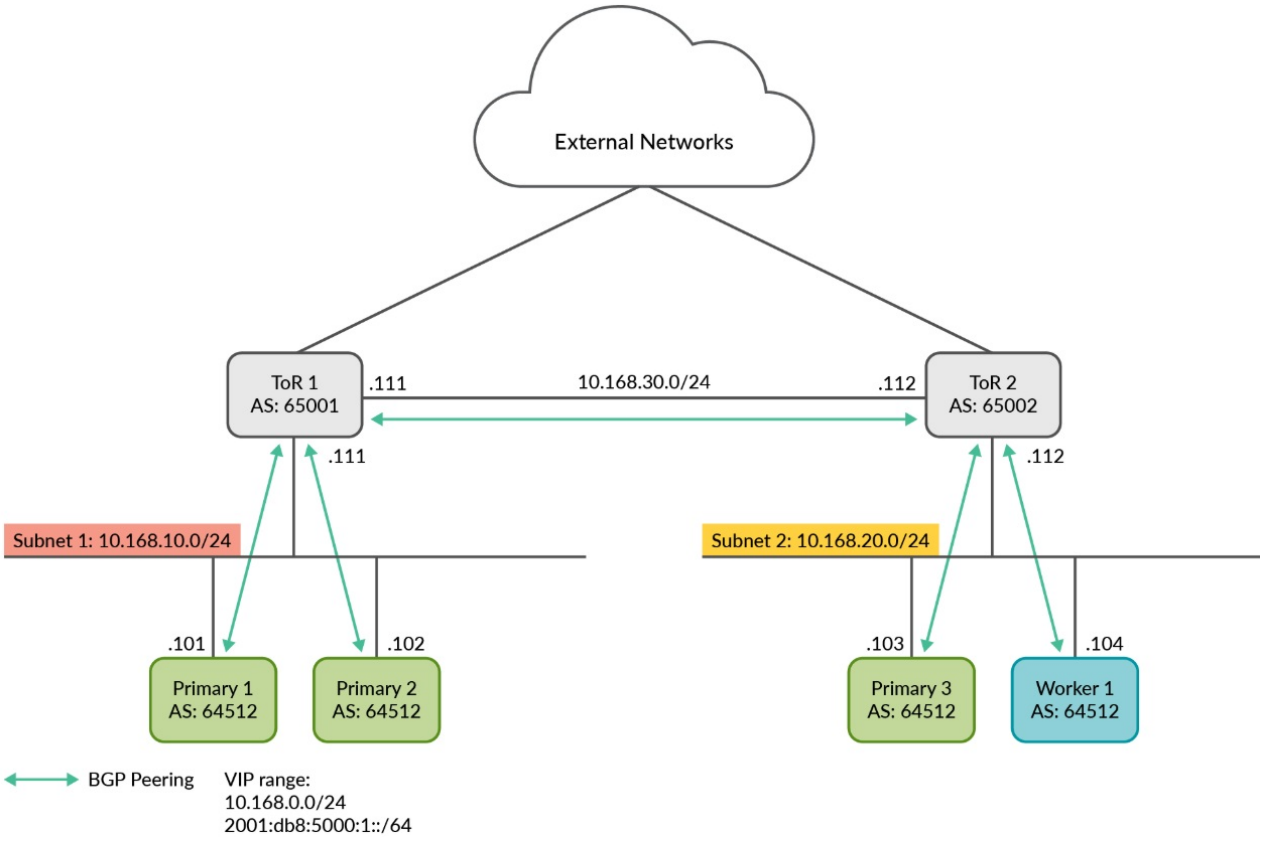
Contents [ hide ]

1 Juniper NETWORKS Routing Director 2.5.0
2 Begin
3 Device Onboarding Workflow
4 Install the Device
5 Prerequisites
6 Up and Running
7 Onboard a Juniper Device
8 Onboard a Device by Using ZTP
9 Onboard a non-Juniper Device
10 Keep Going
11 General Information
12 Learn with Videos
13 FAQ
14 Documents / Resources
14.1 References

# Juniper NETWORKS Routing Director 2.5.0




**Specifications:**

- Product Name: Juniper Routing Director 2.5.0 Onboard Device
- Supported Network Devices: ACX Series, MX Series, PTX Series, EX Series, QFX Series, SRX Series, Cisco Systems devices
- Requirements: A superuser role in Routing Director with organization and site setup

**Step 1:**

## Begin

**SUMMARY**

This guide walks you through the steps to onboard a router (both Juniper and non-Juniper) to Routing Director, 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 Routing Director.

**Supported Network Devices**

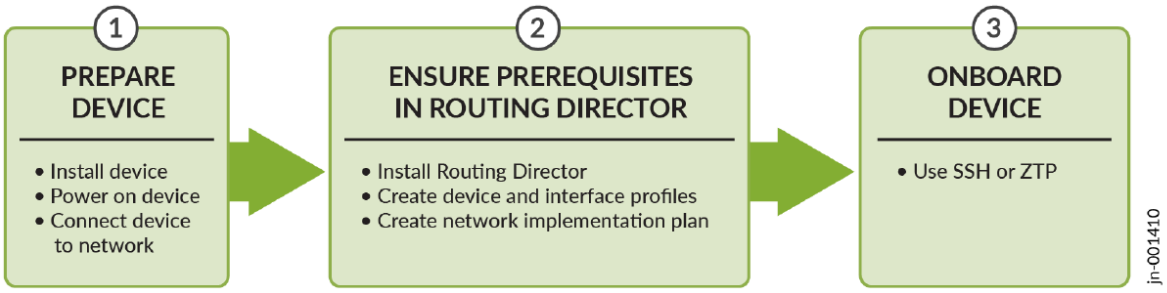
You can onboard ACX Series, MX Series, PTX Series, EX Series, QFX Series, SRX Series, and Cisco Systems devices listed in Supported Hardware to Routing Director

and manage them.

## Device Onboarding Workflow

Figure shows the workflow to onboard a device to Routing Director.

**Figure 1: Workflow to Onboard a Device to Routing Director**




## Install the Device

To install Juniper networks devices, 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/ .
To install devices from other vendors, follow instructions from the respective vendors.

## Prerequisites

Ensure that the following prerequisites are fulfilled before you onboard a device to Routing Director:

1. Routing Director is installed. See Install Routing Director.
2. A superuser in Routing Director has:
   - Created an organization and a site to which the device can be onboarded.
     For information to create an organization, see Add an Organization and to create a site, see Add a Site.
   - Added one or more users with the Network Admin role.
     For more information, see Invite Users.
3. A superuser or a network administrator has:
   - In Routing Director, created:

- Network resource pools; see Add a Resource Instance for details.
- Device profile; see Add a Device Profile for details.
- Interface profile; see Add an Interface Profile for details.
- Network implementation plan; see Add an Onboarding Plan for details.
- On the device, checked if a firewall exists between Routing Director and the device. If a firewall exists, the firewall is configured to allow outbound access on TCP ports 443, 2200, 6800, 4189, and 32,767, and UDP port 162.

**Step 2:**

## Up and Running

**SUMMARY**

To onboard a Juniper device to Routing Director, you must commit the outbound SSH command to connect with Routing Director, 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 Juniper device to Routing Director by using any of the following methods:

- Onboard a Juniper device; see “Onboard a Juniper Device” on page 4.
- Onboard a device by using ZTP; see “Onboard a Device by Using ZTP” on page 5.

To onboard a non-Juniper device, see “Onboard a non-Juniper Device” on page 7.

**NOTE:**

- Among non-Juniper devices, only Cisco Systems devices are supported in this release. For a list of supported Cisco Systems devices, see Supported Hardware.
- For devices to be onboarded and managed by Routing Director, the devices must either use IPv4 addressing or IPv6 addressing to connect with Routing Director. If some devices use IPv4 addressing and others use IPv6, Routing Director might not work as expected.
- For devices to be onboarded and managed by Routing Director, the devices must use either IPv4 addressing only or IPv6 addressing only to connect with Routing Director.

## Onboard a Juniper Device

Routing Director provides the outbound SSH configuration that you can commit on the device to enable the device to connect with Routing Director.
To onboard a Juniper device by committing the SSH configuration:

1. Navigate to Inventory > Network Inventory on the Routing Director GUI.
2. On the Routers tab, click Add Device.
3. On the Add Devices page, click Adopt Router.
4. (Optional) Click the Select Site drop-down list to select the site where the device is installed.
5. In the Select IP Version field, select the IP version (IPv4 or IPv6) to be used in the outbound SSH command for connecting with Routing Director.
   IPv4 is the default version used for the outbound SSH command.
6. Click Copy Cli Commands 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 and close OK.
7. Access the device by using SSH and log in to the device in configuration mode.
8. Paste the contents of the clipboard and commit the configuration on the device.

The device connects to Routing Director and can be managed from Routing Director. 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-s
Where, ip-address is the VIP address of Routing Director. Established in the output indicates that the device is connected with Routing Director. 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 the device. See Approve a Device for Service.

## Onboard a Device by Using ZTP

**Prerequisites:**

- (Recommended) A network implementation plan 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 (in Python or SLAX) by saving the outbound SSH configuration statements in a file. You can obtain the outbound SSH configuration statements by using the get Out bound Ssh Command REST API.
   See API Docs under the Help menu of the Routing Director GUI for information about using the API.
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:**
   - 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.
   - The device configures its management IP address, static default route, and the DNS server address, based on the values obtained from the DHCP network.
   - 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.
   - The device opens an outbound SSH session with Routing Director based on the committed onboarding configuration.
5. After the device connects with Routing Director, Routing Director configures management and telemetry parameters including gNMI by using NETCONF. Routing Director also uses NETCONF to configure the interfaces and protocols based on the

network implementation plan associated with the device.

6. Log in to the Routing Director 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
- $6$Oi4IvHbWNKI.XgXyy$43sTeEU7V0Uw3CBIN/HFKQT.Xl2wsm54HYaS9pfE9d3VrINIK
- set system login user jcloud authentication ssh-rsa \”ssh-rsa
- JJJJJU3NzaC1yc8EAAAADAQABAAABgQCuVTpLmaDwBuB8aTVrzxDQO50BS5GtoGn
  +
  5Xw6a3OCiP7jplr92rFBjbqgh/bYoJRYz1Rc3AirDjROQuDdpHRn+DuUjPlyV17QR9Qvwn4
- + XAeXYM2Vx1b+UCyYoEyDizaRXZvmP5BPpxpb5L2iuXencZMbbpEbnNX/sk3teDc=
  jcloud@5c96fb73-4e3a-4d8b-8257-7361ef0b95e7\”\n\
- set system services outbound-ssh client jcloud secret
  f72b785d71ea9017f911a5d6c8c95f12a265e19e886f07a364ce12aa99c6c1ca072a1ccc7c
- 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/4Bq1gmxBhEb1XFtskr
- 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()

## Onboard a non-Juniper Device

NOTE: In this release, you can onboard a non-Juniper device by using REST APIs. Onboarding a non-Juniper device by using GUI is a Beta feature and may not work as expected. See Help > API Docs for information about Routing Director REST APIs.

**To onboard a non-Juniper device:**

1. Navigate to Inventory > Network Inventory on the Routing Director GUI.
2. On the Routers tab, click Add Device.
3. On the Add Devices page, click Adopt a Device.
4. In the Add A Device section, enter the device details—Device name, IPv4 address and port, site, vendor, model, operating system, connection timeout (in minutes), and retry delay (in minutes).
5. (Optional) Under Authorization:
    - Enable Insecure when TLS is disabled on the device so that the connection with Routing Director is established without any encryption.
      If you enable this option, you don't need to upload any certificate.
    - Enable Skip Verify when TLS is enabled on the device and Routing Director should skip verifying the device's identity when the device establishes a connection.

Enable this option when TLS is enabled on a device and the device has a self-signed certificate that cannot be verified against a certificate authority.
NOTE: We recommend that you enable Insecure or Skip Verify only when security is not a major concern (for example, while testing connectivity in a lab). The connection between the device and Routing Director is vulnerable to man-in-the-middle attack when Insecure or Skip Verify are enabled.

6. If Skip Verify is disabled, under Certificates, upload:
   - TLS certificate for the device in Certificate.
   - Certificate key for the device in Key Certificate.
   - Root certificate of the Certificate Authority (CA) in Certificate Authority.
7. Under Credentials, enter username and password to authenticate the device.
8. Click + Add Device to add more devices.
9. Repeat step4 through step 8 to add more non-Juniper devices.
10. Click OK.

Routing Director connects with the device. You can now manage the device by using Routing Director. After the device connects with Routing Director, you can view the details of the device on the Inventory page (Inventory > Devices > Network Inventory).

**Step 3:**

## Keep Going

### 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 Routing Director to manage and monitor your devices. | See User Guide. |

## General Information

| If you want to | Then |
|---|---|

| | |
|---|---|
| Find out more about the device LCM use case. | See Device Life Cycle Management Overview. |
| Find out more about the observability use case. | See Observability Overview. |

| If you want to | Then |
|---|---|
| Find out more about the trust and compliance use case. | See Trust and Compliance Overview. |
| Find out how to use active, synthetic traffic to monitor your network. | See Active Assurance. |
| Find out how to provision and monitor a network service. | See Service Orchestration. |
| Find out how to optimize your network. | See Network Optimization Overview. |
| Find out more about planning and simulating network scenarios. | See Network Planner Overview |
| Learn to manage, monitor, maintain, automate, and orchestrate network devices and services using Juniper Routing Director. | See Implementing Juniper Routing Director |

### 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. |

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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. Copyright © 2025 Juniper Networks, Inc. All rights reserved.

### FAQ

Can I onboard devices from other vendors to Routing Director?

Yes, you can onboard devices from other vendors by following their respective instructions.

# Documents / Resources

| | |
|---|---|
| | Juniper NETWORKS Routing Director 2.5.0 [pdf] User Guide 2.5.0, Routing Director 2.5.0, Routing Director, Director 2.5.0 |

### References

- User Manual

JUNIPER NETWORKS

2.5.0, Director 2.5.0, JUNIPER NETWORKS, Routing Director, Routing Director 2.5.0

# Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

## Search:

e.g. whirlpool wrf535swhz

Search



This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.