



STRM Series to JSA Series

Migration Guide



Published: 2015-03-03

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

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.

STRM Series to JSA Series Migration Guide

Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

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

	About the Documentation	v
	Documentation and Release Notes	v
	Documentation Conventions	v
	Documentation Feedback	vii
	Requesting Technical Support	viii
	Self-Help Online Tools and Resources	viii
	Opening a Case with JTAC	viii
Part 1	STRM Series to JSA Series Migration	
Chapter 1	JSA Series Appliance Overview	3
	JSA Series Appliance	3
	Configuration and Data Features for STRM and JSA Migration	4
Chapter 2	Migrating an STRM Series Appliance to a JSA Series Appliance	5
	STRM Series to JSA Series Migration Overview	5
	Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance	6
	Upgrading an Existing STRM Appliance	7
	Upgrading an Existing STRM Appliance to JSAx500 Series Appliances	8
	Upgrading an Existing STRM Appliance to JSA3800 or JSA5800 Appliance	8
	Backing Up the STRM Appliance Configuration While Running the Common Image	9
	Installing a JSA and a Virtual JSA Appliance	10
	Reimaging JSA Series to the Common Image Using the Recovery Partition	11
	Restoring an STRM Backup to a JSA Appliance	12
	Copying STRM Event and Flow Data to JSA	13
	Running Automatic Updates on the JSA Appliance	14
Part 2	Distributed STRM Environment to JSA Migration	
Chapter 3	Migrating a Distributed STRM Environment to JSA	19
	Distributed STRM Environment to JSA Migration Overview	19
	Migrating the STRM Console to a JSA Console	20
	Migrating an STRM Managed Host to a JSA Managed Host	21
	Adding Each New JSA Managed Host to a JSA Console	22

Part 3	STRM Series to JSA Series License Migration	
Chapter 4	Migrating Licenses from STRM Series to JSA Series	27
	Migrating Licenses from STRM Series to JSA Series Overview	27
	Obtaining the Serial Number of an STRM Series or a JSA Series Appliance	27
	STRM Series to JSA Series License Migration Assistance	28
Part 4	Index	
	Index	33

About the Documentation

- Documentation and Release Notes on page v
- Documentation Conventions on page v
- Documentation Feedback on page vii
- Requesting Technical Support on page viii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page vi 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] <pre> routing-options { static { route default { nexthop address; retain; } } } </pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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: <http://kb.juniper.net/InfoCenter/>
- 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

STRM Series to JSA Series Migration

- [JSA Series Appliance Overview on page 3](#)
- [Migrating an STRM Series Appliance to a JSA Series Appliance on page 5](#)

CHAPTER 1

JSA Series Appliance Overview

This chapter includes the following topics:

- [JSA Series Appliance on page 3](#)
- [Configuration and Data Features for STRM and JSA Migration on page 4](#)

JSA Series Appliance

The Juniper Secure Analytics (JSA) Series includes the hardware appliances (JSA1500, JSA3500, JSA5500, JSA7500, JSA3800, and JSA5800) and a virtual appliance, which replace Juniper Networks Security Threat Response Manager (STRM) solution for centralized logging, monitoring, and reporting. The JSA Series integrates and automates log management and network behavior analytics and offers increased performance and scaling features.

This guide provides instructions for:

- Migrating the configuration from an existing STRM appliance to a new JSA appliance including network settings (for example, IP address). This process replaces an STRM appliance with a similarly configured JSA appliance.
- Manually copying STRM event and flow data to the JSA appliance. This step is optional.
- Migrating from a distributed STRM environment to JSA.
- Migrating licenses from STRM to JSA.



NOTE: The migration process maintains the existing STRM configuration.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)

Configuration and Data Features for STRM and JSA Migration

The following configuration can be migrated from Security Threat Response Manager (STRM) to Juniper Secure Analytics (JSA):

- Assets
- Custom logos
- Custom rules
- Device Support Modules (DSMs)
- Event categories
- Flow sources
- Flow and event searches
- Groups
- License key information
- Log sources
- Offenses
- User and user roles information
- Custom Dashboards
- Vulnerability data
- Certificates

Optionally, STRM event and flow data can be copied manually to JSA.

The following configuration cannot be migrated from STRM to JSA:

- Audit log information
- Report data
- Indexes
- Reference set elements

Related Documentation

- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)

CHAPTER 2

Migrating an STRM Series Appliance to a JSA Series Appliance

This chapter includes the following topics:

- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
- [Upgrading an Existing STRM Appliance on page 7](#)
- [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
- [Installing a JSA and a Virtual JSA Appliance on page 10](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)
- [Restoring an STRM Backup to a JSA Appliance on page 12](#)
- [Copying STRM Event and Flow Data to JSA on page 13](#)
- [Running Automatic Updates on the JSA Appliance on page 14](#)

STRM Series to JSA Series Migration Overview

The migration process from Security Threat Response Manager (STRM) Series to Juniper Secure Analytics (JSA) Series includes the following steps:

1. Perform a pre-upgrade configuration backup of the STRM appliance.
2. Upgrade or patch the STRM appliance to the common image.
3. Perform a configuration backup of the STRM appliance when running the common image.
4. Install the JSA appliance and, if require, reimage the appliance to the common image.
5. Restore an STRM appliance configuration on the JSA appliance.
6. Copy STRM event and flow data to the JSA appliance (optional).
7. Run automatic updates on the JSA appliance.



NOTE: The STRM to JSA configuration can be migrated from any appliance in the STRM Series to any appliance in the JSA Series. For more information, see *Migrating Licenses from STRM Series to JSA Series*.

For example, a configuration backup from an STRM5000 with NEBS compliance can be restored on any JSA model: JSA5500, JSA7500, or the JSA virtual appliance.

Related Documentation

- [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
- [Upgrading an Existing STRM Appliance on page 7](#)
- [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)
- [Copying STRM Event and Flow Data to JSA on page 13](#)
- [Restoring an STRM Backup to a JSA Appliance on page 12](#)

Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance

When you are about to migrate a Security Threat Response Manager (STRM) Series appliance to a Juniper Secure Analytics (JSA) Series appliance, we recommend that you perform a pre-upgrade configuration backup on the STRM appliance. The pre-upgrade backup is not used when you restore the configuration on a JSA appliance. Rather, you should perform the pre-upgrade backup as a best practice in case you encounter errors while upgrading STRM or JSA to a common image.

By default, STRM creates a complete backup of the appliance configuration each day at midnight. You can either use the automatic backup or initiate an on-demand backup. Either way, the configuration backup should be downloaded before you upgrade STRM or install the patch on STRM.

To create and download an on-demand configuration backup:

1. Log in to the STRM WebUI.
2. Click the Admin tab.
3. On the navigation menu, click **System Configuration**.
4. Click **Backup and Recovery**.



NOTE: Configuration backup files are located in the `/store/backup` directory.

5. From the toolbar, click **On Demand Backup**.

6. Enter a name and description to identify the backup.
7. Click **Run Backup**.
8. Click **OK**.
9. Monitor the backup archive process in the Backup Archives window.

Once complete, the backup will appear in the list of the Existing Backups table.

10. To download the backup, click the backup name.



NOTE: Double-click in the Existing Backups table to display the Restore a Backup dialog box. Single-click on a backup name to download the backup.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Upgrading an Existing STRM Appliance on page 7](#)
- [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)

Upgrading an Existing STRM Appliance

Both Security Threat Response Manager (STRM) and Juniper Secure Analytics (JSA) software have a version number and a build number.

For example, if the software is 2013.2.r3.615469, then the version number is 2013.2.r3 and the build number is 615469. Both STRM and JSA must run the same version and build for the configuration migration to be successful.

Juniper Networks delivers the STRM and JSA software in two ways:

- ISO file—used for fresh installs and major upgrades
- SFS file—called a patch and used for minor upgrades

You can upgrade an existing STRM appliance to a JSA3800 appliance, a JSA5800 appliance, or a JSAX500 Series appliances, where x is one of the JSA Series appliances 1, 3, 5, or 7 (JSA1500, JSA3500, JSA5500, or JSA7500).

- [Upgrading an Existing STRM Appliance to JSAX500 Series Appliances on page 8](#)
- [Upgrading an Existing STRM Appliance to JSA3800 or JSA5800 Appliance on page 8](#)

Upgrading an Existing STRM Appliance to JSAx500 Series Appliances

The image that is certified for this migration is 2013.2.r3.615469 or later version on both STRM and JSA; 2013.2.r3.615469 is referred as common image in this migration documentation.



NOTE: You should use 2013.2.r7 patch or later version as the common image to migrate an STRM Log Manager to JSA. For STRM Log Manager, the patch should be installed before performing pre-migration backup; for JSA, the patch should be installed before restoring the pre-migration backup.

The upgrade path depends on the version that is currently running on the STRM:

- STRM 2012.x uses the ISO file to upgrade to the common image.
- STRM 2013.x requires the SFS patch to upgrade to the common image.

STRM 2010.x and 2009.x must be installed with a patch or upgraded to an interim release before you can upgrade to the common image.

For information on upgrading STRM to 2013.2, see *Upgrading STRM to 2013.2* and the details in the Juniper Networks KnowledgeBase (KB) article [KB28144](#).



NOTE:

- Even though the STRM500 is not supported on the 2013.x software, it can be upgraded to migrate to a JSA configuration. The upgrade should be performed when the appliance is under minimal load or offline (for example, after office hours).
- If you have trouble accessing the STRM user interface after you upgrade to STRM 2013.2, we recommend that you first clear your Java cache.

Upgrading an Existing STRM Appliance to JSA3800 or JSA5800 Appliance

The certified image for this migration is 2014.3.r1.931999 or a later version on both STRM and JSA; 2014.3.r1.931999 is referred to as the common image in this migration documentation.

[Table 3 on page 8](#) helps you determine the upgrade path to the common image depending on the version that is currently running on the STRM Series or JSA Series appliance.

Table 3: Supported Upgrade Paths to the Common Image

Current Version	Step 1	Step 2	Step 3
2014.1, 2014.2, and 2014.3 ISO	2014.3.r1 patch		

Table 3: Supported Upgrade Paths to the Common Image (*continued*)

Current Version	Step 1	Step 2	Step 3
2013.2 R3 ISO with 2013.2.r9 patch or later	2014.3.r2 patch		
2013.2 R3 ISO to 2013.2.r8 patch	2014.3.r1 patch		
2012.X and 2013.X, which are versions earlier than 2013.2 R3 ISO	2013.2 R3 ISO	2013.2.r8 patch	2014.3.r1 patch

For information on upgrading STRM to 2013.2, see *Upgrading STRM to 2013.2* and the details in the Juniper Networks KnowledgeBase (KB) article [KB28144](#).



NOTE:

- Even though the STRM500 is not supported on the 2013.x software, it can be upgraded to migrate to a JSA configuration. The upgrade should be performed when the appliance is under minimal load or offline (for example, after office hours).
- If you have trouble accessing the STRM user interface after you upgrade to STRM 2013.2, we recommend that you first clear your Java cache.

For information on upgrading JSA to 2014.3, see *Upgrading JSA to 2014.3*.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
- [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)

Backing Up the STRM Appliance Configuration While Running the Common Image

When Security Threat Response Manager (STRM) is running the common image, a new configuration backup must be made. This backup is restored to the Juniper Secure Analytics (JSA) appliance. You cannot restore the pre-upgrade backup to JSA because it was made before the STRM was running the common image.

For the STRM backup process that includes copying the backup to a remote server, see [“Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance”](#) on page 6.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration](#) on page 4
- [Migrating Licenses from STRM Series to JSA Series Overview](#) on page 27
- [STRM Series to JSA Series Migration Overview](#) on page 5
- [Upgrading an Existing STRM Appliance](#) on page 7
- [Installing a JSA and a Virtual JSA Appliance](#) on page 10
- [Reimaging JSA Series to the Common Image Using the Recovery Partition](#) on page 11

Installing a JSA and a Virtual JSA Appliance

To install:

- JSA1500, JSA3500, JSA5500, and JSA7500, see the *Juniper Secure Analytics Quick Start Guide*.
- JSA3800, see *How to Set Up Your JSA3800 Appliance*.
- JSA5800, see *How to Set Up Your JSA5800 Appliance*.

These guides provides you the following information:

- Installing a JSA appliance
- Configuring the network settings
- Accessing a JSA appliance

To install a virtual JSA appliance, see the *JSA Virtual Appliance Installation Guide*. This guide provides you the following information:

- Creating a new virtual machine
- Installing the JSA software
- Configuring the network settings
- Accessing a virtual JSA appliance

Assign a temporary IP address when you configure the JSA network settings. When the new JSA appliance is installed and active on the network, you must determine the installed version and reimage if necessary.

The physical JSAX500 appliances (where x is one of the JSA Series appliances 1, 3, 5, or 7; JSA1500, JSA3500, JSA5500, or JSA7500) come with one of two possible factory images:

- Initially, JSA Series appliances were built with 2013.2.r3.607582.
- Now, JSA Series appliances are built with 2013.2.r3.615469 (the common image).

The physical JSA3800 and JSA5800 appliances come with 2014.3.r1.931999 (the common image).

The common image is certified for migration for both STRM and JSA.



NOTE: There is no patch available from 2013.2.r3.607582 to the common image, so JSA appliances with that software must be reimaged for the restore process to succeed.

In the JSA user interface, click **Help** > **About** to view the JSA version information. If the JSA version is:

- 2014.3.r1.931999, there is no need for reimaging. Follow the steps in “[Copying STRM Event and Flow Data to JSA](#)” on page 13.
- 2013.2.r3.615469, there is no need for reimaging if you are migrating to JSAx500 Series appliances. Follow the steps in “[Copying STRM Event and Flow Data to JSA](#)” on page 13. If you are migrating to JSA3800 or JSA5800, you must upgrade the JSA Series appliance to the common image.
- 2013.2.r3.607582, you must reimage the JSA Series appliance to the common image.

Related Documentation

- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
- [Upgrading an Existing STRM Appliance on page 7](#)
- [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)

Reimaging JSA Series to the Common Image Using the Recovery Partition

To reimage the JSA appliance to the common image using the recovery partition:

1. To download the ISO file:
 - a. Access the Juniper Customer Support Center (CSC) website (www.juniper.net/support/).
 - b. Locate the JSA 2013.2.X ISO or 2014.3.r1 ISO file on the CSC website (Where X is r3.615469 or a later version).
 - c. Save the ISO file on a remote server that supports either SCP or FTP.
2. Using SSH, log in to your JSA system as the root user.

3. Copy the ISO or SFS image from a remote server to the JSA appliance using SCP or FTP.

For example, if the IP address of the remote server is 10.10.10.1, run the following command to copy the file to the `/root` directory:

```
[root@jsa]#scp root@10.10.10.1:/<path>/STRM2013.2.X.iso /root
```

Where X is r3.615469 or later version.

4. Run the following command to change to the location of the `recovery.py` script:

```
[root@jsa]# cd /opt/qradar/bin
```

5. Run the following command to execute the recovery script:

- For JSAX500: `[root@jsa]# ./recovery.py -r --default --reboot /root/STRM2013.2.X.iso`

Where x is one of the JSA Series appliances 1, 3, 5, or 7 (JSA1500, JSA3500, JSA5500, or JSA7500) and X is r3.615469 or a later version.

- For JSA3800 and JSA5800: `[root@jsa]# ./recovery.py -r --default --reboot /root/JSA2014.3.r1.iso`

6. After reboot, when prompted, type **FLATTEN** and then press Enter.

The JSA appliance is now running the common image.

Related Documentation

- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
- [Upgrading an Existing STRM Appliance on page 7](#)
- [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
- [Installing a JSA and a Virtual JSA Appliance on page 10](#)
- [Restoring an STRM Backup to a JSA Appliance on page 12](#)
- [Copying STRM Event and Flow Data to JSA on page 13](#)

Restoring an STRM Backup to a JSA Appliance

Because both Security Threat Response Manager (STRM) and Juniper Secure Analytics (JSA) are running the common image, the STRM backup (made while running the common image) can be restored to the JSA appliance.

This procedure restores the STRM configuration on JSA, including network settings like IP address. To avoid a duplicate IP address on the network, the STRM appliance must be turned off before proceeding.

To restore the STRM configuration on the JSA appliance:

1. Log in to the Secure Analytics WebUI.
2. Click the Admin tab.
3. On the navigation menu, click **System Configuration**.
4. Click **Backup and Recovery**.
5. Click **Choose File** to upload the configuration backup.
6. Select the file and then click **Upload**.

The uploaded backup appears under the Existing Backups table.

7. Select the backup file and then click **Restore**.
8. Select all the check boxes except **Select All Configuration Items** and **License** in the Restore a Backup window, and then click **Restore** to restore the backup.

Special Case for STRM HA Clusters

If the configuration backup was made on a high availability cluster, you must click **Deploy Changes** from the JSA appliance console to restore the HA cluster configuration after the restore is complete and before adding the secondary appliance.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)
- [Copying STRM Event and Flow Data to JSA on page 13](#)
- [Running Automatic Updates on the JSA Appliance on page 14](#)

Copying STRM Event and Flow Data to JSA

The configuration restore process duplicates only the Security Threat Response Manager (STRM) configuration to the Juniper Secure Analytics (JSA) Series appliance. To copy the event and flow data, several file transfer methods are possible including rsync, SCP, and FTP.



NOTE: All the event and flow data are stored in the `/store/ariel` directory on both STRM and JSA.

To copy the STRM event and flow data to a JSA appliance:

1. Using SSH, log in to STRM.
2. Run the **rsync** command to copy the event and flow data to JSA. If the temporary IP address of the JSA appliance is 10.10.10.1, run the following commands:

- To copy events, `[root@strm]# /usr/bin/rsync -azv /store/ariel/events root@10.10.10.1:/store/ariel/events`
- To copy flows, `[root@strm]# /usr/bin/rsync -azv /store/ariel/flows root@10.10.10.1:/store/ariel/flows`



NOTE:

- Use the optional `v` option to view the status of the copy operation. Do not use this option if you are connected to STRM through the serial console or over slow links. Use `>` to redirect the output to a file, and use the `tail` command to check the progress periodically.
- If only event or flow data (not both) is desired, specify the directory (either `/events` or `/flows`) specifically. For example, run the following command to copy only STRM event data:

```
[root@strm]# /usr/bin/rsync -azv /store/ariel/events  
root@10.10.10.1:/store/ariel/events
```



NOTE: To verify that the restored data is available:

- a. Log in to the Secure Analytics WebUI.
- b. Click the Log Activity or Network Activity tab.
- c. Select Search > Edit Search from the list.
- d. In the Time Range box, select Specific Interval.
- e. Specify the date of the data you just restored.
- f. Click Search.
- g. View the results to verify the restored data.

**Related
Documentation**

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
- [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)
- [Restoring an STRM Backup to a JSA Appliance on page 12](#)
- [Running Automatic Updates on the JSA Appliance on page 14](#)

Running Automatic Updates on the JSA Appliance

After you have verified that the configuration and data are restored to the Juniper Secure Analytics (JSA) appliance, some system components should be updated, including

installing new or updated DSMs, vulnerability assessment (VA) scanners, and log source protocols.

To run automatic updates on the JSA appliance:

1. In the JSA appliance console, click the Admin tab.
2. On the navigation menu, click **System Configuration**.
3. Click the Auto Update icon.
4. Click the Get New Updates button.
5. Select **OK** to download.



NOTE: By default, DSM, scanner, and protocol updates are automatically installed once they are downloaded. This setting is configured through the **Change Settings** pane. For more information, see the *Automatic Updates* section of the *STRM Administration Guide*.

**Related
Documentation**

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Restoring an STRM Backup to a JSA Appliance on page 12](#)
- [Copying STRM Event and Flow Data to JSA on page 13](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)

PART 2

Distributed STRM Environment to JSA Migration

- [Migrating a Distributed STRM Environment to JSA on page 19](#)

CHAPTER 3

Migrating a Distributed STRM Environment to JSA

This chapter includes the following topics:

- [Distributed STRM Environment to JSA Migration Overview on page 19](#)
- [Migrating the STRM Console to a JSA Console on page 20](#)
- [Migrating an STRM Managed Host to a JSA Managed Host on page 21](#)
- [Adding Each New JSA Managed Host to a JSA Console on page 22](#)

Distributed STRM Environment to JSA Migration Overview

The migration of a distributed Secure Threat Response Manager (STRM) environment to Juniper Secure Analytics (JSA) includes the following steps:

1. Migration from the STRM console to a JSA console.
2. Migration of each STRM managed host to a JSA managed host.
3. Adding each new JSA managed host to the JSA console.

Related Documentation

- [JSA Series Appliance on page 3](#)
- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Migrating the STRM Console to a JSA Console on page 20](#)
- [Migrating an STRM Managed Host to a JSA Managed Host on page 21](#)
- [Adding Each New JSA Managed Host to a JSA Console on page 22](#)

Migrating the STRM Console to a JSA Console

In a distributed Security Threat Response Manager (STRM) environment, managed hosts (distributed event or flow processors) gather and process event and flow data locally, and feed this information into the STRM console. You do not need to change the existing STRM distributed setup to prepare for the console migration. However, if any managed hosts have been added to the new Juniper Secure Analytics (JSA) console (which will be restored with the STRM backup), the managed hosts must be removed before the restoration process.

To migrate the STRM console to a JSA console:

1. If the JSA appliance has managed hosts defined:
 - a. On the JSA console, click the Admin tab to launch the Deployment Editor.
 - b. Click the System View tab.
 - c. Right-click each managed host, and select **Remove host**.



NOTE: The Remove host option is only available when the JSA appliance has a managed host connected to it.

- d. Click **OK**.
 - e. On the Admin tab, select **Advanced > Deploy Full Configuration**.
2. For preparing the console, perform the steps as instructed in the following procedures:
 - a. [Pre-Upgrade Configuration Backup Process of Existing STRM Series Appliance on page 6](#)
 - b. [Upgrading an Existing STRM Appliance on page 7](#)
 - c. [Backing Up the STRM Appliance Configuration While Running the Common Image on page 9](#)
 - d. [Installing a JSA and a Virtual JSA Appliance on page 10](#)
 - e. [Reimaging JSA Series to the Common Image Using the Recovery Partition on page 11](#)
 - f. [Copying STRM Event and Flow Data to JSA on page 13](#)
3. Follow the steps in “[Restoring an STRM Backup to a JSA Appliance](#)” on page 12.

To successfully restore the STRM backup, you must select **Deploy Full Configuration**. You will be prompted to disable iptables on the old STRM managed hosts. You can ignore this prompt because the old managed hosts are being replaced with JSA managed hosts.
4. Once the restore process is complete, log in to the new JSA console.

Ignore the error messages on the dashboard if you receive any.

5.



NOTE: Connections to the old STRM managed hosts are restored along with the configuration. These connections must be removed before you complete the configuration. Before removing each managed host, make a note of the processes assigned to that managed host. After adding corresponding new managed host, remove default processes added by the new host and then assign the corresponding old processes to the new managed host. These old processes should have a red outline as they are currently unassigned. We recommend you to migrate managed hosts one at a time.

To disconnect each managed host:

- a. On the JSA console, click the Admin tab to launch the Deployment Editor.
- b. Click the System View tab.
- c. Right-click each managed host, and select **Remove host**.



NOTE: This option is available only when the JSA appliance is connected to a managed host.

- d. Click **OK**, and then save and close the Deployment Editor.
 - e. On the Admin tab, select **Advanced > Deploy Full Configuration**.
6. Follow the steps in “[Running Automatic Updates on the JSA Appliance](#)” on page 14 to complete the configuration of the new JSA console.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration](#) on page 4
- [Migrating Licenses from STRM Series to JSA Series Overview](#) on page 27
- [STRM Series to JSA Series Migration Overview](#) on page 5
- [Installing a JSA and a Virtual JSA Appliance](#) on page 10
- [Distributed STRM Environment to JSA Migration Overview](#) on page 19
- [Migrating an STRM Managed Host to a JSA Managed Host](#) on page 21
- [Adding Each New JSA Managed Host to a JSA Console](#) on page 22

Migrating an STRM Managed Host to a JSA Managed Host

It is not necessary to restore the configuration of each Security Threat Response Manager (STRM) managed host to Juniper Secure Analytics (JSA). However, the event and flow data on the STRM managed host can optionally be migrated to the JSA managed host.

To migrate each STRM managed host to a JSA managed host:

1. Follow the steps in “[Installing a JSA and a Virtual JSA Appliance](#)” on page 10.

2. If necessary, follow the steps in [“Reimaging JSA Series to the Common Image Using the Recovery Partition”](#) on page 11.
3. Follow the steps in [“Copying STRM Event and Flow Data to JSA”](#) on page 13.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration](#) on page 4
- [Migrating Licenses from STRM Series to JSA Series Overview](#) on page 27
- [STRM Series to JSA Series Migration Overview](#) on page 5
- [Installing a JSA and a Virtual JSA Appliance](#) on page 10
- [Distributed STRM Environment to JSA Migration Overview](#) on page 19
- [Migrating the STRM Console to a JSA Console](#) on page 20
- [Adding Each New JSA Managed Host to a JSA Console](#) on page 22

[Adding Each New JSA Managed Host to a JSA Console](#)

After the successful migration of console and all managed hosts to Juniper Secure Analytics (JSA), you can connect the managed hosts to the new JSA console.

To add the JSA managed hosts to the JSA console:

1. On the JSA console, click the Admin tab to launch the Deployment Editor.
2. Click the System View tab.
3. From the menu, select **Actions > Add a Managed Host**.
4. Click **Next**.
5. Enter the values for the following parameters:
 - **Enter the IP of the server or appliance to add**—Type the IP address of the host you want to add to your system view.
 - **Enter the root password of the host**—Type the root password for the host.
 - **Confirm the root password of the host**—Type the password again.
 - **Host is NATed**—Select the check box to use an existing Network Address Translation (NAT) on this managed host.
 - **Enable Encryption**—Select the check box to create an SSH encryption tunnel for the managed host.
 - **Enable Compression**—Select the check box to enable data compression to the managed hosts.
6. Click **Next**.
7. If you select the Host is NATed check box, the Configure NAT Settings page is displayed. Otherwise, continue to Step 9.
8. To configure NAT settings, enter the values for the following parameters:

- a. **Enter public IP of the server or appliance to add**—Type the public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks using NAT.
- b. **Select NATed network**—From the list box, select the network you want this managed host to use:
 - a. If the managed host is on the same subnet as the console, select the console of the NATed network.
 - b. If the managed host is not on the same subnet as the console, select the managed host of the NATed network.
 - c. Click **Next**.
 - d. Click **Finish**.
9. Click **Finish**.
10. After adding corresponding new managed host, remove default processes added by the new host and then assign the corresponding old processes to the new managed host. These old processes should have a red outline as they are currently unassigned.
11. From the menu, select **File > Save and Close**.
12. On the Admin tab, select **Advanced > Deploy Full Configuration**.

Related Documentation

- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Installing a JSA and a Virtual JSA Appliance on page 10](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)
- [Migrating the STRM Console to a JSA Console on page 20](#)
- [Migrating an STRM Managed Host to a JSA Managed Host on page 21](#)

PART 3

STRM Series to JSA Series License Migration

- [Migrating Licenses from STRM Series to JSA Series on page 27](#)

CHAPTER 4

Migrating Licenses from STRM Series to JSA Series

This chapter includes the following topics:

- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [Obtaining the Serial Number of an STRM Series or a JSA Series Appliance on page 27](#)
- [STRM Series to JSA Series License Migration Assistance on page 28](#)

Migrating Licenses from STRM Series to JSA Series Overview

Juniper Networks supports the migration of licenses from Security Threat Response Manager (STRM) Series to any of the Juniper Secure Analytics (JSA) Series appliances.

To migrate STRM licenses to JSA, you need to access [License Management System \(LMS\)](#) or access LMS through the Juniper Customer Support Center (CSC). For more information, see [“STRM Series to JSA Series License Migration Assistance” on page 28](#).

Juniper Networks also supports the migration of licenses from STRM Series to any of the JSA virtual appliances. To migrate from STRM Series to any of the JSA virtual appliances, you need to purchase the virtual appliance license.

Related Documentation

- [Obtaining the Serial Number of an STRM Series or a JSA Series Appliance on page 27](#)
- [STRM Series to JSA Series License Migration Assistance on page 28](#)
- [JSA Series Appliance on page 3](#)
- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)

Obtaining the Serial Number of an STRM Series or a JSA Series Appliance

The serial number for an STRM or a JSA appliance is a 16-digit number, for example, 0249032008000081. You can locate the serial number label on the back of the appliance.

To obtain the serial number of an STRM or a JSA appliance remotely:

1. Using SSH, log in to your STRM or JSA appliance as the root user.
2. Run the following **dmidecode** command to retrieve the serial number of the appliance:
dmidecode -s system-serial-number

Related Documentation

- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [STRM Series to JSA Series License Migration Assistance on page 28](#)
- [JSA Series Appliance on page 3](#)
- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)

STRM Series to JSA Series License Migration Assistance

To migrate Security Threat Response Manager (STRM) licenses to Juniper Secure Analytics (JSA):

1. Go to [License Management System \(LMS\)](#) or access LMS through the Juniper Customer Support Center (CSC).
2. Log in to LMS with your username and password.
3. Under Generate Licenses, select **Secure Analytics (STRM)** from the list and then click **GO**.
4. Select **Secure Analytics (STRM) Appliance** and then click **Continue**.
5. To transfer unlocking keys to a JSA appliance:
 - a. Click **Transfer unlocking keys to Secure Analytics devices**.
 - b. Enter the serial number of the STRM appliance in **Transfer From Serial Number** and the serial number of the JSA appliance in **Transfer To Serial Number**.

After the availability of the software licenses to transfer is confirmed, LMS starts transferring the license and generates new unlocking keys.

- c. Go to Step 7.
6. To transfer unlocking keys to the multiple JSA appliances:
 - a. Click **Transfer unlocking keys to Secure Analytics devices**.
 - b. Click **Transfer unlocking keys to multiple Secure Analytics devices** to transfer license keys from multiple STRM appliances to JSA appliances, and then follow the instructions provided on the page.

LMS initiates the license transfer in the background. Once the license transfer is complete, you will receive an e-mail notification.

7. Click **Review**.

8. Click **Continue**.

NOTE: If the JSA appliance has the capacity already, then the capacity/key is archived. A new key is generated for the JSA appliance with the transferred capacity.

9. To enter the new license keys in your Secure Analytics appliances:

- a. Log in to the JSA WebUI.
- b. Click the Admin tab.
- c. On the navigation menu, click **System Configuration**.
- d. Click **System and License Management**.
- e. Select the host to which you want to apply the license.
- f. Select **Manage Licenses** from the Actions list.
- g. Click **Choose File**, and then browse for the required license file path.
- h. Select the license file you want to upload.
- i. Click **Save**.

The license key was updated successfully message appears.

- j. After closing the License window, click **Deploy License Changes**.

Related Documentation

- [Migrating Licenses from STRM Series to JSA Series Overview on page 27](#)
- [Obtaining the Serial Number of an STRM Series or a JSA Series Appliance on page 27](#)
- [JSA Series Appliance on page 3](#)
- [Configuration and Data Features for STRM and JSA Migration on page 4](#)
- [STRM Series to JSA Series Migration Overview on page 5](#)
- [Distributed STRM Environment to JSA Migration Overview on page 19](#)

PART 4

Index

- [Index on page 33](#)

Index

Symbols

#, comments in configuration statements.....	vii
(), in syntax descriptions.....	vii
< >, in syntax descriptions.....	vii
[], in configuration statements.....	vii
{ }, in configuration statements.....	vii
(pipe), in syntax descriptions.....	vii

A

adding	
new JSA managed host to JSA console.....	22
automatic updates	
running on the JSA appliance.....	14

B

backup STRM appliance	
running common image.....	9
braces, in configuration statements.....	vii
brackets	
angle, in syntax descriptions.....	vii
square, in configuration statements.....	vii

C

comments, in configuration statements.....	vii
configuration features	
cannot migrate from STRM to JSA.....	4
migrate from STRM to JSA.....	4
conventions	
text and syntax.....	vi
copying	
STRM event and flow data to JSA.....	13
curly braces, in configuration statements.....	vii
customer support.....	viii
contacting JTAC.....	viii

D

distributed STRM environment	
migrating to JSA.....	19
documentation	
comments on.....	vii

E

event and flow data	
copying from STRM to JSA.....	13
existing STRM	
pre-upgrade configuration backup.....	6
upgrade.....	7

F

font conventions.....	vi
-----------------------	----

I

installing	
JSA appliance.....	10
virtual JSA appliances.....	10
introduction	
migration.....	3

J

JSA	
copying event and flow data from STRM.....	13
installing.....	10
migrating from distributed STRM	
environment.....	19
obtaining serial number.....	27
reimaging to common image using the recovery	
partition.....	11
restoring backup from STRM.....	12
running auto update.....	14
JSA console	
adding to JSA managed host.....	22
migrating from STRM console.....	20
JSA managed host	
adding to JSA console.....	22
migrating from STRM managed host.....	21

L

license migration	
overview.....	27
license migration assistance	
STRM to JSA.....	28

M

manuals	
comments on.....	vii
migrating	
distributed STRM environment to JSA	
overview.....	19
STRM console to JSA console.....	20
STRM managed host to JSA managed host.....	21

