

Juniper Networks® CTPView Server Software Release 9.1R5

Published
2023-12-01

RELEASE

Table of Contents

About This Guide

Release Highlights

Resolved Issues in CTPView Release 9.1R5

Known Issues in CTPView Release 9.1R5

Required Install files

Recommended System Configuration for Hosting a CTPView Server

CTPView Installation and Maintenance Policy

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R5

Revision History

About This Guide

This release notes accompany Release 9.1R5 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 9.1R5.

NOTE:

- CTPOS 9.1R5 is CTP 151-specific. However, CTPView software can manage both CTP151 and CTP2000 Series devices, but note that version of the CTPOS image on CTP2000 Series devices must be less than CTPOS Release 9.1R5.
- You cannot use CTPView to perform the upgrade from 9.1Rx to 9.1R5.

However, you can manually upgrade from CTPOS 9.1Rx to 9.1R5 using CTPOS CLI. See [Table 1 on page 2](#)

- CTPView 9.1R5 release supports OpenSSL 3.0 that is FIPS 140-2 compliant. [PR 1580059]
- CTPView 9.1R5 release supports TLS 1.3. [PR 1626634]
- CTPView 9.1R5 release prevents old 7.3 configs from being restored to a 9.1 CTP. [PR 1730056]
- CTPView Node Synchronization page supports external reference of 10MHz. [PR 1737507]

Table 1: CTPView and CTPOS Release 9.1R5 Upgrade Matrix

Current software image on CTP151 platform is a:	then acorn_310_dual_image_upgrade_ctp151_211221.tgz is:	then acorn_310_9.1R3-1_211221.tgz is:
Single image with CTPOS 9.1R1 or 9.1R2	Supported Once the CTP151 device is up with 9.1R3 partition, you must manually copy the acorn_310_9.1R5_231017.tgz to /tmp on your CTP151 and run upgrade y to upgrade CTP151 from 9.1R3 to 9.1R5.	Not supported
Dual image with CTPOS 9.1R1 or 9.1R2 and CTPOS 9.1R3	Supported You can run this image from the current 9.1Rx image to reinstall 9.1R3. Then, you will have 9.1R3 on both partitions after the upgrade. Once the CTP151 device is up with 9.1R3, you must manually copy the acorn_310_9.1R5_231017.tgz to /tmp on your CTP151 and run upgrade y to upgrade CTP151 from 9.1R3 to 9.1R5.	Not supported

Resolved Issues in CTPView Release 9.1R5

The following issues have been resolved in CTPView Release 9.1R5.

- Cannot configure multiple CTPs from multiple admins simultaneously. [PR 1575773]
- Error when submitting node config. [PR 1695689]
- Buffer stats port files grow huge and fill up /var/www/. [PR 1716742]
- Bundle config change freezes GUI screen. [PR 1727332]

- GUI access denied CTPView 9.1R3.1 Server-Cert is expired. [PR 1740443]
- Some CTPView Netmon screens not populating. [PR 1749436]
- Update zlib to address CVE-2018-25032. [PR 1658343]
- Need instructions for renewing CTPView Self Cert. [PR 1670216]
- CTPView CVE hotfix needed. [PR 1732911]
- Radius SSH login does not roll back to local auth in CTPView 9.1R3.1 [PR 1737280]
- CTP groups may be empty when huge port issue happens. [PR 1758167]

Known Issues in CTPView Release 9.1R5

None.

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-9.1R-5.0-0.el7.x86_64.rpm	38c621e3f7eae3e5ac2626801a928463

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.1R5 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 9.1R5

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R5. For more information about individual CVEs, see <http://web.nvd.nist.gov/view/vuln/search>.

Table 3: Critical or Important CVEs Included in linux-firmware

CVE-2020-12321

Table 4: Critical or Important CVEs Included in openssl-libs

CVE-2022-0778

Table 5: Critical or Important CVEs Included in kernel

CVE-2022-0492

Table 6: Critical or Important CVEs Included in zlib

CVE-2018-25032

Revision History

November 2023—Revision 1—CTPView Release 9.1R5.

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 © 2023 Juniper Networks, Inc. All rights reserved.