Juniper Networks | Engineering Simplicity

Quick Start

Juniper Paragon Automation 2.0.0 Onboard Device Quick Start Guide

IN THIS GUIDE

Step 1: Begin

SUMMARY

This guide walks you through the steps to onboard a Juniper Networks® device to Paragon Automation, so that the device can be managed, provisioned, and monitored through automated workflows. Use this guide if you are a user with the Super User or Network Admin role in Paragon Automation.

IN THIS SECTION

Meet Juniper Networks Devices

You can onboard ACX, MX, and PTX devices listed in Supported Hardware to Paragon Automation and manage them.

Install the Device

Follow the instructions in the hardware documentation to unbox the device, mount it on a rack, and power on the device. For details about installing a device, see the device's Hardware Guide at https://www.juniper.net/documentation/.

Prerequisites

Ensure that the following prerequisites are fulfilled before you onboard a device to Paragon Automation:

1. Paragon Automation is installed. See Paragon Automation Installation Guide.
2. A Super User in Paragon Automation has:

   a. Created an organization and a site to which the device can be onboarded.

   b. Added one or more users with the Network Admin role.

   For more information, see Paragon Automation Quick Start Guide.
3. A Super User or a Network Admin has:
   - On Paragon Automation, created network resource pools, device and interface profiles, and a network implementation plan; see Paragon Automation Quick Start Guide.
   - On the device:
     - Checked if a firewall exists between Paragon Automation and the device. If a firewall exists, the firewall is configured to allow outbound access on TCP ports 443, 2200, 6800, and 32,767.
     - Configured static routes on the device to reach Paragon Automation by executing the following command:

       ```
       user@device# set routing-options static route 0.0.0.0/0 next-hop Gateway-IP-address
       ```

     - Configured a DNS server on the device to resolve domain names or allow the device to access an external DNS server (for example, 8.8.8.8).
     - Configured an NTP server on the device.

Step 2: Up and Running

IN THIS SECTION

To onboard a device to Paragon Automation, you must commit the outbound SSH command to connect with Paragon Automation, on the device. This method of onboarding a device by committing the outbound SSH commands is also referred to as "Adopting a Device".

You can onboard a device to Paragon Automation by using any of the following methods:

- Onboard a device without ZTP; see "Onboard a Device without ZTP" on page 3.
- Onboard a device by using ZTP; see "Onboard a Device by Using ZTP" on page 4.

Onboard a Device without ZTP

Paragon Automation provides the outbound SSH configuration that you can commit on the device to enable the device to connect with Paragon Automation.

To onboard a device without using ZTP:

1. Navigate to **Inventory > Network Inventory** on the Paragon Automation GUI.
2. On the Routers tab, click **Adopt Router**.
3. On the Router Adoption page, click the **Select Site** drop-down list to select the site where the device is installed.

   The outbound SSH configuration that is required for the device to establish a connection with Paragon Automation is displayed.
4. Click **Copy** to copy the CLI commands under the **Apply the following CLI commands to adopt a Juniper Device if it meets the requirements** section to clipboard.
5. Access the device by using SSH and log in to the device in configuration mode.
6. Paste the contents of the clipboard and commit the configuration on the device.

   The device connects to Paragon Automation and can be managed from Paragon Automation.

   After you adopt a device, you can verify connectivity status by running the following command on the device:

   ```
   user@host> show system connections |match 2200

   tcp 0 0 ip-address:38284 ip-address:2200 ESTABLISHED 6692/sshd: jcloud-stcp 0 0 <varname>ip-address</varname>:38284
   <varname>ip-address</varname>:2200 ESTABLISHED 6692/sshd:
   ```

   `Established` in the output indicates that the device is connected with Paragon Automation.

After the device is onboarded, the status of the device on the Inventory page (**Inventory > Devices > Network Inventory**) shows as Connected, You can now start managing the device. See Device Management Workflow.

Also, you can move the device to In Service after onboarding so that services can be provisioned on them. See Approve a Device for Service.

Onboard a Device by Using ZTP

Prerequisites:

- A network implementation plan should be configured for the device.
- The device should be zeroized or in its factory-default settings.
- A TFTP server reachable from the device.
- A DHCP server reachable from the device, with the ability to respond to the device with the TFTP server and configuration file (Python or SLAX script) name.

To onboard a device by using ZTP:

1. Create an onboarding script with the required configuration by:
   - Connecting to Paragon Automation GUI and copying the SSH configuration statements. For information on copying the onboarding configuration from the Paragon Automation GUI, see steps 1 to 4 of the "Onboard a Device without ZTP" on page 3.
   - Adding the configuration statements to an onboarding script. See "Sample Onboarding Script for Committing SSH Configuration on a Device" on page 5 for a sample of the onboarding script.
2. Upload the onboarding script to the TFTP server.
3. Configure the DHCP server with the onboarding script filename and path in the TFTP server.
4. Install the device, connect it to the network, and power on the device.

   For information about installing the device, see the respective Hardware guide at https://www.juniper.net/documentation/.

   After the device is powered on:

   a. The factory default settings in the device triggers a built-in script (**ztp.py**) which obtains the IP addresses for the management interface, default gateway, DNS server, TFTP server and the path of the onboarding script (Python or SLAX) on the TFTP server, from the DHCP server.

   b. The device configures its management IP address, static default route, and the DNS server address, based on the values obtained from the DHCP network.

   c. The device downloads the onboarding script, based on the values from the DHCP network, and executes it, resulting in the onboarding configuration statements being committed.

   d. The device opens an outbound SSH session with Paragon Automation based on the committed onboarding configuration.
5. After the device connects with Paragon Automation, Paragon Automation configures management and telemetry parameters including gNMI by using NETCONF. Paragon Automation also uses NETCONF to configure the interfaces and protocols based on the network implementation plan associated with the device.
6. Log in to the Paragon Automation GUI and view the status of device onboarding on the Inventory (**Inventory > Devices > Network Inventory**) page. After the device status changes to Connected, you can start managing the device. See Device Management Workflow for details.

Sample Onboarding Script for Committing SSH Configuration on a Device

The following is a sample of the onboarding script that is downloaded from the TFTP server to the device:

```
#!/usr/bin/python
from jnpr.junos import Device
from jnpr.junos.utils.config import Config
from jnpr.junos.exception import *
import sys

def main():
    config = "set system services ssh protocol-version v2\n\
set system authentication-order password\n\
set system login user jcloud class super-user\n\
set system login user jcloud authentication encrypted-password $6$Oi4IvHbFYT.XgXP7$43sTeEU7V0Uw3CBlN/
HFKQT.Xl2wsm6GEBaS9pfE9d3VrINIKBqlYlJfE2cTcHsCSSVboNnVtqJEaLNUBAfbu.\n\
set system login user jcloud authentication ssh-rsa \"ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCuVTpIyaDwBuB8aTVrzxDQO50BS5GtoGnMBkWbYi5EEc0n8eJGmmbINE8auRGGOtY/
CEbIHKSp78ptdzME0uQhc7UZm4Uel8C3FRb3qEYjr1AMJMU+hf4L4MYWYXqk+Y9RvnWBzsTO2iEqGU0Jk0y7Mev5z/
YI9r8u8MZlWKdQzegBRIkL4HYYOAeAbenNw6ddxRzAP1bPESpmsT+0kChu3jYg8dzKbI+xjDBhQsKCFfO5cXyALjBMI3beaxmXRV02UGCEBl
+5Xw6a3OCiP7jplr92rFBjbqgh/bYoJRYz1Rc3AirDjROQuDdpHRn+DuUjPlyV17QR9Qvwn4OAmWM9YKWS/
LZ375L8nacOHmlv4f0KETU4LScTFQXR6xiJ6RizEpO338+xmiVq6mOcv5VuXfNApdl8F3LWOxLGFlmieB4cEEyJ7MK9U+TgS7MlcAP
+XAeXYM2Vx1b+UCyYoEyDizaRXZvmP5BPpxpb5L2iuXencZMbbpEbnNX/sk3teDc=
jcloud@5c96fb73-4e3a-4d8b-8257-7361ef0b95e7\"\n\
set system services outbound-ssh client jcloud secret
f72b785d71ea9017f911a5d6c8c95f12a265e19e886f07a364ce12aa99c6c1ca072a1ccc7d39b3f8a7c94e7da761d1396714c0b32ef32b6e
7d3c9ab62cf49d8d\n\
set system services outbound-ssh client jcloud services netconf keep-alive retry 12 timeout 5\n\
set system services outbound-ssh client jcloud oc-term.cloud.juniper.net port 2200 timeout 60 retry 1000\n\
set system services outbound-ssh client jcloud device-id
5c96fb73-4e3a-4d8b-8257-7361ef0b95e7.0ad21cc9-1fd6-4467-96fd-1f0750ad2678\n\
set system root-authentication encrypted-password \"$6$OeRp2LWC$/
ZLm9CMiR.SeEunv.5sDksFHIkzafuHLf5f7sp1ZANYT0iiz6rk2A1d/4Bq1gmxBhEb1XFtskrocLD7VHvPU10\""
    dev = Device()
    dev.open()
    try:
        with Config(dev, mode="exclusive") as cu:
            print ("Loading and committing configuration changes")
            cu.load(config, format="set", merge=True)
            cu.commit()
    except Exception as err:
        print (err)
    dev.close()
```

```
if __name__ == "__main__":
    main()
```

Step 3: Keep Going

IN THIS SECTION

What's Next

Now that you've onboarded the device, here are some things you might want to do next.

If you want to	Then
Use Paragon Automation to manage and monitor your devices.	See User Guide

General Information

If you want to	Then
Find out more about the device life cycle management use case	SeeDevice Life Cycle Management Overview
Find out more about the observability use case	See Observability Overview
Find out more about the trust and compliance use case	SeeTrust and Compliance Overview
Find out how to use active, synthetic traffic to monitor your network.	See Active Assurance

(Continued)

If you want to	Then
Find out how to provision and monitor a network service	SeeService Orchestration

Learn With Videos

Our video library continues to grow! Here are some great video and training resources that will help you expand your knowledge of Juniper Network Products.

If you want to	Then
Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies.	See Learning with Juniper on Juniper Networks main YouTube page.
View a list of the many free technical trainings we offer at Juniper.	Visit the Getting Started page on the Juniper Learning Portal.