

Juniper Networks® CTPView Server Software Release 9.2R2

Published
2024-10-16

RELEASE

Table of Contents

About This Guide

Release Highlights

Resolved Issues in CTPView Release 9.2R2

Known Issues in CTPView Release 9.2R2

Required Install files

Recommended System Configuration for Hosting a CTPView Server

CTPView Installation and Maintenance Policy

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.2R2

Revision History

About This Guide

This release notes accompany Release 9.2R2 of the CTPView software. They describe device documentation and known problems with the software.

You can also find these release notes on the Juniper Networks CTP software documentation webpage, which is located at [CTP Series Release Notes](#).

Release Highlights

The following features or enhancements have been added to CTPView Release 9.2R2.

- SAToP bundles is now interoperable with Cisco.
- You can now configure Save/Restore CTP configuration feature in CTPView.
- CTPOS Release 9.2R2 is supported on CTP151 device only.

You can upgrade to CTPOS 9.2R2 from CTPOS 9.2R1 using CTPView 9.2R2.

Table 1: CTPOS Upgrade Path

Model / Platform	Existing CTPOS Version	Version Path
CTP151	9.1R1/9.1R2/9.1R3-x/ 9.1R5/9.1R6-x	9.1R1/9.1R2/9.1R3-x/ 9.1R5/9.1R6-x> 9.2R1 dual -> 9.2R2

- **Upgrading CTP node to 9.2R2 using CTPView 9.2R2**
 1. First, dual upgrade the CTP Node to 9.2R1.
 2. Then, to upgrade the CTP node to 9.2R2 using CTPView, copy `ctp_complete_9.2R2_241015.tgz` in `/ctp` of CTPView 9.2R2.
 3. Select **Node Maintenance > Upgrade CTP Software**.

Resolved Issues in CTPView Release 9.2R2

The following issues have been resolved in CTPView Release 9.2R2.

- SAToP bundles do not interoperate with Cisco [PR 1838126]
- Save/Restore CTP configuration feature is not able configure in CTPView [PR 1841562]

Known Issues in CTPView Release 9.2R2

The following PR is a known issue.

- SSH fails after CTP151 dual upgrade to CTPOS 9.2R1 from CTPView. [PR 1830027]

NOTE: You cannot configure PBS in CTPView 9.2R2.

Required Install files

It is your responsibility to install CentOS on a VM, and the CentOS version must be 7.5.1804 (http://vault.centos.org/7.5.1804/isos/x86_64/).

Installing newer releases of Centos are not supported you must use Centos 7.5.1804. If you have queries or need further assistance, contact Juniper Networks Technical Assistance Center (JTAC).

Following file is provided for installing the CTPView software:

Table 2:

File	CTPView Server OS	Filename	Checksum
Software and Centos OS updates	Centos 7.5	CTPView-9.2R-2.0.el7.x86_64.rpm	4ef2dc5242a8e2cbe7c63b26f9d73a5c

Table 2: (Continued)

File	CTPView Server OS	Filename	Checksum
Web Update		web_update_9.2R2_241015.tgz	4abbe47e7ad7c496a7f144167f5a4e40

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.2R2 server:

- CentOS 7.5.1804 (64-bit)
- 1x processor (4 cores)
- 4 GB RAM
- Number of NICs – 2
- 80 GB Disk space

CTPView Installation and Maintenance Policy

From the release of CTPView 9.0R1, Juniper Networks has adopted a policy for installation and maintenance of the CTPView server. CTPView is now being distributed as an "Application only" product, in the form of an RPM package. You can now install and maintain the OS (CentOS 7.5) according to the guidelines described in [CTPView Network Management System Administration](#). This administration guide also has the complete installation procedure.

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.2R2

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.2R2. For more information about individual CVEs, see <http://web.nvd.nist.gov/view/vuln/search>.

Table 3: Critical or Important CVEs Included in bind

CVE-2023-3341	CVE-2023-4408	CVE-2023-50387	CVE-2023-50868
---------------	---------------	----------------	----------------

Table 4: Critical or Important CVEs Included in glibc

CVE-2024-2961	CVE-2024-33599	CVE-2024-33600	CVE-2024-33601	CVE-2024-33602
---------------	----------------	----------------	----------------	----------------

Table 5: Critical or Important CVEs Included in grub2

CVE-2022-2601

Table 6: Critical or Important CVEs Included in kernel

CVE-2023-3609	CVE-2023-32233	CVE-2023-35001	CVE-2023-42753
---------------	----------------	----------------	----------------

Table 7: Critical or Important CVEs Included in libssh2

CVE-2020-22218

Table 8: Critical or Important CVEs Included in linux-firmware

CVE-2020-12321	CVE-2023-20569	CVE-2023-20593	CVE-2023-20592
----------------	----------------	----------------	----------------

Table 9: Critical or Important CVEs Included in postgresql

CVE-2023-5869

Table 10: Critical or Important CVEs Included in python

CVE-2023-40217

Table 11: Critical or Important CVEs Included in openssh

CVE-2023-48795	CVE-2023-51384	CVE-2023-51385
----------------	----------------	----------------

Revision History

October 2024—Revision 1—CTPView Release 9.2R2

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 © 2024 Juniper Networks, Inc. All rights reserved.