Juniper Networks® CTPOS Release 7.2R1 Software Release Notes

Release 7.2R1
5 February 2016
Revision 1

These release notes accompany Release 7.2R1 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 http://www.juniper.net/techpubs/en_US/ctp7.2/information-products/pathway-pages/ctp-series/index.html.

Contents

New Features

The following features have been added to CTPOS Release 7.2R1.

Support for Separate Interfaces for Management and Circuit Traffic

In certain network topologies, a segregation is required between the circuit traffic and management traffic. Therefore, separate interfaces need to be used for the management and circuit networks so that traffic segregation can be achieved at the physical interface level. Starting with CTPOS Release 7.2, support for configuring two default gateways, one for management traffic and the other for circuit traffic, is available, which enables circuit and management traffic to be segregated.

Support for Configuring NTP Authentication on CTP Devices

Network Time Protocol (NTP) is a UDP protocol for IP networks. It is a protocol designed to synchronize the clock on client machines with the clock on NTP servers. NTP uses Coordinated Universal Time (UTC) as the reference time. Starting with CTPOS Release 7.2R1, NTP authentication is supported. NTP authentication checks the authenticity of NTP server before synchronizing local time with server. This phenomenon helps you to identify secure servers from unauthorized or illegal servers. NTP authentication works with a symmetric key configured by user. The key is shared by the client and an external NTP server. The servers and clients must agree on the key to authenticate NTP packets. Authentication support allows the NTP client to verify that the server is in fact known and trusted and not an intruder intending accidentally or on purpose to masquerade as that server. It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. Also, the “trustedkey keyid” attribute must be mentioned in the server’s ntp.conf file and the NTP process (ntpd) must be started in the server side for successful authentication.

Loss of Signal Detection Capability on CTP Bundles and SAToP Bundles

Starting with CTPOS Release 7.2R1, CTP devices support the detection of a loss of signal (LOS), which denotes a physical link problem.

The T1/E1, CTP, and SAToP bundles support LOS detection and based on this signal, the run state of the bundles switches to TfFail, which initiates a software-based Y cable switchover to a redundant port. Also, for T1/E1 both-ended Y-cable redundancy configuration, only software-based Y cable link protocol is supported and hardware-based redundancy is not supported.

The way in which CTP redundancy is able to work is by using the bundle state to make decisions. To use LOS as a way to take down a RUNNING bundle, the effective method implemented is to treat a T1/E1 LOS condition exactly the same as a serial port with a bad or missing external clock. When the CTP device performs its “check external clock” function, instead of returning an automatic success on T1/E1 ports, the LOS status bit is analyzed to determine whether it is a T1/E1 port. If the LIU LOS status indicates that there is no incoming signal, then the function returns a failure, which causes the bundle to move to the TtFAIL state.

Support for Multiple Master Nodes to Associate With a Single Client Node in NetRef

Network node reference (NetRef) is an extension of the CTP adaptive port clocking. When NetRef is configured for primary or backup operation, the primary node sends clocking information to the backup node. Starting with CTPOS Release 7.2R1, you can configure up to four master modes, each of which can send their clocking information to a maximum of 10 clients or slaves and the client node can receive clocking information from the configured masters. You can configure the four master nodes using CTP Menu or the CTPView web server during Netref client configuration. As a result, a single client node can use the IP address of up to four master nodes while you configure Netref client node settings. Each master node is assigned a priority during Netref client configuration. The master node with the highest priority is assigned Priority 1, the second highest priority for the master node is Priority 2, and so on. When the highest priority master goes down or if there is some problem in the synchronization of the clock, the CTP device switches to its next highest priority master (Priority 2 master node) and so on.

Support for Unlocking Inactive User Accounts

To support the U.S. Department of Defense Joint Interoperability Test Command (JITC) requirements, when the security level of the CTP Series platforms is set as high, the JITC high security mode requires that the CTP device must automatically disable user accounts after a 35-day period of account inactivity. This requirement-standard denotes that the password of all those user accounts that do not login to the CTP device or CTPView server for the past 35 days are locked. You can unlock those user accounts in compliance with the JITC specification.

A lockout warning message is displayed only for System Administrator and CTP Administrator accounts and not for other user accounts. The lockout warning messages are recorded in the network syslog file to inform the list of those system administrator accounts, which are due to be locked in next 10 days. A script “reset_pw_lock <user>” is added on the CTP device. You can run the “reset_pw_lock <user>” script to unlock the user accounts. The “activity_check” script file that is already available on the CTP Series platforms at the **/etc/cron.daily/activity_check** path is enhanced to send the lockout warning messages to the network syslog.

Support for Display of Jitter and Latency in the CTP Bundle Query Output for MIB Browser

Until CTPOS Release 7.1, the CTP bundle query does not provide statistics for jitter and latency. Starting with CTPOS Release 7.2R1, jitter and latency values are displayed in the command used to query the CTP bundles. Two additional values are appended at the end of the following command to support bundle jitter and bundle latency.

[root@ctp_87 ctp_cmd 3]# cmd bndl 0 qry snmp v1;B;0;1;this is ctp bundle description of maximum length on te-0.0
port.;te-0/0;1;-1;10.216.118.88;0;0;0;10.0.0.1;1024;16.000;12.000;8.000;0;255;0x40;-1;-1;3;20206060;20208183;0;24;88;86;0;1;10189;10089;6045;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;4.145;150;

Similarly, MIB objects for bundleJitter and bundleLatency are added in ACORN-MIB used by the MIB Browser.

Jitter and latency fields are added for the CTP, SAToP, CESoPSN, and VComp bundles. However, for VComp bundles, this value is always –1, and for SAToP and CESoPSN bundles, the latency field is always –1.

Support for Full-Duplex Mode Only on NIC Ports Connected to CTP Devices

If the autonegotiation setting of the CTP Ethernet media and the far-end switch or router do not match, it is possible for the CTP Ethernet ports to be in a half-duplex state, although the duplex setting is not configurable and always assumed to be full-duplex on the CTP device. Starting with CTPOS Release 7.2, the half-duplex state at CTP network interface card (NIC) ports are acquired, regardless of the duplex setting configured on the far-end node. After the autonegotiation process is completed, if the CTP NIC cannot acquire full-duplex mode, then the interfaces are considered to be down and a log message is recorded in both the **/var/log/messages** directory and the syslog file stating that the interface is down due to a non-full duplex condition. You are prompted to verify the cable connection, speed, and duplex settings because the NIC link might be down.

Support for Sending Port Descriptor and Bundle Descriptor Attributes in SNMP Traps

Until CTPOS Release 7.1, SNMPv2 traps that were sent from a CTP device did not contain specific bundle descriptor information. Starting with CTPOS Release 7.2, the Bundle Descriptor and Port Descriptor fields are also passed in the SNMP traps summary transmitted to the NMS server.

Support for Disabling Direct Drive by Default on CTP Bundles

Until CTPOS Release 7.1R1, the direct drive feature is enabled by default and this functionality configuration is not displayed in the output of the bundle query. If you explicitly enabled the direct drive capability (using IP tables instead of direct drive for packet-forwarding) by using the selecting **No** for the **Disable direct drive** field in the **Advanced Options** screen of the Configuration window under Bundle Operations of the CTP Main Menu, bundle query displayed "NoDirDrv" when you run the bundle query from the Main Menu of CTP Menu by selecting **1) Query**. Starting with CTPOS Release 7.2, the default behavior is direct-drive disabled (IP table is turned on for forwarding of packets). With default configuration, the bundle query output does not display the direct drive settings. Only if you explicitly enable the direct-drive capability, the bundle query output displays "Bndl Config Flags: DirDrv" in bundle query. CTP bundle circuits that use route redundancy and port forwarding must have direct drive disabled to allow for asymmetric routing. When direct drive is disabled, packets are forwarded based on information in the kernel's IP stack. When direct drive is enabled, packets are forwarded directly between drivers on the local and remote CTP device.

Support for Special Characters in SNMP Location Strings

Starting with CTPOS Release 7.2R1, special characters, such as equal sign (=), semicolon (;), and spaces, are supported in SNMP location strings and SNMP contact strings, and are processed properly.

Upgrade Information

You upgrade to CTPOS 7.2.*x* as follows:

- If you are upgrading to CTPOS Release 7.2.*x* from software releases 4.x, 5.x, 6.0x or 6.1x, you use upgrade kits to upgrade your CTP device to CTPOS Release 7.2.*x*
- If you are upgrading to CTPOS Release 7.2.*x* from software releases 7.1.x, 7.0x, 6.2Rx, 6.3Rx, 6.4Rx, 6.5Rx, or 6.6Rx, you can use software files for the upgrade.

Upgrading from CTPOS Release 4.x, 5.x, 6.0x or 6.1x to CTPOS Release 7.2..x with an Upgrade Kit

Because of the new features and hardware supported in CTPOS Release 7.2.*x*, a direct code upgrade from earlier versions of CTPOS by using an upgrade archive is not supported. CTPOS Release 5.x and earlier require an upgrade kit. You must perform the upgrade to CTPOS Release 7.*x* by using an upgrade kit. There are two upgrade kits, the use of which depends on whether you are using a PP310 or PP332 processor in your CTP2000 Series device.

If the CompactFlash card contains CTPOS 6.1R7 or earlier and you want to upgrade directly to CTPOS Release 7.2.x and later, you need to reburn the CompactFlash card with the CTPOS Release 7.2.x or later code before you perform the upgrade.

Upgrading from CTPOS Release 6.2x or Later to CTPOS Release 7.2R1

To upgrade from CTPOS Release 6.2x or later, use the following files:

- CTPOS Upgrade Archive File: **acorn_429_7.2R1_160203.tgz**
- Flash Archive: **flash_7.2R1.img**—Required only when you are creating a new flash card.
- CTP Complete Package File: **ctp_complete_7.2R1_160203.tgz**—Required only when you use CTPView.
- Migration Flash Archive File: **acorn_xxx_7.2R1_160203_migration_flash.tgz**—Required only when you create a migration flash card.
- CTP2000 BIOS Archive File: **acorn_429_110915_bios_V221.tgz**—Required only during migration. This file is not required for the CTPOS upgrade.
- Voice Card Archive File: **acorn_429_111021_em9c_fxo61_fxs50_voice.tgz**
- NTP: **acorn_429_ntp4.2.8p4_151127.tgz**
- FPGA Archive File: **acorn_429_140915_fpga_150_s27_t1c_2000_s1b_t2c.tgz**
- Boot FPGA Archive File: **acorn_xxx_boot_fpga_s25_t1b_130317.tgz**—Required only for CTP 150 devices.
- CTP2000 Winmon Archive File: **acorn_429_111115_winmon_210.tgz**
- Dcard Archive File: **acorn_429_111121_dcardpld_t1e1_3_4wto_4.tgz**
- KIS Archive File: **acorn_xxx_150909_KIS.tgz**

- Bash Archive File: acorn_429_bash-4.3.30_141212.tgz
- GLIBC Archive File: acorn_429_glibc-2.3.2_150327.tgz
- OpenSSL Archive File: **acorn_429_openssl_1.0.2e_151205.tgz**
- OpenSSH Archive File: **acorn_429_openssh_7.1p2_160127.tgz**

NOTE: The version of the Winmon support file (210) is the same as that in the CTPOS Release 6.2R1 Winmon version. However, the date portion of the file name is modified (111115 vs 100331). Only the installation file is modified. There is no change in the Winmon code, hence the change in date and not the version. The voice daughter card support files are also affected by this.

Make sure you disable all ports and bundles before starting the upgrade process.

CAUTION: When you upgrade CTPOS by using the Boot FPGA archive file, you must ensure that there is no power fluctuation or interruption during the upgrade processes. Any fluctuation or interruption of power during the upgrade can make the device unusable and the device will have to be returned to the factory.

The CTP device must not be used until the upgrade process is complete.

Manually Upgrading from CTPOS Release 7.1R2 to 7.2R1

BEST PRACTICE: Before you start the upgrade process, you must ensure that only the required archive files are present in the **/tmp** directory. You can manually upgrade any package in noninteractive or interactive mode. You can use the **upgrade y** command to upgrade a package in noninteractive mode.

NOTE:

- The Winmon file is used to upgrade CTP2000-IM-8P-T1E1 Cards.
- The FPGA file is used to upgrade both CTP2000-IM-8P-T1E1 and CTP2000-IM-8P-xx cards.
- In the CTP2000 Series, you may have to upgrade the voice support files if they are present.

When you upgrade the archive in interactive mode, you have to select the following two options after issuing the **upgrade** command from the CLI:

```
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 the Winmon Archive in Interactive Mode

To upgrade the Winmon 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
....
Loading Micro Winmon image to SCC0.....
Same version of Micro Winmon is already programmed, skip... !
....
```

Upgrading the Glibc Archive in Interactive Mode

To upgrade the **acorn_429_glibc-2.3.2_150327.tgz** 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
……..
-----
Done...
```

Upgrading the OpenSSL Archive in Interactive Mode

To upgrade the **acorn_429_openssl_1.0.2e_151205.tgz** 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
Continuing...
===== Uncompressing and Extracting Archive =====
      Archive file: acorn_429_openssl_1.0.2e_151205.tgz
acorn_install/
acorn_install/gui_instr
acorn_install/install
acorn_install/openssl-1.0.2e.tgz
Running install interactively
**********************************************************************
This installation script will update openssl version to 1.0.2e
**********************************************************************

Would you like to continue? y[n]: y
.............
.............
done.
```

Upgrading the Open SSH Archive in Interactive Mode

To upgrade the **acorn_429_openssh_7.1p2_160127.tgz** archive:

```
CTP system software upgrade utility - Version 1.4.9
Found kernel version 2.4.29, setting KVER to 429
Checking for active menu sessions
…….
Do you want to install the newest archive in quick mode (no questions)? y[n]: y
Continuing...
…….
+++++ OpenSSH 7.1p2 already installed, did not reinstall! +++++
```

```
…….
===== Archive Cleanup =====
Done...
```

Upgrading the NTP Archive in Interactive Mode

To upgrade the **acorn_429_ntp4.2.8p4_151127.tgz** archive:

```
**********************************************************************
NOTE: CTPOS code upgrades will interrupt data on running circuits.
Say "no" to run more interactive or install a different 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

Continuing...

**********************************************************************
This installation script will update NTP on this system to
version 4.2.8p4. After installation, the box MUST be rebooted.
**********************************************************************

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

Done...
```

Upgrading the Boot FPGA Archive in Interactive Mode

To upgrade the **acorn_xxx_boot_fpga_s25_t1b_130317.tgz** archive:

NOTE: After you upgrade the FPGA archive, you need to upgrade the main archive and restart the system.

NOTE: Boot FPGA is applicable to CTP150 systems only.

```
**********************************************************************
NOTE: CTPOS code upgrades will interrupt data on running circuits.
Say "no" to run more interactive or install a different 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
Continuing...
===== Uncompressing and Extracting Archive =====
      Archive file: acorn_xxx_boot_fpga_s25_t1b_130317.tgz
acorn_install/
acorn_install/gluon_t1e1.rpd
acorn_install/load_fpga
acorn_install/install
acorn_install/nova_2.rbf
acorn_install/epcs
acorn_install/gui_instr
acorn_install/gluon.rpd
acorn_install/nova.rbf
Running install interactively
```

```
***** CTP150 Boot upgrade archives are not for CTP-2000! *****
……..
ManageFlashVersions: Skip... This is a Boot archive.
……..
```

Upgrading the Bash Archive in Interactive Mode

To upgrade the **acorn_429_bash-4.3.30_141212.tgz** 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
Continuing...


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

===== BASH 4.3.30 installed! =====

Done...
```

Upgrading the acorn_429_7.2R1_160203.tgz Archive in Interactive Mode

To upgrade the **acorn_429_7.2R1_160203.tgz** 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
....
```

Resolved Issues in CTPOS Release 7.2R1

The following issues have been resolved in CTPOS Release 7.2R1.

- SNMPv2 traps that are sent from a CTP device do not contain specific bundle descriptor information. In the traps summary, the Bundle Descriptor and Port Descriptor attributes are not sent to the NMS server. [PR/1054258]
- Data through SAToP bundles is not transmitted from a CTP system to the MICs on MX Series routers because the CTP device does not check the bundle type and sets the "isXorPkt" variable for SATOP bundles. [PR/1060422]
- Special characters, such as equal sign (=), semicolon (;), and spaces, are not supported in SNMP location strings and are not processed properly. [PR/1060696]
- A CTP bundle that is set as the data terminal equipment (DTE) with a packet size of 8 bytes does not run and generates a TooFast error (encountered when the bundle is configured for all clocking to be done by the external TT clock). This problem occurs when the port configuration flag is set as HiTTCheck for the CTP bundle, and the packets per second (pps) is shown as 1500 for the bundle in such a scenario. [PR/1074998]

- After the reboot of a CTP device, the serial card in slot 2 is not visible in the software because the CTPOS software identifies the card and reports IRQ 0 is busy in the log file. In such a scenario, you need to reboot the CTP device again for the card to be operational. [PR/1079714]
- On a CTP150 device, where eth0 is the default primary interface, eth1 is the Ethernet failover interface, eth0.999 is the VLAN-enabled interface for management traffic, one static route is defined on eth0.999, when eth0 is up normally and eth0.999 is routable for management traffic. If eth0 fails and switches to eth1, the static route does not switch with it and the static route does not display in the routing table. [PR/1080510]
- The calculation of PPS occurs incorrectly for CTP bundles with Exclusive OR (XOR) packet protector enabled. The PPS value almost doubles from its previous value and the Run State becomes tooFast when you enable XOR packet protector to duplicate and receive packets. [PR/1082106]
- The direct drive capability (using IP tables instead of direct drive for packet-forwarding) is disabled by default. [PR/1083475]
- In compliance with the U.S. Department of Defense Joint Interoperability Test Command (JITC) requirements, when the security level of the CTP Series platforms is set as high, the JITC high security mode requires that the CTP device must automatically disable accounts after a 35-day period of account inactivity. A mechanism to unlock and reenable such disabled user accounts is not available. [PR/1085019]
- With an NMS server that uses SNMP and SSH queries to determine status on a network of CTP devices, SNMP Get operations cause packet loss and starvations in your circuit. [PR/1105651]
- The display of jitter and latency in the CTP bundle query output for MIB browsers is not supported. [PR/1106063]
- Both-ended Y-cable redundancy configuration (hardware-based redundancy or software-based Y cable link protocol) does not support loss of signal (LOS) checking for pulled cable failures. [PR/1110021]
- NTP authentication is not supported on CTP devices to check the authenticity of NTP server before synchronizing local time with the server. [PR/1110250]
- You cannot associate multiple master nodes with a single backup node in Network node reference (NetRef). [PR/1110275]
- The FAIL_DELAY value in **/etc/login.defs** meets the GPOS STIG rule of that requires a minimum of 4 seconds between login failures. The same rule needs to be applied to the **/etc/pam.d/system-auth** file. [PR/1114496]
- Support is needed for separate interfaces to be used for the management and circuit networks so that traffic segregation can be achieved at the physical interface level. [PR/1119202]
- The snmpAcorn.pl script is run in daemon mode because it is observed that snmpAcorn.pl is causing high CPU usage for the complete SNMP walk of Acorn MIB. [PR/1119228]

- Only full-duplex mode must be supported on the network interface card (NIC) ports of the far-end switch or router connected to the CTP devices. [PR/1125632]
- The CTP2008 platform is reset intermittently when the Ethernet ports are operating at different speeds and the bundle traffic is flowing though the Ethernet eth0 interface, which is the default interface for the CTP devices, and eth1 (1G autonegotiation) is used to connect to the management network with the CTPView server. [PR/1133527]
- The 4WE&M interface does not pass audio tone when you configure the interface for a CESoPSN bundle. If you use the same ports and configure for VComp bundles, audio tone passes properly. No audio tone is transmitted even if you delete the bundle and reconfigure as a CESoPSN bundle. [PR/1137814]
- A memory leak occurs when SNMPV3 is enabled. It is observed that after one and a half days, all of the bundles start generating continuous errors until the CTP2056 platform resets. [PR/1139254]
- It is necessary to add login information for RADIUS users into the syslog file and address OpenSSL security vulnerabilities. [PR/1144964]
- BERT counters are not cleared for CESoPSN bundles in the CTP Menu. [PR/1030232]
- CTP systems that are installed with analog cards enter an unusable state when T1/E1 and VComp cards are not present. [PR/1089541]
- Disabling the DTE serial port causes RL signal output to go active. [PR/1153461]

Known Issues in CTPOS Release 7.2R1

This section lists the known issues in CTPOS Release 7.2R1.

- Serial inband signaling does not work properly when multiple output signals are configured to carry inband signals. [PR/733075]
- PBS does not work when configured with PPP encapsulation on CTP 150 devices. [PR/784778]

CVEs and Security Vulnerabilities Addressed in CTPOS Release 7.2R1

The following tables lists the CVEs and security vulnerabilities that have been addressed in CTPOS Release 7.2R1. For more information about the individual CVEs, see http://web.nvd.nist.gov/view/vuln/search .

Table 1: Critical or Important CVEs Included in ntp-4.2.8p4

Critical or Important CVEs Included in ntp-4.2.8p4			
CVE-2015-7871	CVE-2015-7855	CVE-2015-7854	CVE-2015-7853
CVE-2015-7852	CVE-2015-7851	CVE-2015-7850	CVE-2015-7849
CVE-2015-7848	CVE-2015-7701	CVE-2015-7703	CVE-2015-7704

Table 1: Critical or Important CVEs Included in ntp-4.2.8p4 *(continued)*

Critical or Important CVEs Included in ntp-4.2.8p4			
CVE-2015-7705	CVE-2015-7691	CVE-2015-7692	CVE-2015-7702

[PR/1134726]

Table 2: Critical or Important CVEs Included in OpenSSL 1.0.2e

Critical or Important CVEs Included in OpenSSL 1.0.2e			
CVE-2015-3193	CVE-2015-3194	CVE-2015-3195	CVE-2015-3196
CVE-2015-1794			

[PR/1144964]

Table 3: Critical or Important CVEs Included in OpenSSL 1.0.2e

Critical or Important CVEs Included in OpenSSL 1.0.2e			
CVE-2015-0291	CVE-2015-02044	CVE-2015-0290	CVE-2015-0207
CVE-2015-0286	CVE-2015-0287	CVE-2015-0208	CVE-2015-0289
CVE-2015-0292	CVE-2015-0293	CVE-2015-1787	CVE-2015-0285
CVE-2015-0209	CVE-2015-0288		

[PR/1072934]

Table 4: Critical or Important Security Vulnerabilities Addressed in OpenSSH-7.1p2

Critical or Important Security Vulnerabilities Addressed in OpenSSH-7.1p2
OpenSSH 5.4 < 7.1p2 Security Vulnerabilities observed during a Retina scan on CTPOS.

[PR/1156537]

CTP Documentation and Release Notes

For a list of related CTP documentation, see http://www.juniper.net/techpubs/en_US/release-independent/ctp/information-products/pathway-pages/index.html.

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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://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: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://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.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- 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 http://www.juniper.net/support/requesting-support.html .

Revision History

February 2016—Revision 1, CTPOS Release 7.2R1