



Juniper Secure Analytics Virtual Appliance Installation Guide

Release
7.3.2



Modified: 2019-05-20

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

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.

Juniper Secure Analytics Virtual Appliance Installation Guide
7.3.2

Copyright © 2019 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 <https://support.juniper.net/support/eula/>. 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
	Creating a Service Request with JTAC	ix
Part 1	Virtual Appliance Installation	
Chapter 1	Virtual Appliance Installations for JSA and Log Manager	3
	Juniper Secure Analytics and Log Manager Installation Overview	3
	Overview of Supported Virtual Appliances	4
	JSA Virtual All-in-One	4
	JSA Virtual Distributed Event Processors	4
	JSA Virtual Distributed Flow Processors	5
	System Requirements for Virtual Appliances	5
	Creating Your Virtual Machine	10
	Installing the JSA Software on a Virtual Machine	12
	Adding Your Virtual Appliance to Your Deployment	15

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 <https://www.juniper.net/documentation/>.

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 <https://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>

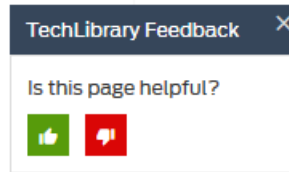
Table 2: Text and Syntax Conventions (continued)

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 <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	<code>stub <default-metric metric>;</code>
(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.	<code>broadcast multicast</code> <code>(string1 string2 string3)</code>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<code>rsvp { # Required for dynamic MPLS only</code>
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	<code>community name members [community-ids]</code>
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<code>[edit]</code> <code>routing-options {</code> <code> static {</code> <code> route default {</code> <code> nexthop address;</code> <code> retain;</code> <code> }</code> <code> }</code> <code>}</code>
;(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 system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- 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 Partner Support Service 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 <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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 <https://support.juniper.net/support/requesting-support/>.

PART 1

Virtual Appliance Installation

- [Virtual Appliance Installations for JSA and Log Manager on page 3](#)

CHAPTER 1

Virtual Appliance Installations for JSA and Log Manager

This chapter describes about the following section:

- [Juniper Secure Analytics and Log Manager Installation Overview on page 3](#)
- [Overview of Supported Virtual Appliances on page 4](#)
- [System Requirements for Virtual Appliances on page 5](#)
- [Creating Your Virtual Machine on page 10](#)
- [Installing the JSA Software on a Virtual Machine on page 12](#)
- [Adding Your Virtual Appliance to Your Deployment on page 15](#)

Juniper Secure Analytics and Log Manager Installation Overview

You can install JSA and Log Manager on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements.



NOTE: Resizing logical volumes by using a logical volume manager (LVM), and EFI installations are not supported.

To install a virtual appliance, complete the following tasks in sequence:

- [Creating Your Virtual Machine on page 10](#)
- [Installing the JSA Software on a Virtual Machine on page 12](#)
- [Adding Your Virtual Appliance to Your Deployment on page 15](#)



NOTE: Install no software other than JSA and Red Hat Enterprise Linux on the virtual machine.

Related Documentation

- [System Requirements for Virtual Appliances on page 5](#)
- [Creating Your Virtual Machine on page 10](#)

- [Adding Your Virtual Appliance to Your Deployment on page 15](#)

Overview of Supported Virtual Appliances

A virtual appliance is a Juniper Secure Analytics (JSA) system that consists of JSA software that is installed on a VMWare ESX virtual machine.

A virtual appliance provides the same visibility and functionality in your virtual network infrastructure that JSA appliances provide in your physical environment.

After you install your virtual appliances, use the deployment editor to add your virtual appliances to your deployment. For more information on how to connect appliances, see the *Juniper Secure Analytics Administration Guide*.

JSA Virtual All-in-One

This virtual appliance is a Juniper Secure Analytics (JSA) system that can profile network behavior and identify network security threats. The JSA Virtual All-in-One or JSA Virtual console deployment virtual appliance includes an on-board Event Collector and internal storage for events.

The JSA Virtual All-in-One or JSA Virtual console deployment virtual appliance supports the following items:

- 600k flows per minute max depending on the configuration of the VM
- 750 event feeds (additional devices can be added to your licensing)
- External flow data sources for NetFlow, sFlow, J-Flow, Packeteer, and Flowlog files
- Flow Processor and Layer 7 network activity monitoring

To expand the capacity of the JSA Virtual All-in-One or JSA Virtual console deployment beyond the license-based upgrade options, you can add one or more of the JSA Virtual Distributed Event or Flow processors or JSA Virtual Distributed Event or Flow processors virtual appliances.

JSA Virtual Distributed Event Processors

This virtual appliance is a dedicated Event Processor that allows you to scale your Juniper Secure Analytics (JSA) deployment to manage higher EPS rates. The JSA Virtual Distributed Event or Flow processors includes an on-board Event Collector, Event Processor, and internal storage for events.

The JSA Virtual Distributed Event or Flow processors appliance supports the following items:

- Up to 20k events per second, depending on the amount of CPU and RAM allocated
- 2 TB or larger dedicated event storage

The JSA Virtual Distributed Event or Flow processors virtual appliance is a distributed Event Processor appliance and requires a connection to any series appliance.

JSA Virtual Distributed Flow Processors

This virtual appliance is deployed with any series appliance. The virtual appliance is used to increase storage and includes an on-board Event Processor, and internal storage.

JSA Virtual Distributed Event or Flow processors appliance supports the following items:

- 600k flows per minute max depending on the amount of CPU and RAM allocated
- 2 TB or larger dedicated flow storage
- Flow Processor and Layer 7 network activity monitoring

You can add JSA Virtual Distributed Event or Flow processors appliances to any series appliance to increase the storage and performance of your deployment.

- Related Documentation**
- [Juniper Secure Analytics and Log Manager Installation Overview on page 3](#)
 - [Creating Your Virtual Machine on page 10](#)
 - [Adding Your Virtual Appliance to Your Deployment on page 15](#)

System Requirements for Virtual Appliances

To ensure that Juniper Secure Analytics (JSA) works correctly, ensure that virtual appliance that you use meets the minimum software and hardware requirements.

To install a virtual appliance, you must first use VMware vSphere Client to create a virtual machine. For more information, see [“Creating Your Virtual Machine” on page 10](#).

[Table 3 on page 5](#) describes the minimum requirements for virtual appliances.

Table 3: Requirements for Virtual Appliances

Requirement	Description
VMware client	VMware ESXi Version 5.0 VMware ESXi Version 5.1 VMware ESXi Version 5.5 VMware ESXi Version 6.0 For more information about VMWare clients, see the <i>VMware website</i> at www.vmware.com
Virtual disk size on appliance	Minimum: 256 GB NOTE: For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available. NOTE: After successful installation, extra disk space cannot be added.

[Table 4 on page 6](#) describes the minimum memory requirements for virtual appliances.

Table 4: Minimum and Optional Memory Requirements for JSA Virtual Appliances

Appliance	Minimum memory requirement	Suggested memory requirement
JSA Virtual Distributed Event processors	12 GB	48 GB
JSA Virtual Distributed Flow processors	12 GB	48 GB
JSA Virtual All-in-One or JSA Virtual console deployment	24 GB	48 GB
JSA Data Node Virtual appliance	12 GB	48 GB
Log Manager Virtual	24 GB	48 GB
JSA Risk Manager	24 GB	48 GB
JSA Vulnerability Manager Processor	8 GB	16 GB
JSA Vulnerability Manager Scanner	2 GB	4 GB

[Table 5 on page 6](#) describes the Log Manager all-in-one requirements.

Table 5: Log Manager All-in-One Requirements

Events Per Second	CPUs	RAM (GB)
100	4	12
200	4	12
500	4	12
1000	4	12
2500	4	12
5000	8	16

[Table 6 on page 6](#) describes the Log Manager Event Processor requirements.

Table 6: Log Manager Event Processor Requirements

Events Per Second	CPUs	RAM (GB)
100	4	12
200	4	12
500	4	12

Table 6: Log Manager Event Processor Requirements (continued)

Events Per Second	CPUs	RAM (GB)
1000	4	12
2500	4	12
5000	8	16
10000	16	24
20000	16	24

Table 7 on page 7 describes the Log Manager dedicated console requirements.

Table 7: Log Manager Dedicated Console Requirements

Console	CPUs	RAM (GB)
Virtual machine as console	4	12



NOTE: Console resource requirements can vary widely with usage.

Table 8 on page 7 describes the Threat Manager all-in-one requirements.

Table 8: Threat Manager All-in-One Requirements

Flows Per Minute	Events Per Second	CPUs
15000	100	4
25000	100	4
50000	100	4
15000	200	4
25000	200	4
50000	200	4
15000	500	4
25000	500	4
50000	500	8
15000	1000	8

Table 8: Threat Manager All-in-One Requirements (continued)

Flows Per Minute	Events Per Second	CPUs
25000	1000	8
50000	1000	8
100000	1000	12
200000	5000	16

[Table 9 on page 8](#) describes the Threat Manager event processor requirements.

Table 9: Threat Manager Event Processor Requirements

Events Per Second	CPUs	RAM (GB)
100	4	12
200	4	12
500	4	12
1000	4	12
2500	4	12
5000	8	16
10000	16	24
20000	16	24

[Table 10 on page 8](#) describes the Threat Manager flow processor requirements.

Table 10: Threat Manager Flow Processor Requirements

Flows Per Minute	CPUs	RAM (GB)
15000	4	12
25000	4	12
50000	4	12
150000	4	12
300000	8	16
600000	16	24

Table 11 on page 9 describes the Threat Manager dedicated console requirements.

Table 11: Threat Manager Dedicated Console Requirements

Console	CPUs	RAM (GB)
Virtual machine as console	4	12



NOTE: Console resource requirements can vary widely with usage.

Table 12 on page 9 describes the Vulnerability Manager processor requirements.

Table 12: Vulnerability Manager Processor Requirements

Event Per Second	CPUs	RAM (GB)	Disk Required
50000	2	16	500 GB
150000	2	16	750 TB
300000	2	16	1 TB

Table 13 on page 9 describes the Vulnerability Manager scanner requirements.

Table 13: Vulnerability Manager Scanner Requirements

Event Per Second	CPUs	RAM (GB)	Disk Required
20000	1	4	150 GB

Table 14 on page 9 describes the Risk Manager requirements.

Table 14: Risk Manager Requirements

Configuration Sources	CPUs	RAM (GB)	Disk Required
Up to 10000	8	48	1 TB

NOTE: Over 10,000 configuration sources, contact your sales representative

Table 15 on page 9 describes the disk space allocation (Events per second) requirements.

Table 15: Disk Space Allocation (Events Per Second) Requirements

Events Per Second	Retention Period	Disk Required
1000	14 days	1 TB
1000	28 days	2 TB

Table 15: Disk Space Allocation (Events Per Second) Requirements (continued)

Events Per Second	Retention Period	Disk Required
1000	90 days	6.5 TB

Table 16 on page 10 describes the disk space allocation (Flows per second) requirements.

Table 16: Disk Space Allocation (Flows Per Second) Requirements

Flows Per Minute	Retention Period	Disk Required
50,000	14 days	500 MB
50,000	30 days	1 TB
50,000	90 days	3 TB

Related Documentation

- [Juniper Secure Analytics and Log Manager Installation Overview on page 3](#)
- [Overview of Supported Virtual Appliances on page 4](#)
- [Adding Your Virtual Appliance to Your Deployment on page 15](#)

Creating Your Virtual Machine

To install a virtual appliance, you must first use VMware vSphere Client to create a virtual machine.

1. Select the host and choose **File > New > Virtual Machine**, and then click **Next**.
2. Select **Custom** In the Configuration pane of the Create New Virtual Machine window, and then click **Next**.
3. Enter a name for the virtual machine in the Name and Location pane, and then click **Next**.
4. Select the datastore in which you want to store the virtual machine files, and then click **Next**.
5. Select **Virtual Machine Version: 7** in the Virtual Machine Version pane, and then click **Next**.
6. Select **Linux** under Guest operating System and then select **Linux Red Hat Enterprise Linux 6 (64-bit)** under Version, and then click **Next**.

7. Configure the number of virtual processors that you want for the virtual machine on the CPUs page, and then click **Next**.

When you configure the parameters on the CPU page, you must configure a minimum of two processors. The combination of number of virtual sockets and number of cores per virtual socket determines how many processors are configured on your system.

[Table 17 on page 11](#) provides examples of CPU page settings you can use.

Table 17: Descriptions for Network Configuration Parameters

Number of Processors	Sample CPU Page Settings
2	Number of virtual sockets = 1 Number of cores per virtual socket = 2
2	Number of virtual sockets = 2 Number of cores per virtual socket = 1
4	Number of virtual sockets = 4 Number of cores per virtual socket = 1
4	Number of virtual sockets = 2 Number of cores per virtual socket = 2

8. In the **Memory Size** field, type or select **24 GB** and then click **Next**.

[Table 4 on page 6](#) describes the minimum memory requirements for virtual appliances.

9. To configure your network connections, perform the following steps:
 - a. Add at least one Network Interface Controller (NIC) for How many NICs do you want to connect.
 - b. Select **VMXNET3** for Adapter.
 - c. Select **Connect at Power On**.
 - d. Click **Next**.
10. Select **VMware Paravirtual** in the SCSI Controller pane, and then click **Next**.
11. Select **Create a new virtual disk** in the Select a Disk pane, and then click **Next**.

12. To configure the virtual disk parameters in the Create a Disk pane, perform the following steps:

- a. Select **256 or higher (GB)** in Capacity.



NOTE: After successful installation, extra disk space cannot be added.

- b. Select **Thin provisioning** in Disk Provisioning.
- c. Select **Store with the virtual machine** in Location.
- d. Click **Next**.

13. In the **Advanced Options** page, do not configure anything.

14. On the Ready to Complete page, review the settings and click **Finish**.

Related Documentation

- [Overview of Supported Virtual Appliances on page 4](#)
- [System Requirements for Virtual Appliances on page 5](#)
- [Adding Your Virtual Appliance to Your Deployment on page 15](#)

Installing the JSA Software on a Virtual Machine

After you create your virtual machine, you must install the JSA software on the virtual machine.

To install the JSA software on the virtual machine:

1. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
2. In the right pane, click the **Summary** tab.
3. Click **Power On** in the Commands pane to power on your machine.
4. Click **Edit Settings** in the Commands pane.
5. Click **CD/DVD Drive 1** in the left pane of the Virtual Machine Properties window.
6. Select **Datastore ISO File** under Device Type, and then click **Browse**.
7. Locate and select the JSA ISO file in the Browse Datastores window and click **Open** and then click **OK**.

8. Select the **Connect at power on** check box under Device Status.
9. Click **OK**.
10. After the JSA product ISO image is installed, right-click your virtual machine and click **Power > Reset** to reboot.
11. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
12. In the right pane, click the **Console** tab.
13. Log in to the virtual machine and type **linux**.
14. Ensure that the End User License Agreement (EULA) is displayed.



TIP: Press the Spacebar key to advance through the document.

15. Select **Skip** using Tab and press Enter to skip the media test and proceed with the installation process.
16. If you choose hardware type 7, select **OK** using Tab and press Enter in the Unsupported Hardware Detected screen.
17. Type **flatten**.

The installer partitions and reformats the hard disk, installs the OS, and then reinstalls the JSA product. You must wait for the flatten process to complete. This process can take up to several minutes. When the process is complete, a confirmation is displayed.
18. Type **SETUP** to begin the installation.
19. Select the appliance ID and select **Next** and press Enter.
20. For the type of setup, select **normal**. Select **Next** and press Enter.
21. For JSA console installations, select the **Enterprise** tuning template. Select **Next** and press Enter.
22. Choose one of the following options for time server:
 - **Manual**—Select this option to manually input the time and date.

To manually enter the time and date, type the current time and date. Select **Next** and press Enter.

The Current Date and Time window is displayed.

- **Server**—Select this option to specify your time server. Select **Next** and press Enter. The Enter Time Server window is displayed.

23. On the Time Zone Continent window, select your time zone continent or area. Select **Next** and press Enter.

24. On the Time Zone Region window, select your time zone region. Select **Next** and press Enter.

25. Select the Internet Protocol version:

- Select **Yes** to auto-configure JSA for IPv6. For more information, see *IPv6 addressing in JSA deployments* section in *Juniper Secure Analytics Administration Guide*.
- Select **No** to configure an IP address manually JSA for IPv4 or IPv6.

26. Select **Next** and press Enter.

27. Select the management interface. Select **Next** and press Enter.

28. In the wizard, enter values for the following parameters:

- **Hostname**—Type a fully qualified domain name as the system hostname.
- **IP Address**—Type the IP address of the system.
- **Network Mask**—Type the network mask address for the system.
- **Gateway**—Type the default gateway of the system.
- **Primary DNS**—Type the primary DNS server address.
- **Secondary DNS**—Optional. Type the secondary DNS server address.
- **Public IP**—Optional. Type the Public IP address of the server.
- **Email Server**—Type the e-mail server. If you do not have an e-mail server, type **localhost** in this field.

29. In the **New Root password** field, create a password that meets the following criteria:

- Contains at least 5 characters
- Contains no spaces
- Can include the following special characters: @, #, ^, and *

30. Select **Next** and press Enter.

31. Follow the instructions in the installation wizard to complete the installation. The installation process might take several minutes.
32. Apply your license key.
 - a. Log in to JSA.

https://<IP_Address_JSA>. The default **Username** is admin. The Password is the password of the root user account.
 - b. Click **login** to JSA.
 - c. Click the **Admin** tab.
 - d. In the navigation pane, click **System Configuration**.
 - e. Click the **System and License Management** icon.
 - f. From the **Display** list box, select **Licenses**, and upload you license key.
 - g. Select the unallocated license and click **Allocate System to License**.
 - h. From the list of licenses, select and license, and click **Allocate System to License**.

Your JSA software is successfully installed on the Virtual Machine.

Related Documentation

- [System Requirements for Virtual Appliances on page 5](#)
- [Creating Your Virtual Machine on page 10](#)
- [Adding Your Virtual Appliance to Your Deployment on page 15](#)

Adding Your Virtual Appliance to Your Deployment

After the JSA software is installed, add your virtual appliance to your deployment.

To add virtual appliance to your deployment:

1. Log in to the JSA console.
2. On the **Admin** tab, click the **Deployment Editor** icon.
3. In the Event Components pane on the Event View page, select the virtual appliance component that you want to add.

4. On the first page of the Adding a New Component task assistant, type a unique name for the virtual appliance.

The name that you assign to the virtual appliance can be up to 20 characters in length and can include underscores or hyphens.

5. Complete the steps in the task assistant.
6. From the Deployment Editor menu, click **File > Save to staging**.
7. On the Admin tab menu, click **Deploy Changes**.

8. Apply your license key.

To apply the license key:

- a. Log in to JSA.

The default **Username** is admin. The Password is the password of the root user account.

- b. Click **Login to JSA**.

- c. Click the Admin tab.

- d. In the navigation pane, click **System Configuration**.

- e. Click the **System and License Management** icon.

- f. From the Display list box, select **Licenses**, and upload your license key.

- g. Select the unallocated license and click **Allocate System to License**.

- h. From the list of systems, select a system, and click **Allocate System to License**.

Your virtual appliance is successfully added to your deployment.

Related Documentation

- [Juniper Secure Analytics and Log Manager Installation Overview on page 3](#)
- [Overview of Supported Virtual Appliances on page 4](#)
- [System Requirements for Virtual Appliances on page 5](#)