

Juniper Networks[®] CTPOS Release 7.3R1 Software Release Notes

Release 7.3R1
August 2016
Revision 1

These release notes accompany Release 7.3R1 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/ctp7.3/information-products/pathway-pages/ctp-series/index.html.

Contents

New Features	3
Support for Autoupgrading FPGA When Incorrect FPGA IS Detected	3
Support for Logging AIS and LOS Condition Exit/Entry Messages	3
Support for Traceroute with Source IP Address	3
Support to Limit the Number of Sessions per User	3
Support for Creating a New Bundle with the Saved Bundle Configuration	3
Support for Generating Traps and Syslog Messages on SdInactive	3
Support to Include the information of Security Patch Versions in cmd Utility	3
Upgrade Information	3
Upgrading from CTPOS Release 4.x, 5.x, 6.0x or 6.1x to CTPOS Release 7.3R1 with an Upgrade Kit	4
Upgrading from CTPOS Release 6.2x or Later to CTPOS Release 7.3R1	4
Manually Upgrading from CTPOS Release 7.2R1 to 7.3R1	5
Upgrading the acorn_429_upgrade_pkg_160308.tgz Archive in Interactive Mode	6
Upgrading the Winmon Archive in Interactive Mode	6
Upgrading the Glibc Archive in Interactive Mode	6
Upgrading the OpenSSH and OpenSSL Archive in Interactive Mode	7
Upgrading the NTP Archive in Interactive Mode	7
Upgrading the Boot FPGA Archive in Interactive Mode	7
Upgrading the Bash Archive in Interactive Mode	8

Upgrading the acorn_429_7.3R1_160826.tgz Archive in Interactive Mode	8
Resolved Issues in CTPOS Release 7.3R1	9
Known Issues in CTPOS Release 7.3R1	9
CVEs and Security Vulnerabilities Addressed in CTPOS Release 7.3R1	9
CTP Documentation and Release Notes	10
Requesting Technical Support	10
Self-Help Online Tools and Resources	10
Opening a Case with JTAC	11
Revision History	12

New Features

The following features have been added to CTPOS Release 7.3R1.

Support for Autoupgrading FPGA When Incorrect FPGA IS Detected

CTP devices enable autoupgrading the FPGA when line cards with different FPGA versions are swapped, a new line card (with a different FPGA version) is added, or an incorrect FPGA is detected. [PR 596068]

Support for Logging AIS and LOS Condition Exit/Entry Messages

For the T1/E1 interface module, alarm indication signal (AIS) and loss of signal (LOS) condition exit or entry messages are printed in the network syslog file. [PR 1164105]

Support for Traceroute with Source IP Address

CTP devices support executing the traceroute command with the source IP address option. [PR 1168875]

Support to Limit the Number of Sessions per User

In High Security level, the CTP Box and CTPView server limit the number of concurrent sessions to three per user, by default. To support this enhancement, a new option **Configure maximum number of concurrent sessions for users** is added under **Node Operations > Config security profile > User Management**. Only the system administrator can configure a value for this option ranging from 1 through 3. [PR 1168938]

Support for Creating a New Bundle with the Saved Bundle Configuration

CTPMenu and CTPView GUI enable CTP administrator and system administrator to copy the existing bundle configuration on similar type of new port. [PR 1171607]

Support for Generating Traps and Syslog Messages on SdInactive

CTP devices support generating syslog messages and sending traps to the SNMP MIB Browser if the SdInactive flag is set. [PR 1173307]

Support to Include the information of Security Patch Versions in cmd Utility

The cmd utility is enhanced to display information of security patch versions released between the standard CTPOS releases. The security patch includes third party package such as SSH/SSL, SNMP, NTP, Kernel, and GLIBC. The cmd utility lists these security patch versions within the **cmd -v** output, when there is a change in the third party package associated with the current CTPOS release. [PR 1174137]

Upgrade Information

Upgrade to CTPOS 7.3R1 as follows:

- If you are upgrading to CTPOS Release 7.3R1 from software releases 4.x, 5.x, 6.0x or 6.1x, you use upgrade kits to upgrade your CTP device to CTPOS Release 7.3.x

- If you are upgrading to CTPOS Release 7.3R1 from software releases 7.2.x, 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 7.3R1 with an Upgrade Kit

Because of the new features and hardware supported in CTPOS Release 7.3R1, 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 7.3R1, you need to burn the CompactFlash card with the CTPOS Release 7.3R1.

Upgrading from CTPOS Release 6.2x or Later to CTPOS Release 7.3R1

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

- CTPOS Upgrade Archive File: **acorn_429_7.3R1_160826.tgz**
- Flash Archive: **flash_7.3R1.img**—Required only when you are creating a new flash card.
- CTP Complete Package File: **ctp_complete_7.3R1_160826.tgz**—Required only when you use CTPView.
- Migration Flash Archive File: **acorn_xxx_7.3R1_160826_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_ntp4.2.8p8_160811.tgz**
- FPGA Archive File: **acorn_429_160822_fpga_150_s29_t20_2000_s1d_t2f.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**
- OpenSSH and OpenSSL Archive File:
acorn_429_openssh_7.1p2_openssl_1.0.2g_160308.tgz
- Upgrade Package File: **acorn_429_upgrade_pkg_160308.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 7.2R1 to 7.3R1



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 acorn_429_upgrade_pkg_160308.tgz Archive in Interactive Mode

To upgrade the `acorn_429_upgrade_pkg_160308.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_upgrade_pkg_160308.tgz
acorn_install/
acorn_install/gui_instr
acorn_install/upgrade
acorn_install/install
Running install interactively
*****
This installation script will update upgrade script on the box
*****

Would you like to continue? y[n]: y
===== Saving /acorn to flash =====
Backing up /var to nonvolatile storage..
Backing up /home to nonvolatile storage..
Backing up / to nonvolatile storage..

===== New upgrade script installed! =====

===== Archive Cleanup =====
Done...

```

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 OpenSSH and OpenSSL Archive in Interactive Mode

```
To upgrade the acorn_429_openssh_7.1p2_openssl_1.0.2g_160308.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_openssh_7.1p2_openssl_1.0.2g_160308.tgz
acorn_install/
acorn_install/gui_instr
acorn_install/install
acorn_install/openssl-1.0.2g.tgz
acorn_install/openssh-7.1p2.tgz
Running install interactively
*****
This installation script will update openssl version to 1.0.2g
*****

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

Upgrading the NTP Archive in Interactive Mode

```
To upgrade the acorn_429_ntp4.2.8p8_160811.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 4.2.8p8. 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_7.3R1_160826.tgz` Archive in Interactive Mode

To upgrade the `acorn_429_7.3R1_160826.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 7.3R1

Following issues have been resolved in CTPOS Release 7.3R1.

- When reconfiguring a bundle from Transparent encoding to NRZ encoding, the clock configuration is not reset properly. [PR 1133625]
- During the first boot process, the CTPOS software does not accept the default value of 09 or 9 for the hour setting. [PR 1161082]
- CTP2056 devices that are heavily loaded with 5 serial line modules and around 50 active bundles randomly reboot. [PR 1172373]
- Upgrading from the CTPOS software release 7.0R5 to 7.2R1 deletes the TACACS configuration. [PR 1173747]
- 4WTO bundle goes to the ttfail (TT=0) state after upgrading CTPOS software from release 6.5R2 to 7.2R1. [PR 1180788]

Known Issues in CTPOS Release 7.3R1

This section lists the known issues in CTPOS Release 7.3R1.

- 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]
- CESoPSN BERT does not work reliably on CTP devices. Due to this issue, BERTs are temporarily disabled for CESoPSN bundles as part of PR 1204779. [PR 1197932]

CVEs and Security Vulnerabilities Addressed in CTPOS Release 7.3R1

The following tables lists the CVEs and security vulnerabilities that have been addressed in CTPOS Release 7.3R1. 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-4.2.8p8

Critical or Important CVEs Included in ntp-4.2.8p8 [PR 1183187]			
CVE-2015-7704	CVE-2015-8138	CVE-2016-1547	CVE-2016-1548
CVE-2016-1549	CVE-2016-1550	CVE-2016-1551	CVE-2016-2516
CVE-2016-2517	CVE-2016-2518	CVE-2016-2519	

Table 2: Critical or Important CVEs Included in OpenSSL 1.0.1s/1.0.2g

Critical or Important CVEs Included in OpenSSL 1.0.1s/1.0.2g [PR 1165847]			
CVE-2016-0800	CVE-2016-0705	CVE-2016-0798	CVE-2016-0797
CVE-2016-0799	CVE-2016-0702	CVE-2016-0703	CVE-2016-0704

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

August 2016—Revision 1, CTPOS Release 7.3R1

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the 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.