

Juniper Networks® CTPView Server Software Release 9.1R6

Published
2024-06-12

RELEASE

Table of Contents

About This Guide

Release Highlights

Resolved Issues in CTPView Release 9.1R6

Known Issues in CTPView Release 9.1R6

Required Install files

Recommended System Configuration for Hosting a CTPView Server

CTPView Installation and Maintenance Policy

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R6

Revision History

About This Guide

This release notes accompany Release 9.1R6 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.

- CTPOS Release 9.1R6 is supported on both CTP151 and CTP2000 Series devices.
- Starting from CTPView 9.1R6, you can choose the 4th option `acorn_310_9.1R6_240329.tgz` from drop down in *CTPView Node Maintenance > Upgrade CTP Software* page.

NOTE:

- If you upgrade CTP Nodes to 9.1R6-1, you must logout and login again to your CTP Nodes to change the password of default CTP user accounts.
- CTP2000-IM-2W-FXS (existing version) is NOT supported in CTP2008-AC-04, CTP2008-DC-04, CTP2024-AC-04, CTP2024-DC-04, CTP2056-AC-04, or CTP2056-AC-04 chassis.

You can upgrade to CTPOS 9.1R6 from CTPOS 7.3R7/R8, 9.0R1, or 9.1R1/R2 through a two step upgrade process.

If you are upgrading a CTP2000 or a CTP151 platform to CTPOS 9.1R6, you must first upgrade to CTPOS 9.1R3-4, and then upgrade to CTPOS 9.1R6.

Here are the possible upgrade paths:

Table 1: CTPOS Upgrade Path

Model / Platform	Existing CTPOS Version	Version Path
CTP2000	7.3R7/R8	7.3R7/R8 > 9.1R3-4 > 9.1R6

Table 1: CTPOS Upgrade Path (Continued)

Model / Platform	Existing CTPOS Version	Version Path
CTP2000	9.0R1	9.0R1 > 9.1R3-4 > 9.1R6
CTP151	9.1R1/R2	9.1R1/R2 > 9.1R3-4 > 9.1R6

NOTE: CTPOS 9.1R3-4 is required to dual image your compact flash or SSD.

There are three ways through which you can upgrade to 9.1R6:

1. Using CTPView 9.1R6
2. Manually upgrading via the CTP shell
3. Using USB (only for CTP151)

Resolved Issues in CTPView Release 9.1R6

The following issues have been resolved in CTPView Release 9.1R6.

- Error when submitting CESoPSN Bundle on FXS port with multiple channels attached from CTPView. [PR 1733949]
- Remove yum command in CTPView. [PR 1755263]
- Add support of CTP Node upgrade from CTPView using acorn_310_9.1Rx_XXXXXX.tgz. [PR 1766296]
- Penetration Test: CTPView has SELinux disabled and missing CSP Header. [PR 1775838]
- Not able to configure bundles on M/S ports of (CTP2000-IM8PT1E1-B, CTP2000-IM-8P-B, CTP2000-IM-8P-MS-B) cards. [PR 1781039]
- Penetration Test: CTPView has Debug code, verbose server headers, missing CSRF and arbitrary files are created during directory traversal.. [PR 1783061]
- Penetration Test: Cookie discloses full application path and lacks Samesite Attribute. [PR 1783064]
- CTPView_9.1R6 upgrade using RPM package fails on 9.1R5 CTPView systems. [PR 1783448]

Known Issues in CTPView Release 9.1R6

The following PRs are known issues in both CTPView 9.1R6 and CTPOS 9.1R6 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 2:

File	CTPView Server OS	Filename	Checksum
Software and Centos OS updates	Centos 7.5	CTPView-9.1R-6.0-0.el7.x86_64.rpm	c15a65fbfe20646404894d75be9a518c

Recommended System Configuration for Hosting a CTPView Server

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

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R6. 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

June 2024—Revision 1—CTPView Release 9.1R6

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.