

CTPOS 9.1R2.1 Circuit Emulation Software Release Notes

Release 9.1R2.1
March 2021

These release notes accompany Release 9.1R2.1 of the CTPOS Software. This document describes the enhancements, fixes as well as known issues with the software. CTPOS Release 9.1R2.1 runs on Juniper Networks CTP 151 platforms.

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

Note: Flash installation image is not provided for 9.1R2.1 release. Presently the only way to upgrade to 9.1R2.1 is manual/CTPView-based upgrade from CTPOS 9.1R1/9.1R2. CTPView 9.1R2.1 must be used for managing CTPOS 9.1R2.1 devices.

Please note that release version 9.1R2.1 and 9.1R2-1 are interchangeable and synonymous.

Release Highlights

CTPOS Release 9.1R2.1 is functionally like CTPOS Release 9.1R2. Please refer CTPOS 9.1R2 release notes for a complete list of features supported/not supported and defects fixed/not fixed in CTPOS 9.1R2.

CTPOS Release 9.1R2.1 release adds support for the new Octal T1/E1 framer (DS26518) which replaces the EOL version (DS26528) on the CTP T1/E1 interface modules. The required support has been provided through the following PR:

- [PR 1468092] Added support for switch from DS26528 to DS26518

Note: The CTPOS 9.1R2.1 release only supports the CTP151 platform (no other existing platforms: CTP2008, CTP2024, CTP2056, and CTP150).

Note: CLI syntax has changed for remotely executed commands

In 7.x CTPOS releases (and earlier) it is possible to use SSH to remotely access a CTP and issue "cmd" commands. Starting in CTPOS 9.x the syntax to do this has changed.

For instance, to check the CTPOS version in CTPOS 7.x you can run this command from another device (another CTP in this case):

```
[ctp_sa@ctp2008top ~ 1]> ssh ctp_cmd@192.168.1.10 cmd -v
```

```
CTPOS CLI version: 7.3R7 201101           // this is what the remote CTP returns
Compile Time: Sun Nov 01 2020 06:17:03 PM
Flash: Single Image
```

To issue the same command on CTPOS 9.x you must append the 'sudo' argument to the start of the command:
[ctp_sa@ctp2056-833-1 ~ 3]> ssh ctp_cmd@192.168.1.10 sudo cmd -v

CTPOS CLI version: 9.1R2-1 210302
Compile Time: Tue Mar 02 2021 04:29:17 PM

Note: When issuing “cmd” commands locally from the CTP shell you do not need to append “sudo” to the command string. The above change is only needed when you execute these commands remotely on a CTP running 9.x.

Known Issues

None

Required Archive Files

CTP Complete Package File(ctp_complete_9.1R2-1_210302.tgz) contains:

- CTPOS Upgrade Archive File: acorn_310_9.1R2-1_210302.tgz

File Information

File/s	Filename	MD5 Checksum
CTP complete Package	ctp_complete_9.1R2-1_210302.tgz	6c1a11614c97128527261564f51c47da

Manual upgrade from 9.1R1

While upgrading any archive on CTP boxes, it is necessary to make sure that only the intended archive is present in the “/tmp” directory. No other archives should be present in the /tmp directory. Manually we can upgrade any package in non-interactive mode or in interactive mode. “upgrade y” is the console command to upgrade any package without any user interaction.

Note: 9.1R1 is the minimum CTPOS version that needs to be running to upgrade to 9.1R2.1. During any of the archive interactive upgrade following two options has to be selected on triggering “upgrade” command on console.

Do you want to install the newest archive in quick mode (no questions)? y[n]: n
Do you want to install the newest archive interactively (w/ questions)? y[n]: y

Upgrading acorn_310_9.1R2-1_210302.tgz Archive in Interactive Mode

Following are the interactive upgrade steps for the above archive.

Do you want to install the newest archive in quick mode (no questions)? y[n]: n
Do you want to install the newest archive interactively (w/ questions)? y[n]: y

.....

Would you like to continue? y[n]: y

.....

Would you like to continue? y[n]: y

.....

Done...

Changing password of Default User accounts:

This step is applicable only when you reset to factory defaults in 9.1R2.1. You can reset system to factory defaults using CTPoS menu->Node Operations->Reset system. During firstboot prompt you will be asked for changing the default password. Change the passwords for all the default user accounts as shown below:

***** First boot of this flash. Setting up basic system configuration. *****

***** Setting up system passwords *****

Changing root's password!

```
#####
#####
#####
PLEASE REMEMBER THESE PASSWORDS!!!
```

Password recovery is not a simple process:

- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device

```
#####
#####
#####
```

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for root

Retype New Password for root

Changing ctp_cmd's password!

```
#####
#####
#####
PLEASE REMEMBER THESE PASSWORDS!!!
```

Password recovery is not a simple process:

- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device

```
#####
#####
#####
```

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for ctp_cmd

Retype New Password for ctp_cmd

Changing ctp's password!

```
#####
#####
#####
```

PLEASE REMEMBER THESE PASSWORDS!!!

Password recovery is not a simple process:

- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device

```
#####
#####
#####
```

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for ctp

Retype New Password for ctp

Changing ctp_sa's password!

```
#####
#####
#####
```

PLEASE REMEMBER THESE PASSWORDS!!!

Password recovery is not a simple process:

- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device

```
#####
#####
#####
```

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for ctp_sa

Retype New Password for ctp_sa

Changing ctp_audit's password!

```
#####  
#####  
#####
```

PLEASE REMEMBER THESE PASSWORDS!!!

Password recovery is not a simple process:

- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device

```
#####  
#####  
#####
```

The new password must be alphanumeric or the characters

@ { } # % ~ [] = & , - _ !

The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for ctp_audit

Retype New Password for ctp_audit

Note - You can also reset the password to default for all user accounts from CTPOS menu->Node Operations->Reset system passwords to default. To enable "Reset system passwords to default " and "Reset system to factory defaults" need to set lab mode "Enabled" using CTPOS menu->Node Diagnostics->Set Lab Mode->Enabled.

CTP Documentation and Release Notes

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.

Revision History

March 2021—Revision 1, CTPOS Release 9.1R2.1

Copyright © 2021 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.