JUNIPER NETWORKS | Engineering Simplicity

Day One+

Junos OS Evolved

IN THIS GUIDE

Step 1: Begin

IN THIS SECTION

In this guide, we provide a simple, three-step path, to quickly get you up and running with Junos OS Evolved. We've simplified and shortened the configuration steps, and included how-to videos. You'll learn how to configure and deploy Junos OS Evolved in your network.

NOTE: Are you interested in getting hands-on experience with the topics and operations covered in this guide? Visit Juniper Networks Virtual Labs and reserve your free sandbox today! You'll find the Junos Day One Experience sandbox in the stand alone category.

Meet Junos OS Evolved

Junos OS Evolved is a unified, end-to-end network operating system that provides reliability, agility, and open programmability for successful cloud-scale deployments. With Junos OS Evolved, you can enable higher availability, accelerate your deployments, innovate more rapidly, and operate your network more efficiently. We've aligned Junos OS Evolved with Junos OS so that you can seamlessly continue to manage and automate your network.

Initial Configuration

Have the following information ready before you begin to configure Junos OS Evolved on your networking device:

- A root password
- The hostname you want to use to identify the device
- The domain name you want to use
- The IP address of a DNS server
- The IP address of the default gateway

Here's how to configure Junos OS Evolved for the first time:

1. Connect a laptop or desktop PC to the console port on the front panel of the device.

2. Power on the device and wait for it to boot.

   Junos OS Evolved boots automatically. When the boot process is complete, you'll see the **re0 login:** prompt on the console.

3. Log in as the user **root**.

   Initially, you won't need a password for the root user account. The device prompt **[vrf:none] root@re0:~#** indicates that you are the root user.

4. Type **cli** to start the Junos OS Evolved CLI.

   ```
   [vrf:none] root@re0:~# cli
   root@re0>
   ```

5. Type **configure** to access CLI configuration mode.

   ```
   root@re0> configure
   [edit]
   root@re0#
   ```

6. Give a name to the device.

   We don’t recommend using spaces in the hostname.

   ```
   [edit]
   root@re0# set system host-name hostname
   ```

7. Configure the domain name of the device.

   ```
   [edit]
   root@re0# set system domain-name domain-name
   ```

8. Configure the IP address and prefix length for the management Ethernet interface on the device.

   The management Ethernet interface provides a separate out-of-band management network for the device.

   > **NOTE:** The management interface name is **re0:mgmt-*number*** for Routing Engine 0 and **re1:mgmt-*number*** for Routing Engine 1. If your device has a single Routing Engine, then the management interface name will be **re0:mgmt-*number***. The *number* parameter is normally “0” when using the RJ-45 management port. The number “1” is used when desired on platforms that also support a SFP based management port.

   ```
   [edit]
   root@re0# set interfaces management-interface unit 0 family inet address address/prefix-length
   ```

9. Configure a static (default) route for the management interface. In most cases your router will need to reach destinations that are not local to the management subnet. This route should point the a gateway that is directly reachable over the management network.

   ```
   [edit]
   root@re0# set routing-options static route 0.0.0.0/0 next-hop address
   ```

10. Configure the IP address of a backup or default network device.

    The backup device is used only when the routing protocol process (rpd) isn't running. This route is used on the primary RE during initial boot, and on the backup Routing Engine (which does not run rpd).

    If your device has two Routing Engines, the backup Routing Engine can be accessed through the configured backup device after the device boots. This enables you to access both the primary and the backup Routing Engine. (RE0 is the default primary Routing Engine.) Choose a backup device that’s directly connected to your device through the management interface. The default gateway is commonly used as the default backup device.

    ```
    [edit]
    ```

```
root@re0# set system backup-router address
```

11. Configure the IP address of a Domain Name System (DNS) server.

    The DNS server translates hostnames into IP addresses.

    ```
    [edit]
    root@re0# set system name-server address
    ```

12. (Optional) Disable automatic software downloads.

    By default, Junos OS will automatically download software upgrades using Zero Touch Provisioning (ZTP) when a device is booted. To disable this feature, delete the **auto-image-upgrade** statement under the **[edit chassis]** hierarchy level.

    ```
    [edit]
    root@# delete chassis auto-image-upgrade
    ```

13. Set the root password.

    Enter a plain-text password that the system will encrypt, or a password that is already encrypted, or an SSH public key string.

    - To enter a plain-text password:

      ```
      [edit]
      root@re0# set system root-authentication plain-text-password
      New password: type password
      Retype new password: retype password
      ```

    - To enter a password that is already encrypted:

      ```
      [edit]
      root@re0# set system root-authentication encrypted-password encrypted-password
      ```

    - To enter an SSH public key string:

      ```
      [edit]
      root@re0# set system root-authentication ssh-rsa key
      ```

14. Enable remote access using SSH.

    Refer to the documentation for information on enabling other access methods like Telnet or netconf. Note that by default the root user can only login on the console port, and that root login is not permitted over Telnet connections. In this example we enable remote access for the root user using ssh.

```
[edit]
root@re0# set system services ssh root-login allow
```

15. (Optional) Display the configuration statements.

```
[edit]
root@re0# show
system {
    host-name hostname;
    root-authentication {
        (encrypted-password "password" | public-key);
        ssh-rsa "public-key";
    }
    services {
        ssh {
            root-login allow;
        }
    }
    domain-name domain.name;
    backup-router address;
    name-server {
        address;
    }
    interfaces {
        re0:mgmt-0* {
            unit 0 {
                family inet {
                    address address/prefix-length;
                }
            }
        }
    }
}
```

You'll see the management interface name that you configured in place of **re0:mgmt-0** in the **show** command output.

16. (Optional) Disable DHCP.

DHCP services automate assigning network-parameters to network devices. The DHCP service process is enabled by default. To disable this feature, use the **dhcp-service disable** configuration statement at the **[edit system processes]** hierarchy level.

```
[edit]
root@# set system processes dhcp-service disable
```

17. Commit the changes to activate the configuration on the device:

```
[edit]
root@re0# commit
```

After committing the configuration, you’ll see the hostname you configured after the username in the CLI prompt, for example, **root@*hostname*#**.

Congratulations! The initial configuration is now complete.

18. Exit from CLI configuration mode.

```
[edit]
root@ hostname# exit
root@ hostname>
```

Back Up the Configuration

After you commit the configuration and the new configuration is running successfully, run the **request system snapshot** command to back up the new software to the file system on your hard drive. If you don’t run the **request system snapshot** command, the configuration on the backup device will be out-of-sync with the configuration on the primary device. Depending on the device model you may need to insert a supported USB storage device for the snapshot to succeed.

Step 2: Up and Running

Configure User Accounts

You can add new user accounts to the device's local database. User accounts enable authorized users to access the device. You can control the permissions and access privileges of user accounts through login classes. Multiple login classes can be assigned per user account, and you can define as many login classes as you need.

The login password must meet the following criteria:

- The password must be at least six characters long.
- You can include most character classes in a password (alphabetic, numeric, and special characters), but you cannot use control characters.
- The password must contain at least one change of case or character class.

In this example, we show you how to create a login class named **operator-and-boot**. You'll assign this login class permissions to use the clear, network, reset, trace, and view commands. Then you'll assign the login class to a username and define the encrypted password for the user. You’ll also assign the login class **super-user** authentication privileges.

NOTE: This example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

Here's how you configure user accounts:

1. Set the name of the login class, and allow use of the **reboot** command.

```
[edit system login]
root@ hostname# set class operator-and-boot allow-commands “request system reboot”
```

2. Set the permissions for the login class.

```
[edit system login]
root@ hostname# set class operator-and-boot permissions [clear network reset trace view]
```

3. Define the user name, bind the user to the *operator-and-boot* class, and configure a pre-encrypted password for the user.

   NOTE: In the below step you are entering a pre-encrypted password. You can use the **plain-text-password** argument if you wish to enter a clear text password that will then be encrypted.

```
[edit system login]
root@ hostname#set user name class operator-and-boot authentication encrypted-password $1$ABC123
```

4. From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, try the configuration instructions in this example again.

```
[edit]
root@ hostname# show system login
  class operator-and-boot {
  permissions [ clear network reset trace view ];
  allow-commands "request system reboot";
}
user name {
  classoperator-and-boot;
    authentication {
    encrypted-password "$1$ABC123";
  }
}
```

5. If you are done configuring the device, enter **commit** from configuration mode to apply the configuration.

Step 3: Keep Going

Congratulations! You've completed the initial configuration for Junos OS Evolved. Here are some things you can do next:

Table 1: User Access

If you want to	Then
Recover the root password for your device	See Recover a Root Password in the User Access and Authentication Administration Guide for Junos OS Evolved
Secure the console port to prevent unauthorized access	See Configuration Guidelines for Securing Console Port Access in the User Access and Authentication Administration Guide for Junos OS Evolved
Configure LLDP to allow networked devices to advertise information onto a LAN	See Device Discovery Using LLDP in the User Access and Authentication Administration Guide for Junos OS Evolved

Table 2: System Recovery and Upgrade

If you want to	Then
Configure a recovery snapshot so you can recover your files if you need to rollback after software installation.	See Backing Up an Installation Using Snapshots in the Junos OS Evolved Software Installation and Upgrade Guide
Configure a rescue configuration to ensure that you can always revert to a working configuration.	See Back up and Recover the Configuration in the Junos OS Evolved Software Installation and Upgrade Guide
Upgrade or reinstall Junos OS Evolved.	See Install, Upgrade, and Downgrade Software in the Junos OS Evolved Software Installation and Upgrade Guide

Table 3: General Information

If you want to	Then
Download, activate, and manage your Junos OS Evolved software license	See Activate Junos OS Licenses in the Juniper Licensing Guide
Learn about new and changed features, limitations, and known and resolved problems in the hardware and software	Visit the Junos OS Evolved Release Notes

Table 3: General Information *(continued)*

If you want to	Then
Learn more about the fundamentals of Junos OS Evolved	Read Introducing Junos OS Evolved
Learn how to configure common system management features on devices running Junos OS Evolved	Visit the Getting Started Guide for Junos OS Evolved