



Junos Space

Junos Space Security Design Release Notes

Release

11.4



Published: 2011-12-21

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, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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.

Junos Space Security Design 11.4 Release Notes
Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
December 2011—Junos Space Security Design Release 11.4 Release Candidate Test

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Chapter 1	Junos Space Security Design Release Notes	5
	Security Design	5
	Technical Documentation	5
	Installing Security Design	6
	Supported Devices	7
	Supported OS Versions	7
	Supported Browsers	7
	Management Scalability	7
	Features	7
	Known Issues	8

CHAPTER 1

Junos Space Security Design Release Notes

- [Security Design on page 5](#)
- [Technical Documentation on page 5](#)
- [Installing Security Design on page 6](#)
- [Supported Devices on page 7](#)
- [Supported OS Versions on page 7](#)
- [Supported Browsers on page 7](#)
- [Management Scalability on page 7](#)
- [Features on page 7](#)
- [Known Issues on page 8](#)

Security Design

Junos Space Security Design application is a powerful but easy-to-use solution that allows you to create and publish firewall policies, IPSec VPNs, NAT policies, IPS policies and AppFirewall to provide appropriate security on the network. You would need to procure an IPS license to be able to push IPS signatures and App Firewall signatures to a device.

Technical Documentation

Please refer to the following link for updated documentation for Junos Space Security Design 11.4 -

https://www.juniper.net/beta/spg/space/beta1/techpubs/en_US/junos-space114/junos-space-security-design-sub-index.html

This version of documentation is a more updated than the one available on the Beta Software build for Junos Space Security Design 11.4.

Installing Security Design

To install Junos Space Security Design 11.4, you would need to upgrade your 11.3R1.6 platform version with a patch version 11.3P3.1 and then install the Security Design build. Perform the following steps to do this:

1. Log to the space appliance UI and enter the username and password.

The default username is **super** and the default password is **juniper123**.

2. Click the Network Application Platform icon on the screen.

You can also click the Application Switcher icon and select **Network Application Platform** from the list of applications.

3. Click the Administration icon from the **Network Application Platform** Task ribbon.

4. Click **Manage Applications**.

The Manage Applications page is displayed.

5. Right-click **Network Application Platform** in the **Manage Applications** page and click **Upgrade Platform**.

6. Click **Upload via HTTP** at the bottom of the page. The **Upload** window is displayed.

7. Browse for the patch version 11.3P3.1 and click **Upload**.

The patch file will now be uploaded.

8. Select the patch image you uploaded in the same page and click **Upgrade**.

You will receive a pop-up stating that your patch upgrade is successful. Network Application Platform will now be upgraded to patch version 11.3P3.1

9. Click **Exit from maintenance mode**.

10. Click the Application Switcher icon and select **Network Application Platform** from the list of applications.

11. Click the Administration icon and then click **Manage Applications**.

The **Manage Applications** page is displayed.

12. Click **Add Application** and then click **Upload via HTTP** at the bottom of the page.

The **Upload** window is displayed.

13. Browse for the Security Design build you have downloaded (Security-Design.11.4R1.5) and click **Upload**.

The Security Design build will now be uploaded.

14. Select the downloaded image and click install to install the Security Design application.

It will take at least 5 minutes for Security Design application to show up in the application list once **Install** button is clicked.



NOTE: Security Design 11.4 version is currently being qualified for compatibility with the Junos Space Platform 11.4 version.

Supported Devices

Junos Space Security Design 11.4 is supported on the following SRX hardware devices:

- SRX 100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX650
- SRX1400
- SRX 3400
- SRX 3600
- SRX 5600
- SRX 5800

Supported OS Versions

Junos Space Security Design 11.4 is supported on SRX OS version 10.3 and above.

SRX OS version 11.4 is needed to turn on full AppFW feature support. Also on the Junos Space side you would need to upgrade to 11.4 schema file manually and set 11.4 schema to default for junos-es device family to avail AppFW and template based custom object support.

Supported Browsers

Junos Space Security Design 11.4 is best viewed on Mozilla Firefox 4.0 and Internet Explorer 8.0.

Management Scalability

Junos Space Security Design 11.4 is designed to support management of large scale security deployments. Security Design 11.4 was tested to manage 4,000 devices, 20,000 address objects, and 10,000 rules with rule groups of 500 rules.

Features

Junos Space Security Design 11.4 application presents the following new features:

- **Firewall Policies**— Allows you to create and update firewall policies on SRX devices and SRX device clusters. You can create two types of policies - Group policy and Device policy and add different type of rules for these policies. You can also group the rules based on your preference.
- **IPsec VPNs**— Allows you to create Site to Site, Hub And Spoke, and Full Mesh IPsec VPNs and update the VPN configurations on SRX devices and SRX device clusters. You can configure the tunnel settings, endpoint settings, and routing settings using an intuitive VPN creation workflow. You can also preview and validate these settings before saving the VPN configuration.
- **NAT Policies**— Allows you to create and update NAT policies on SRX devices and device clusters. You can create two types of NAT policies - Group policy and Device policy and add different type of rules for these NAT policies. You can also group the rules based on your preference.
- **Object Builder**— An exclusive workspace that allows you to create sub-configuration objects which can be used across multiple firewall policy, NAT policy, and VPN configurations. You can create and manage address objects, service objects, application signatures, NAT pools, VPN profiles, Policy profiles, Template definitions, Templates and Polymorphic variables using this workspace.
- **Templates**— Allows you to create custom objects that support SRX device features such as Scheduler and UTM. You can apply templates to a policy either at the policy level or at the rule level. If a rule in a policy used a template, then it takes precedence than the templates used for the policy.
- **VPN Profiles**— Allows you to export define the VPN proposals, IKE settings, and IPsec settings. VPN profiles are stored in the Junos Space database and can be re-used to create multiple IPsec settings.
- **Export Policies**— Allows you to export firewall policies and NAT policies to HTML format.
- **Signature Management**— Allows you to download, install, view, and filter App signatures and IPS signatures. You can create application signatures/groups, IPS signatures/groups, and IPS signature-sets from the downloaded and installed signatures. You can also create static Application signature groups (Static) and both static and dynamic IPS signature groups.
- **App Firewall and IPS Integration with Firewall Policy**— Allows you to enable App Firewall and IPS for every rule in a firewall policy. You can view all the IPS policies and rules in the IPS Management workspace.

Known Issues

- Security Design 11.4 does not support concurrent firewall policy, VPN, NAT policy, and IPS changes by multiple administrators. Since locking is not performed, overlapping updates can result in the loss of changes.
- Current version of Security Design does not import existing policies, objects, VPNs from the devices.

- Clicking on the buttons on the top platform ribbon in the GUI during any changes (Policy, VPN, objects etc) will cause changes to be not saved and no warning will be displayed.
- Device to address mapping cannot be modified in a polymorphic address object.

Workaround: Delete the device to address mapping in variables; and add them again. [PR 717808]

- Wildcard address type or DNS address type objects cannot be modified once created. [PR 710403]

- “External Interface” column cannot be edited in VPN if the “Protected Networks/Zone” cell of the same row is expanded and more than one page. [PR 706402]

Recommended usage: Collapse the “Protected Networks/Zone” cell by clicking “Less” and then edit “External Interface”.

- Sometimes, switching IPS mode to none may cause device configuration update fail.

Workaround: Republish and update the configuration to device. [PR 722213]

