Junos Pulse

Mobile Device Integration Guide

Published: 2010-12-17

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
408-745-2000
www.juniper.net

Junos Pulse Mobile Device Integration Guide

Revision History
2010-10-25—Initial release

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html .

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

List of Tables

About This Guide

Objectives

The *Junos Pulse Mobile Device Integration Guide* describes how to enable network access for mobile devices through an SA Series gateway.

Audience

The *Junos Pulse Mobile Device Integration Guide* is for network administrators who are responsible for setting up and maintaining network access for mobile (handheld) devices through Juniper Networks gateways. Before using the procedures in this guide, be sure you already have configured the access gateway and that you are familiar with how to administer the gateways. This guide refers to the access gateway administration guides.

Document Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.

Related Documentation

Table 2 on page xii describes related Junos Pulse documentation.

Table 2: Junos Pulse Documentation

Title	Description
Junos Pulse Administration Guide	Describes Junos Pulse for Windows endpoints and includes procedures for network administrators who are responsible for setting up and maintaining network access using Junos Pulse client software through Juniper Networks gateways.
Junos Pulse Mobile Security Gateway Administration Guide	Describes the Pulse Mobile Security Suite and includes procedures for network administrators who are responsible for setting up and managing security on mobile devices.
SA Series SSL VPN Appliances Administration Guide	Describes how to configure and maintain a Juniper Networks SA Series Appliance.

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To order a documentation CD, which contains this guide, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the documentation CDs and at http://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

PART 1

Junos Pulse for Mobile Devices

CHAPTER 1

Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite

Overview

Junos Pulse for mobile devices enables authenticated access from mobile (handheld) devices to corporate applications such as corporate e-mail and the corporate intranet through an SA Series Appliance. The Pulse client software for mobile devices includes remote VPN capabilities as well as device security capabilities activated by the Junos Pulse Mobile Security Suite.

The Junos Pulse Mobile Security Suite provides antivirus, antispam, and personal firewall services and enables an administrator to monitor and remove device applications and content, perform backup and restore operations, activate remote lock and remote wipe operations, and track devices using GPS. Each supported mobile device supports a specific list of Pulse Mobile Security Suite features.

Each supported mobile device requires that the user install the Pulse VPN client software for the particular device type. The Pulse mobile device software is available as a free download from the app stores of the supported mobile devices. Pulse for mobile devices and Pulse Mobile Security software cannot be deployed directly from an SA Series Appliance. The type of secure connectivity and the supported security features vary according to what is supported on each mobile operating system.

NOTE: For all devices, you should already have your authentication server configured and user accounts created for mobile device users.

Pulse is supported on the following mobile devices:

- Junos Pulse for Apple® iOS
- Junos Pulse for Google Android™
- Junos Pulse for BlackBerry

NOTE: The BlackBerry client does not support VPN connectivity to an SA Series Appliance.

Table 3 on page 18 lists the mobile device OS versions supported by Pulse and the security features supported on each mobile device OS.

Junos Pulse Mobile Security Gateway

Although you enable network access for Pulse on mobile devices using the SA admin console, you manage the security features of the mobile devices by using the Junos Pulse Mobile Security Gateway. The administration interface of the Pulse Mobile Security Gateway enables you to protect and manage mobile devices. The Pulse Mobile Security Gateway is available as software-as-a-service. For more information, see the *Junos Pulse Mobile Security Gateway Administration Guide*.

CHAPTER 2

Junos Pulse for Apple iOS

Junos Pulse for Apple iOS Overview

Junos Pulse can create an authenticated Layer 3 SSL VPN session between an Apple iOS device (iPhone, iPad, iPod Touch) and an SA Series Appliance. Junos Pulse enables secure connectivity to corporate applications and data based on identity, realm, and role. Junos Pulse is available for download from the iTunes App Store.

SSL VPN access to a Juniper Networks SA Series Appliance requires the following software versions:

- Apple iOS 4.1 or later
- Juniper Networks SA Series Appliance Release 6.4 or later

The Junos Pulse VPN app supports the following features:

- Full Layer 3 tunneling of packets
- UDP/ESP and NCP/SSL modes
- All types of authentication, including client certificate authentication
- Split tunneling modes:
  - Split tunneling disabled with access to local subnet
  - Split tunneling enabled
- Apple VPN on Demand

A VPN on Demand configuration enables an iOS device to automatically initiate a VPN connection when any application running on the phone initiates a connection to a host in a predefined set of hosts. A VPN on Demand connection uses client certificate-based authentication so the user does not have to provide credentials every time a VPN connection is initiated. For details about how to create a VPN on Demand configuration, see the *iPhone OS Enterprise Deployment Guide*, which is available at www.apple.com.

Before You Begin

Before you configure support for Apple iOS devices on your SA Series Appliance, keep in mind the following client software behaviors:

- With Wi-Fi connectivity, Pulse reconnects the VPN tunnel automatically when the user wakes up the device. With 3G connectivity, the VPN reconnects when the user generates network traffic using an application like Safari or Mail.
- Connecting through proxies that require authentication is not supported.
- Static host mapping is not created for the SA/proxy hostname.
- DNS considerations:
  - When split tunneling is set to Split tunneling disabled with access to local subnet, Pulse uses the DNS servers that are configured through the SA Series Appliance.
  - When split tunneling is set to Split tunneling enabled, DNS servers that are configured through the SA Series Appliance are used only for hostnames within SA domains.
- Session scripts are not supported.
- RADIUS accounting is not supported.
- Web-based installation from a Juniper gateway that supports Junos Pulse is not supported.
- Session timeout reminders are not supported.
- When you use client certificate authentication, and the user is enabled to select from among assigned roles, the user is prompted to enter the role name instead of being presented with a list of roles.

Configuring a Role and Realm for Pulse for Apple iOS

To enable SSL/VPN access from an Apple iOS device to an SA Series Appliance, the device user must download, install, and configure the Junos Pulse app, and the SA administrator must configure specific realm and role settings on the SA Series Appliance.

To configure an SA Series Appliance for Apple iOS device access:

1. Log in to the SA Series Appliance admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.

4. In the Access Features section of the New Role page, select the **Network Connect** check box and the **Network Connect** option.

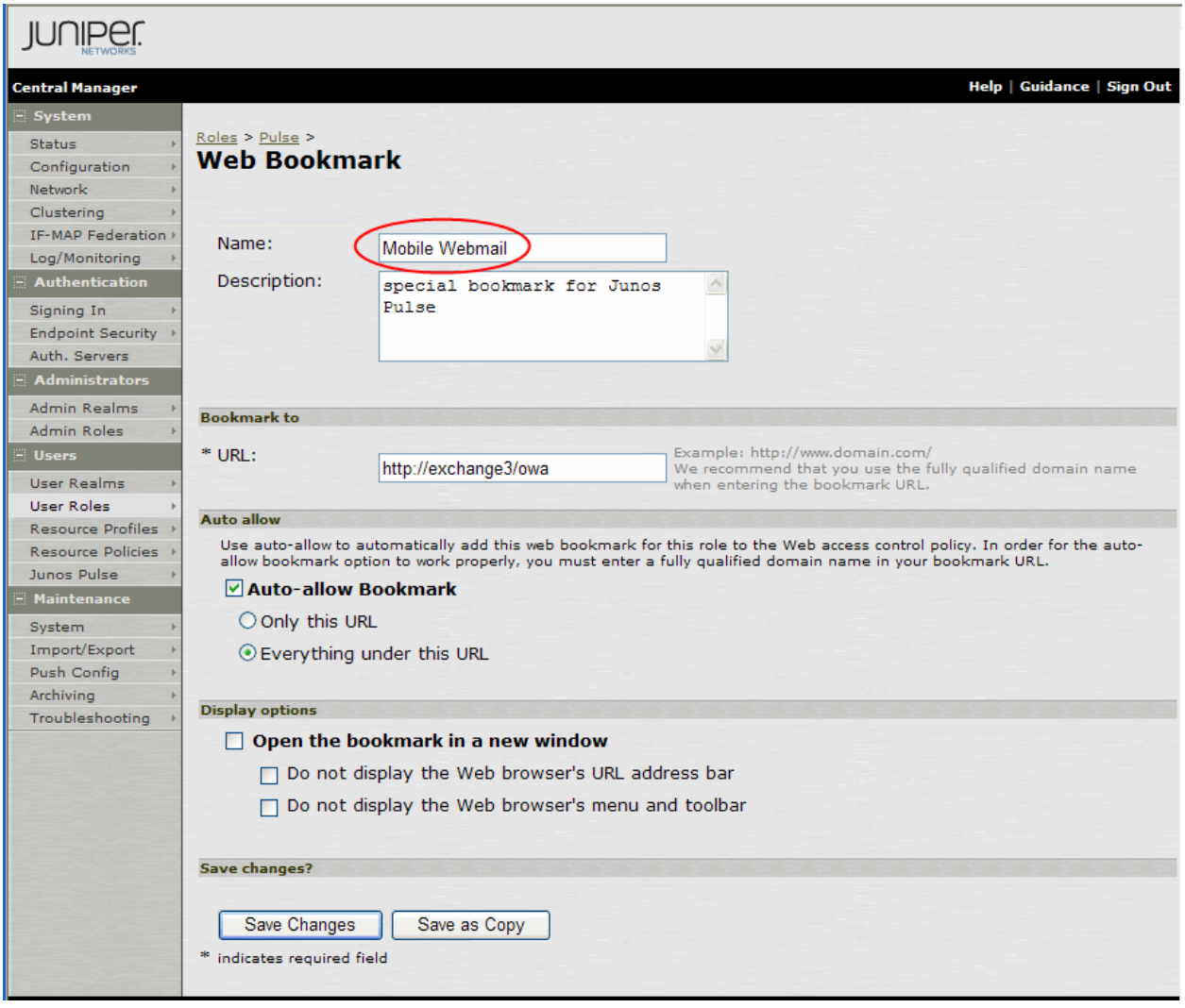
   Although you are configuring access for a Junos Pulse client, you must select the **Network Connect** option.

5. Click **Save Changes** to create the role and to display the role configuration tabs.

6. Select **Web > Bookmarks** and then click **New Bookmark**.

   You must create bookmarks to enable the buttons that appear in the Pulse for Android user interface. Typically, you create a bookmark for your company intranet and for Web e-mail. You must create an e-mail bookmark to enable the e-mail button within the Pulse interface on the Android, and that e-mail bookmark must be named **Mobile Webmail**.

Figure 1: Creating the E-mail Bookmark for the Pulse Client



NOTE: Alternatively, you can use Web resource policies to define the bookmarks. See the *SA Series SSL VPN Administration Guide* for more information on resource policies.

7. To change default session timeouts, select **General > Session Options**.
8. In the Session lifetime section, specify **Max. Session Length** in minutes. The remaining session time appears on the Pulse interface of the mobile device client in the format **days hours:minutes:seconds**. The other session settings are not applied to mobile clients.
9. On the Network Connect tab for the role, be sure that the **Split Tunneling Options** are set correctly and then click **Save Changes**.
10. Select **Users > Resource Policies > Network Connect > NC Connection Profiles**.
11. Click **New Profile**.

    When the SA Series Appliance receives a client request to start a session, it assigns an IP address to the client based on the IP address policies you define. When you define the connection profile, note the following:

    - Proxy Server Settings—Automatically modifying the client proxy configuration when split tunneling is enabled is not supported.
    - DNS Settings—Searching IVE DNS first with split tunneling enabled is not supported. With split tunneling enabled, Junos Pulse uses the IVE DNS for queries for hosts in the IVE DNS search domains only. All other queries go to the client's DNS servers.

12. In the Roles area, select **Policy applies to SELECTED roles**. Then add the role you created for iOS devices to the Selected roles list.
13. Click **Save Changes**.
14. Select **Users > User Realms > New User Realm**.
15. Specify a name and description. Then click **Save Changes** to create the realm and to display the realm option tabs.
16. On the General tab for the realm, select the **Session Migration** check box.
17. On the Authentication Policy tab for the realm, click **Host Checker** and make sure that all Host Checker policies are disabled. iOS devices do not support Host Checker.
18. On the Role Mapping tab for the realm, create a new rule that maps all users to the iOS device role you created earlier in this procedure.

Installing Custom Sign-in Pages

We recommend that you install a set of sign-in pages on your SA Series Appliance that are properly formatted for a mobile device screen. After you install the custom sign-in pages on your SA Series Appliance, you must create a sign-in URL that uses the sign-in pages.

To download and install mobile device sign-in pages:

1. Download the custom sign-in page zip file from juniper.net, and put the file in a location where you can then upload it to the SA Series Appliance.

   Go to http://kb.juniper.net/KB17749. A Juniper Knowledge Base article includes a link to download a custom sign-in pages file, junos_pulse_custom_pages.zip.
2. On the SA Series Appliance admin console, select **Authentication > Signing In > Sign-in Pages**.
3. Click **Upload Custom Pages**.
4. Specify a name that allows you to easily identify this set of pages.
5. For Page Type, select **Access**.
6. Click **Browse**, select the custom sign-in pages file, and then click **Open**.
7. Click **Upload Custom Pages**.

Creating a Custom Sign-in URL

The following procedure describes how to specify the settings that are required for creating a mobile device sign-in policy that includes the URL for user access. For mobile devices, you need a different policy for each type of mobile device that will access the SA Series Appliance. Before you begin, be sure you have installed the custom sign-in pages for the mobile devices. For complete information about sign-in policies, see the *SA Series SSL VPN Appliances Administration Guide*.

1. On the SA Series Appliance admin console, select **Authentication > Signing In > Sign-in Policies**.
2. Click **New URL**.
3. In the **Sign-in URL** box, specify the URL using the format <*host*>/<*path*>. The path can be any string you want. For example, *yourcompany*.com/iphone-connect.
4. In the **Sign-in page** box, select a custom sign-in page you uploaded for device access.
5. In the Authentication realm section, if you select **User picks from a list of authentication realms**, be sure to add to the **Selected realms** list the realm you created for mobile device access.

   NOTE: Make note of the URL. You must communicate this URL to mobile device users so they can create the proper Junos Pulse configuration.
6. Click **Save Changes**.

Installing the Junos Pulse VPN App

Perform the following configuration on each iOS device that is to connect to the SA Series Appliance.

1. Download the Junos Pulse app from the iTunes App Store.
2. On the iOS device, launch Junos Pulse.
3. Tap the Configuration item on the main status page to display Pulse configurations.
4. Create a new configuration with the URL that you defined as the sign-in URL for mobile devices. Then configure the certificate settings as required.

NOTE: When iPhone users launch Pulse for the first time, they see a security warning and a prompt for enabling Pulse SSL VPN functionality. This security precaution helps deter the silent installation of malicious VPN software. If the user declines the Pulse software, the Pulse splash screen appears until the user presses the Home button on the device. If the user accepts the Pulse software, the security warning no longer appears when Pulse is started.

NOTE: For certificate authentication, the SA gateway SSL certificate must be issued by a CA. It cannot be self-signed. If the CA is not one of the built-in trusted CAs on the iOS device, then the CA certificate must be imported into the iOS device. Also, the SA gateway must be accessed using a hostname (not an IP address), and the hostname must match the Common Name of the SA gateway's SSL certificate.

Using Configuration Profiles

Instead of instructing users to create Junos Pulse VPN configurations manually, you can use a Configuration Profile to define Pulse configurations for the iOS device, and then distribute the configuration profiles by e-mail or by posting them on a Web page. When users open the e-mail attachment or download the profile using Safari on their iOS device, they are prompted to begin the installation process.

You use the iPhone Configuration Utility to create configuration profiles and specify Juniper SSL as the Connection Type for the VPN Payload. You can download the iPhone Configuration Utility (3.0 or later) from the Apple support Web. For details about the utility and how to create Configuration Profiles, see the *iPhone OS Enterprise Deployment Guide*, which is available at www.apple.com.

Collecting Log Files

The iOS device user can use the following procedure to e-mail the Pulse log files:

1. On the iOS device, start the Junos Pulse app.
2. Tap **Status**.
3. Tap **Logs > Send Logs**.
4. Enter an e-mail address and tap **Send**.

Launching a Pulse Connection from Another Application

An iOS system allows applications to register custom URL formats to enable one application to launch another application. For example, launch a Junos Pulse connection from a Web page displayed in Mobile Safari.

When you install Pulse, it registers a custom URL format with the following form:

junospulse://<server-host>/<server-path>?method={vpn}&action={start|stop}&DSID=<dsid-cookie>&SMSESSION=<smsession-cookie>

The DSID and SMSESSION parameters are optional.

When the URL is launched by Safari or some other application, the following actions occur:

1. The Pulse application is launched.
2. If a Pulse VPN connection is not already running and the action in the URL is **start**, the following actions occur:

   a. If Pulse does not already have a configuration defined with a URL that matches the host and path specified in the launch URL, the Add Configuration screen appears and the user can define the configuration. If a configuration with the correct URL exists, Pulse attempts to connect using that configuration.

   b. If there are session cookies specified in the launch URL, a new VPN connection is established with the given session cookies.

   c. If there are no session cookies specified in the launch URL, the login window appears and the user must complete the login process.

3. If the specified VPN connection is already established, Pulse uses that connection. If Pulse already has an active connection to a different server, Pulse creates a new connection to the server specified in the command and closes the existing connection. You can only have one active VPN connection at a time.

Example1: To connect to access.myserver.com, use the following URL:

junospulse://access.myserver.com/?method=vpn&action=start

Example2: To connect to access.myserver.com/iphone, use the following URL:

```
junospulse://access.myserver.com/iphone/?method=vpn&action=start
```

Example3: This example shows the URL that you would use to launch Pulse from the SA Web portal page. To connect to access.myserver.com/iphone, and have the connection established without having the user prompted for login credentials, use the following URL:

```
junospulse://access.myserver.com/iphone/?method=vpn&action=start&DSID=<dsid-cookie>
  &<SMSESSION=<smsession-cookie>
```

The following describes the sequence of events in Example3:

- The user launches the Mobile Safari web browser (or any other web browser) on their iOS device and signs in to the SA. The user's home page includes a link that says **VPN** or something similar.
- The user taps on the VPN link, and then code within the Web page constructs a "junospulse" custom URL that includes the user's DSID and possibly their SMSESSION cookie (if they are using Netegrity authentication). The browser uses this URL to launch Junos Pulse and establishes the VPN connection without prompting the user for login credentials.

CHAPTER 3

Junos Pulse for Google Android

Junos Pulse for Android Overview

Junos Pulse can create an authenticated SSL session between a device running Google Android and an SA Series Appliance. Junos Pulse enables secure connectivity to Web-based applications and data based on identity, realm, and role. Junos Pulse is available for download from the Android Market. Table 3 on page 18 lists the mobile device OS versions supported by Pulse. Android device access is supported by SA Series Release 6.5 and later.

Configuring a Role and Realm for Pulse for Android

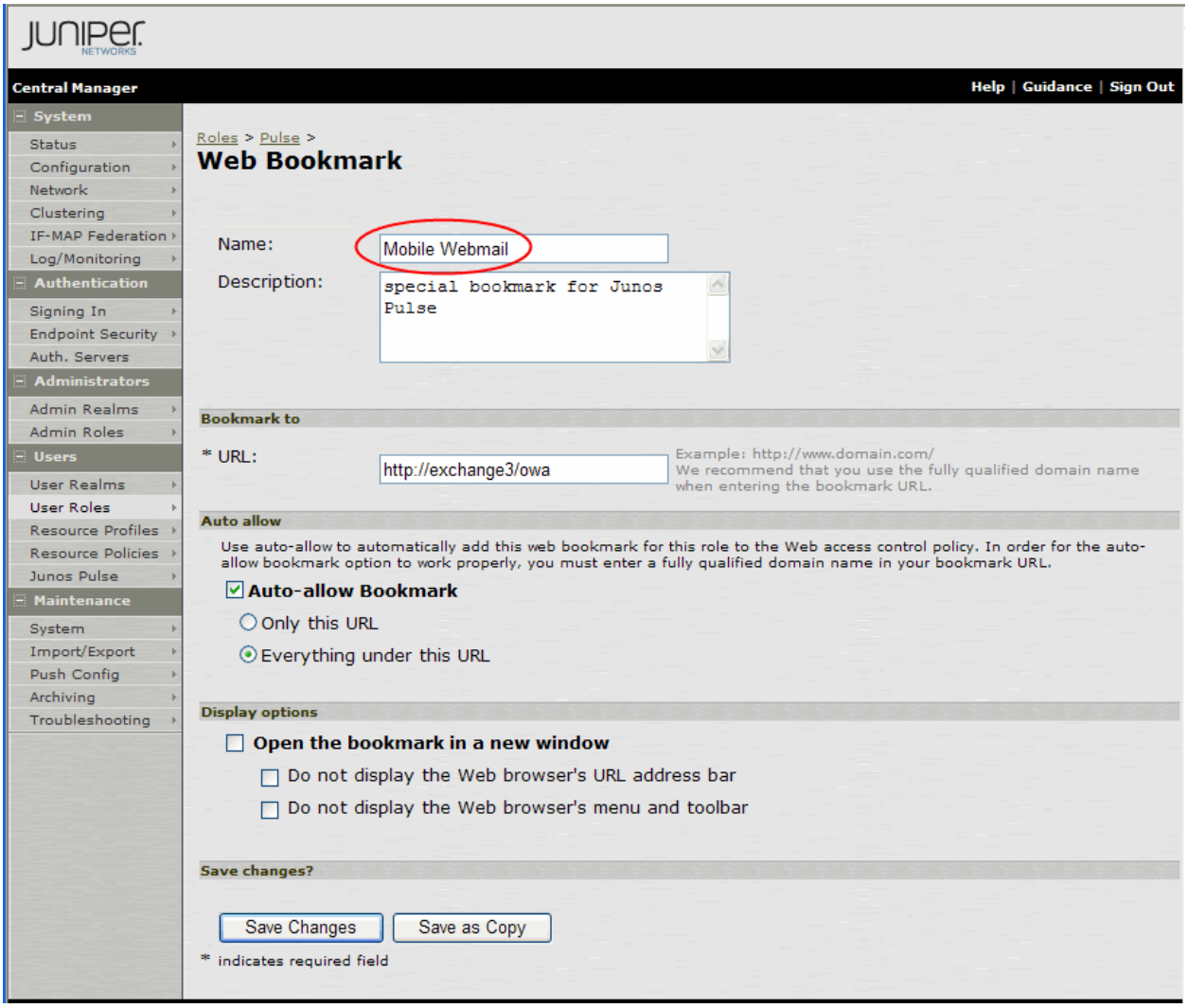
To enable access from an Android device to an SA Series Appliance the SA administrator must configure specific realm and role settings on the SA Series Appliance.

To configure an SA Series Appliance for Android device access:

1. Log in to the SA Series Appliance admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access Features section, select **Web**.
5. Click **Save Changes** to create the role and to display the role configuration tabs.
6. Select **Web > Bookmarks** and then click **New Bookmark**.

   You must create bookmarks to enable the buttons that appear in the Pulse for Android user interface. Typically, you create a bookmark for your company intranet and for Web e-mail. You must create an e-mail bookmark to enable the e-mail button within the Pulse interface on the Android, and that e-mail bookmark must be named **Mobile Webmail**.

Figure 2: Creating the E-mail Bookmark for the Pulse Client



NOTE: Alternatively, you can use Web resource policies to define the bookmarks. See the *SA Series SSL VPN Administration Guide* for more information on resource policies.

7. To change default session timeouts, select **General > Session Options**.
8. In the Session lifetime section, specify **Max. Session Length** in minutes. The remaining session time appears on the Pulse interface of the mobile device client in the format **days hours:minutes:seconds**. The other session settings are not applied to mobile clients.
9. Select **Users > User Realms > New User Realm**.
10. Specify a name and, optionally, a description and then click **Save Changes** to create the realm and to display the realm option tabs.

11. On the Authentication Policy tab for the realm, click **Host Checker** and make sure that all Host Checker policies are disabled except for the optional Pulse Mobile Security check.

    You can require that mobile device users have Pulse Mobile Security software installed and enabled. See Junos Pulse Mobile Security Overview for more information.

12. On the Role Mapping tab for the realm, create a new rule that maps all users to the Android role you created earlier in this procedure.

Installing Custom Sign-in Pages

We recommend that you install a set of sign-in pages on your SA Series Appliance that are properly formatted for a mobile device screen. Each supported mobile device has its own set of custom sign-in pages. After you install the custom sign-in pages on your SA Series Appliance, you must create a sign-in URL that uses the sign-in pages.

To download and install mobile device sign-in pages:

1. Download the custom sign-in page zip file, and put the file in a location where you can then upload it to the SA Series Appliance.

   Go to http://kb.juniper.net/KB17749. A Juniper Knowledge Base article includes a link to download a custom sign-in pages file, junos_pulse_custom_pages.zip.

2. On the SA Series Appliance admin console, select **Authentication > Signing In > Sign-in Pages**.
3. Click **Upload Custom Pages**.
4. Specify a name that allows you to easily identify this set of pages.
5. For Page Type, select **Access**.
6. Click **Browse**, select the custom sign-in pages file, and then click **Open**.
7. Click **Upload Custom Pages**.

Creating a Custom Sign-in URL

The following procedure describes how to specify the settings that are required for creating a mobile device sign-in policy that includes the URL for user access. For mobile devices, you need a different policy for each type of mobile device that will access the SA Series Appliance. Before you begin, be sure you have installed the custom sign-in pages for the mobile devices. For complete information about sign-in policies, see the *SA Series SSL VPN Appliances Administration Guide*.

1. On the SA Series Appliance admin console, select **Authentication > Signing In > Sign-in Policies**.
2. Click **New URL**.
3. In the Sign-in URL box, specify the URL using the format <*host*>/<*path*>. The path can be any string you want. For example, *yourcompany*.com/android-connect.

4. In the Sign-in page box, select a custom sign-in page you uploaded for device access.
5. In the Authentication realm section, if you select **User picks from a list of authentication realms**, be sure to add to the **Selected realms** list the realm you created for mobile device access.

NOTE: Make note of the URL. You must communicate this URL to mobile device users so they can create the proper Junos Pulse configuration.

6. Click **Save Changes**.

CHAPTER 4

Junos Pulse Mobile Security Suite

Junos Pulse Mobile Security Overview

The Junos Pulse Mobile Security Suite is an optional feature of the Junos Pulse application for mobile devices. It provides mobile security and device management. It protects mobile devices against viruses, spyware, Trojans and worms, and includes tools to mitigate the risks of lost and stolen devices.

The Junos Pulse Mobile Security Suite provides the following features:

- Antivirus—Protects mobile devices against viruses and malware delivered via e-mail, Short Message Service (SMS), Multimedia Messaging Service (MMS), direct download, Bluetooth, or infrared transmission.
- Firewall—Protects users from threats by filtering and blocking TCP/IP traffic. A bidirectional, port-based and IP-based packet filtering option protects the mobile device from harmful or questionable content and prevents malicious content from being transferred to the device. The firewall monitors cellular data and WI-FI traffic.
- Antispam—Provides call and message filtering. Users can prevent interruptions and disturbances by blocking voice and SMS spam by customizing contacts into groups of blacklisted (blocked) numbers.
- Device monitoring and control—Provides real time content monitoring of SMS, MMS, and e-mail messages. The administrator can access call logs, address books, and even photos stored on the device.
- Loss and theft protection—Loss and theft protection features include remote lock, remote wipe, GPS tracking, backup and restore, remote alarms, and SIM change notification by means of commands run from the Pulse Mobile Security Gateway by the administrator.
- Backup and restore—Allows a user to back up the contacts and calendar PIM data stored on the device.

NOTE: The user can initiate a backup but the administrator must perform the restore.

Device Management—The Pulse Mobile Security Gateway provides a management interface for managing and controlling mobile devices. The Pulse Mobile Security Gateway enables you to create user accounts and profiles, create rules and policies for devices, remotely execute features on the client, remove undesirable applications from devices, and generate reports related to malware detection and security levels. For more information, see the *Junos Pulse Mobile Security Gateway Administration Guide*.

Pulse Mobile Security Suite Features

Table 3 on page 18 shows the Pulse Mobile Security Suite features that are supported on each mobile device. Connectivity and security features can operate independently from each other. The security features rely on the device's 3G, 4G, or Wi-Fi access. For example, virus definitions are updated without regard to the device's VPN status.

Table 3: Pulse Mobile Security Suite Features

Pulse Mobile Security Feature	Google Android (1.6, 2.0, 2.1, 2.2)	Apple iOS (4.1)	BlackBerry (4.2 and later)
VPN	Access is through an authenticated SSL browser session.	✓	
Antivirus	✓		✓
Personal firewall			
Antispam			
Backup and restore NOTE: The user can initiate a backup. A restore operation must be performed by the administrator.	✓		✓
Monitor and Control	✓		✓
Antitheft NOTE: Antitheft features are controlled from the gateway.	✓		✓

- Android device access is supported by SA Series Release 6.5 and later.
- Apple iOS device access is supported by SA Series Release 6.4 and later.
- The Pulse Mobile security check feature is available on SA Series Release 7.0 Release 2 and later.

Pulse Mobile Security Configuration Overview

After users install the Junos Pulse app, which includes Pulse Mobile Security software, the user must register the security software to activate it. The software prompts the user

for an optional username and password and for a license key. The Pulse Mobile Security administrator must provide the license key to each user via e-mail or SMS. A successful registration adds device information to the Pulse Mobile Security Gateway database.

NOTE: The optional username and password are reserved for future use.

Requiring Pulse Mobile Security for SA Series Appliance Access

Pulse Mobile Security is an optional licensed feature of the Pulse mobile device app. An SA administrator can configure the SA Series Appliance to perform a host check and require that Pulse Mobile Security be activated on mobile devices before granting access to the device through the SA Series Appliance. If you select security feature, a Pulse client is permitted to connect to the SA only if the following criteria are met:

- The mobile device user has registered Pulse Security Suite.
- The mobile device has been scanned and is free of viruses.

NOTE: The Pulse Mobile Security Check feature is available on SA Series Appliances Release 7.0 Release 2 or later. The Pulse Mobile Security Check feature is not supported on Apple iOS devices.

To require Pulse Mobile Security software on the device:

1. On the SA Series Appliance admin console, select **Users > User Realms**.
2. Select the realm you created for mobile devices. If necessary, create a new one now.
3. On the Authentication Policy tab, select **Host Checker**.
4. Select the **Enable Mobile Security Check** check box, and then click **Save Changes**.

   The Mobile Security Check is now applied to all realm users. If you have created more than one realm for mobile device access, enable this check box on each realm.

Mobile device users must perform the following tasks:

- Download and install the Pulse client software app for the particular device type. The Pulse Mobile Security client software is bundled with the VPN app.
- Start Pulse Mobile Security by tapping the Pulse icon.
- If the device is not registered, respond to the prompts for registration information, including a license key.

PART 2

Index

Index

W

