

# Juniper Networks<sup>®</sup> CTPOS Release 9.1R3.1 Software Release Notes

Release 9.1R3.1  
December 2021  
Revision 1

This release notes accompany Release 9.1R3.1 of the CTPOS software. They describe device documentation and known problems with the software.

**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/ctp2008](https://www.juniper.net/documentation/product/en_US/ctp2008).

Contents	Release Highlights   2
	Upgrade Information   2
	Resolved Issues in CTPOS Release 9.1R3.1   3
	Known Issues in CTPOS Release 9.1R3.1   4
	Known Limitations in CTPOS Release 9.1R3.1   4
	Security Vulnerability Addressed in CTPOS Release 9.1R3.1   4
	CTP Documentation and Release Notes   4
	Requesting Technical Support   5
	Self-Help Online Tools and Resources   5
	Opening a Case with JTAC   6
Revision History   7	

# Release Highlights

The following features have been added to CTPOS Release 9.1R3.1.

- CTPOS 9.1R3.1 release supports creating dual image partitioning on the CompactFlash card. Dual image on the CompactFlash contains two logical images, where the first image consists first five partitions (1,5,6,7,8) and the second image consists five partitions (1,9,10,11,12). The first partition (bootable) is common to both images. You can upgrade any one of the images anytime after creating the dual image partitioning. [PR 1360833]
- All CTPOS 7.x features and bug fixes are now migrated to CTPOS 9.1R3. [PR 1361165]
- CESoPSN analog voice bundles are now supported. [PR 1417135]
- You can now upgrade from CTPOS 9.0Rx to CTPOS 9.1R3, while retaining the existing configuration. [PR 1428842]
- Support is added for CTP2000 and CTP150 platforms. [PR 1439855 and PR 1491003]
- Support is added for PBS and L2Agg features. [PR 1534569]
- Prevent upgrades of CTPOS 7.x installed on dual image CTP system. [PR 1535866]
- Insensitive language in CTP product software and documents are removed to reflect gender neutrality, diversity, and inclusion. [PR 1542648]
- Dual Image feature is enhanced to work on CTP151 platform. [PR 1576051 and PR 1616690]
- Support is added for **snmpwalk** and **snmpget** of sensors data on CTP150 and CTP151 platforms. [PR 1616678]

## Upgrade Information

You can upgrade to CTPOS 9.1R3.1 from older releases (7.x and 9.x) by using the dual image upgrade procedure only. The traditional upgrade using the "upgrade" utility will not be supported for upgrading CTPOS 9.1R3.1 from earlier releases ( 7.x and 9.x). Refer to the [Upgrading to CTPOS 9.1R3.1](#) guide for more information on how to perform the dual image upgrade procedure.

**NOTE:** The dual image feature is supported on the CTP150, CTP151, and CTP2000 (only PP332 and PP833 processors are supported, PP310 is not supported) platforms.

The dual image upgrade feature is supported on CTPOS 7.3R7-1 and above including 9.0R1, 9.1R1 and 9.1R2 releases. If you want to upgrade an older CTP, then you need to first upgrade to one of these releases.

There are a few older generation PP332 CPUs which will not support 9.1R3.1. The installation process will detect such CPUs and prevent the upgrade.

## Resolved Issues in CTPOS Release 9.1R3.1

Following issues have been resolved in CTPOS Release 9.1R3.1.

- rsync package is upgraded to fix error "**rsync error: error in rsync protocol data stream (code 12) at io.c(165)**". [PR 1335303]
- CTP bundle on IPv6 is not working in protocol mode-IPv4 and IPv6. [PR 1409765]
- Permission problem is observed on NTP drift.temp file. [PR 1446648]
- CTP boots up, but ethernet links are down. [PR 1459162]
- Menu does not always enforce the maximum PDV buffer settings. [PR 1467575]
- Error message during upgrade. [PR 1520725]
- CTP bundle counters show negative values. [PR 1527717]
- Invalid-NAK error seen during NTP sync with two server using authentication key. [PR 1541390]
- Destination port mirror using IPv6 cannot distinguish between local and remote address on 7.3R7. [PR 1558402]
- Strong password requirements for default user accounts relaxed for firstboot in CTPOS. [PR 1602909]
- Show correct data in plots when a new bundle is created on a port after deleting the existing bundle. [PR 1579681]

## Known Issues in CTPOS Release 9.1R3.1

This section lists the known issues in CTPOS Release 9.1R3.1.

- Unable to set GRUB password for CTP151. [PR 1543777]

## Known Limitations in CTPOS Release 9.1R3.1

- Support for legacy T1E1 DCARD is no longer available. [PR 1567520]
- Problem installing 9.1R3 on older PP332 CPUs. [PR 1609851]

## Security Vulnerability Addressed in CTPOS Release 9.1R3.1

- Weak key exchange algorithms disabled (diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1)

## CTP Documentation and Release Notes

For a list of related CTP documentation, see

[https://www.juniper.net/documentation/product/en\\_US/ctp2008](https://www.juniper.net/documentation/product/en_US/ctp2008).

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 post-sales 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, CTPOS 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.