
- Windows Mobile 6.0 / 6.1 / 6.5 Professional and Standard
- Windows Mobile 5.0 Pocket PC and Phone Edition

### Port Usage

The following table provides the port usage information for Symantec Mobile Security:
<table>
<thead>
<tr>
<th>Traffic</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway &gt; Symantec Management Platform (SMP)</td>
<td>SMP: 80, 443 inbound</td>
</tr>
<tr>
<td>SMP &gt; Gateway</td>
<td>SMP: 50120-50124 outbound</td>
</tr>
<tr>
<td>SMP &gt; SQL</td>
<td>SMP: standard SQL ports</td>
</tr>
<tr>
<td>SMP &gt; Active Directory / LDAP</td>
<td>SMP: standard LDAP ports</td>
</tr>
<tr>
<td>Android device &gt; Gateway</td>
<td>Gateway: 80, 443 inbound</td>
</tr>
<tr>
<td>Console &gt; SMP</td>
<td>SMP: 80, 443 inbound</td>
</tr>
<tr>
<td>SMP &gt; Google Cloud Messaging (GCM)</td>
<td>SMP: 80 outbound</td>
</tr>
<tr>
<td>Android device &gt; GCM</td>
<td>Android: 5228, 5229, 5230 outbound</td>
</tr>
<tr>
<td>Windows Mobile device &gt; SMP</td>
<td>SMP: 80 inbound (by default; port is configurable)</td>
</tr>
<tr>
<td>Reverse proxy &gt; SMP (Android traffic)</td>
<td>SMP 80, 443 inbound</td>
</tr>
<tr>
<td>Reverse proxy &gt; SMP (Windows traffic)</td>
<td>SMP: 80 inbound</td>
</tr>
<tr>
<td>Android device &gt; Reverse proxy</td>
<td>Reverse proxy: 80, 443 inbound</td>
</tr>
<tr>
<td>Windows Mobile device &gt; Reverse proxy</td>
<td>Reverse proxy: 80 inbound (by default; port is configurable)</td>
</tr>
</tbody>
</table>

See “Mobile Security implementation architectures” on page 103.
Port Usage
This appendix includes the following topics:

- Mobile Security implementation architectures
- Single-box implementation
- Typical implementation
- Reverse proxy implementation

**Mobile Security implementation architectures**

The flexibility of Symantec Mobile Security and the Symantec Management Platform let you optimize the installation architecture for best performance. You can add additional Gateway servers, include a reverse-proxy to add security, and connect to existing resources such as SQL and Active Directory. The diagrams in this appendix depict three common implementation architectures that you can use to help you design your installation of Symantec Mobile Security.

*Note:* These diagrams apply to Symantec Mobile Security 7.2 MR1 and later.
Single-box implementation

This architecture is established when you first install Symantec Mobile Security. By default, a Gateway server is installed on the same computer as the Symantec Management Platform. You can add additional Gateways as needed. You can also add a computer in the DMZ to serve as a reverse proxy for additional security. See the Reverse proxy architecture diagram for reverse proxy port assignments.
The typical implementation of Mobile Security places the Gateway server in the DMZ. The Gateway serves to isolate the Management Platform from Android traffic that may carry malware that is intended to circumvent network security.
Reverse proxy implementation

A computer in the DMZ is configured as a reverse proxy to pass inbound traffic from the mobile devices, providing an extra layer of security.
Third-party Attributions

This appendix includes the following topics:

- Third-Party Legal Notices
- Bouncy Castle Crypto C#
- Iquery
- Log4Net

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.

Third-party components included in Symantec Mobile Security include:

Bouncy Castle Crypto C#

Copyright (c) 2000 - 2011 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

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.

**Iquery**

Copyright (c) 2011 John Resig, http://jquery.com/

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.

**Log4Net**

Copyright © 2004-2011 Apache Software Foundation. You may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES
OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Apache log4net, Apache, log4net, the Apache feather logo, the Apache Logging Services project logo and the Built by Maven logo are trademarks of The Apache Software Foundation.


TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by

Third-party Attributions

Log4Net
the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part...
of the Derivative Works, in at least one of the following places: within a NOTICE
text file distributed as part of the Derivative Works; within the Source form or
documentation, if provided along with the Derivative Works; or, within a display
generated by the Derivative Works, if and wherever such third-party notices
normally appear. The contents of the NOTICE file are for informational purposes
only and do not modify the License. You may add Your own attribution notices
within Derivative Works that You distribute, alongside or as an addendum to the
NOTICE text from the Work, provided that such additional attribution notices
cannot be construed as modifying the License. You may add Your own copyright
statement to Your modifications and may provide additional or different license
terms and conditions for use, reproduction, or distribution of Your modifications,
or for any such Derivative Works as a whole, provided Your use, reproduction,
and distribution of the Work otherwise complies with the conditions stated in
this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any
Contribution intentionally submitted for inclusion in the Work by You to the
Licensor shall be under the terms and conditions of this License, without any
additional terms or conditions. Notwithstanding the above, nothing herein shall
supersede or modify the terms of any separate license agreement you may have
executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names,
trademarks, service marks, or product names of the Licensor, except as required
for reasonable and customary use in describing the origin of the Work and
reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in
writing, Licensor provides the Work (and each Contributor provides its
Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS
OF ANY KIND, either express or implied, including, without limitation, any
warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY,
or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for
determining the appropriateness of using or redistributing the Work and assume
any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort
(including negligence), contract, or otherwise, unless required by applicable law
(such as deliberate and grossly negligent acts) or agreed to in writing, shall any
Contributor be liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a result of this
License or out of the use or inability to use the Work (including but not limited to
damages for loss of goodwill, work stoppage, computer failure or malfunction, or
any and all other commercial damages or losses), even if such Contributor has
been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS
accessing the Management Console 19
Activity Log 95
Agent app
distributing Android 22
distributing Windows Mobile 22
alarm
triggering on Android device 42
Alerts
about 96
Android
assigning policy to 50
checking at-risk devices 49
checking device compliance 48
configuring default security policy 43
configuring new security policy 48
device, locating lost or stolen 39
device, locking lost or stolen 40
device, triggering alarm on 42
devices, checking Web security events 49
devices, push security scan command to 51
reports
At-Risk Devices 93
Device Compliance 93
Device Overview 93
Web Protection Events 93
security and device details 93
security, common tasks 39
verifying device enrollment 52
wiping data from 41
Antivirus protection
Auto-Protect 61
managing 61
assigning
policy to Android device or group of devices 50
Auto-Protect
about 61
actions 63
settings 63
See also Antivirus protection
Client Software License Details Report 93
compliance
checking device 48
configuring
Active Directory for enrolling mobile devices 33
alerts and notifications 96
Android enrollment and management settings 53
default Android security policy 43
Gateway server 28
Mobile Security server 25
new Android security policy 48
policy
Windows Mobile File Access Log 70
console
opening 19
securing 33
using, navigating 15
Critical events
about 95
Custom firewall level 64
device
Android, verifying enrollment 52
assigning Android policy to 50
checking compliance 48
locating lost or stolen 39
locking lost or stolen 40
lost or stolen
triggering alarm on 42
lost or stolen Android
wiping data from 41
device protection
monitoring 93
devices
identifying at-risk 49
scanning or updating 51
distributing
Android Agent app 22
Windows Mobile Agent app 22
E
enrollment
verifying Android device 52
Event log
about 95
Excluding files from scans 62

F
File Access Log
decrypting 72
how to read 74
retrieving 71
File exclusions 62
Firewall protection
Custom protection level 64
High protection level 65
Low protection level 68
managing 63
Medium protection level 67

G
Gateway server
configuring 28
group
assigning Android policy to 50

H
High firewall level 65
Highest Severity Events Report 93

I
identifying at-risk devices 49

L
License
status
report 93
License Overview report 93
Licensed Clients Count Report 93
Linked and Unlinked Mobile Devices Report 93
LiveUpdate Administrator 88
LiveUpdate Repackager
command-line options 89
using 88
locating
a lost or stolen device 39
locking
a lost or stolen device 40
Logging
about 95
Lost device
managing 71
See also File Access Log
lost device
locking 40
triggering alarm on 42
wiping data from 41
lost or stolen device
locating 39
Low firewall level 68

M
Management Console
opening 19
Medium firewall level 67
Migrating
overview 83
Symantec Management Platform and Symantec Mobile Security together 84
Mobile Security server
configuring 25
Mobile Security Status Dashboard Report 93
monitoring
device compliance 48

N
Notifications
about 96

O
options
Android policy
app control 43
communications 43
LiveUpdate 43
security 43

P
patches 87
policies
Windows Mobile
creating and applying 60
policy
  Android
    app control options 43
    communications options 43
    LiveUpdate options 43
    security options 43
  assigning to Android device or group of devices 50
  configuring
    Windows Mobile File Access Log 70
  updates 87

R
Report
  Highest Severity Events 93
  Licensed Clients Count 93
  Linked and Unlinked Mobile Devices 93
  Mobile Security Status Dashboard 93

Reports
  about 93
  all other 93
  Android 93
  Android security and device details 93
  At-Risk Devices 49
  Device Compliance 48
  Web Protection 49

S
scan
  forcing 51
scanning
  devices 51

Scans
  about 61
  after inserting memory card 68
  after LiveUpdate 68
  after synchronization 68
  automatic 68
    See also Antivirus protection
  excluding files from 62
  updating 87
  Security the management console 33

security
  policy (continued)
    configuring new Android 48
  server
    Gateway
      configuring 28
  software updates 87
  stolen Android device
    wiping data from 41
  stolen device
    locking 40
    triggering alarm on 42
  Symantec Data\Updates directory 88
  Symantec Security Response 87
  symupdates_ppc.zip file 88

T
threat definition file 87
  Threat Overview report 93

U
update
  forcing 51

Updates directory. See Symantec Data\Updates directory
Upgrading
  overview 83
  Symantec Management Platform and Symantec Mobile Security together 84

V
verifying
  Android device enrollment 52

W
Web Protection
  security events report 49
Web security
  checking events 49
wiping data
  from lost or stolen Android device 41