Juniper Networks® CTPOS Release 9.1R1 Software Release Notes

Release 9.1R1
December 2019
Revision 1

These release notes accompany Release 9.1R1 of the CTPOS 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 https://www.juniper.net/documentation/.

Contents

Release Highlights

The following feature has been added to CTPOS Release 9.1R1.

- CTPOS 9.1R1 release provides CTPOS software support for the new CTP151 platform. [PR 1448617]

> **NOTE:** CTPOS 9.1R1 release is only for the new CTP151 platform (not for other CTP platforms: CTP2008, CTP2024, CTP2056, and CTP150).

Bringing Up CTP151 with CTPOS 9.1R1 on Internal SSD

> **NOTE:** CTPOS Release 9.1R1 does not support dual image upgrade or other upgrade procedures. So, you cannot upgrade to CTPOS Release 9.1R1 from older releases. The dual image upgrade procedure will be supported in a future release.

On the CTP151 device, the flash media (running the CTPOS software) is not removable, therefore CTPOS installation is done using a USB flash device. To bring up the CTP151 device with CTPOS on the internal SSD:

1. Download and burn the CTPOS software USB installation image to a USB flash device.

2. Insert the USB flash device to the CTP151 chassis, power on the CTP151 device, and monitor the console.

3. Press the **Del** key to open the BIOS menu.

4. Select the **Boot** tab and make the first boot device the one that includes “UEFI” and “Flash” in the name, which indicates that it is the USB install media.

5. Save and exit the setup.

   The device goes through a boot process, and then CTPOS USB installation menu opens.

6. Select a destination disk (the internal SSD on CTP151), and then verify installation selections.

7. Enter **y** to continue with the CTPOS software installation.

8. Enter **y** to reboot the system.

9. After the system reboots, go back to the BIOS menu and change the first boot device to the one that includes “UEFI OS (P5: SFSA20...”:

10. Save and exit from the BIOS menu.

For the first-time boot process, there is a series of login prompts that require the following settings:

1. The ctp and ctp_cmd user accounts have the default passwords. A password must be provided for the root account. The default password for the ctp user account is "ctp", and the default password for the ctp_cmd user account is "ctp_cmd". You can change the default passwords later.

2. Supported protocol or protocols—(0) IPv4 only, (1) IPv6 only, or (2) IPv4 and IPv6. Enter the appropriate number value.

3. Default interface—From the list of available devices, such as eth0 and eth1 (or more), enter the one to be the default.

4. Hostname of the device.

5. IP address of the interface—Enter the IP address of the selected interface, or accept the loopback address (127.0.0.1) by default.

6. Netmask of the IP address—Enter the netmask (such as 255.255.255.128), or accept 255.255.255.0 as the default.

7. Gateway IP address—Enter the IP address of the gateway, or accept the local address (127.0.0.1) as the default

8. Maximum transmission unit (MTU)—Enter the MTU in bytes, or accept 1500 bytes as the default.

9. Static routes added to the default interface, if any.

10. Date and time GMT (more precisely, UTC)—Enter these separately in digits for the month, day, hour, and minutes in Coordinated Universal Time (UTC), or accept the internal settings.

    The device goes into startup mode.

For example:

```
***** First boot of this flash. Setting up basic system configuration. *****
*********** Setting up the root password ************
Changing root's password!
Changing password for user root.
New password:
Retype new password:
BAD PASSWORD: it is too short
passwd: all authentication tokens updated successfully.
Backing up /etc to nonvolatile storage..
************** Setting up the network ***************
Configure supported protocols:
0)  IPv4 Only
1)  IPv6 Only
2)  IPv4 & IPv6

Please select your option (rtn for 0):

There are 2 ethernet devices available for use. The default device
is the device through which the default gateway can be accessed.
Ctp circuits can run over any ethernet device, default or not.
A default device must be configured, other devices may be configured
and enabled, or disabled. Here is a list to the available devices
and their descriptions:

       eth0: 10/100/1000 Copper (labeled 0 on processor card)
       eth1: 10/100/1000 Copper (labeled 1 on processor card)
       eth2: 10/100/1000 Copper (labeled 2 on processor card)
       eth3: 10/100/1000 Copper (labeled 3 on processor card)
       eth4: 10/100/1000 Copper (labeled MGMT on processor card)

What device would you like to make the IPV4 default device? (rtn for eth0):
OK, eth0 (10/100/1000 Copper (labeled 0 on processor card)) will be configured as
 IPV4 default device.

Please input the hostname (return for (none)): ctp150bot

===== Configuration for eth0 (default device):
Please input the ip (return for 127.0.0.1): 10.3.206.10
Please input the netmask (return for 255.255.255.0): 255.255.0.0
Please input the gateway (return for 127.0.0.1): 10.3.0.1
Please input the mtu in bytes (return for 1500):

Add route to interface eth0 [n]
```

```
======================================
=== OS Security level set to LOW ===
======================================

Backing up /etc to nonvolatile storage..
Backing up /usr/local to nonvolatile storage..
************** Setting up date/time *****************
Setting the date (GMT). Please input the year [2008-2020] (return for 2010):

Setting the date (GMT). Please input the month [1-12] (return for 11):

Setting the date (GMT). Please input the day [1-31] (return for 14):

Setting the date (GMT). Please input the hour [0-23] (return for 16):

Setting the date (GMT). Please input the minute [0-59] (return for 41):

INIT: Entering runlevel: 3
Entering non-interactive startup
```

Resolved Issues in CTPOS Release 9.1R1

Following issues have been resolved in CTPOS Release 9.1R1.

- Able to enter in to shell in high security mode. [PR 1264980]
- CTPOS becomes unresponsive due to “max menu sessions active” condition. [PR 1470627]
- CTP Menu does not always enforce the maximum PDV buffer settings. [PR 1467575]
- Add support for the new T1/E1 interface module of CTP151 platform. [PR 1468092]

Known Issues in CTPOS Release 9.1R1

The following features are not supported in CTPOS 9.1R1 release:

- The PBS and L2Agg feature configuration options have been removed from the CTPOS 9.1R1 release. These features will be reintroduced in a future release. [PR 1407698]

- VCOMP bundle and CESoPSN analog voice bundle configuration options have been removed from the CTPOS 9.1R1 release. These features will be reintroduced in a future release. [PR 1407829]
- The dual image upgrade procedure is not supported in CTPOS 9.1R1 release. This procedure will be supported in a future release.

CVEs and Security Vulnerabilities Addressed in CTPOS Release 9.1R1

The following tables lists the CVEs and security vulnerabilities that have been addressed in CTPOS Release 9.1R1. For more information about the individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 1: Critical or Important CVEs Included in Open SSH

Critical or Important CVEs Included in Open SSH		
CVE-2015-5600	CVE-2015-6564	CVE-2015-6563

Table 2: Critical or Important CVEs Included in kernel

Critical or Important CVEs Included in kernel [PR 1443871]			
CVE-2019-11477	CVE-2019-11478	CVE-2019-5599	CVE-2019-11479

CTP Documentation and Release Notes

For a list of related CTP documentation, see 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 2019—Revision 1, CTPOS Release 9.1R1

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.