



CTP Series Circuit to Packet Platforms

CTPView Server Release Notes

Release 3.4

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS 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.

Products made or sold by Juniper Networks (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS, JUNOSE, and SDX-300 software) or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Copyright © 2009, Juniper Networks, Inc.
All rights reserved. Printed in USA.

CTPView Server Release Notes Release 3.4
Writing: Diane Florio, Robert Winter
Editing: Fran Mues

Revision History
July 2009

The information in this document is current as of the date listed in the revision history.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer or FCC Notice

This CTP products have been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

- 1. The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").
- 2. The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.
- 3. License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:
 - a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
 - b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.
 - c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
 - d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

CTPView Server Release 3.4

Release Overview

These *Release Notes* accompany Release 3.4 of the CTPView server software. They describe the enhancements as well as known issues with the software. CTPView software is compatible with Juniper Networks® CTP1000 Series and CTP2000 Series platforms running CTPOS version 5.4 or earlier.

If the information in these *Release Notes* differs from the information found in the published documentation set, follow these *Release Notes*. These *Release Notes* include the following sections:

- Release Overview on page 5
- Required Files on page 6
- Installing CTPView Software on page 6
- New Features and Enhancements on page 7
- Resolved Issues on page 19

You can also find these release notes on the Juniper Networks Technical Publications CTP documentation Web page, which is located at <http://www.juniper.net/techpubs/hardware/ctp/>.



NOTE: Documentation for all new CTPView server Release 3.4 features is provided in the New Features and Enhancements section of these release notes. We will incorporate this CTPView server Release 3.4 feature information in the appropriate documentation for CTPView server Release 3.5. The Juniper Networks Technical Documentation Web page contains links to the CTPView server documentation.

Required Files

See *CTP Software Configuration Guide, Chapter 6, Installing the Software and Configuring Security Settings*, for help in choosing the correct upgrade archive file:

- `ctpview_fc4_complete_3.4R1_090715.tgz`
- `ctpview_fc9_complete_3.4R1_090715.tgz`
- `web_fcX_3.4R1_090715.tgz`
- Fedora 9 systems running 3.4R1 or later require the `web_fcX_3.4R1_090715.tgz` file to upgrade. The system will not reboot during the upgrade process.
- Fedora 9 systems running 3.3Rx require the `ctpview_fc9_complete_3.4R1_090715.tgz` file to upgrade. The system will not reboot during the upgrade process.
- Fedora 9 systems running 3.2Rx require the `ctpview_fc9_complete_3.4R1_090715.tgz` file to upgrade. Additionally, on systems running 3.2R1 or 3.2R2 the server will reboot during the upgrade process.
- Fedora Core 4 systems running 2.2R2 or later require the `web_fcX_3.4R1_090715.tgz` file to upgrade. The system will not reboot during the upgrade process.
- Fedora Core 4 systems running 2.2R1 or earlier require the `ctpview_fc4_complete_3.4R1_090715.tgz` file to upgrade. Additionally, the server will reboot during the upgrade process.

Installing CTPView Software

To install the software using a `ctpview_fcX_complete` file:

1. Copy the `ctpview_fcX_complete` file to the `/tmp` directory on the server.
2. Unpack the archive: `tar -xzvf ctpview_fc9_complete_3.4R1_090715.tgz`
3. Run the installation script as root: `/tmp/upgrade`

To install the software using a `web_fcX` file:

1. Copy the `web_fcX` file to the `/tmp` directory on the server.
2. Run the installation script as root: `upgrade`

For further information about software installation, see *CTP Software Configuration Guide, Chapter 6, Installing the Software and Configuring Security Settings*. You can download this document from the Juniper Networks Technical Publications CTP documentation Web page, which is located at <http://www.juniper.net/techpubs/hardware/ctp/>.

Uploading CTP Software Archives to CTPView

You can upload CTP software archives to the CTPView server using the destination directory */ctp* as an alternative to using the full pathname of */var/www/html/acorn/ctp*. To copy software into this directory from an external source, you must be a member of the UNIX group *server*, such as the default user *juniper*. System settings prohibit copying external files to the server as the user root.

New Features and Enhancements

This section describes features and enhancements new to this release:

- “Support for User Authentication to the CTPView Browser Application by Means of a Steel-Belted RADIUS (SBR) Server” on page 7
- “Support for Two-Factor User Authentication to the CTPView Browser Application by Means of an RSA SecurID Appliance” on page 10
- “Support for CTP TDM TDC” on page 14
- “Support for CTP PLAR” on page 14
- “Support for CESoPSN and VCOMP Bundle Statistical Data Graphs” on page 15
- “Support for User Customization of Y-Axis and Time Interval for Statistical Data Graphs” on page 15
- “Ability to Monitor and Control CTP Database Changes” on page 16
- “New Print Buttons for Select CTPView Frames” on page 16
- “Support for Port Mirroring of VCOMP Bundles” on page 17
- “Support for CTP NetRef feature ” on page 18

Support for User Authentication to the CTPView Browser Application by Means of a Steel-Belted RADIUS (SBR) Server

CTPView 3.4R1 installed on a server using the Fedora 9 operating system provides RADIUS authenticated user login to the CTPView browser application when used in conjunction with a Steel-Belted RADIUS (SBR) server.

To enable this feature you must perform the following steps:

1. “Configure RADIUS Settings on the CTPView Server” on page 8
2. “Configure the SBR Server’s Dictionary Files” on page 9
3. “Configure the SBR Server’s Authentication Policies” on page 9
4. “Add CTPView as a RADIUS Client on an SBR Server” on page 10
5. “Add CTPView Users to an SBR Server:” on page 10

The order of user authentication is:

1. SBR server
2. Local CTPView application

You can configure your SBR server to authenticate both Native and SecurID users. The order of authentication between these two categories of users is set on the SBR server. The same user (that is, user ID) may be added to both the SBR server and the local CTPView application.

At this time, CTPView does not support RADIUS authentication for shell access to the CTPView server.

We have tested this feature using SBR release 6.1. This documentation is also based on that release.

Configure RADIUS Settings on the CTPView Server

To configure RADIUS settings on the CTPView server:

1. Log in to CTPView server shell (CLI) and open the menu application.
2. Select the **RADIUS Function** option.
3. Select the **Add/Update RADIUS Template Accounts** option. You will be asked for the MySQL root account password. The required template accounts will be added to CTPView. These accounts are not configurable. This step needs to be performed as part of the initial configuration of CTPView as a RADIUS client. However, repeating this step has no detrimental effect on the RADIUS configuration.
4. Return to the RADIUS Menu.
5. Select the **View/Set RADIUS Servers** option and add the RADIUS server's IP address. You will also be prompted to enter the:
 - shared secret
 - timeout period
 - number of retries.

You may add up to 10 RADIUS servers.

6. Return to the RADIUS Menu.
7. Select the **View/Set RADIUS State** option. Select the option to **Enable RADIUS**.

Configure the SBR Server's Dictionary Files

To configure the SBR server's dictionary files:

1. Log in to the SBR server as an administrator.
2. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\juniper.dct and append the following new block of text to the bottom of the file:

```
#####
# CTP Specific Attributes
#####

ATTRIBUTE Juniper-CTP-Group      Juniper-VSA(21, integer) r
VALUE      Juniper-CTP-Group      Read_Only          1
VALUE      Juniper-CTP-Group      Admin               2
VALUE      Juniper-CTP-Group      Privileged_Admin   3

ATTRIBUTE Juniper-CTPView-APP-Group  Juniper-VSA(22, integer) r
VALUE      Juniper-CTPView-APP-Group  Net_View           1
VALUE      Juniper-CTPView-APP-Group  Net_Admin          2
VALUE      Juniper-CTPView-APP-Group  Global_Admin       3

ATTRIBUTE Juniper-CTPView-OS-Group    Juniper-VSA(23, integer) r
VALUE      Juniper-CTPView-OS-Group    Admin              1
VALUE      Juniper-CTPView-OS-Group    Privileged_Admin   2

#####
# CTP Specific Attributes
#####
```

3. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\vendor.ini and locate the block of text beginning with the line:

```
vendor-product = Juniper M/T Series
```

4. Add the following new block of text after the Juniper M/T Series block you located above:

```
vendor-product    = Juniper CTP Series
dictionary        = Juniper
ignore ports      = no
port-number-usage = per-port-type
help-id           = 2000
```

5. Restart the Steel-Belted RADIUS service on the server.

Configure the SBR Server's Authentication Policies

To configure the SBR server's authentication policies:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing **http://<SBR_IP_ADDRESS>:1812** in the address bar. Click the **Launch** button when the page loads.

2. Select the **Steel-Belted RADIUS > Authentication Policies > Order of Methods** link in the directory frame. Ensure that **Native User** is listed under the section **Active Authentication Methods**.

Add CTPView as a RADIUS Client on an SBR Server

To add CTPView as a RADIUS client on an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing **http://<SBR_IP_ADDRESS>:1812** in the address bar. Click on the Launch button when the page loads.
2. Select the **Steel-Belted RADIUS > RADIUS Clients** link in the directory frame. Add your CTPView server as a client. In the Make or model field, select Juniper CTP Series from the drop-down menu.

Add CTPView Users to an SBR Server:

To add CTPView users to an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing **http://<SBR_IP_ADDRESS>:1812** in the address bar. Click on the Launch button when the page loads.
2. Select the **Steel-Belted RADIUS > Users > Native** link in the directory frame. Add a user using the **Add Native User** dialog box.
3. In the Attributes section, click on the **Return List** tab and select the **Add** button. A new dialog box titled **Add Return List Attribute** will open.
 1. In the Attributes section select **Juniper-CTPView_APP-Group**.
 2. In the Value section select the authorization level of the user you are adding. The choices are:
 - Global_Admin
 - Net_Admin
 - Net_View

See the CTPView documentation for more information about the properties of each of these authorization levels.

Support for Two-Factor User Authentication to the CTPView Browser Application by Means of an RSA SecurID Appliance

CTPView 3.4R1 installed on a server using the Fedora 9 operating system provides two-factor authenticated user login to the CTPView browser application when used in conjunction with an RSA SecurID appliance. The RSA appliance incorporates a Steel-Belted RADIUS (SBR) server, making the configuration here very similar to systems using SBR only.

To enable this feature you must perform the following steps:

1. “Configure RADIUS Settings on the CTPView Server” on page 11
2. “Configure the SBR Server’s Dictionary Files” on page 12
3. “Configure the SBR Server’s Authentication Policies” on page 13
4. “Add CTPView as a RADIUS Client on an SBR Server” on page 13
5. “Add CTPView Users to an SBR Server:” on page 13
6. Assign SecurID tokens to CTPView users

The order of user authentication is:

1. SBR server
2. Local CTPView application

You may configure your SBR server to authenticate both Native and SecurID users. The order of authentication between these two categories of users is set on the SBR server. The same user (that is, user ID) may be added to both the SBR server and the local CTPView application.

At this time CTPView does not support RADIUS authentication for shell access to the CTPView server.

We have tested this feature using SBR release 6.1. This documentation is also based on that release.

Configure RADIUS Settings on the CTPView Server

To configure RADIUS settings on the CTPView server:

1. Log in to CTPView server shell (CLI) and open the menu application.
2. Select the **RADIUS Function** option.
3. Select the **Add/Update RADIUS Template Accounts** option. You will be asked for the MySQL root account password. The required template accounts will be added to CTPView. These accounts are not configurable. This step needs to be performed as part of the initial configuration of CTPView as a RADIUS client. However, repeating this step has no detrimental effect on the RADIUS configuration.
4. Return to the RADIUS Menu.

5. Select the **View/Set RADIUS Servers** option and add the RADIUS server's IP address. You will also be prompted to enter the:
 - shared secret
 - timeout period
 - number of retries.

You may add up to 10 RADIUS servers.
6. Return to the RADIUS Menu.
7. Select the **View/Set RADIUS State** option. Select the option to **Enable RADIUS**.

Configure the SBR Server's Dictionary Files

To configure the SBR server's dictionary files:

1. Login to the SBR server as an administrator.
2. Open the file C:\Program Files\Juniper Networks\Steel-Belted Radius\Service\juniper.dct and append the following new block of text to the bottom of the file:

```
#####
# CTP Specific Attributes
#####

ATTRIBUTE Juniper-CTP-Group      Juniper-VSA(21, integer) r
VALUE      Juniper-CTP-Group      Read_Only      1
VALUE      Juniper-CTP-Group      Admin           2
VALUE      Juniper-CTP-Group      Privileged_Admin 3

ATTRIBUTE Juniper-CTPView-APP-Group  Juniper-VSA(22, integer) r
VALUE      Juniper-CTPView-APP-Group  Net_View       1
VALUE      Juniper-CTPView-APP-Group  Net_Admin      2
VALUE      Juniper-CTPView-APP-Group  Global_Admin   3

ATTRIBUTE Juniper-CTPView-OS-Group    Juniper-VSA(23, integer) r
VALUE      Juniper-CTPView-OS-Group    Admin           1
VALUE      Juniper-CTPView-OS-Group    Privileged_Admin 2

#####
# CTP Specific Attributes
#####
```

3. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\vendor.ini and locate the block of text beginning with the line:

```
vendor-product = Juniper M/T Series
```

4. Add this new block of information after the Juniper M/T Series block you located.

```
vendor-product = Juniper CTP Series
dictionary     = Juniper
ignore ports   = no
port-number-usage = per-port-type
help-id        = 2000
```

5. Restart the Steel-Belted RADIUS service on the server.

Configure the SBR Server's Authentication Policies

To configure the SBR server's authentication policies:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing **http://<SBR_IP_ADDRESS>:1812** in the address bar. Click the **Launch** button when the page loads.
2. Select the **Steel-Belted RADIUS > Authentication Policies > Order of Methods** link in the directory frame. Ensure that **SecurID User** is listed under the section **Active Authentication Methods**.

Add CTPView as a RADIUS Client on an SBR Server

To add CTPView as a RADIUS client on an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing **http://<SBR_IP_ADDRESS>:1812** in the address bar. Click the **Launch** button when the page loads.
2. Select the **Steel-Belted RADIUS > RADIUS Clients** link in the directory frame. Add your CTPView server as a client. In the **Make or model** field, select **Juniper CTP Series** from the drop-down menu.

Add CTPView Users to an SBR Server:

To add CTPView users to an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing **http://<SBR_IP_ADDRESS>:1812** in the address bar. Click on the **Launch** button when the page loads.
2. Select the **Steel-Belted RADIUS > Users > SecurID** link in the directory frame. Add a user using the **Add SecurID User** dialog box.
3. In the **Attributes** section, click on the **Return List** tab and select the **Add** button. A new dialog box titled **Add Return List Attribute** will open.
 1. In the **Attributes** section select **Juniper-CTPView_APP-Group**.
 2. In the **Value** section select the authorization level of the user you are adding. The choices are:
 - Global_Admin
 - Net_Admin
 - Net_View

See the CTPView documentation for more information about the properties of each of these authorization levels.

Assign SecurID Tokens to CTPView Users

To assign SecurID tokens to CTPView users, launch the RSA Authentication Manager Host Mode application on the RSA SecurID appliance. From the menu bar, select **User > Add User**. At a minimum, complete these required fields:

- Last Name
- Default Login
- Required to Create a PIN
- Assign Token.

The first time a new user logs in to CTPView, he or she must use the SecurID token Passcode as the password. The user will be prompted to create a PIN. Thereafter, the user must log in using the PIN + Passcode as the password.

Support for CTP TDM TDC

CTPView 3.4R1 supports Time-Division Multiplexing (TDM) using Time Data Correlation (TDC) on CTP2000 Series serial interface cards. The CTP node must be running CTPOS 5.4R1 or later.

To configure CTP bundles to use the TDM TDC feature:

1. Open the bundle configuration page by clicking the link **Bundle > Configuration** in the directory at the left of the main CTPView frame.
2. Create a new CTP bundle or select an existing CTP bundle.

Even-numbered ports can be configured for TDM serial encoding, TDM Function and TDM Rate. Odd-numbered ports can be configured for TDM/TDC Interleaved Slow Port clock configuration.

Setting a CTP node to use this feature requires specific configuration parameters to be correctly selected. See the CTPOS documentation for more detailed information on the TDM TDC feature.

Support for CTP PLAR

CTPView 3.4R1 supports private-line automatic ringdown (PLAR) for Voice FXS ports attached to a VCOMP bundle. The CTP node must be running CTPOS 5.4R1 or later.

To configure the PLAR option:

1. Open the bundle configuration page by clicking the link **Bundle > Configuration** in the directory at the left of the main CTPView frame.
2. Create a new VCOMP bundle or select an existing VCOMP bundle which has a FXS port attached. The PLAR option is located near the bottom of the Port Options column.

See the CTPOS documentation for more detailed information on the PLAR feature.

Support for CESoPSN and VCOMP Bundle Statistical Data Graphs

CTPView 3.4R1 supports the display of bundle statistical data graphs for CESoPSN and VCOMP bundles. The CTP node must be running CTPOS 5.4R1 or later. Previous versions do not provide graphs for these type bundles.

To display statistical graphs:

1. Open the Plots page by clicking the link **Statistics > Plots**.
2. You can select a single bundle to display or choose all configured bundles. The plots from the remote end of the circuit can also be displayed if you select a single bundle. Place a check mark in the check box if you want this option.

Support for User Customization of Y-Axis and Time Interval for Statistical Data Graphs

The behavior of CTPView when it displays statistical plots for CTP nodes running CTPOS 4.x or earlier has not changed. You have two options to choose from when selecting data graphs, preset or custom.

CTPView releases in the 3.x series before 3.4 do not support user customization of the y-axis or time interval of the data graphs for CTP nodes running CTPOS 5.x.

User customization of data graphs for CTP nodes running CTPOS 5.x is reintroduced with the release of CTPView 3.4R1. This implementation varies from the scheme used in CTPOS 4.x. releases.

1. Open the Plots page by clicking the link **Statistics > Plots**.
2. Select a single bundle to display, or choose all configured bundles. The plots from the remote end of the circuit can also be displayed if you select a single bundle. Place a check mark in the check box if you want this option.
3. Open the custom y-axis dialog box by clicking the **Custom Y-axis Options** button. For each of the plot types Buffer, PDV and RTD you can set any or all of these parameters:
 - Min Y-axis
 - Max Y-axis
 - Units Y-axis

The default value is auto, which allows CTPView to set the parameters to best fit the plot data. You can reset all fields to auto by clicking the **Reset Custom Y-axis** button. You can close the dialog box by clicking the **Custom Y-axis Options** button.

The custom y-axis values apply to the plots for all bundles, regardless whether the dialog box is open or closed. Custom y-axis values remain set after a bundle is selected and its plots are displayed. Reopening the page from the Directory frame link will reset the y-axis values to auto.

4. Open the custom time interval dialog box by clicking the **Custom Time Options** button. The start and end time can then be set. You can reset the custom time values to the default interval of the past 24 hours by clicking the **Reset Custom Time** button. The custom time interval is used when you select the **Custom Time** button located at the far right of the bundle button row to display the plots.

The dialog box can be closed by clicking the **Custom Time Options** button.

Ability to Monitor and Control CTP Database Changes

CTPView 3.4R1 supports the CTP database control feature designed to monitor CTP configuration changes by other users during a CTPView session and notify you when they occur. The CTP node must be running CTPOS 5.4R1 or later.

This feature is available on these pages:

- Bundle > Configuration
- Bundle > Change Status
- Node > PBS/Bridge Config
- Node > Config

When you submit a configuration from one of these pages, the CTP database is checked for changes from the database that was in use at the time the CTPView page was opened. If changes are detected, the system gives you the option to overwrite the CTP database with the new one you are submitting, or to abort the submission.

Overwriting the CTP database will return all settings in the database to their values when the current CTPView page was opened, not just the settings displayed on the page. This process will remove any changes other users made after the current CTPView page was opened.

If you abort your submission, you can reload the CTPView page to bring in the CTP database changes made by other users, and then resubmit the configuration modifications you originally attempted to make.

New Print Buttons for Select CTPView Frames

CTPView 3.4R1 allows you to print designated portions of the main frame for certain pages. When you click the print button, a new window will open which contains the selected frame. You can then use your browser functions to print or save the frame.

The print button is available on the following pages:

- Bundle > Configuration
- Bundle > Query
- Bundle > Runtime Query

- Node > Summaries
- Node > PBS/Bridge Config
- Node > PBS/Bridge Query
- Node > Config
- Node > Query
- System > Configuration
- System > Query

The following pages use the same printer friendly functions as in previous CTPView versions:

- Node > Maintenance > View Network Host Reports
- Statistics > Plots
- Server > Diagnostics > Validate Server Configuration

Support for Port Mirroring of VCOMP Bundles

CTPView 3.4R1 provides support for port mirroring of VCOMP bundles. This CTP feature was introduced in CTPOS 5.4.

To configure port mirroring:

1. Access the bundle configuration page by clicking the link **Bundle > Configuration** in the directory at the left of the main CTPView frame.
2. Create a new VCOMP bundle, or select an existing VCOMP bundle.
3. Locate the port mirroring options near the bottom of the Bundle Options column.
4. Place a check mark in the Show check box to display or reconfigure the existing port mirroring values.
5. You can configure up to 10 source tails and 10 destination tails for each bundle. To remove a tail, check the Remove Tail check box.



NOTE: To add a new port mirroring tail, values must be entered for both the remote address and the remote CID.

Support for CTP NetRef feature

CTPView 3.4R1 supports the network node reference (NetRef) feature to provide clocking to a CTP node over a network. The CTP node must be running CTPOS 5.4R1 or later.

To configure NetRef to provide clocking to a CTP node:

1. Open the node configuration page by clicking the link **Node > Node Config** in the directory at the left of the main CTPView frame.
2. In the configuration table, look for the row labeled NetRef.

Setting a CTP node to use the NetRef feature requires that configuration parameters be set correctly on other CTP nodes using this feature in your network. See the CTPOS documentation for more detailed information about the NetRef feature.

Resolved Issues

The following are resolved issues for this release.

Configuration Changes Failed for a VCOMP T1E1 Port When the Port Was Shared with Another Bundle That Was Active

When configuring multiple VCOMP bundles using the same T1E1 interface module, you no longer receive an error message when you submit a bundle change if one of the other bundles sharing the same port is active. [PR/442256: This issue has been resolved.]

On a Very High Latency Network, the CTP www_nid Query Timed Out

When operating in a high latency network, you may have experience a timeout during the CTPView-to-CTP Node dialog that is part of the connection protocol with a CTP node, even though you had set the **Network Latency** option for CTPview to high. This issue has been fixed. [PR/442260: This issue has been resolved.]

For VCOMP T1E1 Bundles, the Source Port Field on the Change Bundle Status Page Included Errant "1" Characters

When you created VCOMP bundles using a T1E1 interface module, the source port field in the selection table on the **Bundles > Change Status** page showed one or more errant 1's in the channel list. This has been fixed. [PR/442270: This issue has been resolved.]

For VCOMP T1E1 Bundles, the Bundle Configuration Page Did Not Display Properly

When you created VCOMP bundles using a T1E1 interface module, the bundle configuration table on the **Bundles > Configuration** was not displayed when it was selected from the menu. This has been fixed. [PR/442272: This issue has been resolved.]

Required New User Password to Be Dissimilar from the Old Password

The previous password-changing function for the browser interface of CTPView did not analyze the similarity of the old password with the submitted new password. [PR/456777: This issue has been resolved.]

Order of Attached Ports in a VCOMP Bundle Were Sorted When Configured with CTPView

CTPView did not allow you to set the order of attached voice ports on a VCOMP bundle. This issue has been fixed. [PR/456782: This issue has been resolved.]

User Could Not Remove Port Mirroring Tails From Bundles Using CTPView

There was no mechanism in CTPView release 3.3 to allow you to remove port mirroring source or destination tails from a bundle. This issue has been fixed.[PR/458709: This issue has been resolved.]

User Could Not Configure SATOP Port to E1 Interface Using CTPView

When configuring a T1/E1 DCARD port in a SATOP bundle, the option to switch between the T1 and E1 interfaces was not being displayed on the CTPView configuration page. [PR/437547: This issue has been resolved.]

Known Issues

There are no known issues for this release.

