



Redhat Installer

support@peersoftware.com

©1993-2025 Peer Software, Inc. All Rights Reserved

Updated May 2, 2025

Contents

1	PeerIQ Installation for Red Hat and Rocky Linux	2
1.1	Introduction	2
1.1.1	Purpose of this Document	2
1.1.2	Intended Audience	2
1.1.3	System Update (Recommended)	2
1.2	System Requirements	2
1.2.1	Supported Operating Systems	2
1.2.2	Hardware Requirements	3
1.2.3	Software Requirements	3
1.3	Installation of PeerIQ	3
1.3.1	Task 1. Extract the Provided Tar File	4
1.3.2	Task 2. Run Installer Script	4
1.3.3	Task 3. Complete Installation through the PeerIQ Service Administration interface	5
1.3.4	Services Added to the System	5
1.4	Networking and Firewall Settings	6
1.4.1	Default Inbound Ports	6
1.4.2	Outbound Internet Traffic	6
1.4.3	Local Network Outbound (LAN Traffic)	7
1.4.4	Optional Services Local Network Outbound (LAN Traffic)	7

1 PeerIQ Installation for Red Hat and Rocky Linux

1.1 Introduction

1.1.1 Purpose of this Document

This manual provides instructions and requirements for installing and configuring the PeerIQ solution on a supported Red Hat Enterprise Linux (RHEL) or Rocky Linux 9.2 system. It outlines system prerequisites, network requirements, essential packages, and services to ensure a successful deployment.

1.1.2 Intended Audience

This document is designed for **system administrators** and **technical personnel** responsible for the installation, configuration, and maintenance of the PeerIQ platform. Familiarity with Linux system administration, networking, and basic command-line tools is assumed.

1.1.3 System Update (Recommended)

It's generally good practice to ensure the underlying operating system is fully updated before installing PeerIQ. You can do this by running the following:

```
sudo dnf update
```

Keeping your OS up to date helps prevent dependency conflicts and ensures the latest security patches are in place.

1.2 System Requirements

1.2.1 Supported Operating Systems

- Red Hat Enterprise Linux (RHEL) 9.2 or later
- Rocky Linux 9.2 or later

Note: If you wish to install PeerIQ on other distributions or versions, please review with Peer Software support prior to attempting an install.

1.2.2 Hardware Requirements

- **CPU:** Minimum 4 cores
- **Memory:** Minimum 8 GB RAM
- **Storage:** Minimum 120 GB HDD

In deployments with larger numbers of volumes and agents, higher specifications may be required.

1.2.3 Software Requirements

All software components are installed via the `dnf` or `pip` package manager. The installer script handles the installation of these dependencies automatically when run as **sudo**.

The PeerIQ installation process requires the following packages.

- Common System Packages:
 - `getopt`
 - `util-linux`
 - `sort`
 - `coreutils`
- Additional Packages:
 - `whiptail`
 - `newt`
 - `jq`
- PeerIQ-Specific Packages:
 - `Podman v5.2.0` or later (Older versions of Podman will be upgraded by the installer as needed).
 - `Podman-Compose`
 - `Python3-Pip`

1.3 Installation of PeerIQ

PeerIQ is a container-based solution. It leverages **podman** to manage containers and includes two `systemd` services to simplify administration and startup routines.

1.3.1 Task 1. Extract the Provided Tar File

The installation package for PeerIQ is provided as a `peeriq_redhat_xxxxxx.tar` file.

To extract the contents of this tar file, run the following command:

```
tar -xvf peeriq_redhat_xxxxxx.tar
```

This will extract 4 files

- `config.json`
- `docker-compose.yml`
- `installer.sh`
- `start_peeriq.sh`

If any of these files are missing, please contact Peer Software support.

1.3.2 Task 2. Run Installer Script

Run the `installer.sh` and follow the instructions.

```
sudo ./installer.sh
```

Important: The PeerIQ installer script must be run with **sudo or root privileges** to properly install packages, configure services, and set up firewall rules.

Follow the steps through the installation wizard. Once complete, you will be presented with the following message:

The PeerIQ Software Updater was successfully installed.

Please log into the PeerIQ Software Updater web interface to complete the PeerIQ installation:

`https://<ip>:4443`

1.3.3 Task 3. Complete Installation through the PeerIQ Service Administration interface

Navigate to the provided web URL in the message to select which version of PeerIQ to install.

Important: You must log in to the PeerIQ Software Updater interface using Linux credentials for an account on the server that has sudo privileges.

If you require assistance in this stage, please see the Updating PeerIQ section in the PeerIQ user guide.

1.3.4 Services Added to the System

Two systemd services are installed and managed automatically by PeerIQ:

peeriq_software_updater.service

- **Purpose:**
 - Hosts the PeerIQ service administration web portal, used for software updates and container restarts.
- **Behavior:**
 - Runs continuously, monitoring and updating PeerIQ components.
 - By default, listens on **TCP 4443** (HTTPS), though it can be changed during installation.

peeriq_startup.service

- **Purpose:**
 - Automatically starts the PeerIQ container stack on system boot.
- **Behavior:**
 - Ensures containers are up and running after any system restart.
 - Enabled and started automatically by the installer.

1.4 Networking and Firewall Settings

1.4.1 Default Inbound Ports

1. TCP 4430

- Main PeerIQ web interface (HTTPS).

2. TCP 4443

- PeerIQ service administration and software updater portal.

3. TCP/UDP 5140 (*For internal use only*)

- **Rsyslog**: Used by the rsyslog service to receive logs from the `peeriq_service_administration.service`.
- This port is **not** exposed externally, as it is only used for internal log forwarding.

These default ports can be changed during the installation process. If you configure firewall settings using a different method, the following commands show the automatically applied rules. These can be modified as needed for alternative firewall solutions such as `nftables` or `ufw`.

```
sudo firewall-cmd --permanent \  
  --add-port=4430/tcp \  
  --add-port=4443/tcp \  
  --add-rich-rule \  
    'rule family="ipv4" \  
      'source address="127.0.0.1" \  
      'port port=5140 protocol=tcp accept' \  
  --add-rich-rule \  
    'rule family="ipv4" \  
      'source address="127.0.0.1" \  
      'port port=5140 protocol=udp accept' \  
  
sudo firewall-cmd --reload
```

1.4.2 Outbound Internet Traffic

A default Red Hat install doesn't typically block outbound connections. However, in a hardened security environment, PeerIQ requires outbound access to the following for updates, container images, and diagnostics:

1. Firmware/Software Updates

- <https://peerdownloads.blob.core.windows.net/>
- <https://downloads.peersoftware.com/>

2. Container Registry

- <https://peersoftware.azurecr.io>

3. Diagnostics

- [*.s3.amazonaws.com](https://s3.amazonaws.com)

4. System Updates (References for container images)

- RedHat
 - cdn.redhat.com
 - subscription.rhsm.redhat.com
- Rocky
 - *.rockylinux.org

1.4.3 Local Network Outbound (LAN Traffic)

- **Broker/PMC Connection**
 - Ports: TCP 61616/61617.
 - Required for PeerIQ receive data from the PMC and Agents.

1.4.4 Optional Services Local Network Outbound (LAN Traffic)

- **AD/OpenLDAP/Red Hat Identity Management**
 - Ports: TCP 389/636 (or custom).
 - Only required if PeerIQ is to be integrated with your directory service.