

How to Set Up Your JATP400 Appliance

Overview

Juniper Networks Advanced Threat Prevention 400 (JATP400) appliance is an advanced threat prevention platform that is designed to identify and prevent targeted attacks across multiple threat vectors. The appliance can be deployed as a Core device, Traffic Collector, Email Collector, Manager of Central Managers (MCM), Secondary Core, or as an All-In-One device.

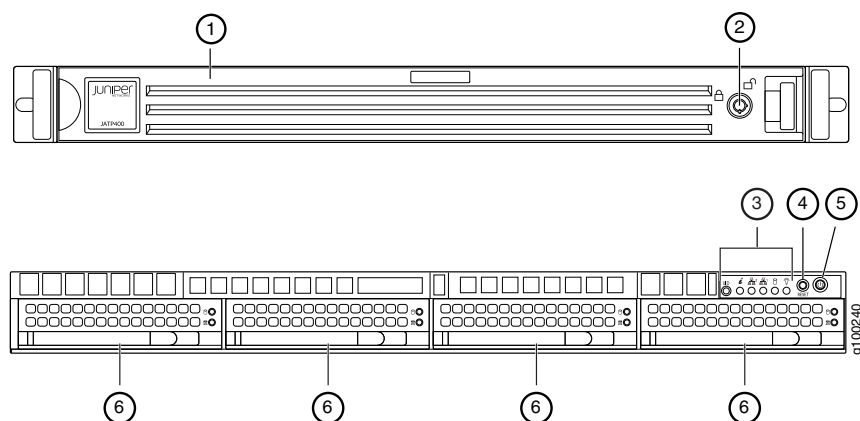
The JATP400 appliance is a 1-rack-unit (1-U), rack-mountable chassis with hot-swappable dual AC power supplies (or optional dual DC power supplies), four hot-swappable hard disk drives that support RAID, 32-GB memory, two 10-Gigabit Ethernet interfaces, two 10-Gigabit Ethernet SFP+ interfaces, and four 1-Gigabit Ethernet interfaces.

Package Contents

Verify that you have the following parts available:

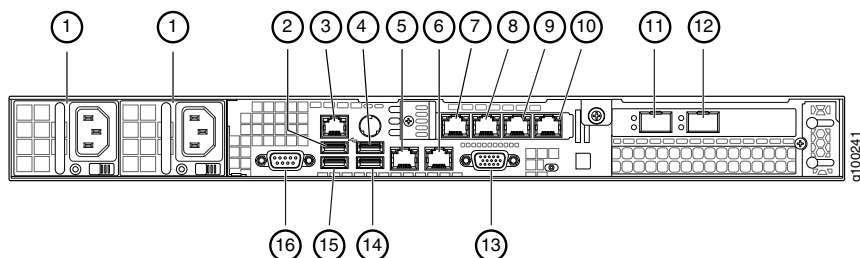
- JATP400 appliance
- End User License Agreement
- Product registration information
- Documentation roadmap card
- Front bezel
- 7 feet Ethernet cable, Qty 2
- DB-9 to RJ-45 adapter
- Rail kit
- Screws bag
- Rail adapters
- AC power cord, Qty 2

Front Panel



1—Front bezel	4—Reset button
2—Lock	5—Power button
3—LEDs	6—Hard drive

Back Panel

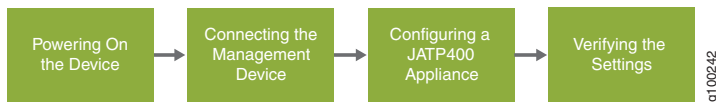


1—Power supplies	9—RJ-45 1-Gigabit Ethernet LAN port (eth2, Alternate exhaust interface)
2—USB1 (2.0)	10—RJ-45 1-Gigabit Ethernet LAN port (eth3)
3—Dedicated IPMI LAN port	11—10-Gigabit Ethernet SFP+ ports (eth5)
4—USB7 (3.0)	12—10-Gigabit Ethernet SFP+ ports (eth1), eth4 when this port is used as 1-Gigabit Ethernet copper port for traffic monitoring
5—10-Gigabit Ethernet LAN port (GLAN1, eth6). This port is not supported.	13—VGA port
6—10-Gigabit Ethernet LAN port (GLAN2, eth7). This port is not supported.	14—USB8 (3.0)
7—RJ-45 1-Gigabit Ethernet LAN port (eth0, management interface)	15—USB2 (2.0)
8—RJ-45 1-Gigabit Ethernet LAN port (eth4), eth1 when this port is used as 1-Gigabit Ethernet copper port	16—COM port. This port is not supported.

Specifications

Dimensions (H x W x D)	1.7 in. x 17.2 in. x 25.6 in.
Chassis weight	36 lbs (16.33 kg)
Power	<ul style="list-style-type: none"> 500 W AC-DC redundant power supply 650 W DC -DC redundant power supply

Initial Configuration Process



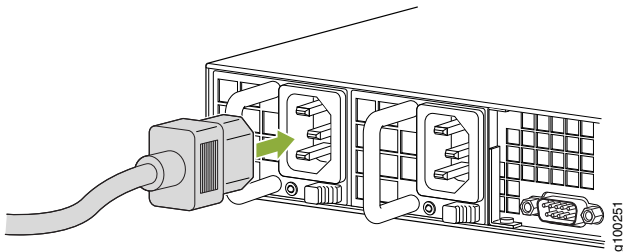
Step 1: Powering On the Appliance



CAUTION: Before connecting the appliance to the power supply, attach an ESD strap to an ESD point and fasten the other end of the strap around your bare wrist.

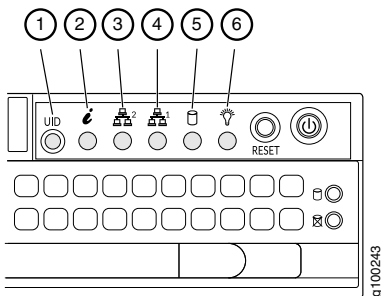
1. Plug the power cord into the AC receptacle on the rear panel.

If your appliance contains two power supplies, plug each of the power cords into each of the AC receptacles.



NOTE: Grounding for the appliances is provided through the power supply ground terminal. Ensure that you connect the AC power supply module in the appliance to a grounded AC power outlet by using an AC power cord (with the grounding pin) appropriate for your geographical location.

2. Plug the other end of the power cord into a wall socket.
3. Press the Power button on the front panel.
4. Note the following indications:



Use the reset button to reboot the appliance and the power button to power on or power off the appliance.

Callout	LED	State
1	UID button	Depressing the UID (unit identifier) button illuminates an LED on both the front and rear of the chassis for easy system location in large stack configurations. The LED will remain on until the button is pushed a second time.
2	Information	<ul style="list-style-type: none"> • Solid red—Indicates an overheat condition, which might be caused due to cable congestion. TIP: Check the routing of the cables if they are obstructing the airflow from the system. • Blinking red (1Hz)—Fan failure; check for an inoperative fan. • Blinking red (0.25Hz)—Power failure; check for an inoperative power supply. • Solid blue—Local UID has been activated. Use this function to locate the server in a rack environment. • Blinking blue (300 msec)—Remote UID is on. Use this function to locate the server from a remote location.
3	GLAN2	<ul style="list-style-type: none"> • Flashing—Indicates network activity on LAN port 2. • Steady—Indicates link.
4	GLAN1	<ul style="list-style-type: none"> • Flashing—Indicates network activity on LAN port 1. • Steady—Indicates link.
5	Hard drive	Indicates activity on a hard drive when flashing.
6	Power	<p>For AC power supply:</p> <ul style="list-style-type: none"> • Solid green—Indicates that the appliance is receiving power. • Solid amber—Indicates that the power supply is plugged in and turned off, or the system is off but in an abnormal state. <p>For DC power supply:</p> <ul style="list-style-type: none"> • Solid green—Indicates that the appliance is receiving power. • Solid amber—Indicates that the power supply is plugged in and turned off, or the system is off but in an abnormal state. • Amber (blinking)—Indicates that the system power supply temperature has reached 63° C. • The system powers down automatically when the power supply temperature reaches 70° C and restarts when the power supply temperature goes below 60° C.

Step 2: Connecting the Management Device

You can connect external devices to the JATP400 appliance using the ports on the back panel.

To connect a keyboard and monitor to the JATP400 appliance:

1. Connect the end of the keyboard cable to any of the USB ports on the back panel of the appliance.
2. Connect the end of the video monitor cable to the VGA port on the back panel of the appliance.

Step 3: Configuring a JATP400 Appliance

The following topics describe the steps to configure a JATP400 appliance:

- [Selecting the Form Factor on page 5](#)
- [Configuring the IP Address and Domain Name Servers on page 6](#)
- [Configuring the Device Host Name on page 6](#)

- [Configuring the Alternate Exhaust Interface on page 7](#)
- [Configuring the Device Basic Attributes on page 7](#)

Selecting the Form Factor

To select a form factor:

1. At the console prompt, log in to JATP with the following default credentials: username *admin* and the password *1JATP234*.



NOTE: The username is case sensitive.

2. Press **Enter**.

The End User License Agreement (EULA) appears.

3. Read the information and press the Spacebar to advance each window until you have reached the end of the agreement.

4. Type **Yes** to accept the agreement, and then press **Enter**.

5. Enter a new CLI admin password to change the default password and then press **Enter**.



NOTE: The password must be at least eight characters long.

6. Reenter the new password and then press **Enter**.

Juniper Networks Advanced Threat Prevention window appears.



NOTE: By default, the JATP400 is installed as an All-In-One appliance.

```
*****
*      Juniper Networks Advanced Threat Prevention Appliance      *
*                                                                  *
*****

***** Current Appliance form factor is All In One *****
1. Core/Central Manager
2. Traffic Collector
3. Email Collector
4. Return current form factor i.e All-In-One

Do you want to change the appliance form factor from an All-In-One to any of the above form factors (Yes/No)? Yes
Enter the number (1-2-3-4) to choose the desired form factor: 2
Are you sure you want to change the form factor to Traffic Collector (Yes/No)? Yes
***** Restarting services *****
***** Successfully changed the appliance form factor *****
Do you want to configure the system by using the configuration wizard (Yes/No)? █
```

7. Type **Yes** if you want to change the appliance form factor.



NOTE: If you type **No**, then:

- a. Type **Yes** to confirm that you do not want to change the appliance form factor.
- b. Proceed to [Step 10](#).

8. Enter a number from 1-4 to choose your desired form factor. For example, enter **2** to change the All-In-One to Traffic Collector form factor.
9. Type **Yes** to reconfirm to change the current form factor of the appliance.
Services are restarted and a successful confirmation message displays about the change of the form factor.
10. Type **Yes** to configure the system by using the configuration wizard.

Configuring the IP Address and Domain Name Servers

To configure the JATP network settings, enter the values for the following parameters:



NOTE: Use the up or down arrow keys to navigate the fields.

1. Type the IP address of the management interface (eth0).
2. Enter the network mask address for the eth0 interface.
3. Enter the default gateway for the eth0 interface.
4. Enter the primary DNS server for the eth0 interface.
5. (Optional) Type **Yes** and enter the IP address of the secondary DNS server for the eth0 interface.
6. (Optional) Type **Yes** and enter the search domain for the eth0 interface. For example, example.com.



NOTE: Provide a space to enter multiple search domains.

7. Type **Yes** and press **Enter** to restart the management (eth0) interface.



NOTE: The network interface restart can take up to more than 60 seconds.

Configuring the Device Host Name

To configure the device host name:

1. Enter a valid hostname. For example, JATP400.



NOTE: Enter a unique name for the host and do not include the domain.

Updates server to JATP400.example.com.

2. Type **Yes** to create a new SSL certificate for the JATP Appliance Server Web UI.



NOTE: If you decline the self-signed certificate by entering **No**, the JATP400 appliance will continue to use the existing certificates. These certificates might contain an incorrect hostname or fully qualified domain name (FQDN). To resolve this issue on the Web UI, regenerate a new self-signed SSL certificate or upload your private key and certificate. For more information on the certificates, see the *Managing Certificates* section in the *Operator's Guide*.

SSL self-signed certificate is regenerated successfully and the hostname will be updated after the next login.

```
*****
*      Juniper Networks Advanced Threat Prevention Appliance      *
*                                                                  *
*****

**** Setting the device host name ****
Please enter a valid hostname: JATP400
Updating server FQDN to JATP400.example.com
Regenerate the SSL self-signed certificate? (Yes/No)? yes
SSL Self-signed certificate re-generated successfully!
The hostname will be updated after the next login.
```

Configuring the Alternate Exhaust Interface

To configure the alternate exhaust interface:

1. (Optional) Type **No** to not to use the alternate exhaust interface for the analysis engine exhaust traffic.

Use the alternate exhaust interface for external connectivity in threat detection.



NOTE: You can configure alternate exhaust interface only for Core or All-In-One appliance.

Configuring the Device Basic Attributes

To configure basic server attributes:

1. Type **Yes** if the device is a Core, an All-In-One, or a Manager of Central Managers (MCM) system.



NOTE: If your device is a Traffic Collector, a Secondary Core, or an Email Collector, type **No** and enter the Core or All-In-One IP address.

2. Enter the device name.

3. Enter the device description.

4. Enter the device key passphrase.



NOTE: You must enclose white space and \ special characters in double quotation marks.

```

*****
*      Juniper Networks Advanced Threat Prevention Appliance      *
*                                                                  *
*****

***** Setting the device basic attributes *****
Please enter the following server attributes...
Is this a Central Manager device (Yes/No)? yes
Device name: JATP400
Device description: JATP400
Device key passphrase: *****
---Restarting all services---

```

5. Press **Enter** to complete the installation.

All services are restarted. You are now ready to access JATP.

6. Type **exit** and press **Enter**.

Step 4: Verifying the Settings

To verify the appliance configuration settings.

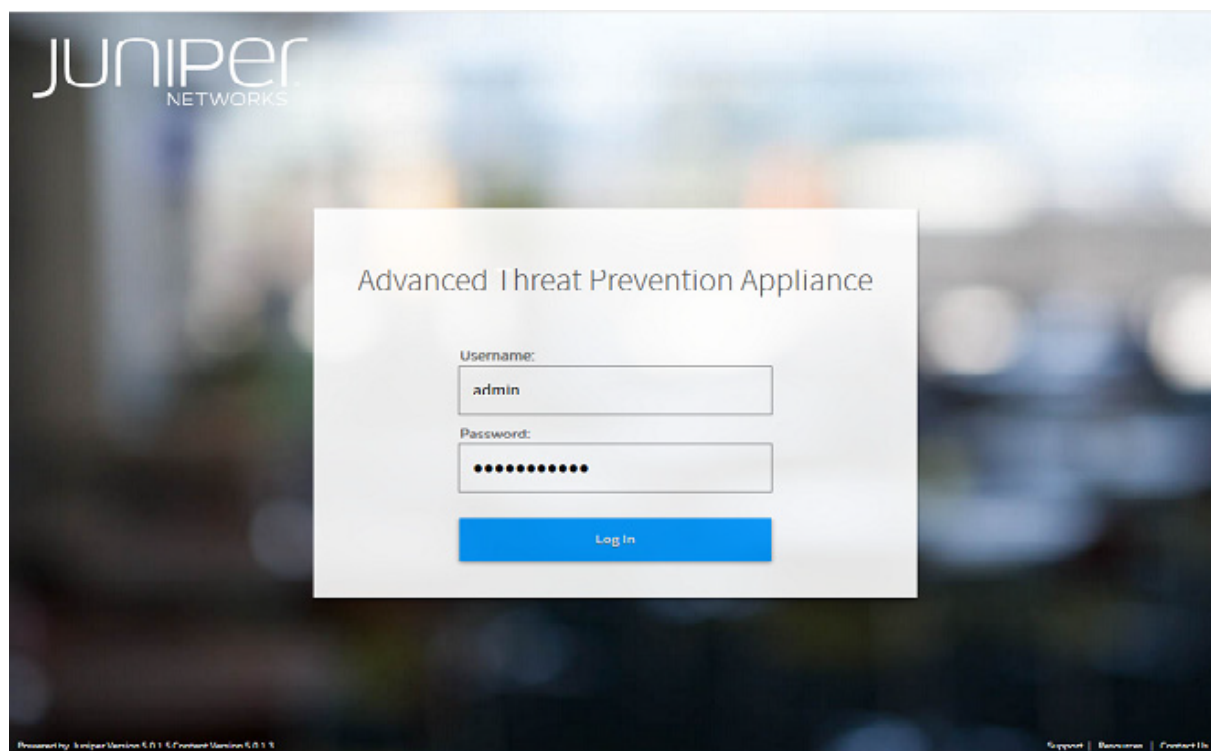
1. Open your Web browser.

2. Log in to your JATP appliance: <https://<IP Address>>

Where <IP Address> is the IP address of the JATP appliance.

3. Enter the default username *admin* and the default password *juniper*.

Ensure to change the default password after the login. The password must be at least eight characters long.



4. Click **Log In**.

With this step, you have successfully completed the configuration, and your JATP400 appliance is ready for use.

Powering Off the Appliance

You can power off the JATP400 appliance in one of the following ways:

- Graceful shutdown—Press and immediately release the *Power* button. Or

You can run the following command in the server configuration mode:

shutdown

- Forced shutdown—Press the Power button, and hold it for five seconds. Use this method only if the appliance is not responding to the graceful shutdown method.

References

- JATP Product Documentation
https://www.juniper.net/documentation/product/en_US/advance-threat-prevention-appliance
- JATP400 Hardware Documentation
https://www.juniper.net/documentation/en_US/release-independent/jatp/information-products/pathway-pages/hardware/jatp400-hw-guide.html
- Technical Support
<https://www.juniper.net/support/requesting-support.html>