CTPView Management System, version 7.1R2
Software Release Notes

Release 7.1R2
18th Nov 2015

These release notes accompany Release 7.1R2 of the CTPView Management System software. They describe the defects fixes as well as known issues with the software. CTPView Management System software runs on all CTPView appliances. This release provides management services for CTP systems running CTPOS 7.1 and below.

New Features and Enhancements:

- None at this time.

Security Updates of CentOS Operating System

- None at this time.

Fixes:

- [PR 1084594] JITC: TAINT not enabled on PERL scripts.
- [PR 1116023] JITC: Add pam_faildelay rule to /etc/pam.d/system-auth file in CTP View.
- [PR 1084593] JITC: Remove RC4 ciphers from the NSS SSL configuration.
- [PR 1087204] Security Vulnerabilities on CTPView server running 7.0R3.
- [PR 1136283] Vulnerabilities found in Linux kernel package on CTP View.
- [PR 1136821] Vulnerabilities found in Apache version 2.2.29.
- [PR 1135991] Vulnerabilities found in OpenLDAP package.
- [PR 1135997] Vulnerabilities found in Perl package.
- [PR 1139247] SSH vulnerabilities found during retina scan.

Known Issues:

- None.

Notes:

Security Deployment Guide
The guide is available for download at
http://www.juniper.net/techpubs/en_US/ctp7.0/information-products/pathway-pages/ctp-series/index.html

Required Files:

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

- web_update_7.1R2_151118.tgz [Software Updates]
- ctpview_complete_centos_7.1R2_ 151118.tgz [Software and CentOS OS Updates]
- ctpview_complete_fc9_7.1R2_ 151118.tgz [Software and Fedora 9 OS Updates]
- ctpview_complete_fc4_7.1R2_ 151118.tgz [Software and Fedora 4 OS Updates]

Use the following table to determine the correct file to use:

CTPView Server OS	Installed CTPView Release	File for Upgrade	Server Reboots During Upgrade ?
Cent OS 5.11	4. 5R2 or earlier 4.6R1 or earlier 7.0R4 or earlier 7.1R1_JITC or earlier	ctpview_complete_centos_7.1R2_ 151118.tgz	Yes

Installing Software:

On systems running 3.4R2-p1 or 3.4R3 or later:

1. Copy the File for Upgrade to the /tmp directory on the server.
2. Log into server shell.
    a. On CentOS systems as a System Administrator
    b. On FC9 or FC4 systems switch to the root user after log in.
3. Run the upgrade script: ***upgrade***

Note: When upgrading CentOS 5.11 systems running a release earlier than 4.1R1 you will be prompted to enter the MySQL Administrator's password. This is necessary in order to upgrade the database structures. If you fail to enter the correct password the upgrade process will continue and the server will remain usable. However, to properly complete the upgrade process you will need to

manually initiate the database structure upgrade script from the cli menu. The path to this function is menu > MySQL Functions > Upgrade Database Structures.

On systems running 3.4R2 or earlier and requiring a ctpview_complete file:

1. Copy the Upgrade File to the /tmp directory on the server.
2. Log into server shell. Switch to the **root** user after log in.
3. Unpack the ctpview_complete file. For example,
   tar –xzvf ctpview_complete_centos_7.1R2_ 151118.tgz
4. Run the upgrade script: ***upgrade***

On systems running 3.4R2 or earlier and requiring the web_update file:

1. Copy the Upgrade File to the /tmp directory on the server.
2. Log into server shell. Switch to the **root** user after log in.
3. Run the upgrade script: ***upgrade***

Note: - Disable all the ports/bundles of the CTP box before initiating the CTPOS upgrade process using CTP complete package.