Juniper Networks® CTPView Server Software Release 9.1R3.1 Release Notes

Release 9.1R3.1
December 2021
Revision 1

These release notes accompany Release 9.1R3.1 of the CTPView Server Software. They contain install information and describe the enhancements to the software. The CTPView Release 9.1R3.1 software is compatible with Juniper Networks CTP Series platforms running CTPOS versions 7.3R7-1, 7.3R8, 9.0R1, 9.1R1, or 9.1R2 for the features supported on those releases. Features which were not available in the older CTPOS releases prior to 9.1R3.1, remain unavailable. They will be available for configuration once the CTP(s) are upgraded to 9.1R3.1.

NOTE: Release version *9.1R3.1* and *9.1R3-1* are interchangeable and synonymous.

You can also find these release notes on the Juniper Networks CTP Software Documentation webpage, which is located at https://www.juniper.net/documentation/product/en_US/ctpview.

Contents

Release Highlights

The following features or enhancements have been added to CTPView Release 9.1R3.1.

- Support is added for upgrading CTPOS from 9.0Rx to 9.1Rx using CTPView. [PR 1534404]
- Support is added for CTPOS Dual image upgrades using CTPView. [PR 1534405]
- Support is added for CTPView certificate with a large key size of 3072 or 4096. [PR 1544253]
- CTPView now supports setting up the hostname of a CTP device up to 25 characters long. [PR 1573307]
- Strong password requirement for default user accounts after firstboot following CTPView installation is now relaxed. [PR 1602910]
- Insensitive language in CTP product software and documents are removed to reflect gender neutrality, diversity, and inclusion. [PR 1542654]
- Support is added for PBS and L2Agg features. [PR 1534572]
- CESoPSN analog voice bundle support in CTPView 9.1R3 is reintroduced. [PR 1409293]

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.

Resolved Issues in CTPView Release 9.1R3.1

The following issue has been resolved in CTPView Release 9.1R3.1:

- GUI tacacs users cannot login; they see "Authentication Error". [PR 1546767]

Known Issues in CTPView Release 9.1R3.1

None.

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R3.1

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R3.1. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 1: Critical or Important CVEs Included in bind

CVE-2020-8625	CVE-2021-25215	CVE-2021-25214

Table 2: Critical or Important CVEs Included in glib2

CVE-2021-27219

Table 3: Critical or Important CVEs Included in glibc

CVE-2019-25013	CVE-2020-10029	CVE-2020-29573

Table 4: Critical or Important CVEs Included in kernel

CVE-2019-19532	CVE-2020-0427	CVE-2020-14351	CVE-2020-25211
CVE-2020-25645	CVE-2020-25656	CVE-2020-25705	CVE-2020-28374
CVE-2020-29661	CVE-2020-7053	CVE-2021-20265	CVE-2021-27363
CVE-2021-27364	CVE-2021-27365	CVE-2020-12362	CVE-2020-12363
CVE-2020-12364	CVE-2020-27170	CVE-2020-8648	CVE-2021-3347
CVE-2019-20934	CVE-2020-11668	CVE-2021-33033	CVE-2021-33034

Table 4: Critical or Important CVEs Included in kernel *(continued)*

CVE-2021-33909	CVE-2020-27777	CVE-2021-22555	CVE-2021-29154
CVE-2021-29650	CVE-2021-32399	CVE-2021-3715	

Table 5: Critical or Important CVEs Included in libxml2

CVE-2015-8035	CVE-2016-5131	CVE-2017-15412	CVE-2017-18258
CVE-2018-14404	CVE-2018-14567		

Table 6: Critical or Important CVEs Included in libX11

CVE-2021-31535

Table 7: Critical or Important CVEs Included in linux-firmware

CVE-2020-12321

Table 8: Critical or Important CVEs Included in microcode

CVE-2020-0543	CVE-2020-0548	CVE-2020-0549	CVE-2020-24489
CVE-2020-24511	CVE-2020-24512	CVE-2020-8695	CVE-2020-8696
CVE-2020-8698			

Table 9: Critical or Important CVEs Included in net-snmp

CVE-2020-15862

Table 10: Critical or Important CVEs Included in OpenSSL

CVE-2020-1971

Table 11: Critical or Important CVEs Included in perl

CVE-2020-10543	CVE-2020-10878	CVE-2020-12723

Table 12: Critical or Important CVEs Included in postgresql

CVE-2019-10208	CVE-2020-25694	CVE-2020-25695

Table 13: Critical or Important CVEs Included in python

CVE-2018-20852	CVE-2019-16056	CVE-2019-20907	CVE-2019-16935

Table 14: Critical or Important CVEs Included in sudo

CVE-2021-3156

Table 15: Critical or Important CVEs Included in screen

CVE-2021-26937

CTP Documentation and Release Notes

For a list of related CTP documentation, see https://www.juniper.net/documentation/product/en_US/ctpview.

If the information in the latest release notes differs from the information in the documentation, follow the *CTPOS Release Notes* and the *CTPView Server Release Notes*.

To obtain the most current version of all Juniper Networks technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Open a case with JTAC online at https://my.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

Revision History

December 2021—Revision 1, CTPView Release 9.1R3.1

Copyright © 2022 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.