JUNIPER
NETWORKS

Engineering
Simplicity

Juniper Networks® CTPView Server Software Release 9.1R6-2

Published
2025-02-11

RELEASE

Table of Contents

About This Guide

This release notes accompany Release 9.1R6-2 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 9.1R6-2.

- You can save a ctp config from a 9.1R6.1 CTPView.

- CTPView server is now able to authenticate via RADIUS when using IPv6.

Resolved Issues in CTPView Release 9.1R6-2

The following issues have been resolved in CTPView 9.1R6-2.

- Unable to save a ctp config from a 9.1R6.1 CTPView [PR 1852969]

- CTPView server unable to authenticate via RADIUS when using IPv6 [PR 1849190]

Known Issues in CTPView Release 9.1R6-2

The following PRs are known issues in both CTPView 9.1R6-2 and CTPOS 9.1R6-3 software.

- Unidirectional and Bi-directional remote CTP IPv6 bundle is not working on CTP151. [PR 1612155]

- L2Aggregator functionality is not working on CTP2000-IM8P-B and CTP2000-IM8P-MS-B cards. [PR 1781032]

- Provide support of CESoPSN Bundles over IPv6 only protocol and IPv4 and IPv6 protocol on CTP nodes. [PR 1290128]

- Remote and hairpin CTP IPv6 bundle is not working on MS-4WTO port. [PR 1618593]

- PBS functionality is not working on CTP2000 Series cards (CTP2000-IM8PT1E1-B, CTP2000-IM-8P-B, CTP2000-IM-8P-MS-B). [PR 1781033]

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 1:

File	CTPView Server OS	Filename	Checksum
Software and Centos OS updates This includes CTPView software and security updates.	Centos 7.5	CTPView-9.1R-6.2.el7.x86_64.rpm	c15fa971370ec1b402691e8935877b4e
This includes CTPView software.		web_update_9.1R6-2_250207.tgz	9a297af750acbefb3c4f0815db5d97c9

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.1R6-2 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 9.1R6-2

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R6-2. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 2: Critical or Important CVEs Included in grub2

CVE-2020-14372	CVE-2020-25632	CVE-2020-25647	CVE-2020-27749
CVE-2020-27779	CVE-2021-20225	CVE-2021-20233	

Table 3: Critical or Important CVEs Included in libxslt

CVE-2019-11068	CVE-2019-18197

Table 4: Critical or Important CVEs Included in unixODBC

CVE-2018-7409	CVE-2018-7485

Table 5: Critical or Important CVEs Included in curl

CVE-2022-43552

Table 6: Critical or Important CVEs Included in php-pear

CVE-2020-28948	CVE-2020-28949	CVE-2020-36193

Table 7: Critical or Important CVEs Included in rsyslog

CVE-2022-24903

Revision History

February 2025—Revision 1—CTPView Release 9.1R6-2