Juniper Networks | Engineering Simplicity

Juniper Networks® CTPView Server Software Release 9.1R1

Published
2026-02-19

RELEASE

Table of Contents

About This Guide

These release notes accompany Release 9.1R1 of the CTPView Server Software. They contain install information and describe the enhancements to the software. The CTPView Release 9.1R1 software is compatible with Juniper Networks CTP Series platforms running CTPOS version 9.1R1 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/documentation/product/en_US/ctpview.

Release Highlights

The following features or enhancements have been added to CTPView Release 9.1R1.

- CTPView Release 9.1R1 uses PostgreSQL database. [PR 1387325]
- Support is added for using CTPView to manage the CTP151 device. [PR 1422572]
- CTPView Release 9.1R1 enables you to prevent a guest login via TACACS. [PR 1399085]
- CTPView Release 9.1R1 supports a FIPS compliant database. [PR 1415801]
- CTPView Release 9.1R1 enables you to change banners. [PR 1417740]
- Several usability enhancements to MS-DCARD have been added. [PR 1421150]
- Support is added for a customizable bundle runtime query. [PR 1427982]

NOTE: CTPView 9.1R1 runs on an updated OS (CentOS 7.5.1804) which provides better security with improved resilience and robustness.

The following features are not supported in CTPView Release 9.1R1.

- PBS and L2Agg features are not supported in CTPView 9.1R1 release. These features will be reintroduced in a future release. [PR 1409289]
- VCOMP bundle and CESoPSN analog voice bundle features are not supported in CTPView 9.1R1 release. These features will be reintroduced in a future release. [PR 1409293]
- Deprecated Apache cron jobs have been removed. [PR 1343265]

Required Install Files

It is your responsibility to install CentOS on a VM, and the CentOS version must be 7.5.1804 (http://vault.centos.org/7.5.1804/isos/x86_64/). For information on how to create a CentOS 7 virtual machine, see "Creating a CentOS 7 Virtual Machine" on page 4. We recommend you to not install the latest CentOS version. If you have queries or need further assistance, contact Juniper Networks Technical Assistance Center (JTAC).

We provide the following files for installing the CTPView software:

- **CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm** [CTPView Software RPM]

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

CTPView Server OS	Installed CTPView Release	File to install CTPView	Server Reboots During Installation?
CentOS 7.5	NA	CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm	Yes

Recommended System Configuration for Hosting a CTPView Server

The following are the recommended hardware configuration to setup a CTPView 9.1R1 server:

- CentOS 7.5.1804 (64-bit)
- 1x processor (4 cores)
- 4 GB RAM
- Number of NICs - 2
- 80 GB Disk space

CTPView Installation and Maintenance Policy

From the release of CTPView 9.0R1, Juniper Networks has adopted a new policy for installation and maintenance of the CTPView server. CTPView is now being distributed as an "Application only" product, in the form of an RPM package. You can now install and maintain the OS (CentOS 7.5) according to the guidelines described in "Installing CTPView 9.1R1" on page 12. With the CTPView 7.3Rx and earlier releases, the OS (CentOS 5.11) and CTPView application were combined and distributed as a single installation ISO, and all updates (OS and CTPView application) were only available from Juniper Networks. This causes a delay in getting CTPView maintenance releases for important security updates (including Linux OS applications and CTPView application).

With this new model, you can update individual CentOS applications independently from the CTPView application if any security vulnerabilities are reported for the Linux OS applications. This provides more flexibility you need to ensure the security of your Linux-based platforms.

CTPView is made up of:

- Type 1—Stock CentOS 7.5 RPMs
- Type 2—Stock CentOS RPMs from other CentOS versions
- Type 3—Modified CentOS RPMs
- Type 4—CTPView application file

Where, "Stock" RPMs are the packages that are associated with a particular release of CentOS and readily available on the Internet. "Modified" RPMs are stock versions of RPMs that are modified by Juniper Networks for the needs of the CTPView platform. The CentOS 7.5 installation ISO only contains the components of type 1. The monolithic CTPView RPM contains the remaining components of types 2, 3, and 4, which can be unpacked and installed.

When Juniper Networks delivers a CTPView maintenance release RPM, it contains the updated component versions of types 2, 3, and 4. It also contains dependencies to make sure that type 1 components are also up to date and warn the user if any of them need to be updated.

Juniper Networks maintains a list of RPMs for CTPView that we suggest to be upgraded for security and functional reasons. The following methods are used for determining which CTPView RPMs need updates:

- Regular Retina scans
- Notifications from Juniper's SIRT team
- Reports from customers

When an RPM update is required, Juniper Networks validates the new version of the component to make sure that it functions properly before adding it to the RPM list. This list will be shared to you via a KB. Although CTPView maintenance updates mandate (and possibly provide) up-to-date RPMs before installation, this RPM list helps you to update your CTPView software between releases. If there is an RPM added to the RPM list, you can take immediate action. Juniper Networks delivers the components of type 3 via maintenance releases only. For type 1 and 2 components, the RPMs should be freely available on the web, and Juniper Networks provides sample links. If you discover that an RPM needs a security update and it is not in the RPM list, you can notify us so that we can test it and add it to the list.

CAUTION: A bulk RPM update using "yum update" is strictly forbidden. CTPView 9.x, although mainly based on CentOS 7.5, is also made up of RPMs from other distributions. Performing an update to the latest version of CentOS 7 may cause CTPView to be non-functional, and a reinstallation may be required.

If you update RPMs that are not on the KB RPM list, CTPView may not function properly.

Creating a CentOS 7 Virtual Machine

Before you begin:

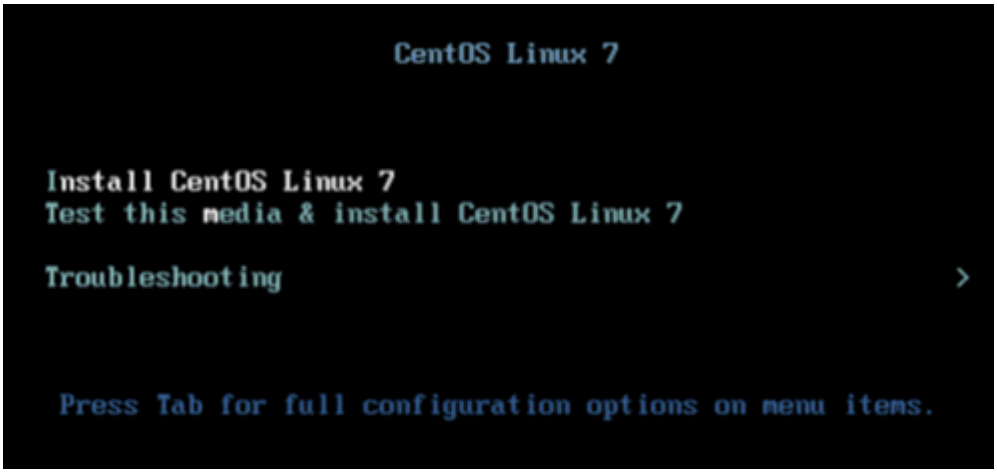
- Make sure that vSphere client is installed on your workstation.

NOTE: Within vSphere, there are numerous ways to perform a particular task. The following example illustrates one such method. You can use the procedure that suits your network deployment effectively.

NOTE: If you are installing CTPView on a bare metal, you can skip this topic and continue with the CTPView installation procedure (see "Installing CTPView 9.1R1" on page 12). To install the ISO file (centOS-7-x86_64-DVD-1804.iso) on a bare metal server, copy the ISO file to a bootable CD and then install the ISO file from the CD. At the boot prompt, you should select the installation option as "ctpview-vmware" and the Ethernet NIC type as “E1000”. Recommended hardware configurations are 1 GB RAM with 60 GB disk space and 2 cores per CPU.

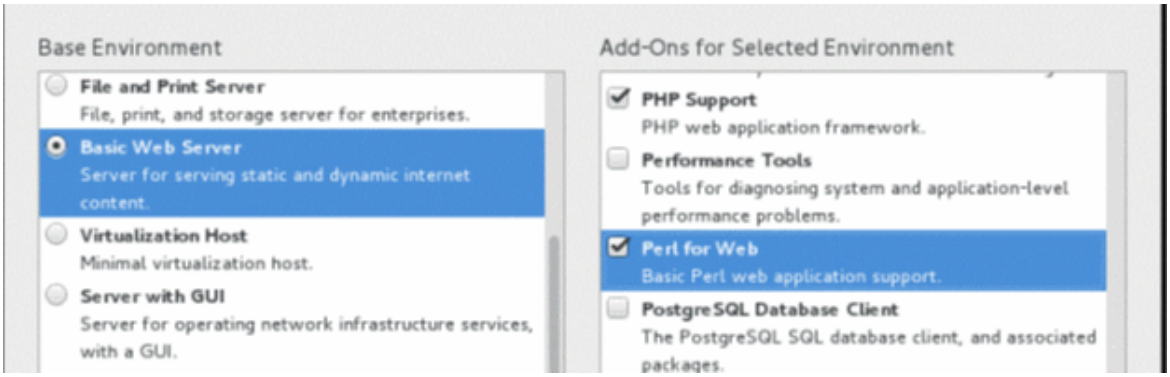
To create a new CentOS 7 STIG’d VM instance of CTPView server on an ESXi Server:

1. Copy the CentOS 7 ISO file (**centOS-7-x86_64-DVD-1804.iso**) to the ESXi datastore. The CentOS 7 ISO can be downloaded from http://vault.centos.org/7.5.1804/isos/x86_64/.
2. Start the vSphere client and enter the ESXi server IP address and your login credentials.
3. Start the wizard to create a new virtual machine. Select **File** > **New** > **Virtual Machine**.
4. Select the configuration as **Typical** and click **Next**.
5. Enter a name for the VM. For example, CTPView_9.1R1.
6. Select the datastore (with at least 80 GB free space) and click **Next**.
7. Select Guest OS as **Linux** and version as **Other Linux (64-bit)**, and then click **Next**.
8. Select the number of NICs as **2** and adapter type as **E1000**, and then click **Next**.
9. Select the virtual disk size as **80 GB** and select **Thick Provision Lazy Zeroed**.
10. Select the **Edit the virtual machine settings before completion** check box and click **Continue**.
11. Click the **Hardware** tab and select memory size as **4 GB**.
12. In the **Hardware** tab, select **CPU**. Then, select the number of virtual sockets as 2 and number of cores per socket as 1 (you can select up to 4 cores).
13. In the **Hardware** tab, select **CD/DVD**. Then, select the device type as **Datastore ISO File** and browse to CentOS 7 ISO file. Select the **Connect at power on** check box under **Device Status**.
14. Click **Finish**.
15. Select your created virtual machine in the left panel of **vSphere** > **Inventory**.
16. In the **Getting Started** tab, select **Power on the virtual machine**.
17. Switch to the **Console** tab and click inside the terminal emulator.
18. Select the **Install CentOS Linux 7** option with the Up Arrow key and press **Enter**.

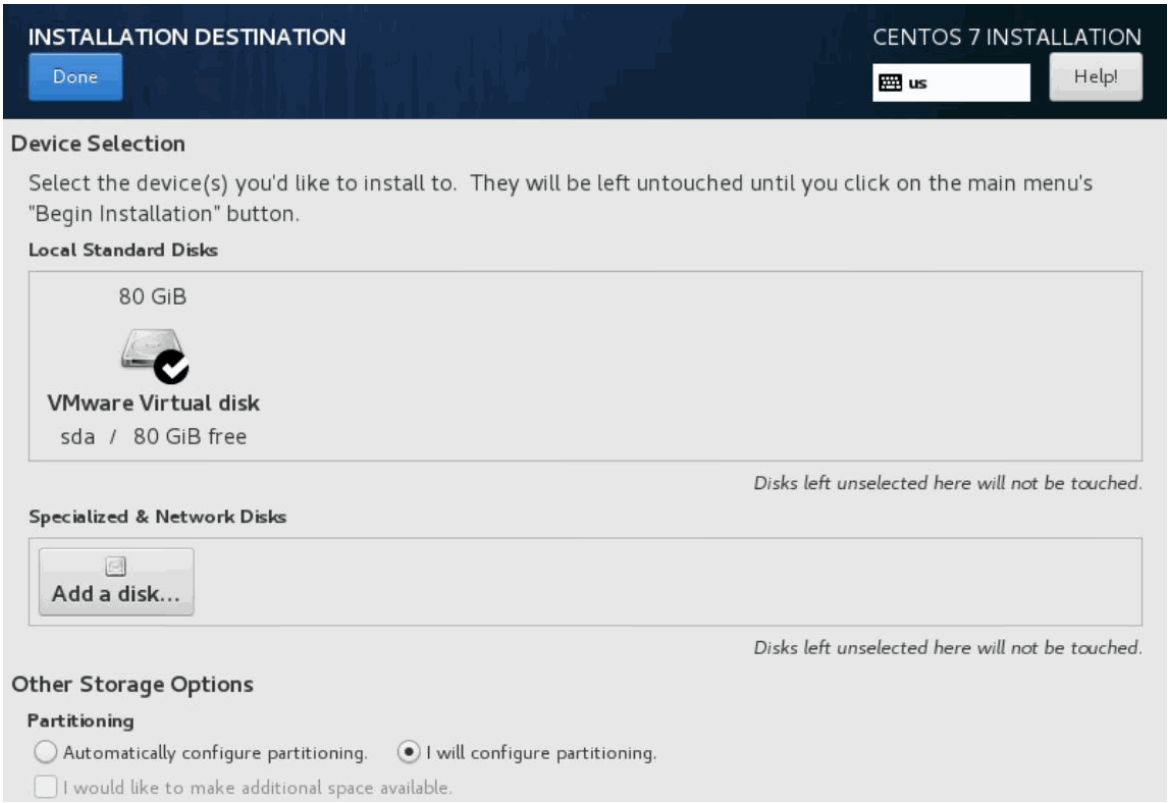


19. Press the **Enter** key to begin the installation process.
20. Select the language and your desired country time zone (if necessary) and then click **Continue**.
21. Click the **SOFTWARE SELECTION** option.

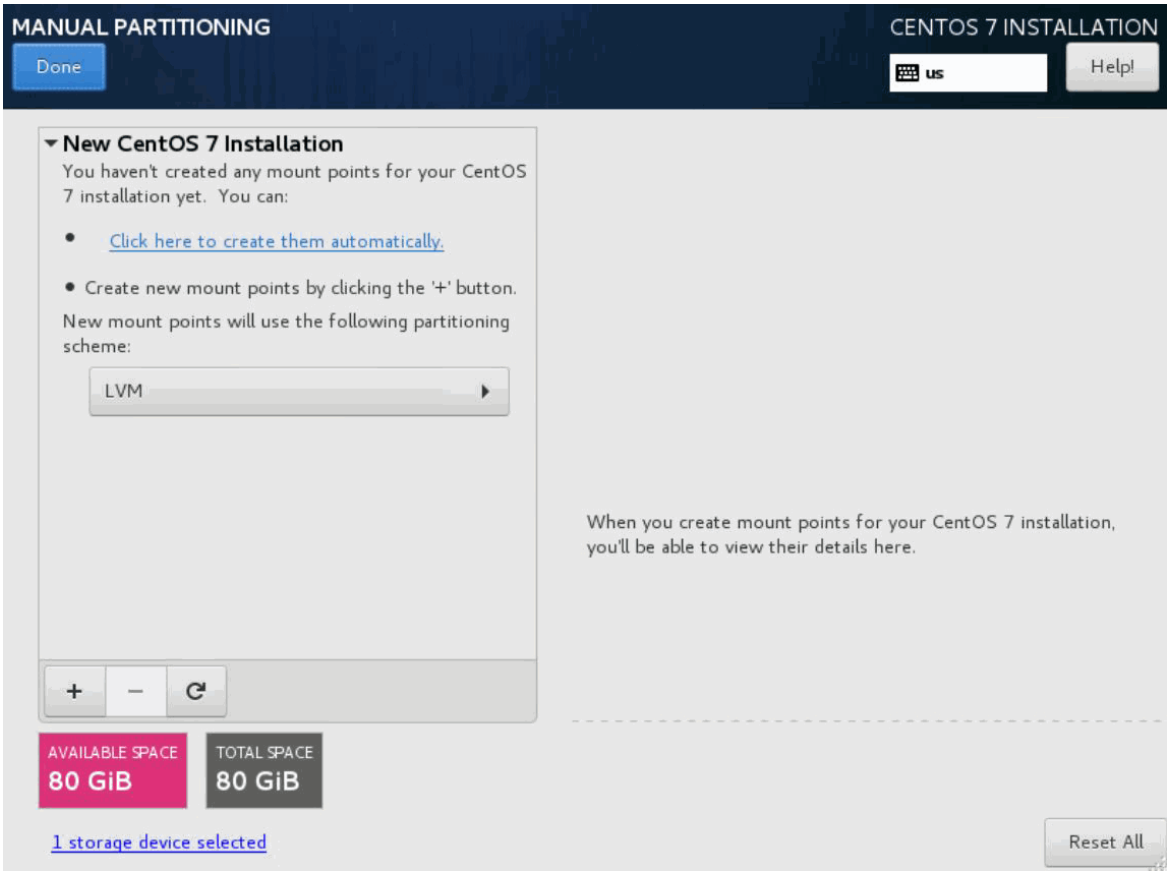
22. In the **Basic Environment** section, select the **Basic Web Server** radio button. In the **Add-Ons for Selected Environment** section, select **PHP Support** and **Perl for Web** check boxes and click **Done**.



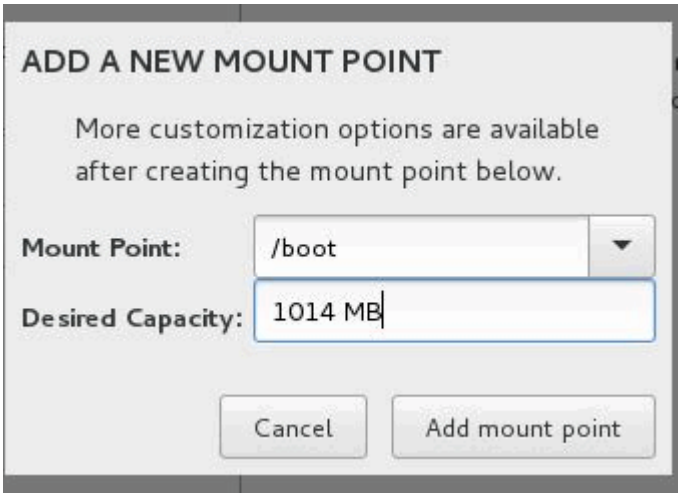
23. Click **INSTALLATION DESTINATION** and verify that the **VMware Virtual disk** (80 GB) is selected.
24. In the **Other Storage Options** section, select the **I will configure a partitioning** option button.



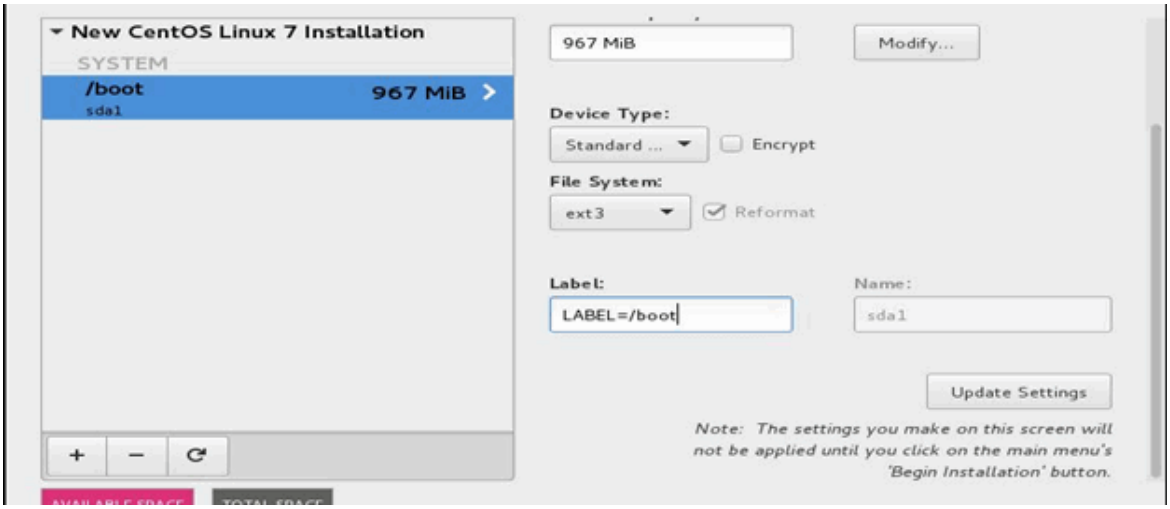
25. Click **Done**. The **MANUAL PARTITIONING** page appears.



26. Click the **+** button. The **ADD A NEW MOUNT POINT** dialog box appears.
27. To create a partition for /boot, enter **/boot** in the **Mount Point** field and enter **1014 MB** in the **Desired Capacity** field. Then, click **Add mount point**.



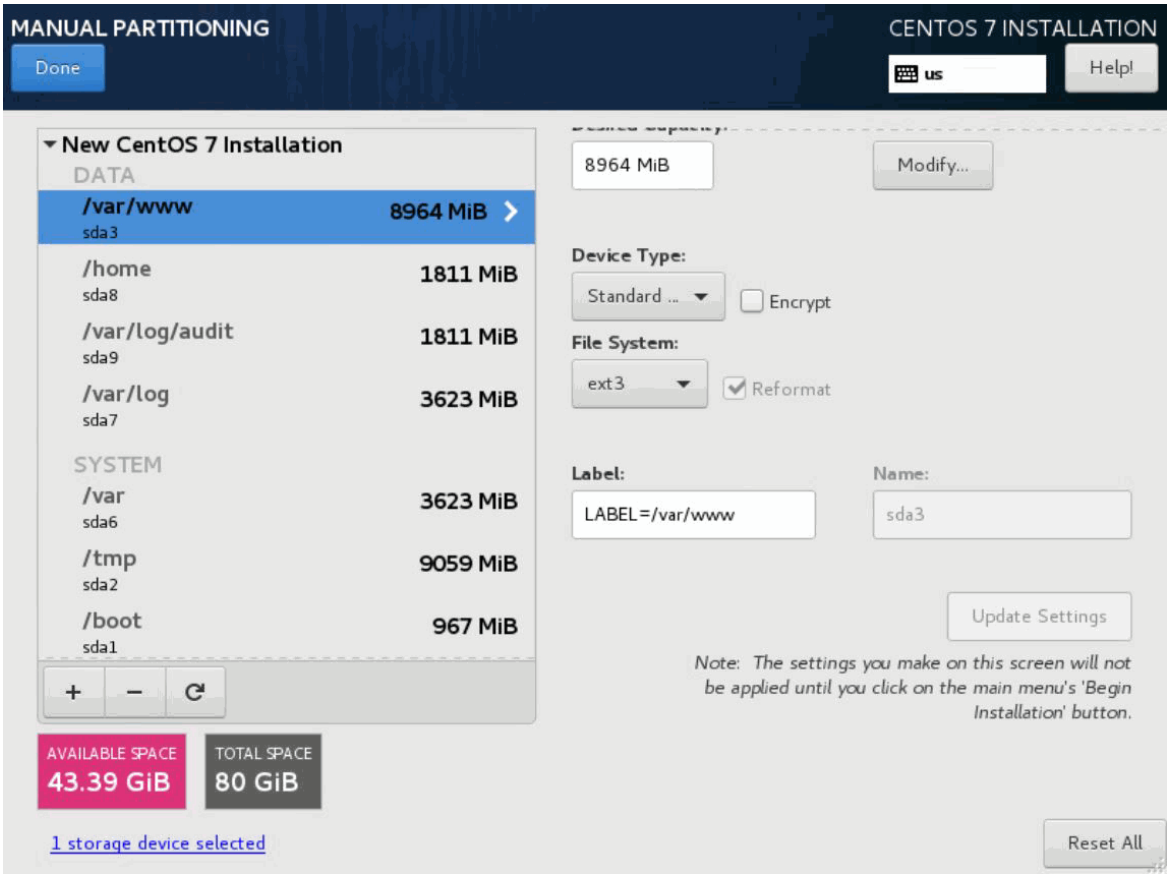
28. Select **Standard Partition** from the **Device Type** list and select **ext3** from the **File System** list. Enter **LABEL=/boot** in the **Label** field and then click **Update Settings**.



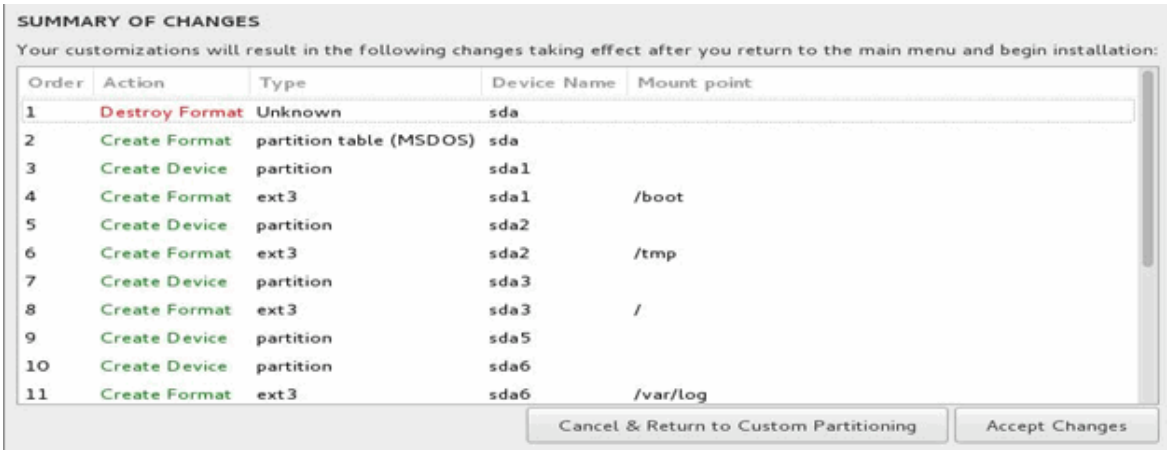
29. Similarly, repeat the steps 26 through 28 to create partitions for the following mount points with the provided settings.

Table 1: Mount Points and Their Settings

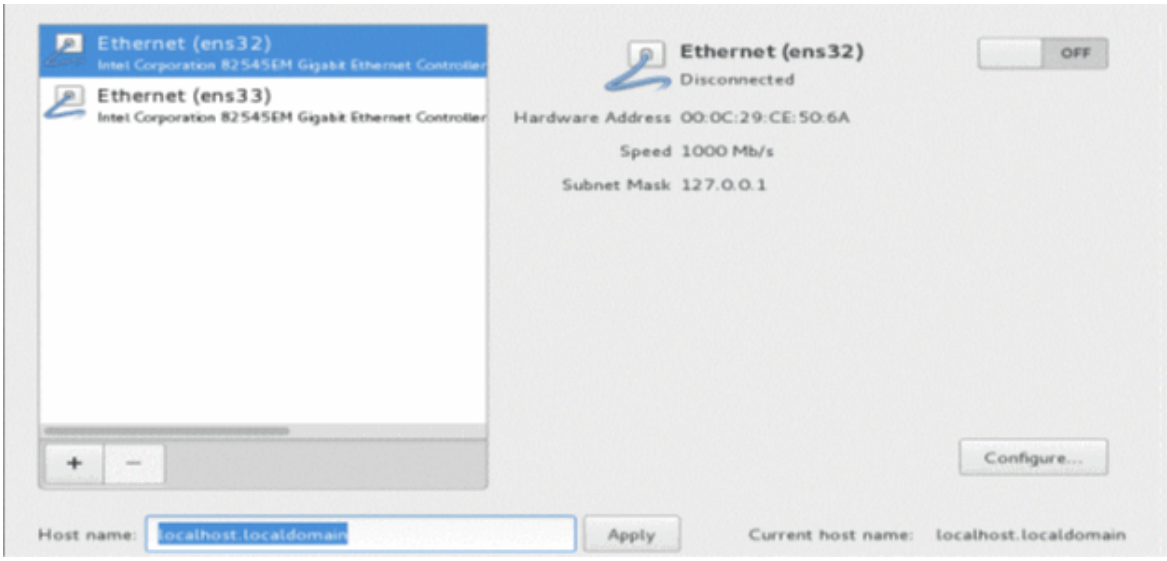
Mount Point	Desired Capacity	Device Type	File System	Label
/tmp	9.5 GB	Standard Partition	ext3	LABEL=/tmp
/	8 GB	Standard Partition	ext3	LABEL=/
/var/log	3.8 GB	Standard Partition	ext3	LABEL=/var/log
/var	3.8 GB	Standard Partition	ext3	LABEL=/var
/var/log/audit	1.9 GB	Standard Partition	ext3	LABEL=/var/log/a
/home	1.9 GB	Standard Partition	ext3	LABEL=/home
/var/www	9.4 GB	Standard Partition	ext3	LABEL=/var/www



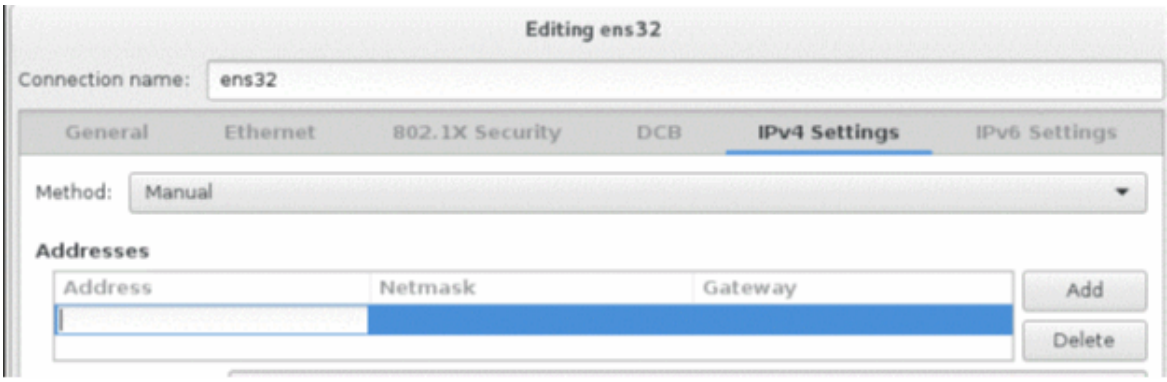
30. Click **Done** twice and then click **Accept Changes**.



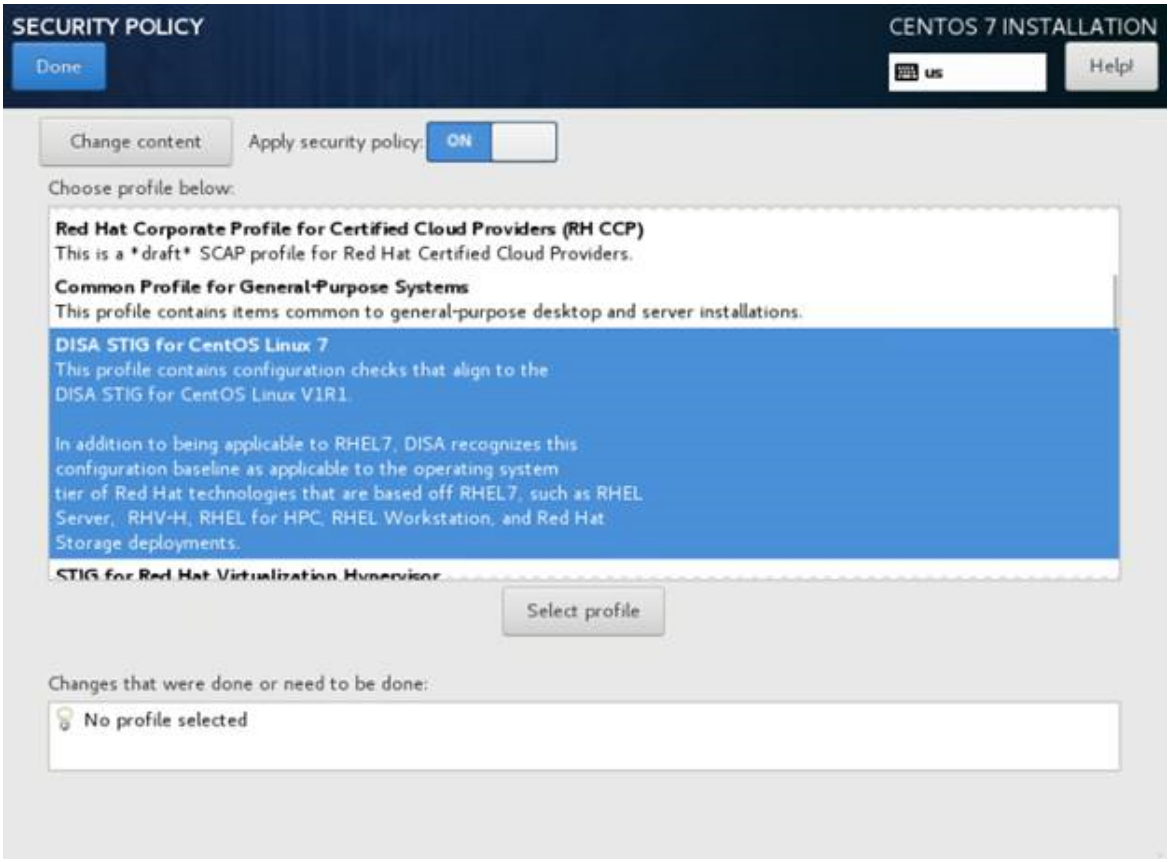
31. Click **NETWORK & HOST NAME**.
32. Select an Ethernet option (for example, Ethernet (ens32)), enter the hostname (for example, ctpview) in the **Host name** field, and then click **Apply**.



33. Click **Configure**. Then, click the **IPv4 Settings** tab.



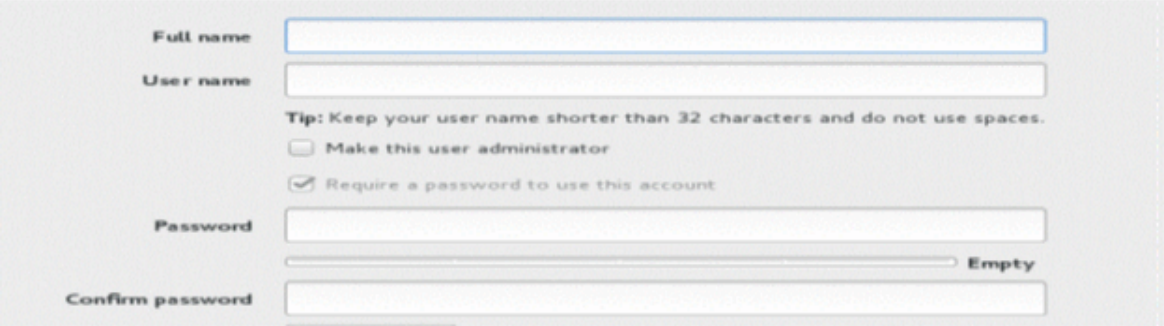
34. Select **Manual** from the **Method** list and click **Add**.
35. Enter values for **Address**, **Netmask**, and **Gateway** fields, and then click **Save**.
36. Click the toggle button in the right-top corner to bring the configured Ethernet up and running, and then click **Done**.
37. Click **SECURITY POLICY**.
38. Select the **DISA STIG for CentOS Linux 7 Server** option and click **Select Profile**. Then, click **Done**.



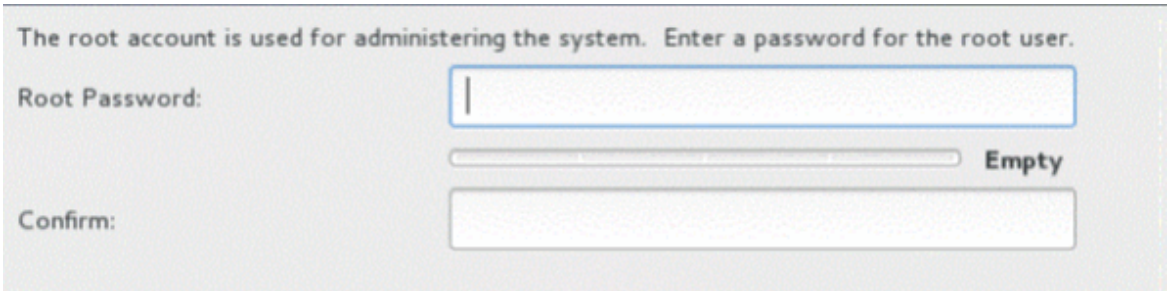
NOTE: Skip this step, if you are creating a non-STIG'd VM.

39. Click **Begin Installation**. The **USER SETTINGS** page appears.

40. Click **USER CREATION**, enter the username as "admin", and enter a password.



41. Select the **Make this user administrator** check box and click **Done**.
42. In the **USER SETTINGS** page, click **ROOT PASSWORD**, enter the password as “CTPView-2-2” and click **Done**.



43. After the installation process is completed, click **Reboot**.

Installing CTPView 9.1R1

CTPView can be installed on the newly created CentOS 7.5[1804] VM or CentOS 7.5[1804] bare metal server. Steps are as follows:

1. Create a new CentOS 7 Virtual Machine (VM) instance as mentioned in "Creating a CentOS 7 Virtual Machine" on page 4.

> **NOTE**: You can skip this step if you are installing CTPView on a bare metal. To install the ISO file (centOS-7-x86_64-DVD-1804.iso) on a bare metal server, copy the ISO file to a bootable CD and then install the ISO file from the CD. At the boot prompt, you should select the installation option as "ctpview-vmware" and the Ethernet NIC type as “E1000”. Recommended hardware configurations are 1 GB RAM with 60 GB disk space and 2 cores per CPU.

2. Copy the CTPView RPM (CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm) to **/tmp** directory of the newly created CentOS 7.5[1804] VM or CentOS 7.5[1804] bare metal.

3. On a VM, log in as "admin" and install CTPView using the command “sudo rpm -ivh CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm”.

   On a bare metal server, log in as the default CTPView admin user "juniper_sa" and install CTPView using the command “sudo rpm -ivh CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm”.

Upgrading to CTPView 9.1R1

To upgrade the CTPView server from 9.0R1 to 9.1R1 release:

1. Copy the CTPView RPM (CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm) to the **/tmp** directory of the existing CentOS 7.5[1804] VM or CentOS 7.5[1804] bare metal.
2. Log in as the default CTPView admin user "juniper_sa" and upgrade the CTPView server using the command "sudo rpm -Uvh --force CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm".

Uninstalling CTPView 9.1R1

CTPView 9.1R1 can be uninstalled from Centos 7 by performing the following steps:

1. Check if root login is permitted. If not, enable root login from menu -> Security Profile(1) -> Modify Security Level(5) -> Set OS level to 'very-low'(3).
2. Login via “root” user and run the command “sudo rpm -evh CTPView-9.1R-1.0-0.el7.centos.x86_64.rpm”.
3. System will reboot after uninstalling, use user (the one you created while creating CentOS) to login.

Resolved Issues in CTPView Release 9.1R1

The following issues have been resolved in CTPView Release 9.1R1:

- Changing a password for an existing SNMPv3 user fails. [PR 1358582]
- Round trip delay graph shows gaps in CTPView plot. [PR 1411113]
- CTPView copy bundle feature does not copy port settings. [PR 1420732]

Known Issues in CTPView Release 9.1R1

None.

CVEs and Security Vulnerabilities Addressed in CTPView Release 9.1R1

The following tables list the CVEs and security vulnerabilities that have been addressed in CTPView 9.1R1. For more information about individual CVEs, see http://web.nvd.nist.gov/view/vuln/search.

Table 2: Critical or Important CVEs Included in OpenSSL

CVE-2017-3735	CVE-2018-0495	CVE-2018-0732	CVE-2018-0737
CVE-2018-0739	CVE-2018-5407	CVE-2018-15473	CVE-2018-0734
CVE-2019-1559	CVE-2007-1858		

Table 3: Critical or Important CVEs Included in kernel

CVE-2017-16939	CVE-2018-1000199	CVE-2018-1068	CVE-2018-1087
CVE-2018-1091	CVE-2018-8897	CVE-2017-11600	CVE-2018-3639
CVE-2018-14634	CVE-2018-14633	CVE-2018-14646	CVE-2018-18397
CVE-2018-18559	CVE-2018-17972	CVE-2018-18445	CVE-2018-9568
CVE-2019-6974	CVE-2019-7221	CVE-2019-11477	CVE-2019-11478
CVE-2019-11479	CVE-2018-16871	CVE-2018-16884	CVE-2019-11085

CVE-2019-11811	CVE-2018-3639	CVE-2018-3665	CVE-2018-12126
CVE-2018-12127	CVE-2018-12130	CVE-2019-11091	CVE-2019-14821
CVE-2019-15239			

Table 4: Critical or Important CVEs Included in yum-utils

CVE-2018-10897

Table 5: Critical or Important CVEs Included in GNOME

CVE-2017-18267	CVE-2018-10733	CVE-2018-10767	CVE-2018-10768
CVE-2018-12910	CVE-2018-13988		

Table 6: Critical or Important CVEs Included in vim

CVE-2019-12735

Table 7: Critical or Important CVEs Included in libX11

CVE-2018-14598	CVE-2018-14599	CVE-2018-14600	CVE-2018-15853
CVE-2018-15854	CVE-2018-15855	CVE-2018-15856	CVE-2018-15857
CVE-2018-15859	CVE-2018-15861	CVE-2018-15862	CVE-2018-15863
CVE-2018-15864	CVE-2015-9262		

Table 8: Critical or Important CVEs Included in linux-firmware

CVE-2018-5383

Table 9: Critical or Important CVEs Included in sudo

CVE-2019-14287

Table 10: Critical or Important CVEs Included in php

CVE-2019-11043

Table 11: Critical or Important CVEs Included in procps-ng

CVE-2018-1124	CVE-2018-1126

Table 12: Critical or Important CVEs Included in python

CVE-2016-2183	CVE-2019-9636	CVE-2019-10160	CVE-2018-1060
CVE-2018-1061	CVE-2019-9948	CVE-2018-14647	CVE-2019-5010
CVE-2019-9740	CVE-2019-9947		

Table 13: Critical or Important CVEs Included in gnupg2

CVE-2018-12020

Table 14: Critical or Important CVEs Included in systemd

CVE-2018-15688	CVE-2018-16864	CVE-2018-16865	CVE-2019-6454

Table 15: Critical or Important CVEs Included in dhcp

CVE-2018-1111

Table 16: Critical or Important CVEs Included in perl

CVE-2018-18311

Table 17: Critical or Important CVEs Included in libssh2

CVE-2019-3855	CVE-2019-3856	CVE-2019-3857	CVE-2019-3863
CVE-2019-3862			

Table 18: Critical or Important CVEs Included in wget

CVE-2019-5953

Table 19: Critical or Important CVEs Included in nss

CVE-2018-12384

Table 20: Critical or Important CVEs Included in polkit

CVE-2019-6133

Table 21: Critical or Important CVEs Included in bind

CVE-2018-5743

Table 22: Critical or Important CVEs Included in openssh

CVE-2017-15906

Table 23: Critical or Important CVEs Included in tcpdump

CVE-2018-19519

Revision History

December 2019—Revision 1—CTPView Release 9.1R1.

May 2020—Revision 2—CTPView Release 9.1R1.

August 2020—Revision 3—CTPView Release 9.1R1.