



Secure Access

Getting Started Guide for SA Series 2500, 4500
and 6500 SSL VPN Appliances

Release



Published: 2010-06-08
Part Number: , Revision 1

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Secure Access Getting Started Guide for SA Series 2500, 4500 and 6500 SSL VPN Appliances

Revision History
2010—Revised for SA release 7.0.

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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

	Front Part	xiii
Part 1	Installation and Start-Up Procedures for SA Series 2500, 4500 and 6500 Appliances	
Chapter 1	Getting Started With the SA Series 2500, 4500 and 6500 SSL VPN Appliances	3
Part 2	Index	
	Index	11

Table of Contents

	Front Part	xiii
	Related Documentation	xiii
	Document Conventions	xiii
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xiv
Part 1	Installation and Start-Up Procedures for SA Series 2500, 4500 and 6500 Appliances	
Chapter 1	Getting Started With the SA Series 2500, 4500 and 6500 SSL VPN Appliances	3
	Step 1: Installing the Hardware	3
	Device Status LED Behavior	4
	Ethernet Port LED Behavior	5
	Bonding Ports	5
	Step 2: Performing Basic Setup	5
	Step 3: Licensing and Configuring Your Secure Access	7
Part 2	Index	
	Index	11

List of Tables

	Front Part	xiii
	Table 1: Notice Icons	xiii
Part 1	Installation and Start-Up Procedures for SA Series 2500, 4500 and 6500 Appliances	
Chapter 1	Getting Started With the SA Series 2500, 4500 and 6500 SSL VPN Appliances	3
	Table 2: Device Status LEDs	4
	Table 3: 4-Port Copper Gigabit Ethernet LEDs (available on SA 4500 and SA 6500)	5

Front Part

- Related Documentation on page xiii
- Document Conventions on page xiii
- Requesting Technical Support on page xiv





Related Documentation

- To download a PDF version of the Secure Access Administration Guide, go to the Secure Access/SSL VPN Product Documentation page of the Juniper Networks Customer Support Center.
- For information about the changes that Secure Access clients make to client computers, including installed files and registry changes, and for information about the rights required to install and run Secure Access clients, refer to the Client-side Changes Guide.
- For information on how to personalize the look-and-feel of the pre-authentication, password management, and Secure Meeting pages that Secure Access displays to end-users and administrators, refer to the Custom Sign-In Pages Solution Guide.

Document Conventions

Table 1 on page xiii 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.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

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

Installation and Start-Up Procedures for SA Series 2500, 4500 and 6500 Appliances

- Getting Started With the SA Series 2500, 4500 and 6500 SSL VPN Appliances on page 3

CHAPTER 1

Getting Started With the SA Series 2500, 4500 and 6500 SSL VPN Appliances

Thank you for choosing the Juniper Networks SA Series SSL VPN appliance. You can install Secure Access and start configuring your system using the following easy steps:



NOTE: After installing and setting up your Secure Access, refer to the Initial Configuration task guide in the administrator Web console to install the most current Secure Access OS service package, license your Secure Access appliance, and create a test user to verify user accessibility. To test initial set-up and continue configuring your Secure Access, refer to the “Getting started” section of the *Juniper Networks Secure Access Administration Guide*.

We recommend that you install the Secure Access appliance on your LAN to ensure that it can communicate with the appropriate resources, like authentication servers, DNS servers, internal Web servers via HTTP/HTTPS, external Web sites via HTTP/HTTPS (optional), Windows file servers (optional), NFS file servers (optional), and client/server applications (optional).



NOTE: If you decide to install your Secure Access appliance in your DMZ, ensure that the Secure Access appliance can connect to these internal resources.

- Step 1: Installing the Hardware on page 3
- Step 2: Performing Basic Setup on page 5
- Step 3: Licensing and Configuring Your Secure Access on page 7

Step 1: Installing the Hardware

The Secure Access 2500, 4500 and 6500 ship with mounting ears and mid-mounts. The Secure Access 6500 includes rear mounting rails for use in a four-post mounting rack. We recommend you use the rear mounting rails when installing the Secure Access 6500 in a rack.

If you require an additional mounting kit, contact Juniper Networks.

Next, connect the included cables and power on the Secure Access appliance following these steps:

1. On the front panel:
 - a. Connect an Ethernet cable from one of the Ethernet ports on the device to a Gigabit switch port set to 1000BaseTX. DO NOT use autoselect on either port. Once you apply power to the Secure Access device, the port uses two LEDs to indicate the connection status, which is described in “Ethernet Port LED Behavior” on page 5.
 - b. Plug the serial cable into the console port.
2. On the rear panel, plug the power cord into the AC receptacle. There is no on/off switch on Secure Access. Once you plug the power cord into the AC receptacle, Secure Access powers up.

Hardware installation is complete after you rack-mount the appliance and connect the power, network, and serial cables. The next step is to connect to the appliance’s serial console as described in “Bonding Ports” on page 5.

Device Status LED Behavior

Startup takes approximately one minute to complete. If you want to turn the device off and on again, we recommend you wait a few seconds between shutting it down and powering it back up.

There are three device status LEDs located on the left-side of the front panel:

- Power
- Hard disk access
- Fault

Table 2 on page 4 lists the name, color, status, and description of each device status LED.

Table 2: Device Status LEDs

Name	Color	State	Description
POWER	Green	Off	Device is not receiving power
		On Steady	Device is receiving power
HARD DISK ACCESS	Yellow	Off	Hard disk is idle
		Blinking	Hard disk is being accessed
FAULT	Red	Off	Device is operating normally
		Slow blinking	Power supply fault

Table 2: Device Status LEDs (*continued*)

Name	Color	State	Description
		Fast blinking	Fan failure
		Solid	Thermal failure

Ethernet Port LED Behavior

The Ethernet port LEDs show the status of each Ethernet port.

Table 3: 4-Port Copper Gigabit Ethernet LEDs (available on SA 4500 and SA 6500)

LED	Color and State	Description
Link/Activity	Green	Link
	Blinking green	Activity
Link Speed	Off	10 Mbps
	Green	100 Mbps
	Yellow	1 Gbps

Bonding Ports

By default, on the SA 6500 only, Secure Access uses bonding of the multiple ports to provide failover protection. Bonding describes a technology for aggregating two physical ports into one logical group. Bonding two ports on Secure Access increases the failover capabilities by automatically shifting traffic to the secondary port when the primary port fails.

The SA 6500 appliance bonds ports as follows:

- Internal port = Port 0+Port 1
- External port = Port 2+Port 3

Secure Access indicates in a message on the System > Network > Overview page whether or not the failover functionality is enabled.

Step 2: Performing Basic Setup

When you boot an unconfigured Secure Access appliance, you need to enter basic network and machine information through the serial console to make the appliance accessible to the network. After entering these settings, you can continue configuring the appliance through the administrator Web console. This section describes the required serial console setup and the tasks you need to perform when connecting to your Secure Access appliance for the first time.

To perform basic setup:

1. Configure a console terminal or terminal emulation utility running on a computer, such as HyperTerminal, to use these serial connection parameters:
 - 9600 bits per second
 - 8-bit No Parity (8N1)
 - 1 Stop Bit
 - No flow control
2. Connect the terminal or laptop to the serial cable plugged in to the appliance's console port and press **Enter** until you are prompted by the initialization script.
3. Enter **y** to proceed and then **y** to accept the license terms (or **r** to read the license first).
4. Follow the directions in the serial console and enter the machine information for which you are prompted, including the:
 - IP address of the internal port (you configure the external port through the administrator Web console after initial configuration)
 - Network mask
 - Default gateway address
 - Primary DNS server address
 - Secondary DNS server address (optional)
 - Default DNS domain name (for example, **acmegizmo.com**)
 - WINS server name or address (optional)
 - Administrator username
 - Administrator password
 - Common machine name (for example, **connect.acmegizmo.com**)
 - Organization name (for example, **Acme Gizmo, Inc .**)



NOTE: Secure Access uses the common machine and organization names to create a self-signed digital certificate for use during product evaluation and initial setup.

We strongly recommend that you import a signed digital certificate from a trusted certificate authority (CA) before deploying Secure Access for production use.

For more information, refer to the “Certificates” chapter in the *Juniper Networks Secure Access Administration Guide*.

5. (FIPS only) The Secure Access FIPS appliances utilize FIPS 140-2 certified Hardware Security Modules (HSM) and require the following pieces of information to initialize the HSM and manage the HSM protected storage:
 - When prompted by the serial console, enter the security officer name and password. Save these credentials as they are required for creating new restore passwords and for changing the security officer password.
 - Enter the key store restore or HSM master key backup password.
 - Enter the username and password for the HSM private key storage.

Security officer names, usernames and key store names must adhere to the following requirements.

Requirement	Description
Minimum length	At least one character.
Maximum length	63 characters for security officer names and user names. 32 characters for keystore names.
Valid characters	Alphanumeric, underscore (_), dash (-) and period (.)
First character	Must be alphabetic.

Passwords must be at least six characters. Three characters must be alphabetic and one character must be non-alphabetic.

6. In a browser, enter the machine's URL followed by `/admin` to access the administrator sign-in page. The URL is in the format: `https://a.b.c.d/admin`, where `a.b.c.d` is the machine IP address you entered in step 4. When prompted with the security alert to proceed without a signed certificate, click **Yes**. When the administrator sign-in page appears, you have successfully connected your Secure Access appliance to the network.
7. On the sign-in page, enter the administrator user name and password you created in step 4 and then click **Sign In**. The administrator Web console opens to the **System>Status>Overview** page.

Step 3: Licensing and Configuring Your Secure Access

After you install Secure Access and perform basic setup, you are ready to install the most current Secure Access OS service package, license Secure Access, verify accessibility, and complete the configuration process:

- To install the most current Secure Access OS service package, license your Secure Access and create a test user to verify user accessibility, follow the task guide embedded in the administrator Web console.
- To test initial set-up and continue configuring your Secure Access, refer to the "Getting Started" section of the *Juniper Networks Secure Access Administration Guide*.

PART 2

Index

- Index on page 11

Index

C

customer support.....xiv
 contacting JTAC.....xiv

S

support, technical See technical support

T

technical support
 contacting JTAC.....xiv

