Juniper Networks® CTPView Server Software Release 7.3R1 Release Notes

Release 7.3R1
August 2016
Revision 1

These release notes accompany Release 7.3R1 of the CTPView Server Software. They contain upgrade information and describe the enhancements to the software. The CTPView Release 7.3R1 software is compatible with Juniper Networks CTP Series platforms running CTPOS version 7.3 or earlier.

You can also find these release notes on the Juniper Networks CTP Software Documentation webpage, which is located at https://www.juniper.net/techpubs/en_US/ctp7.3/information-products/pathway-pages/ctp-series/index.html.

Contents

New Features . . . 2
Displaying Runtime Query Results of both Remote and Active Bundles . . . 2
Support for Sorting CTP Devices in Numerical Order . . . 2
Bundle Description Option Added under the Network Monitoring Page . . . 2
Support to Limit the Number of Sessions per User . . . 2
Support for Creating a New Bundle with the Saved Bundle Configuration . . . 2
Required Upgrade Files . . . 2
Upgrading the CTPView Software . . . 3
Upgrading the CTPView Software for Systems Running Version 3.4R2-p1 or 3.4R3 or Later . . . 3
Upgrading the CTPView Software for Systems Running Version 3.4R2 or Earlier . . . 4
Resolved Issues in CTPView Release 7.3R1 . . . 4
Known Issues in CTPView Release 7.3R1 . . . 4
CVEs and Security Vulnerabilities Addressed in CTPView Release 7.3R1 . . . 4
CTP Documentation and Release Notes . . . 5
Requesting Technical Support . . . 5
Self-Help Online Tools and Resources . . . 6
Opening a Case with JTAC . . . 6
Revision History . . . 7

New Features

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

Displaying Runtime Query Results of both Remote and Active Bundles

The **Bundle Runtime Query** page is enhanced to display runtime query results of the remote bundle as well as the active bundle simultaneously or by switching views on the same page. [PR 1183370]

Support for Sorting CTP Devices in Numerical Order

CTPView Release 7.3R1 enables you to sort CTP devices in a numerical order within their respective groups. [PR 1193662]

Bundle Description Option Added under the Network Monitoring Page

The **Network Monitoring** page is enhanced to include the **Bundle Description** option under the CTP label. [PR 1177198]

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]

Required Upgrade Files

The full suite of security enhancements is available only when the CTPView software is installed on servers running CentOS 5.11. Contact Juniper Networks Technical Assistance Center (JTAC) if you need to upgrade your operating system.

We provide the following files for upgrading the CTPView software:

- **web_update_7.3R1_160823.tgz** [Software updates]
- **ctpview_complete_centos_7.3R1_160823.tgz** [Software and CentOS OS updates]
- **ctpview_complete_fc9_7.3R1_160823.tgz** [Software and Fedora 9 OS Updates]
- **ctpview_complete_fc4_7.3R1_160823.tgz** [Software and Fedora 4 OS Updates]

The upgrade files that you use depend on the current CTPView server's operating system and the current CTPView software release. Use Table 1 on page 3 to determine the correct file to use.

Table 1: Determining the Required Upgrade Files for Your System

CTPView Server OS	Installed CTPView Release	File for Upgrade	Server Reboots During Upgrade?
CentOS 5.11	4.5R2 or earlier 4.6R1 or earlier 7.0R4 or earlier 7.1R2 or earlier 7.2R1 or earlier	**ctpview_complete_centos_7.3R1_160823.tgz**	Yes

Upgrading the CTPView Software

These sections describe how to upgrade CTPView Server Software to Release 7.3R1.

This topic includes the following tasks:

- Upgrading the CTPView Software for Systems Running Version 3.4R2-p1 or 3.4R3 or Later on page 3
- Upgrading the CTPView Software for Systems Running Version 3.4R2 or Earlier on page 4

Upgrading the CTPView Software for Systems Running Version 3.4R2-p1 or 3.4R3 or Later

This topic describes how to upgrade systems that run CTPView Server Software Release 3.4R2-p1 or 3.4R3 or later to CTPView Server Software Release 7.0 and later

To install the CTPView Server software for systems running 3.4R2-p1 or 3.4R3 or later:

1. Use Secure Copy Protocol (SCP) to copy the **web_update** or **ctpview_complete** file to the **/tmp** directory on the server.
2. Log in to the server shell. On CentOS systems, log in as system administrator.
3. Run the installation script as root: **upgrade** or as system administrator: **upgrade**.

NOTE: When upgrading CentOS 5.3 systems running a release earlier than CTPView Release 4.2, you are prompted to enter the MySQL administrator's password. This password is needed to upgrade the database structures. If you do not enter the correct password, the upgrade process continues, but the server remains usable with limited MySQL functionality. In this case, to complete the upgrade process you need to manually initiate the database structure upgrade script from the CTPView CLI menu. The path to this function is **Menu** > **MySQL Functions** > **Upgrade Database Structures**.

Upgrading the CTPView Software for Systems Running Version 3.4R2 or Earlier

To install the CTPView software by using one of the **ctpview_complete** files:

1. Use SCP to copy the **ctpview_complete** file to the **/tmp** directory on the server.
2. Log in to the server shell and switch to the **root** user.
3. Unpack the archive.
4. Run the upgrade script: **upgrade**.

To install the CTPView software by using the **web_update** file:

1. Copy the upgrade file to the **/tmp** directory on the server.
2. Log in to the server shell and switch to the root user.
3. Run the upgrade installation script: **upgrade**.

Resolved Issues in CTPView Release 7.3R1

The following issue has been resolved in CTPView Release 7.3R1:

- After upgrading the CTPView Server Software, the OS security level setting is changed to high from very-low. [PR 1157827]

Known Issues in CTPView Release 7.3R1

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

- PBS configured with PPP encapsulation does not function on a CTP150 device. [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 CTPView Release 7.3R1

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 7.3R1. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 2: Critical or Important CVEs Included in ntp-4.2.8p8

Critical or Important CVEs Included in ntp-4.2.8p8 [PR 1183185]			
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 3: 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 1165849]			
CVE-2016-0702	CVE-2016-0703	CVE-2016-0704	CVE-2016-0705
CVE-2016-0797	CVE-2016-0798	CVE-2016-0799	CVE-2016-0800

Table 4: Critical or Important CVEs Included in NSS or NPR

Critical or Important CVEs Included in NSS or NPR (mod_nss-1.0.8-4.el5_6.1, nss-3.12.8-4.el5_6, nss-tools-3.12.8-4.el5_6, pkinit-nss-0.7.6-1.el5, and nss_db-2.2-38.el5_11 [PR 1199020]			
CVE-2013-5605	CVE-2013-5607	CVE-2013-1739	CVE-2013-1741
CVE-2013-5606	CVE-2013-0791	CVE-2013-1620	CVE-2014-1490
CVE-2014-1491	CVE-2014-1492	CVE-2014-1544	CVE-2014-1545
CVE-2014-1568			
Critical or Important CVEs Included in kernel-2.6.18-406.el5 [PR 1199020]			
CVE-2015-5364	CVE-2015-5366	CVE-2013-2596	CVE-2015-2151
Critical or Important CVEs Included in dhcpv6-client-1.0.10-16.el5 [PR 1199020]			
CVE-2011-0997	CVE-2011-2748	CVE-2011-2749	CVE-2012-3571

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 postsales 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, CTPView Release 7.3R1