Juniper Networks® CTPView Server Software Release 7.2R1 Release Notes

Release 7.2R1
5 February 2016
Revision 1

These release notes accompany Release 7.2R1 of the CTPView Server Software. They contain upgrade information and describe the enhancements to the software. The CTPView Release 7.2R1 software is compatible with Juniper Networks CTP Series platforms running CTPOS version 7.2 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/ctp7.2/information-products/pathway-pages/ctp-series/index.html.

Contents

New Features

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

Support for OpenSSL Authentication of Users by Creating a Self-Signed Web Certificate

Until CTPView Release 7.1, an existing security protocol called NSS is used for authentication of user login through the CTPView GUI. Starting with CTPView Release 7.2R1, the CTPView GUI user login authentication is implemented through OpenSSL instead of NSS. Authentication of users logging in to the CTPView GUI using OpenSSL enables secure and protected transfer of information, and also compliance with OpenSSL as validated by Federal Information Processing Standards (FIPS) 140-2.

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 and the CTPView server. 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 and CTPView server at the **/etc/cron.daily/activity_check** path is enhanced to send the lockout warning messages to the network syslog.

Support for CTPView Servers on Virtual Machines

The CTPView server on a virtual machine or a virtualized CTPView server consists of the CTPView software with a built-in operating system and application stack that is easy to deploy, manage, and maintain. A CTPView virtual server includes the same software and all the functionality available in a CTPView physical appliance. You can configure CTPView servers on a VMWare ESXi Server and a Microsoft Hyper-V Server.

Support for Configuring IP ACLs for Restricting Access to Resources

Starting with CTPView Release 7.2R1, you can configure IP access control lists (ACLs) using the CTPView server menu to regulate and restrict access to network resources for devices with specific IP addresses that attempt to access the network utilities. You can add or remove ACLs, and define permit and deny rules or conditions, which enable or disallow access from specific IP addresses or address ranges.

Support for Auditing CTPView Commands

Starting with CTPView Release 7.2R1, support is added for the **EXECVE** type attribute in the **audit.rules** file, which enables auditing to be performed for all the CTPView commands.

Increased PHP Session Lifetime and Changes to Transaction Isolation

Starting with CTPView Release 7.2R1, the PHP session lifetime has been increased to 900 seconds (15 minutes) to comply with JITC requirements. Also, the transaction isolation setting has been changed to REPEATABLE-READ in my.conf file to comply with JITC requirements.

Resolution of Security Vulnerabilities on the CTPview Server

Starting with CTPView Release 7.2R1, some of the vulnerabilities in CentOS implementation of CTPView OS are resolved. Vulnerabilities in the areas of an outdated operating system usage, backup files containing sensitive information, and reflected cross-site scripting are resolved. Several vulnerabilities were previously addressed in CTPView Release 7.1R1. For more information, see http://kb.juniper.net/jsa10691.

Support for Configuring the Loss of Signal Detection on CTP Bundles

Starting with CTPView Release 7.2R1, CTP devices support the detection of a loss of signal (LOS), which denotes a physical link problem, on CTP bundles in a serial and T1/E1 both-ended Y-cable redundancy configuration (hardware-based redundancy or software-based Y cable link protocol). You can configure advanced port options for CTP bundles using CTPView, you can select the **LOS checking (T1E1 only)** field as Yes or No to specify whether you want to enable or disable loss of signal (LOS) detection for CTP bundles in a T1/E1 both-ended Y cable configuration (hardware-based redundancy or software-based Y cable link protocol).

Support for Subdomains in Hostnames of CTPView Server

Until CTPView Release 7.1R1, when you enter valid fully qualified domain names (FQDN) with subdomains, CTPView does not enable the subdomains (labels or dots) to be entered and has restrictions with the maximum length of the hostname length to be 24 characters. Starting with CTPView Release 7.2R1, you can specify hostnames of CTP devices (when you select **2) System Configuration** from the CLI menu on the CTPView server and select the **Change Hostname/Domain** menu option to make the changes and to enter the hostname) in compliance with the domain name system (DNS) standards, which enables you to enter labels or subdomains in a hostname. Each label in a hostname can have a maximum of 63 characters and the entire FQDN can be up to a maximum of 253 characters. No specific restriction on the number of labels exists.

Support for Accepting the I.S. User Terms and Agreement After Logging In to CTPView Server

Starting with CTPView Release 7.2R1, after you enter the credentials on the CTPView server login page, a pop-up dialog box is displayed prompting you to confirm that you have read and consent to the terms of the U.S. Government (USG) Information System (IS) User Agreement. Click OK to navigate to the home page of the CTPView server. Alternatively, click Cancel to log out of the CTPView server.

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_7.2R1_160203.tgz** [software updates]
- **ctpview_complete_centos_7.2R1_160203.tgz** [software and CentOS OS updates]
- **ctpview_complete_fc9_7.2R1_160203.tgz** [Software and Fedora 9 OS Updates]
- **ctpview_complete_fc4_7.2R1_160203.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 5 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	**ctpview_complete_centos_7.2R1_160203.tgz**	Yes

Upgrading the CTPView Software

These sections describe how to upgrade CTPView Server Software to Release 7.2R1.

This topic includes the following tasks:

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 7.2R1

The following issues have been resolved in CTPView Release 7.2R1:

- Upgrade of the CTPView software fails when the KIS file is attempted to be copied using Secure Copy protocol (SCP) to the CTP system. [PR/975967]
- 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/1085043]
- RC4 ciphers need to be removed from the Apache NSS and SSL configuration files. [PR/1084593]
- Perl scripts do not have the Taint mode enabled, which enables special security checks to be performed for security purposes. [PR/1084594]

- Security vulnerabilities are observed on a CTPView server running CTPView Release 7.0R3. [PR/1087204]
- Some vulnerabilities are present in CentOS OS implementation of CTPView OS. Vulnerabilities in the areas of an outdated operating system usage, backup files containing sensitive information, and reflected cross-site scripting. [PR/1094262]
- You cannot use the advanced port options in the CTPView server menu to enable or disable loss of signal (LOS) detection for CTP bundles in a serial interface or T1/E1 both-ended Y cable configuration (hardware-based redundancy or software-based Y cable link protocol). [PR/1145768]
- On a CTPView server, 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/1116023]
- CTPView servers accept CTP system passwords that are only up to 15 characters in length, which causes certain passwords do not work for connecting CTPView to CTP devices. [PR/1116143]
- In Apache, the ServerSignature directive must be set to "Off" instead of "On". [PR/1126007]
- Attempts to log in that are unsuccessful and failed login attempts to access-denied functionalites are not recorded in the log file on the CTPView server. [PR/1127686]
- Hostnames in CTPView are not compliant with fully qualified domain name (FQDN) standards. [PR/1128559]
- The PHP session lifetime attribute, session.gc_maxlifetime, needs to be increased to 900 seconds (15 minutes) in the **/etc/php.ini** file to comply with JITC requirements. [PR/1130464]
- The transaction isolation setting, transaction_isolation, needs to be changed to REPEATABLE-READ in the **/etc/my.cnf** file to comply with JITC requirements.[PR/1133439]
- OpenSSL, instead of NSS, is needed for authentication of user login through the CTPView GUI to comply with the FIPS 140-2 standard. [PR/1135070]
- Support is needed in the **audit.rules** file for auditing to be performed for all the CTPView commands. [PR/1135114]
- Having a user attempt to login simultaneously with a user currently logged in causes the invalid login counter to increment. It is observed that this behavior locks out the local account. Additionally, the valid logged-in user session was terminated, which causes that user to wait for the default timeout before the user can log back in. [PR/1143900]
- You cannot manage IP access control lists (ACLs) for accessing CTPView unless you use MySQL and modify the tables directly. [PR/1144358]
- The complete resolution for CVE-2015-8126 is needed in the CTPView server. [PR/1144457]
- OpenSSL upgrade to 1.2.0e is required to address security vulnerabilities. [PR/1144746]

- When a user logs into the CTPView server using a common access card (CAC), and then selects the logout button, the user is not logged out. [PR/1146110]
- You cannot start the SNMP daemon in CTPView. Also, a "Segmentation fault" message is returned when you perform an SNMP walk, run SNMP traps, or perform an SNMP Get operation. This SNMP version supports SNMP authentication for which the SNMPV3 user needs to be added in the **/etc/snmp/snmpd.conf** file. [PR/1147782]
- A positive acceptance screen with display of the banner to continue the login to CTPView server web page is needed. [PR/1149566]
- You can enter incorrect IP addresses for NTP client and peer fields on the CTPView Admin page. [PR/1079115]
- CTPView does not synchronize with the remote NTP server. [PR/1104114]

Known Issues in CTPView Release 7.2R1

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

- PBS configured with PPP encapsulation does not function on a CTP150 device. [PR/784778]

CVEs and Security Vulnerabilities Addressed in CTPView Release 7.2R1

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

Table 2: Critical or Important CVEs Included in Apache Version 2.2.31

Critical or Important CVEs Included in Apache Version 2.2.31	
CVE-2015-3183	CVE-2014-0231

[PR/1136821, PR/1081228]

Table 3: Critical or Important CVEs Included in Red Hat Linux Kernel and SQLite Packages

Critical or Important CVEs Included in Red Hat Linux Kernel and SQLite Packages	
CVE-2015-4167	CVE-2015-3416

[PR/1105559]

Table 4: Critical or Important Security Vulnerabilities Addressed in POODLEV2

Critical or Important Security Vulnerabilities Addressed in POODLEV2
TLS 1.0 Padding Oracle Attack Vulnerability (POODLEV2)

[PR/1110561]

Table 5: Critical or Important CAT I Cross Site Scripting Vulnerabilities Addressed

Critical or Important CAT I Cross Site Scripting Vulnerabilities Addressed
Multiple CAT I Cross Site Scripting Vulnerabilities

[PR/1080683]

Table 6: Critical or Important CAT I SQL Injection and Integer Overflow Vulnerabilities Addressed

Critical or Important CAT I SQL Injection and Integer Overflow Vulnerabilities Addressed
Multiple CAT I SQL Injection and Integer Overflow Vulnerabilities

[PR/1080681]

Table 7: Critical or Important CVEs Included in Linux Kernel Package

Critical or Important CVEs Included in Linux Kernel Package	
CVE-2014-8159	CVE-2014-8867

[PR/1136283]

Table 8: Critical or Important CVEs Included in OpenLDAP Package

Critical or Important CVEs Included in OpenLDAP Package			
CVE-2010-1168	CVE-2011-3597	CVE-2012-5195	CVE-2012-6329
CVE-2013-1667	CVE-2008-5302	CVE-2008-5303	CVE-2012-5526
CVE-2010-2761	CVE-2010-4410		

[PR/1135991]

Table 9: Critical or Important CVEs Included in Perl Package

Critical or Important CVEs Included in Perl Package		
CVE-2010-0212	CVE-2011-1024	CVE-2013-4449

[PR/1135997]

Table 10: Critical or Important CVEs Included in libuser Package of CentOS

Critical or Important CVEs Included in libuser Package of CentOS
CVE-2011-0002

[PR/1087204], [PR/1094262]

Table 11: Critical or Important CVEs Included in device-mapper-multipath Package of CentOS

Critical or Important CVEs Included in device-mapper-multipath Package of CentOS
CVE-2009-0115

[PR/1087204], [PR/1094262]

Table 12: Critical or Important CVEs Included in udev Package of CentOS

Critical or Important CVEs Included in udev Package of CentOS
CVE-2009-1185

[PR/1087204], [PR/1094262]

Table 13: Critical or Important CVEs Included in tar Package of CentOS

Critical or Important CVEs Included in tar Package of CentOS	
CVE-2010-0624	CVE-2007-4476

[PR/1087204], [PR/1094262]

Table 14: Critical or Important CVEs Included in cpio Package of CentOS

Critical or Important CVEs Included in cpio Package of CentOS	
CVE-2010-0624	CVE-2007-4476

[PR/1087204], [PR/1094262]

Table 15: Critical or Important CVEs Included in Perl Package of CentOS

Critical or Important CVEs Included in Perl Package of CentOS			
CVE-2010-1168	CVE-2010-1447	CVE-2008-5302	CVE-2008-5303
CVE-2011-3597	CVE-2010-4410	CVE-2011-3597	CVE-2012-5195
CVE-2012-5526	CVE-2012-6329	CVE-2013-1667	

[PR/1087204], [PR/1094262]

Table 16: Critical or Important CVEs Included in Glib Package of CentOS

Critical or Important CVEs Included in Glib Package of CentOS
CVE-2013-0292

[PR/1087204], [PR/1094262]

Table 17: Critical or Important CVEs Included in krb5 Package of CentOS

Critical or Important CVEs Included in krb5 Package of CentOS	
CVE-2014-4345	

[PR/1087204], [PR/1094262]

Table 18: Critical or Important CVEs Included in rpm Package of CentOS

Critical or Important CVEs Included in rpm Package of CentOS	
CVE-2013-6435	

[PR/1087204], [PR/1094262]

Table 19: Critical or Important CVEs Included in newt Package of CentOS

Critical or Important CVEs Included in newt Package of CentOS	
CVE-2009-2905	

[PR/1087204], [PR/1094262]

Table 20: Critical or Important CVEs Included in libtool Package of CentOS

Critical or Important CVEs Included in libtool Package of CentOS	
CVE-2009-3736	

[PR/1087204], [PR/1094262]

Table 21: Critical or Important CVEs Included in Ipsec-tools Package of CentOS

Critical or Important CVEs Included in Ipsec-tools Package of CentOS	
CVE-2009-1632	CVE-2009-1574

[PR/1087204], [PR/1094262]

Table 22: Critical or Important CVEs Included in Gcc and Gcc4 Packages of CentOSs

Critical or Important CVEs Included in Gcc and Gcc4 Packages of CentOSs	
CVE-2009-3736	

[PR/1087204], [PR/1094262]

Table 23: Critical or Important CVEs Included in Gzip Package of CentOS

Critical or Important CVEs Included in Gzip Package of CentOS
CVE-2010-0001

[PR/1087204], [PR/1094262]

Table 24: Critical or Important CVEs Included in pcsc-lite Package of CentOS

Critical or Important CVEs Included in pcsc-lite Package of CentOS	
CVE-2010-0407	CVE-2009-4901

[PR/1087204], [PR/1094262]

Table 25: Critical or Important CVEs Included in OpenLdap Package of CentOS

Critical or Important CVEs Included in OpenLdap Package of CentOS			
CVE-2010-0211	CVE-2010-0212	CVE-2011-1024	CVE-2011-1081
CVE-2011-1025	CVE-2013-4449		

[PR/1087204], [PR/1094262]

Table 26: Critical or Important CVEs Included in postgresql and postgresql84 Packages of CentOS

Critical or Important CVEs Included in postgresql and postgresql84 Packages of CentOS			
CVE-2010-3433	CVE-2010-4015	CVE-2011-2483	CVE-2012-0868
CVE-2012-0866	CVE-2012-2143	CVE-2012-3488	CVE-2014-0060
CVE-2014-0061	CVE-2014-0062	CVE-2014-0063	CVE-2014-0064
CVE-2014-0065	CVE-2014-0066		

[PR/1087204], [PR/1094262]

Table 27: Critical or Important CVEs Included in postfix Package of CentOS

Critical or Important CVEs Included in postfix Package of CentOS		
CVE-2008-2937	CVE-2011-0411	CVE-2011-1720

[PR/1087204], [PR/1094262]

Table 28: Critical or Important CVEs Included in dbus Package of CentOS

Critical or Important CVEs Included in dbus Package of CentOS			
CVE-2011-2200	CVE-2008-3834	CVE-2009-1189	CVE-2010-4532

[PR/1087204], [PR/1094262]

Table 29: Critical or Important CVEs Included in quota Package of CentOS

Critical or Important CVEs Included in quota Package of CentOS
CVE-2012-3417

[PR/1087204], [PR/1094262]

Table 30: Critical or Important CVEs Included in TCL Package of CentOS

Critical or Important CVEs Included in TCL Package of CentOS	
CVE-2007-4772	CVE-2007-6067

[PR/1087204], [PR/1094262]

Table 31: Critical or Important CVEs Included in autofs Package of CentOS

Critical or Important CVEs Included in autofs Package of CentOS
CVE-2012-2697

[PR/1087204], [PR/1094262]

Table 32: Critical or Important CVEs Included in wget Package of CentOS

Critical or Important CVEs Included in wget Package of CentOS
CVE-2009-3490

[PR/1087204], [PR/1094262]

Table 33: Critical or Important CVEs Included in libjpeg Package of CentOS

Critical or Important CVEs Included in libjpeg Package of CentOS
CVE-2013-6629

[PR/1087204], [PR/1094262]

Table 34: Critical or Important CVEs Included in net-snmp Package of CentOS

Critical or Important CVEs Included in net-snmp Package of CentOS	
CVE-2012-6151	CVE-2014-2285

[PR/1087204], [PR/1094262]

Table 35: Critical or Important CVEs Included in CCID Package of CentOS

Critical or Important CVEs Included in CCID Package of CentOS
CVE-2010-4530

[PR/1087204], [PR/1094262]

Table 36: Critical or Important CVEs Included in libxml2 Package of CentOS

Critical or Important CVEs Included in libxml2 Package of CentOS
CVE-2014-3660

[PR/1087204], [PR/1094262]

Table 37: Critical or Important CVEs Included in NSS Package of CentOS

Critical or Important CVEs Included in NSS Package of CentOS
CVE-2014-3566

[PR/1087204], [PR/1094262]

Table 38: Critical or Important CVEs Included in Kernel Package of CentOS

Critical or Important CVEs Included in Kernel Package of CentOS	
CVE-2014-8159	CVE-2014-8867

[PR/1087204], [PR/1094262]

Table 39: Critical or Important CVEs Included in dbus-Glib Package of CentOS

Critical or Important CVEs Included in dbus-Glib Package of CentOS
CVE-2010-1172

[PR/1087204], [PR/1094262]

Table 40: Critical or Important CVEs Included in NSS_Db Package of CentOS

Critical or Important CVEs Included in NSS_Db Package of CentOS
CVE-2010-0826

[PR/1087204], [PR/1094262]

Table 41: Critical or Important CVEs Included in Libgcrypt Package of CentOS

Critical or Important CVEs Included in Libgcrypt Package of CentOS
CVE-2013-4242

[PR/1087204], [PR/1094262]

Table 42: Critical or Important CVEs Included in NSS_Db Package of CentOS

Critical or Important CVEs Included in NSS_Db Package of CentOS
CVE-2010-0826

[PR/1087204], [PR/1094262]

Table 43: Critical or Important CVEs Included in SSL Package

Critical or Important CVEs Included in SSL Package	
CVE-2014-3566	CVE-2009-4901

[PR/1087204], [PR/1094262]

Table 44: Critical or Important CVEs Included in SSH Package

Critical or Important CVEs Included in SSH Package
CVE-2008-5161

[PR/1087204], [PR/1094262]

Table 45: Critical or Important CVEs Addressed for ICMP

Critical or Important CVEs Addressed for ICMP
CVE-1999-0524

[PR/1087204], [PR/1094262]

Table 46: Critical or Important CVEs Included in ntp-4.2.8p5

Critical or Important CVEs Included in ntp-4.2.8p5			
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
CVE-2015-7705	CVE-2015-7691	CVE-2015-7692	CVE-2015-7702

[PR/1144300]

Table 47: CVEs Addressed in LibPNG Package

CVEs Addressed in glibc
CVE-2015-08126

[PR/1144457]

Table 48: 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/1144746]

Table 49: Critical or Important Security Vulnerabilities Addressed in OpenSSH-7.1p2

Critical or Important Security Vulnerabilities Addressed Included in OpenSSH-7.1p2
The following security vulnerabilities are addressed in openssh-7.1p2: • OpenSSH 5.4 < 7.1p2 Security Vulnerabilities observed during a Retina scan on CTPView server. • OpenSSH < 6.9 XSecurity Security Bypass - Remote • OpenSSH < 7.0 Multiple Vulnerabilities • OpenSSH < 7.1 Security Bypass Vulnerability

[PR/1156538,PR/1139247]

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

February 2016—Revision 1, CTPView Release 7.2R1