Engineering Simplicity

CTPView Network Management System

Published
2023-09-03

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

RELATED DOCUMENTATION

CTP Network Management System Administration Guide

1

PART

Overview

CHAPTER 1

Circuit to Packet System Overview

IN THIS CHAPTER

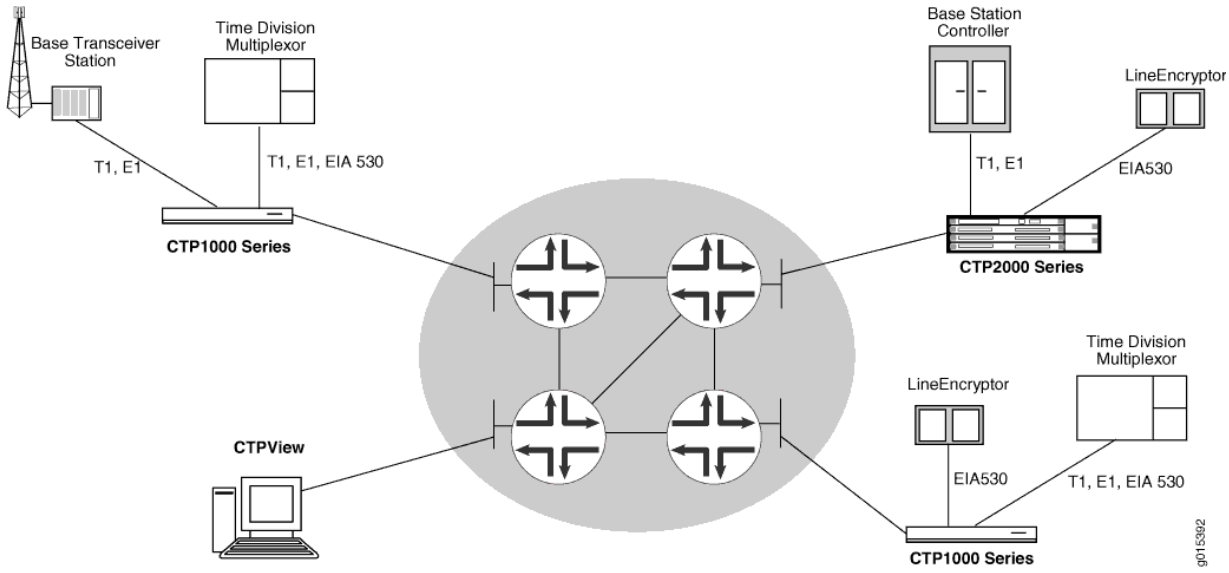
Circuit to Packet Network Overview

IN THIS SECTION

The CTP products are designed to create an IP packet flow from a serial data stream or analog voice connection, providing the necessary processing to re-create the serial bit stream or analog signal from an IP packet flow.

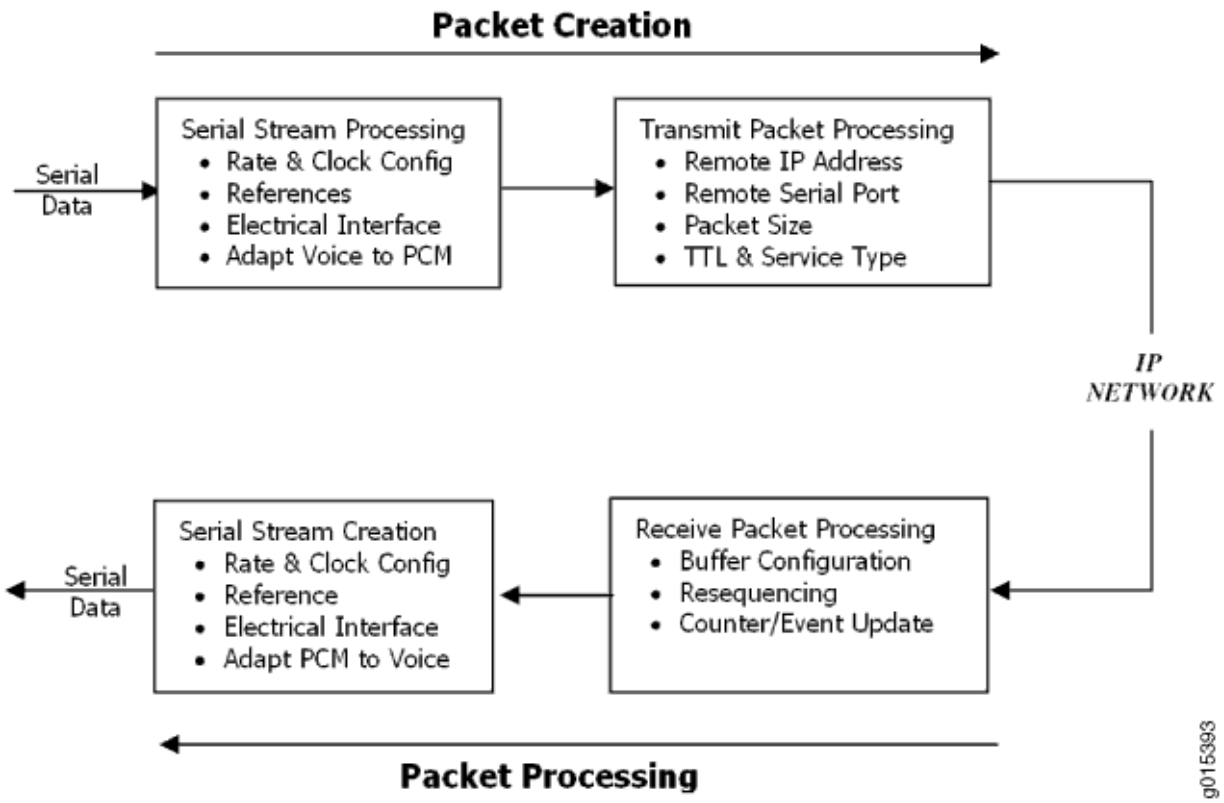
CTP products are designed to accommodate the delay, delay *jitter*, and packet reordering characteristics of an IP network. Figure 1 on page 3 shows examples of applications that use CTP products.

Figure 1: Sample Application Using CTP Products



Numerous processes must occur to adapt serial data to and from IP packets. These processes are summarized in Figure 2 on page 4. You configure the characteristics of the processes by using the CTP menu interface or the CTPView graphical user interface.

Figure 2: Circuit-to-Packet Conversion Processes



Using the menu interface, you can configure the CTP products to accept a serial data stream and create an IP flow that will be transferred across an IP network. The connection provided by the CTP platform is a physical layer circuit between the end user equipment.

Serial Stream Processing

Rate selection and clock configuration allow the serial interface rate to be configured through the software. Rates supported range from less than 300 bps to 12.288 Mbps (in subhertz increments).

You can configure the CTP systems by using the menu interface to provide multiple prioritized node clock references. An external reference input and any of the serial interfaces may be used for the node reference clock. Reference frequencies must be 32 KHz, n x 64 KHz, or 1,544 KHz up to a maximum of 4096 KHz (2048 KHz maximum on the CTP1002).

The electrical characteristics and encoding of the CTP ports are software configurable. The available options are EIA530, EIA530A, RS-232, V.35, analog 4WTO, conditioned diphase, isochronous, T1, and E1.

An analog voice signal terminated on the 4WTO interface is converted into a 64-Kbps pulse-code modulation (PCM) digital bit stream before adaptation to and from an IP flow. The analog interface allows transmit and receive levels to be adjusted.

Transmit Packet Processing

The CTP platform is configured with the remote IP address of the device where the packets created from the local serial port are to be routed.

The CTP remote port is specified by the IP address and physical port number of the remote unit and port.

The packet size created by the CTP platform may be set from 32 to 1456 bytes. Larger packet sizes are more bandwidth-efficient but introduce more serialization delay when the packet is created. The menu interface verifies that the combination of packet size and data rate does not result in a packet rate exceeding 1200 packets per second.

Time to live (TTL) may be set from 0 to 255. The TTL is the maximum number of hops in the IP network that the packet may travel before it is discarded by the network. You can configure the service type byte, which some IP networks use to determine the *quality of service* provided to the IP flow.

Receive Packet Processing

A receive buffer is required to smooth the timing jitter of received packets because of the delay variance that is inevitably encountered in the IP network. The configuration allows you to configure both the size of the buffer (in 1-ms increments) and the maximum amount of buffering delay allowed before the buffer will recenter. The size of the buffer configured should depend on the performance and characteristics of the IP network.

The CTP platform automatically resequences packets when they arrive out of order. If a packet is not received, the CTP platform inserts all data in lieu of the packet information so that bit count integrity is maintained.

You can prompt the menu interface to display detailed information about the port status, such as packet counts, late packets, missing packets, and buffer fill.

Serial Stream Creation

The packet receive process allows the serial data rate to be configured through the software. Rates supported range from less than 300 bps to 12.288 Mbps in subhertz increments. Conditioned diphase and isochronous interfaces operate at rates up to 1.024 Mbps.

Clock Options

The CTP platform provides numerous options for physical layer clocking:

- Interface clocking options—The CTP platform allows complete configuration flexibility of interface clocking. This flexibility includes your ability to specify how clocks are generated (that is, from the node clock, which can be phase locked to an external clock input) and what clocks are used to process the data from the attached device. The CTP platform can synthesize over 1.5 billion rates between 1 bps and 12.288 Mbps.
- Asymmetric clocking—You can configure CTP circuits to synthesize asymmetric rates.
- Reference clock input—The CTP platform can phase lock its node clock to an interface clock or external reference input. Up to five prioritized references can be configured. The node provides a reference holdover if all references are lost.
- Plesiochronous operation—Calibrated Clock is a patented CTP feature that allows the one-time calibration of the CTP oscillator to a known reference. Depending on environmental factors, two units calibrated to the same clock will have a clock difference as small as 100 parts per billion. This calibration enables CTP circuits to operate for long periods of time before a buffer recenter occurs.
- Adaptive clocking—Although IP router networks do not transfer physical layer clocking, the CTP adaptive clocking feature, using patented Advanced Time Domain Processing (ATDP), allows the CTP platform to recover clocking information from the remote CTP port and adjust the local clock accordingly. ATDP provides rapid convergence to the correct clock, and does not vary due to changes in the average jitter buffer fill. As a result, a CTP circuit will continuously operate without a buffer recenter, even when clock references are not used.

RELATED DOCUMENTATION

Adding a Bundle (CTPView)

Adding a Bundle (CTP Menu)

Selecting the Type of Clocking on Serial Ports for CTP Bundles (CTPView)

Configuring Custom Clocking for CTP Bundles (CTPView)

Configuring Adaptive Clocking for CTP Bundles (CTPView)

Configuring IP Parameters for CTP Bundles (CTP Menu)

Circuit to Packet Network Software Overview

This topic provides an overview of the software components of the CTPView Network Management System and the CTP platforms.

A typical Circuit to Packet network consists of one or more CTP platforms and a CTPView server. The CTPView server runs the CTPView Network Management System software to manage the CTP platforms and construct the circuit-to-packet traffic bundles.

The software components consist of the following:

- CTPOS—Operating system that runs on the CTP platforms.
- Fedora Core (FC) OS—Operating system that runs on the CTPView server.
- CTPView Network Management System—Software that you use to build circuits and manage the CTP platforms. You can access this software through a browser application or through a text-based menu set.

  In this document, we use the term *CTPView GUI* to refer to the browser application, and the term *CTPView server menu* to refer to the text-based menus. *CTPView software* typically refers to the CTPView Network Management System without regard to the method used to access the server.

RELATED DOCUMENTATION

Updating the CTPView Server Operating System and CTPView Network Management System Software | **11**

Adding a VLAN ID to the System

When you add a VLAN to a node, the network and CTP devices are restarted to update the network parameters. The node is not restarted.

> **NOTE**: For VLAN failover to function correctly, VLANs must be configured on the primary Ethernet interface (for example, eth1) that has IPv4 configured and Ethernet failover enabled.

To add a VLAN ID to the system from the CTP Menu:

1. From the Main Menu, select **5) Node Operations** > **3) Configure network settings** > **8) VLAN Configuration**.

```
==========================================================================
= (ctp_90 05/08/14 23:03:48 WST) | Network Configuration Menu
==========================================================================
Please select a number from the following list:
-------------------------------------
0) Back to Previous Menu
1) Supported Protocols: IPv4 only
2) IPv4 Configuration
3) IPv6 Configuration
4) Virtual IP addresses
5) OAM port (IPv4): 16
6) CTP Bndl Data pkt protocol: 47
7) CTP Bndl OAM port (IPv6): 32
8) VLAN Configuration
9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [0]: 8
***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
*** system may not be reachable via the network
*** after the network restarts.
***
Are you sure? y[n]: y
Exsisting VLAN interfaces :
No VLAN is configured yet
How do you want to change VLANs (add/delete/quit) ? (rtn for show): add
Which ethernet port the new VLAN will be added on? (0-3)[0] 1
What is the new VLAN id? (0-4095)[0] 111
```

```
Exsisting VLAN interfaces :
eth1.111: Vlan ID 111 on ethernet port 1
How do you want to change VLANs (add/delete/quit) ? (rtn for show): quit
```

2. Follow the onscreen instructions and configure the options as described in Table 1 on page 9.

Table 1: Configuring a VLAN Interface

Field	Function	Your Action
How do you want to change VLANs ?	Enter `add` to add a new VLAN, `delete` to remove a VLAN, and `rtn` to show existing VLANs.	Enter `add` to create a new VLAN.
Which ethernet port the new VLAN will be added on ?		Specify the ethernet port number. The default value is 0 (zero).
What is the new VLAN id ?		Assign the VLAN ID for the newly created VLAN in the range 0–4095. The default value is 0 (zero).

2

PART

Installation

CHAPTER 2

Installation Tasks Overview

IN THIS CHAPTER

Updating the CTPView Server Operating System and CTPView Network Management System Software

This topic provides an overview of installing and upgrading the software on the CTPView server. You can install or upgrade the server operating system (OS), and you can upgrade the CTPView software that you use to manage the CTP Series devices. CTPView servers are provided with an OS and the CTPView software already installed. You can upgrade any CTPView server to a higher-numbered software release.

Your choice of upgrade procedure depends on the version of the operating system (OS) running on the CTPView server to be upgraded. To upgrade to the current release, your CTPView server must be running either Fedora Core 4 (FC4) OS or Fedora Core 9 (FC9) OS. CTPView servers are shipped with the latest supported version. CTPView servers have been shipped with the following OS versions:

- FC9 on servers shipped after August 2008.
- FC4 on servers shipped from November, 2006 through August 2008.
- FC1 on servers shipped before November 2006.

You can determine your server OS version in any of the following ways:

- In CTPView, navigate to **Server > Diagnostics**. The OS version is displayed in the Distro Name field in the System Vital block section of the page.
- Log in to the server shell and enter **uname -r** on the command line. The kernel version that is displayed includes the OS version: **fc1**, **fc4**, **fc9**.
- Log in to the server shell and enter **menu** and then the root password on the command line. The heading of the configuration menu that is displayed includes the OS release and kernel versions.

> **NOTE**: If your server is running FC1, we recommend that you upgrade to a more recent model server.

Depending on your goals and your current software versions, upgrading your system software includes one or more of the following tasks:

- Install or upgrade to the latest server OS version, and upgrade to the latest CTPView software versions.

  You can choose this task for any CTP server. *Installing* the OS reformats the server hard drives and deletes all existing data and settings. These actions put your server into a stable known state with all security features enabled. *Upgrading* to the latest OS version does not format the server hard drives; your existing data and settings are preserved. In either case, you also upgrade to the latest CTPView software version.

  See "Installing or Upgrading the CTPView Server OS" on page 14.

- Upgrade to the latest CTPView software version.

  When you do not need or want to change the OS version, you can simply upgrade to the latest CTPView version.

  See "Upgrading Only the CTPView Software" on page 25.

- Configure administrative settings to complete the upgrade.

  When you receive a new CTP server from Juniper Networks that is running CTPView 3.2R1 or higher, you need only configure the administrative settings. To enable all of the security updates, an administrator must configure certain server settings during the upgrade process.

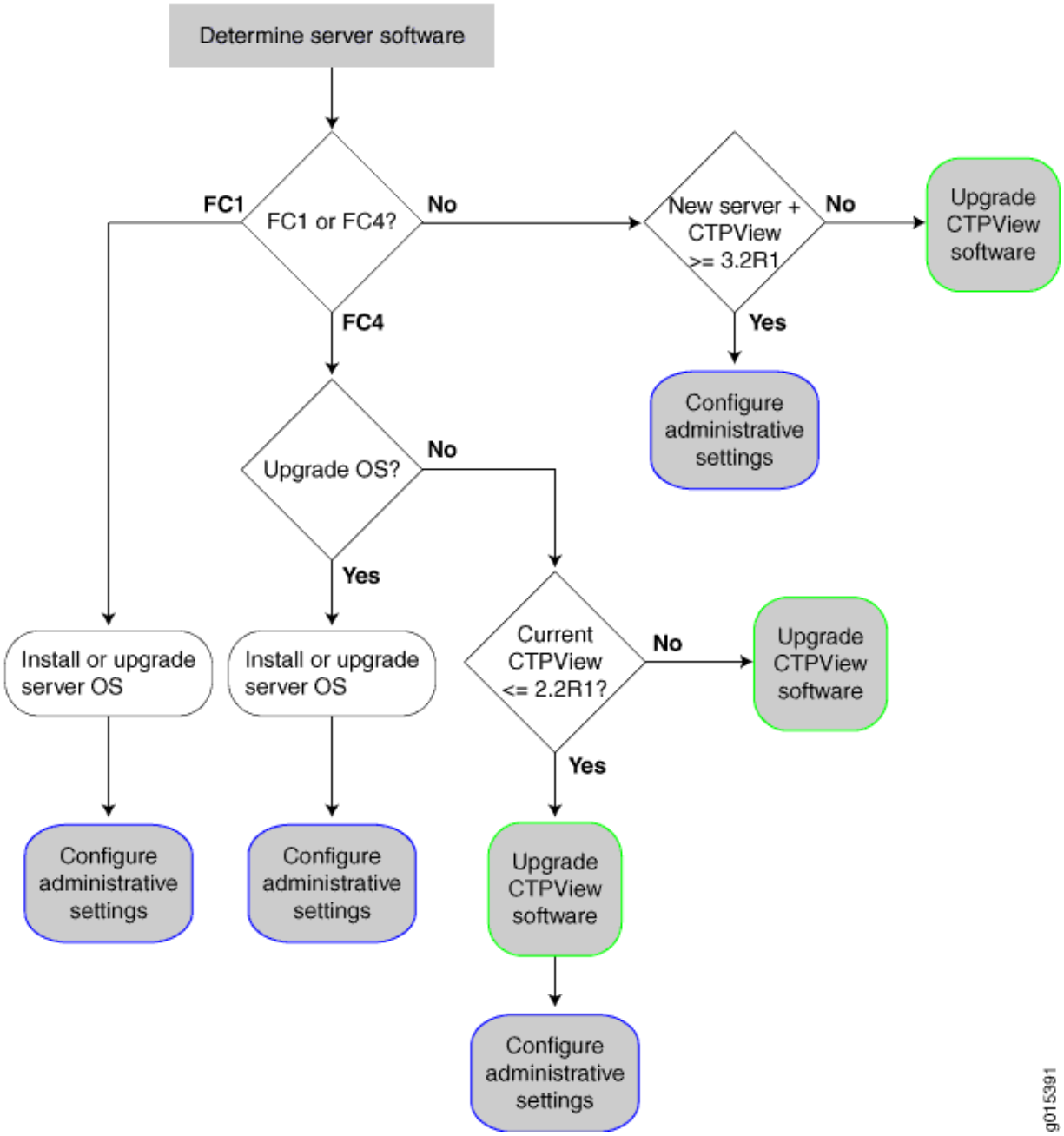
  You must also perform this task to validate the administrative settings in either of the following cases:

  - You upgraded the CTPView software on a server running FC4 and CTPView 2.2R1 or lower.
  - You installed or upgraded the server to the latest OS version.

  See Configuring the CTPView Administrative Settings.

Figure 3 on page 13 illustrates the decision process you use to determine which tasks to perform.

Figure 3: Decision Tree for Updating CTPView Server Software



RELATED DOCUMENTATION

Accessing a Shell on the CTPView Server (CTPView Server CLI) | 255

CHAPTER 3

Installation and Upgrade Tasks for the CTPView Server OS and CTPView Software

IN THIS CHAPTER

Installing or Upgrading the CTPView Server OS

This topic provides an overview of installing and upgrading the operating system (OS) for the CTPView server.

Before you begin, do all of the following:

- Verify that this is the procedure you wish to use to update the software on the CTPView server. See "Updating the CTPView Server Operating System and CTPView Network Management System Software" on page 11.

- Ensure that you have a monitor and keyboard connected to the CTPView server. You must also have an external storage device connected to the server in order to save the current data and settings for CTPView.

- Ensure that the server is connected to the network.
- If your server is currently running FC1, you must be running CTPView 2.1R2 or 2.1R3 in order to back up your existing data and configuration settings before upgrading the OS version. See "Upgrading Only the CTPView Software" on page 25 for information on upgrading the CTPView software before you perform the tasks in this topic.

> **NOTE**: If your server is running FC1, we recommend that you upgrade to a more recent model server.

Perform the following tasks

1. Save the current configuration settings and data to an external storage device.

   See "Saving the CTPView Configuration Settings and Data (CTPView Server Menu)" on page 16.
2. Install or upgrade the CTPView server OS.

   See "Installing the CTPView Server OS (CTPView Server CLI)" on page 19.
3. Restore the configuration settings and data.

   See "Restoring CTPView Software Configuration Settings and Data (CTPView)" on page 20.
4. Review the installation log for errors.

   See "Reviewing the Installation Log for Errors (CTPView Server CLI)" on page 23.
5. Configure CTPView administrative settings to complete server setup and ensure that security settings are correct.

   See "Configuring the CTPView Administrative Settings" on page 32.
6. Verify that the server OS was successfully installed or upgraded.

   See "Verifying the CTPView Server OS Installation (CTPView)" on page 23.
7. Validate the server configuration.

   See "Validating the CTPView Server Configuration (CTPView)" on page 24.

RELATED DOCUMENTATION

Default CTPOS and CTPView Accounts and Passwords | 94

Saving the CTPView Configuration Settings and Data (CTPView Server Menu)

This topic describes how to save the current configuration settings and data for the CTPView software. Although you can perform this task at any time, it is typically performed before you upgrade the CTPView server OS and the CTPView software.

You can use the backup utility in the CTPView server menu to save the information into an archive (`.tgz`) file and, if desired, move the archive to an external storage device. If you do not use the utility to move the archive, you can later copy or move it manually from outside the CTPView server menu.

> **NOTE**: If you do not move the archive file to an external storage device, you are not protected from loss of the backed-up data. If you are upgrading the software, you must move the file to an appropriate location.

Alternatively, when you have more than one CTPView server, you can use the CTPView software GUI to synchronize the server with another server to save the settings and data. See "Synchronizing Multiple CTPView Servers (CTPView)" on page 159 for the synchronization procedure.

> **NOTE**: We recommend that you use the CTPView server backup utility to save your current information.

Before you use the CTPView server backup utility:

- Confirm that the external storage device is running a UNIX-like operating system and is enabled for SSH connections.

  > **NOTE**: Although the external storage device can use any operating system, the CTPView backup utility can automatically transfer the backup file only to a device that is running a UNIX-like operating system. If the device is running a different kind of OS, you must transfer the backup file with a copy utility that is compatible with that OS.

- Confirm that a network path exists between the CTPView server and the external storage device used for storing the backup file.
- Confirm that the hard drive on the CTPView server that you are backing up has at least 25 percent free space. If you attempt to run the backup utility when less than 25 percent free space is available, the utility prompts you to delete more old data files before you continue. See "Creating More Disk Space on the CTPView Server (CTPView)" on page 17.

- Log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To back up your current information with the CTPView server backup utility:

1. From the CTPView Configuration Menu, select **5) Backup Functions**.

   The Backup Functions Menu is displayed.
2. Select **1) Save Current Settings and Data**.

   If an archive file already exists in the `/var/www/html/acorn/data` directory on the server, the utility prompts you to delete or move the archive.
3. (Optional) From outside the menu (for example, in another terminal window), manually move the old archive to an external storage device if you want to save the information.
4. Enter **y** to delete the old archive.

   The utility deletes the old archive file and creates the new archive file.
5. Enter **y** to move the new archive to an external location.
6. Follow the prompts to enter the IP address, username, and absolute path to the external device.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | **14**

Creating More Disk Space on the CTPView Server (CTPView) | **17**

Creating More Disk Space on the CTPView Server (CTPView Server Menu) | **18**

Creating More Disk Space on the CTPView Server (CTPView)

This topic describes how to determine the amount of free disk space on the CTPView server and how to ensure that sufficient free space is always available on the server.

To determine the amount of free disk space that is available on the CTPView server:

1. In the side pane, select **Server > Diagnostics**.

   The System Information pane is displayed.
2. Find the value for Totals in the Mounted Filesystems section. The value should be `75%` or less.

To automatically delete old files to create more free disk space:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.

2. Click **Automatic Functions**.

3. Under the Action heading in the Add New Automatic Entry section, select old data files to delete. You can choose to remove outdated files that are over 6 months old, over 9 months old, or over 12 months old.

4. Click **Add New Entry**. From this point forward, files are deleted from the server when they exceed the selected age.

   If you subsequently no longer want old files to be automatically removed, select that Action under Current CTPView Automatic Settings and click **Remove Selected Lines**.

RELATED DOCUMENTATION

Saving the CTPView Configuration Settings and Data (CTPView Server Menu) | **16**

Installing or Upgrading the CTPView Server OS | **14**

Creating More Disk Space on the CTPView Server (CTPView Server Menu)

This topic describes how to create free space by removing redundant data files from the server.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To delete old files to create more free disk space:

1. From the CTPView Configuration Menu, select **5) Backup Functions**.

   The Backup Functions menu is displayed.

2. Select **3) Remove Redundant Binary Data Files**.

RELATED DOCUMENTATION

Saving the CTPView Configuration Settings and Data (CTPView Server Menu) | **16**

Installing or Upgrading the CTPView Server OS | **14**

Installing the CTPView Server OS (CTPView Server CLI)

This topic describes how to install the latest CTPView server OS. The server OS must be installed from the CTPView Management System CDs. Contact Juniper Networks Customer Support to send you the CDs.

> **NOTE**: The CTPView software is automatically installed when you install or upgrade the server OS with the CTPView Management System CDs.

To install or upgrade CTPView server OS:

1. Insert the first CD from the latest CTPView Management System CD set into the server.
2. From the CLI, select **System Configuration > Reboot System** to reboot the server.

   The reboot process halts at the Juniper CTPView Management System window.
3. At the boot prompt, enter **ctpview-install** or **ctpview-upgrade**.

   > **NOTE**: We recommend that you choose **ctpview-install**. This action reformats the server hard drives, installs the latest version of the server OS, and creates a conforming instance of the OS. If you choose **ctpview-upgrade**, the latest version of the OS is installed, but the server hard drives are not reformatted.
4. Follow the prompts to remove and insert the remaining CDs to complete the installation or upgrade process.

On some early hardware systems a RAMDISK error may be reported at the beginning of the upgrade process. If this occurs, perform the following steps:

1. Leave the first CD in the server and use the server power switch to reboot the server.
2. When the boot prompt appears, enter **mediacheck**. The server displays the message “Could not find kernel image: mediacheck”.
3. At the boot prompt, enter **ctpview-install** or **ctpview-upgrade**.

   The upgrade process should proceed normally.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Configuration Settings and Data (CTPView)

This topic lists two methods to restore the CTPView software configuration settings and data. Typically you restore this information only after one of the following events has occurred:

- An installation of the latest version of the CTPView server operating system, which reformats the server's hard drives.
- In the unlikely event of a data loss.

Use one of the following methods to restore saved CTPView information:

- Use the CTPView restore utility in the CTPView server menu. You must use this method when you have only a single CTPView server.

  See "Restoring CTPView Software Configuration Settings and Data with the Restore Utility (CTPView Server Menu)" on page 20.

- Synchronize the server. This method is available only when you have two or more CTPView servers in your network.

  See "Restoring CTPView Software Data by Manually Synchronizing the CTPView Server (CTPView)" on page 21.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Configuration Settings and Data with the Restore Utility (CTPView Server Menu)

This topic describes how to use the CTPView restore utility to restore the CTPView software configuration settings and data from a previously saved archive file.

Before you begin:

- Copy the backup (archive) file from its externally saved location to the `/var/www/html/acorn/data` directory on the server. The filename is in the format `ctpview_data_`*`server-name_date`*`.tgz`.
- Log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To restore your saved information with the CTPView restore utility:

1. From the CTPView Configuration Menu, select **5) Backup Functions**.

   The Backup Functions menu is displayed.
2. Select **2) Restore Settings and Data**.

   You are prompted to use the archive file. After the restore script runs, you are prompted to run it again.

Using the restore utility, you can restore the following CTPView configuration settings and data:

- Server synchronization on CTPView
- AutoSwitch configuration for CTP devices
- Configuration of CTP devices on CTPview (addition of CTP devices in groups)
- Configuration of remote bundles (CTP, SAToP, and CESoPSN)
- Network monitoring configuration on CTPView
- NTP configuration for CTP devices
- RADIUS configuration for CTP devices
- Syslog configuration for CTP devices
- SNMP and SNMP trap configurations for CTP devices

NOTE: We recommend that you use CTPView server synchronization to restore your data.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Configuration Settings and Data (CTPView) | 20

Restoring CTPView Software Data by Manually Synchronizing the CTPView Server (CTPView)

This topic describes how to use CTPView server synchronization to restore the CTPView software configuration settings and data.

To restore your saved information by synchronizing the CTPView server with another server:

1. Log in to the CTPView GUI on the server for which you are restoring the data.
2. In the side pane, select **Server > Administration** to display the Administrative Functions pane.
3. Click **Server Synchronization**.
4. Verify that the server is either not listed or its Server Type is set to Not Selected.
5. Log in to the CTPView GUI on the server from which you are restoring the data.
6. In the side pane, select **Server > Administration** to display the Administrative Functions pane.
7. Click **Server Synchronization**.
8. Ensure that the Server Type is set to Primary Server for this server, Secondary Server for the server being updated, and Not Selected for all other CTPView servers listed.
9. Click **Manually Synchronize Network**.

   The Synchronize Secondary Servers window opens.
10. Click **Select All Hosts**, and then click **Synchronize Servers**.
11. When the synchronization is completed, restore the Server Type for all CTPView servers to the values that you normally use for your network.

Using CTPView server synchronization, you can restore the following CTPView configuration settings and data:

- AutoSwitch configuration for CTP devices
- Configuration of CTP devices on CTPview (addition of CTP devices in groups)
- Configuration of remote bundles (CTP, SAToP, and CESoPSN)
- Network monitoring configuration on CTPView
- NTP configuration for CTP devices
- RADIUS configuration for CTP devices
- Syslog configuration for CTP devices
- SNMP and SNMP trap configurations for CTP devices

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Configuration Settings and Data (CTPView) | 20

Reviewing the Installation Log for Errors (CTPView Server CLI)

This topic describes how to use the CTPView installation log to check for errors. This log file maintains a record of all CTPView installations and upgrades.

To check the installation log for errors:

1. Using an SSH application, log in to the CTPView server.

   NOTE: If you do not successfully log in within 60 seconds, the session is closed.

2. Enter **su -** and then the root password.
3. Enter `more /var/log/ctpview_autoinstall.log` to view the log.

   Press the Spacebar to scroll through the log. Verify that no unresolved errors are listed for the latest installation or upgrade.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Verifying the CTPView Server OS Installation (CTPView)

This topic describes how to determine whether the CTPView server OS installation or upgrade completed successfully.

To validate the system configuration:

1. Log in to the CTPView GUI.
2. In the side pane, select **Server > Diagnostics**.

   The System Information pane is displayed.
3. In the System Vital section, verify that the following values match the information listed in the release notes or in "Understanding CTPView Software Upgrade Files" on page 98 for the OS version that you installed.
   - Kernel Version
   - Distro Name (distribution name)

> **NOTE**: The kernel version and distribution name are also displayed in the heading on the CTPView Configuration Menu.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Validating the CTPView Server Configuration (CTPView)

This topic describes how to validate the CTPView server system configuration. Examining the system configuration information is a useful first step in troubleshooting many issues. Validate the configuration after installing or upgrading the CTPView software or server OS to determine whether the operation completed successfully.

The validation utility reports on a long list of configuration details that are critical or desirable for proper operation of the CTPView software. Instructions are provided for correcting items that are out of compliance.

To validate the system configuration:

1. Log in to the CTPView GUI.
2. In the side pane, select **Server > Diagnostics**.

   The System Information pane is displayed.
3. Click **Validate Server Configuration**.

   The Server Configuration Validation pane is displayed.
4. Confirm that all fields are set to their default values.

   The display indicates whether each item is valid or noncompliant. A highlighted field indicates a problem. Follow the displayed instructions to correct the problem.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

CHAPTER 4

Upgrade Tasks for Only the CTPView Software

IN THIS CHAPTER

Upgrading Only the CTPView Software

This topic provides an overview of upgrading the CTPView software.

Before you begin, do all of the following:

- Using an SSH application, log in to the CTPView server, and enter **uname -r** on the CLI to determine the version of the operating system (OS). The initial characters in the output correlate to an OS version as follows:
  - 2.6.25 indicates that the operating system is FC9.
  - 2.6.11, 2.6.16, or 2.6.17 indicates that the operating system is FC4.
  - 2.4 indicates that the OS version is FC1.
- Determine the version of the CTPView software. In the CTPView server shell, enter **menu**, and then enter the root password when prompted. The software version is displayed in the heading. Alternatively, you can log in to the CTPView GUI and look in the heading next to the server IP address to determine the version of the CTPView software.
- Determine which upgrade file is required for your combination of currently installed CTPView server OS and CTPView software. See "Understanding CTPView Software Upgrade Files" on page 98 for guidance. The *CTPView Release Notes* for the version you are upgrading to also describes the required upgrade files.

The steps you must perform to upgrade the CTPView software depend on the currently installed versions of the server OS and the CTPView software. Two kinds of CTPView update archive files are available, *web* files and *complete* files:

- Web files are used for minor software updates. Their filenames are in the format **web_*server-os-version_upgrade-version_date*.tgz**. For example, the file **web_fcX_3.4R1_090715.tgz** provides an upgrade to CTPView 3.4R1 for CTPView servers running either FC4 or FC9.

  To upgrade the CTPView software with a web archive file, see "Upgrading the CTPView Software with a Web Archive File" on page 31.

- Complete files are used for more significant upgrades, and include additional software modules compared to the web files. Their filenames are in the format **ctpview_*server-os-version*_complete_*upgrade-version_date*.tgz**. For example, the file **ctpview_fc4_complete_3.4R1_090715.tgz** provides an upgrade to CTPView 3.4R1 for CTPView servers running either FC4.

  To upgrade the CTPView software with a complete archive file, see "Upgrading the CTPView Software with a Complete Archive File" on page 27.

NOTE: The CTPView Release Notes for the version you are upgrading to describes the upgrade files required for various combinations of currently installed CTPView server OS and CTPView software. "Understanding CTPView Software Upgrade Files" on page 98 also provides a more complete list of upgrade files and their associated software combinations.

NOTE: When the CTPView server OS version is FC1, you must first upgrade to a higher OS version. See "Installing or Upgrading the CTPView Server OS" on page 14.

NOTE: When you upgrade a version of CTPView that is lower than 2.2, the existing server CLI passwords and server accounts are not modified other than that the user account *Juniper* is added. However, all the existing CTPView user accounts are removed. Browser access to CTPView 2.2R1 and higher is through a new login interface that requires an administrator to create new usernames and passwords.

When you upgrade a version of CTPView that is lower than 2.0.4R1, you may need to update the server Ethernet settings after the upgrade. If so, use the CLI menu on the CTPView server to make the changes: **2) System Configuration > 1) Display Current Configuration**. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

RELATED DOCUMENTATION

Updating the CTPView Server Operating System and CTPView Network Management System Software | **11**

Upgrading the CTPView Software with a Complete Archive File

This topic describes how to upgrade the CTPView software with a complete archive file.

Before you begin, ensure that you have determined the correct archive file to use for your upgrade. See "Upgrading Only the CTPView Software" on page 25 for more information.

To upgrade the CTPView software with a complete archive file:

1. Access the CTPView software download page at the Juniper Networks Customer Support site at https://www.juniper.net/customers/csc/software/ctp/#sw.
2. Locate the update archive file appropriate for your current CTPView server OS and your CTPOS version.
3. Use a Secure Copy Protocol (SCP) program to copy the complete archive file to the **/tmp** directory on the server.

   The filename is in the format **ctpview**_*server-os-version*_**complete**_*upgrade-version*_*date*.**tgz**.
4. Log in to the server and switch to the root account.
5. Change the directory to**/tmp**.
6. Extract the archive by entering **tar -xzvf** *filename*.

   > **NOTE**: This step is not required when the CTPView server is running CTPView 3.4R2–p1 or higher-numbered releases. In these releases, the complete archive is automatically extracted when you run the upgrade script in the next step.

7. Run the installation script by entering **upgrade**.
8. Change the passwords for all the default user accounts (juniper_sa, root, Juniper, ctpview_pgsql) at the end during upgrade process. This step is applicable only when you upgrade the CTPView software to 7.3R7 release.

```
##########################################################################################
###################
CTPView has been installed on your system. Now, You need to set the passwords for all the
default user accounts.
##########################################################################################
```

```
####################
##########################################################################
##########################################################################
##########################################################################
                  PLEASE REMEMBER THESE PASSWORDS!!!


Password recovery is not a simple process:
- It is service affecting.
- It requires console access to the CTPView
- It requires rebooting the CTPView (Possibly even a system repower)
##########################################################################
##########################################################################
##########################################################################

The new password must be alphanumeric or the characters

           @ { } # % ~ [ ] = & , - _ !


The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use “CTPView-2-2”


Enter New UNIX Password for root

Retype New UNIX Password for root

Changing password for user root.
passwd: all authentication tokens updated successfully.

This will be a System Administrator

adduser: user juniper_sa exists

The new password must be alphanumeric or the characters

           @ { } # % ~ [ ] = & , - _ !
```

```
The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use “CTPView-2-2”


Enter New UNIX Password for juniper_sa

Retype New UNIX Password for juniper_sa

Changing password for user juniper_sa.
passwd: all authentication tokens updated successfully.

The new password must be alphanumeric or the characters

           @ { } # % ~ [ ] = & , - _ !


The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use “CTPView-2-2”



Changing password for user Juniper
Enter the new password:


Re-Enter the new password:


You will now be asked for the password of the PostgreSQL Administrator account:
Password for user postgres:
UPDATE 1
===== Successfully updated the CTPView password for default user Juniper. =====

Note:  The user Juniper has been assigned to the default user group TempGroup
       and has been given default user properties.  Review the values using
       the CTPView Admin Center and make any appropriate modifications.
```

```
The new password must be alphanumeric or the characters

          @ { } # % ~ [ ] = & , - _ !



The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Note : If unique passwords are not required, use “CTPView-2-2”




Changing password for user ctpview_pgsql
Enter the new password:

Re-Enter the new password:

You will now be asked for the password of the PostgreSQL Administrator account:
Password for user postgres:===== Successfully updated the PostgreSQL Apache password. =====
Stopping httpd:                                            [  OK  ]
Closing CTPView sockets:                                   [ NONE ]
Starting httpd:                                            [  OK  ]

>>>>>>   JUNIPER  CTPVIEW  UPGRADE  COMPLETE.   <<<<<<
```

9. Configure CTPView administrative settings to complete server setup, and ensure that security settings are correct.

   See Configuring the CTPView Administrative Settings.

10. To validate the system configuration, see "Validating the CTPView Server Configuration (CTPView)" on page 24.

RELATED DOCUMENTATION

Updating the CTPView Server Operating System and CTPView Network Management System Software | **11**

Upgrading Only the CTPView Software | **25**

Understanding CTPView Software Upgrade Files | **98**

Upgrading the CTPView Software with a Web Archive File

This topic describes how to upgrade the CTPView software with a web archive file.

Before you begin, ensure that you have determined the correct archive file to use for your upgrade. See "Upgrading Only the CTPView Software" on page 25 for more information.

To upgrade the CTPView software with a web archive file:

1. Access the CTPView software download page at the Juniper Networks Customer Support site at https://www.juniper.net/customers/csc/software/ctp/#sw.
2. Locate the update archive file appropriate for your current CTPView server OS and your CTPOS version.
3. Use a Secure Copy Protocol (SCP) program to copy the web archive file to the **/tmp** directory on the CTPView server.

   The filename is in the format **web**_*server-os-version*_*upgrade-version*_*date*.**tgz**.
4. Log in to the server and switch to the root account.
5. Change the directory to**/tmp**.
6. Run the installation script by entering **upgrade**.
7. Configure CTPView administrative settings to complete server setup, and ensure that security settings are correct.

   See Configuring the CTPView Administrative Settings.
8. To validate the system configuration, see "Validating the CTPView Server Configuration (CTPView)" on page 24.

RELATED DOCUMENTATION

Updating the CTPView Server Operating System and CTPView Network Management System Software | **11**

Upgrading Only the CTPView Software | **25**

Understanding CTPView Software Upgrade Files | **98**

CHAPTER 5

Configuration Tasks for CTPView Administrative Settings

IN THIS CHAPTER

Configuring the CTPView Administrative Settings

This topic provides an overview of configuring CTPView administrative settings. You must configure these settings when you receive a new CTPView server and after you install or upgrade the CTPView

server operating system (OS) or the CTPView software. Many of the settings provide better access security for your CTP network. Juniper Networks recommends that you perform some of the following tasks at least every year; details are in the task.

To configure the administrative settings:

- If the CTPView server is new, prepare the server for configuring the administrative settings.

  See "Preparing a New Server" on page 34.

- Change the default password used to access the BIOS menu.

  See "Changing the BIOS Menu Password (CTPView Server CLI)" on page 35.

- Change the default password for the server's default user account.

  See "Changing the Server's Default User Account Password (CTPView Server CLI)" on page 36.

- Change the default password for the server's root account.

  See "Changing the Server's Root Account Password (CTPView Server CLI)" on page 36.

- Change the default password used to access the GRUB Boot Loader menu.

  See "Changing the GRUB Boot Loader Password (CTPView Server Menu)" on page 37.

- Change the default password for the PostgreSQL server Apache user account.

  See "Changing the PostgreSQL Apache Account Password (CTPView Server Menu)" on page 38.

- Change the default password for the PostgreSQL server Administrator user account.

  See "Changing the PostgreSQL Administrator Account Password (CTPView Server Menu)" on page 39.

- Configure the server to operate on your network.

  See "Configuring the Network Access (CTPView Server Menu)" on page 40.

- Create a self-signed Web certificate.

  See "Creating a Self-Signed Web Certificate (CTPView Server Menu)" on page 40.

- Enable OpenSSL authentication by creating and importing a self-signed Web certificate.

  See "Enabling OpenSSL Authentication of Users by Creating a Self-Signed Web Certificate (CTPView Server Menu)" on page 47.

- Update the CTPView software to ensure that you have the latest features.

  See "Updating the CTPView Software" on page 42.

- Verify that you can log in to the CTPView GUI from your Web browser.

  See "Logging In with a Browser (CTPView)" on page 43.

- Change the default password for the CTPView GUI default user account.

  See "Changing the CTPView GUI Default User Account Password (CTPView)" on page 43.

- Create at least one global administrative account to access the CTPView Admin Center in the CTPView GUI.

  See "Creating a New Global_Admin Account (CTPView)" on page 44.

- Configure the hostnames as fully qualified domain names (FQDNs), as necessary, for your network needs. See "Configuring Subdomains in Hostnames (CTPView Server Menu)" on page 63.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Preparing a New Server

When you receive a new CTPView server, you must perform some physical tasks before proceeding.

To prepare a new server for use:

1. If you wish to install the server in an equipment rack, follow the instructions provided in the *Rack Installation Guide* that is included with the server.
2. Connect a monitor and keyboard to the server.

   The server's serial COM1 port connection has the following configuration:

   - Speed—9600 bps
   - Data bits—8
   - Parity—none
   - Stop bits—1
3. Connect the server to the appropriate Ethernet network through the 10/100Base-T port labeled **1**.
4. Verify that all ground and power connections to the server chassis are secure. Power on the server and monitor the front panel LEDs to verify that the server boots properly.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Changing the BIOS Menu Password (CTPView Server CLI)

For security purposes, change the default password for BIOS menu access. This account has no username associated with it. The BIOS menu password should conform to your local password requirements.

> **BEST PRACTICE**: Change the BIOS menu password at least yearly and whenever administrators change.

To change the BIOS menu password:

1. Power on or reboot the server.
2. During the boot process, press F2 while the Dell logo is displayed on the monitor. The boot process continues and displays several messages in turn on the screen.
3. Enter the default password when the process pauses and displays “Enter Setup Password.”

   For the default BIOS menu password, see "Default CTPOS and CTPView Accounts and Passwords" on page 94.
4. At the BIOS menu, select **System Security** and press Enter.
5. Highlight **Setup Password**—be sure that you have not selected **System Password**—and press Enter.
6. Enter your new BIOS password, reenter it, and then Press Enter to continue.
7. Press Esc.
8. In the window that opens, select **Save Changes and Exit** and press Enter.

   The server restarts.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

Changing the Server's Default User Account Password (CTPView Server CLI)

For security purposes, change the password for the server's default user account at regular intervals. You can choose instead to delete the default user account when all other administrative configuration tasks have been completed.

> **CAUTION**: Do not delete the default user account until after you have created another user account. Otherwise, you will not be able to log in to the server.

To change the password for the server’s default user account:

1. Log in to the CTPView server as the default user, using either a directly connected keyboard and monitor or an SSH application over your network.

   > **NOTE**: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

   For the default account username, see "Default CTPOS and CTPView Accounts and Passwords" on page 94. You cannot log in using the root account.
2. Enter **passwd**.
3. When prompted, enter the new password for the default user account.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

CTPOS and CTPView Software Password Requirements | 96

Changing the Server's Root Account Password (CTPView Server CLI)

For security purposes, change the password for the server's root user account at regular intervals. The root account password should conform to your local password requirements.

> **BEST PRACTICE**: Change the root account password at least yearly and whenever administrators change.

To change the root account password:

1. Log in to the CTPView server as a non-root user, using either a directly connected keyboard and monitor or an SSH application over your network.

   > **NOTE**: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

2. Enter **su -** to switch to the root account.
3. Enter the root password that you have set.

   You cannot log in using the root account.
4. Enter **passwd**.
5. Enter your new password.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

Changing the GRUB Boot Loader Password (CTPView Server Menu)

For security purposes, change the default password for the GRUB Boot Loader menu.

> **BEST PRACTICE**: Change the GRUB Boot Loader password at least yearly and whenever administrators change.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

NOTE: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To change the GRUB Boot Loader password:

1. From the CTPView Configuration Menu, select **Option 8 (GRUB Functions)**.
2. Select **1) Change GRUB password**.
3. Follow the prompts to complete changing the password.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

Changing the PostgreSQL Apache Account Password (CTPView Server Menu)

For security purposes, change the password for the PostgreSQL server Apache user account at regular intervals.

BEST PRACTICE: Change the PostgreSQL Apache password at least yearly and whenever administrators change.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

NOTE: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To change the PostgreSQL Apache password:

1. From the CTPView Configuration Menu, select **6) PostgreSQL Functions**.
2. Select **2) Change PostgreSQL Apache password**.
3. Follow the prompts to complete changing the password.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96
Configuring the CTPView Administrative Settings | 32
Changing Passwords to Improve Access Security | 238

Changing the PostgreSQL Administrator Account Password (CTPView Server Menu)

For security purposes, change the default password for the PostgreSQL server administrator user account.

> **BEST PRACTICE**: Change the PostgreSQL administrator account password at least yearly and whenever administrators change.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

> **NOTE**: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To change the PostgreSQL administrator account password:

1. From the CTPView Configuration Menu, select **6) PostgreSQL Functions**.
2. Select **1) Change PostgreSQL Administrator password**.
3. Follow the prompts to complete changing the password.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

Configuring the Network Access (CTPView Server Menu)

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

> **NOTE**: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address.

To configure server access to your network:

1. From the CTPView Configuration Menu, select **2) System Configuration** and enter **y** to continue.
2. Select **1) Display Current Configuration** to review the current configuration.
3. Use options **2)** through **5)** to configure the server to operate on your network.
4. Exit the submenu to implement your changes.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Creating a Self-Signed Web Certificate (CTPView Server Menu)

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To create a self-signed Web certificate:

1. From the CTPView Configuration Menu, select **9) AAA Functions**.

   The AAA functions for CTPView can be viewed and set in the AAA sub-menu of the CLI menu script. Only System Administrators have authorization to view or modify the AAA functions. Configuration of the CTPView AAA functions has three major components:

- Configuring the global configuration parameters, for example entering the IP addresses of the RADIUS servers you want to use for authentication.
- Configuring the global configuration parameters, for example entering the IP addresses of the TACACS+ servers you want to use for authentication.
- Then selecting the options which the various access methods will use. For example, enabling HTTPS – CAC/PKI with OCSP certificate validation.

2. Select **7) CAC/PKI Configuration**.

   This selection enables you to perform CAC/PKI configuration (HTTPS). CTPView is built with a default server certificate installed which is sufficient for testing purposes only. Before deploying the server in a production environment you must obtain and install a server certificate issued by a Trusted Signing CA. If you attempt to access multiple CTPView servers running on CentOS which are still using their default self-signed certificates you may be denied access by your browser because it will detect that multiple servers are presenting certificates with the same serial number. Obtaining and installing a signed server certificate is a simple process. First, you must create a certificate signing request (CSR) for your server which you will present to the Trusted Signing CA you have selected to use. To start, go to the CAC/PKI Configuration menu. The path is menu > AAA Functions > CAC/PKI Configuration.

3. In the CAC/PKI Menu, select **2) Self-Sign CSR**.

   While it is preferred that you have your server CSR signed by a Trusted Signing CA, where that is not possible you may generate a self-signed server certificate using the CTPView_CA issued by Juniper Networks. Note that if you use the CTPView_CA certificate, the self-signed certificate will generate an error in client browsers to the effect that the signing certificate authority is unknown and not trusted. However you will be able to successfully complete the connection. To use the CTPView_CA to sign your CSR select Self-Sign CSR from the CAC/PKI Menu.

   Enter the CSR filename and the utility will create a signed server certificate which you can then import into the certificate database. No additional Chain of Trust certificates are required to use the CTPView_CA. As when creating a CSR, repeating the signing process has no effect on the configuration or operation of the server since a separate process is required to import the certificate. When the Trusted Signing CA sends you the signed server certificate you will need to import it into your server's certificate database. You will also need to import all of the certificates that make up the Chain of Trust for your new server certificate. These are available from your Trusted Signing CA. Copy all of the certificates into the /tmp directory of the server. They can have any filename and file extension.

4. Enter answers for each question that is subsequently displayed.

   You are required to enter the Encryption Key Size, Common Name, Organization Name and Country. You may also include any combination of these optional fields: Organizational Unit (3 possible fields), State, and City/Town. The script will generate a random seed to use when creating the CSR by using the timing of keystrokes on your keyboard. The CSR will be a RSA certificate in ASCII format (i.e. plain text), using either 1024 or 2048 bit encryption depending on your choice when creating the CSR. The CSR name will be <Common Name>.csr and is created in the /tmp directory on the server.

If you want to change any of the information you entered when creating the CSR simply create a new CSR. Creating a CSR has no effect on the configuration or operation of the server. Send the CSR which you created to your Trusted Signing CA. You may be asked to send the CSR as an email attachment or to paste the CSR into a web form. You can do that by opening the CSR file with a text editor, such as WordPad or VI, then use the copy and paste editing functions to transfer the new certificate request to the web form.

> **NOTE**: For **Common Name**, enter the IP address of the server. Otherwise, your users' browsers will report a domain name mismatch when users connect to the server.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Updating the CTPView Software

or a new server, upgrade to the latest version of the CTPView software to ensure that you have the latest features available.

To update the CTPView software:

1. Use your Juniper Networks customer support username and password to log in to the CTP support site at https://www.juniper.net/customers/csc/software/ctp/.
2. If present, download an update for your version of the CTPView software and the associated Release Notes.

   The CTPView version number is displayed in the heading of the CTPView Configuration Menu utility.
3. Upgrade the CTPView software according to the instructions presented in "Upgrading Only the CTPView Software" on page 25.

> **NOTE**: Always refer to the Release Notes associated with the update. These Release Notes may contain information that supersedes the information in that topic.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Logging In with a Browser (CTPView)

Verify that you can log in to the CTPView software from a Web browser. You must be able to access the CTPView software to complete the administrative configuration.

To log in to the server with a browser:

1. In the address bar of a browser enter the address https:// *your-server-IP-address*.
2. Accept the certificate when your browser warns that the security certificate presented by the website was not issued by a trusted certificate authority.
3. When the CTPView login page appears, log in as the default CTPView user for the Global_Admin account.

   > **NOTE**: 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.

   For the default password, see "Default CTPOS and CTPView Accounts and Passwords" on page 94.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Changing the CTPView GUI Default User Account Password (CTPView)

For security purposes, change the password for the CTPView GUI default user account at regular intervals.

To change the CTPView default user account password:

1. Log in to the CTPView GUI with the default username and the password you have set previously.

   For the default username, see "Default CTPOS and CTPView Accounts and Passwords" on page 94. You cannot log in using the root account.
2. Click **Edit My Account**.
3. Type the current password and the new password, and reenter the new password.

   Click **Password Help** to learn how to create an acceptable CTPView password.

4. Click **Update Password**.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Configuring the CTPView Administrative Settings | 32

Creating a New Global_Admin Account (CTPView)

A global administrative (Global_Admin) account is required to access the CTPView Admin Center. Do not use the default user account for routine access. Create a separate account for each user that requires administrative access. Beginning with CTPView 2.2R2, the security-enhanced interface allows only one active session per username. When a second user attempts to log in with the same username in an active session, both IP addresses for the clients and the username are locked from access for a preset lockout period.

To create a Global_Admin account:

1. Log in to the CTPView GUI with the default username and the password you have set previously. For the default username, see "Default CTPOS and CTPView Accounts and Passwords" on page 94.
2. Click **Admin Center**.
3. Select **Users > All Users**.
4. Type the desired username, group name, and password, and click **Add User**.
5. Select **Users > Modify User Properties**.
6. Select the **Global_Admin** user level.
7. Log out of CTPView and use the new account to log back in.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Configuring the CTPView Administrative Settings | 32

Changing the User Password (CTP Menu)

You can change your password by logging in to the CTP system. The new password must meet the requirements that are specified in the Configuration Security Profile menu.

To change your password by using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **13) Set your password**.

   The CTP system displays the password requirements based on your security profile. Table 2 on page 46 lists the security profiles and their password requirements.

```
##########################################################################
##########################################################################
##########################################################################
                  PLEASE REMEMBER THESE PASSWORDS!!!


Password recovery is not a simple process:
- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device
##########################################################################
##########################################################################
##########################################################################

The new password must be alphanumeric or the characters

           @ { } # % ~ [ ] = & , - _ !


The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for ctp

Retype New Password for ctp

Changing password for user ctp.
```

```
passwd: all authentication tokens updated successfully.
Backing up /etc to nonvolatile storage..
```

Follow the onscreen instructions to set the new password.

The following message is displayed if you do not have the permissions required to change password:

```
This user does not have privileges to do this.
```

Table 2: Requirements for New Password

Password Attributes	Units	Security Profiles and Their Attribute Range in CTPView		Security Profiles and Their Attribute Range in CTPOS	
		High	Low	High	Low/Very Low
Minimum length	char	15–64	5–64	15–256	15–256
Maximum length	char	15–64	5–64	256	256
Minimum lowercase characters	char	1–10	0–10	1–15	0–15
Minimum uppercase characters	char	1–10	0–10	1–15	0–15
Minimum digits	char	1–10	0–10	1–15	0–15
Minimum other characters	char	1–10	0–10	1–15	0–15
Contains username	–	no	no	no	no
Checked with cracklib library	–	yes	no	yes	yes

Table 2: Requirements for New Password *(Continued)*

Password Attributes	Units	Security Profiles and Their Attribute Range in CTPView		Security Profiles and Their Attribute Range in CTPOS	
		High	Low	High	Low/Very Low
Min required new characters	number	5	0	5	5
Allowed authentication retries	–	1–3	1–3	1–3	1–3
Lockout after login failure	seconds	60-indefinite	60-indefinite	900	900

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96
Default CTPOS and CTPView Accounts and Passwords | 94
Managing User Passwords (CTPView Server Menu) | 200

Enabling OpenSSL Authentication of Users by Creating a Self-Signed Web Certificate (CTPView Server Menu)

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.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

A new CA certificate is needed to support this feature. All logging in of users using CTPView uses this new CA certificate. For this feature, Mod_ssl “mod_ssl-2.2.31-1.el5” and OpenSSL “openssl-1.0.2d-1”

libraries are required. A certificate authority (CA) database is created on the CTPView server with this feature. This database is required for the OpenSSL tool to manage certificates and its path is "/etc/httpd/CA". OpenSSL CA certificate, server certificates, certificate revocation lists (CRLs), and private keys are stored in the CA database directory.

The following configuration files are modified to support this feature:

- Openssl.cnf—The following entries are enhanced in the openssl.cnf file for CA certificate management:

  dir—CA database path certificate—CA certificate

  private_key—CA private key

  crl—CRL Path

- Along with the preceding modifications, "countryName" and "stateOrProvinceName" are modified to support generation of server certificates for multiple countries and states. The nss.conf file is used by NSS protocol that uses secured web on port 443. To disable NSS protocol, all instances of the port number of 443 used in this file are replaced by 8443.

- The ssl.conf file is utilized by mod_ssl library that uses secured web on port 443. To enable MOD_SSL protocol on port 443, all port numbers of 8443 used in this configuration file are replaced by 443. The SSLProtocol, SSLCertificateFile, SSLCertificateKeyFile, SSLCertificateChainFile, and SSLCACertificateFile entries in the ssl.conf file are modified.

OpenSSL Certificate Database

OpenSSL maintains a certificate database that contains CA certificate, CA private key, server certificates, server private key, Certificate Revocation List (CRL) files, serial and index file. The OpenSSL certificate database is stored in the "/etc/httpd/CA" directory. The OpenSSL certificate database directory contains following entities:

- certs—This directory contains all OpenSSL certificates.

- crl—This directory contains all OpenSSL CRLs.

- currCert—This directory contain current installed server certificate.

- index.txt—The index file consists index of all certificates.

- newcerts—This directory is used by OpenSSL to create new certificates.

- private—This directory contains private keys.

- revokedCert—This directory contains all revoked certificates.

- serial—This file is used for OpenSSL that contain the next available serial number of certificate in hexadecimal format.

- crlnumber—This file is used for OpenSSL that contain the next available serial number of CRL in hexadecimal format.

The OpenSSL authentication for user login feature is not supported with user interface for CRL. Instead, CRL is managed by OpenSSL CA database.

This procedure describes the steps to create a CSR, self-sign the CSR, and import it.

To enable OpenSSL method of authentication for logging in of users by creating a self-signed Web certificate:

1. From the CTPView Configuration Menu, select **9) AAA Functions**.

   The AAA functions for CTPView can be viewed and set in the AAA sub-menu of the CLI menu script. Only System Administrators have authorization to view or modify the AAA functions. Configuration of the CTPView AAA functions has three major components:

   - Configuring the global configuration parameters, for example entering the IP addresses of the RADIUS servers you want to use for authentication.
   - Configuring the global configuration parameters, for example entering the IP addresses of the TACACS+ servers you want to use for authentication.
   - Then selecting the options which the various access methods will use. For example, enabling HTTPS – CAC/PKI with OCSP certificate validation.

2. Select **7) CAC/PKI Configuration**.

   This selection enables you to perform CAC/PKI configuration (HTTPS). CTPView is built with a default server certificate installed which is sufficient for testing purposes only. Before deploying the server in a production environment you must obtain and install a server certificate issued by a Trusted Signing CA. If you attempt to access multiple CTPView servers running on CentOS which are still using their default self-signed certificates you may be denied access by your browser because it will detect that multiple servers are presenting certificates with the same serial number. Obtaining and installing a signed server certificate is a simple process. First, you must create a certificate signing request (CSR) for your server which you will present to the Trusted Signing CA you have selected to use. To start, go to the CAC/PKI Configuration menu. The path is menu > AAA Functions > CAC/PKI Configuration.

3. In the CAC/PKI Menu, select **1) Create CSR**. You need to enter information about your server and organization. You are required to enter the Encryption Key Size, Common Name, Organization Name and Country. You may also include any combination of these optional fields: Organizational Unit (3 possible fields), State, and City/Town.

```
CAC/PKI Menu

Please choose a menu item from the following list:
```

```
0)  Return to previous menu
1)  Create CSR
2)  Self-Sign CSR
3)  List Certificates
4)  Import Certificate
5)  Display Certificate
6)  Validate Certificate
7)  Remove Certificate
8)  List CRL's
9)  Import CRL
10) Display CRL
11) Remove CRL

Please input your choice [0]: 1

Answer these questions to generate a CSR:

 Enter encryption key size(1024 or 2048)(Only <ENTER> to abort):
    ctpview_server
Enter 1024 or 2048...
 Enter encryption key size(1024 or 2048)(Only <ENTER> to abort):
    2048
Enter Common Name, i.e. IP or FQDN (Only <ENTER> to abort):
    ctpview_server
 Enter Organization Name (Only <ENTER> to abort):
    Juniper
 Enter Organizational Unit Name #1 (optional):

 Enter Organizational Unit Name #2 (optional):

 Enter Organizational Unit Name #3 (optional):

 Enter Country (2 characters):
    IN
 Enter State (optional):
    Del
 Enter City/Town (optional):
    Del
CSR filename = ctpview_server.csr
Generating a 2048 bit RSA private key
...............+++
..........+++
writing new private key to '/tmp/ctpview_server.key'
```

```
-----

==============================================
Your certificate signing request has been created in ascii format.

Your CSR file is /tmp/ctpview_server.csr

You must now have this CSR signed by a CA.
==============================================

Hit return to continue...

CAC/PKI Menu

Please choose a menu item from the following list:

0)  Return to previous menu
1)  Create CSR
2)  Self-Sign CSR
3)  List Certificates
4)  Import Certificate
5)  Display Certificate
6)  Validate Certificate
7)  Remove Certificate
8)  List CRL's
9)  Import CRL
10) Display CRL
11) Remove CRL

Please input your choice [0]: 2

It is preferred that you have your server CSR signed by a Trusted CA.
Where that is not possible, this utility will create a self-signed
server certificate using the CTPView CA issued by Juniper Networks.
This self-signed certificate will generate an error in client browsers to
the effect that the signing certificate authority is unknown and not trusted.

Place the CSR you wish to self-sign into the /tmp directory.

Enter the CSR filename (Only <ENTER> to abort):
    ctpview_server.csr
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/httpd/alias/demoCA/private/CTPView_CA.key:
```

```
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Nov 19 10:02:00 2015 GMT
            Not After : Nov 18 10:02:00 2016 GMT
        Subject:
            countryName               = IN
            stateOrProvinceName       = Del
            organizationName          = Juniper
            organizationalUnitName    =
            organizationalUnitName    =
            organizationalUnitName    =
            commonName                = ctpview_server
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                BE:0C:E8:66:E1:F8:7E:DE:50:38:07:4A:A0:14:39:62:AE:5D:00:E1
            X509v3 Authority Key Identifier:
                keyid:91:1A:8E:67:B6:C4:71:CB:63:62:9C:61:A9:44:54:DE:AC:23:9D:D2

Certificate is to be certified until Nov 18 10:02:00 2016 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

=============================================
Your CSR has been signed.

The certificate file is /tmp/ctpview_server.crt

You must now import this certificate.
=============================================

Hit return to continue...
```

```
Please input your choice [0]: 4

There are two catagories of certificates you may import.
The first is the returned CSR certificate signed by a Signing CA.
The second is the group of certificates which are in the chain

Place the certificate you wish to import into the /tmp directory.

Enter the certificate filename (Only <ENTER> to abort):
    ctpview_server.crt

Is this the signed CSR certificate for this server? [N] Y
ctpview_server.crt: OK
Stopping httpd:                                            [OK]
Starting httpd: Apache/2.2.29 mod_ssl/2.2.29 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server ctpview:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful.
                                                           [  OK  ]

Hit return to continue...

CAC/PKI Menu

Please choose a menu item from the following list:

0)  Return to previous menu
1)  Create CSR
2)  Self-Sign CSR
3)  List Certificates
4)  Import Certificate
5)  Display Certificate
6)  Validate Certificate
7)  Remove Certificate
8)  List CRL's
9)  Import CRL
10) Display CRL
11) Remove CRL
```

```
Please input your choice [0]: 5

Current listing of installed Certificates:
CTPView_CA.crt  ctpview_server.crt

Enter the Certificate Name (Only <ENTER> to abort):
    ctpview_server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IN, ST=Delhi, L=Delhi, O=Juniper, OU=Jun ODC, CN=juniper.net CA/
emailAddress=saurav.kumar@juniper.net
        Validity
            Not Before: Nov 19 10:02:00 2015 GMT
            Not After : Nov 18 10:02:00 2016 GMT
        Subject: C=IN, ST=Del, O=Juniper, OU= , OU= , OU= , CN=ctpview_server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bf:49:00:19:38:82:c8:1f:3c:db:41:28:cb:01:
                    4e:b5:b4:26:f0:2e:48:f5:33:f4:81:fd:3b:6b:fc:
                    ae:c7:c9:f6:b7:68:fd:b2:b1:45:cc:63:ca:04:91:
                    10:36:c3:65:27:42:ef:3f:c0:75:88:b5:e6:d3:fa:
                    a6:bd:fb:51:a7:72:da:59:63:b8:8d:ad:79:a0:e6:
                    7b:0f:89:33:2a:71:c9:0a:2f:66:90:39:32:ec:4a:
                    d1:a0:f5:af:1a:b7:5a:96:ae:b7:cf:d1:df:dc:37:
                    35:d8:df:17:8d:50:a9:e6:5b:c6:08:e8:39:9f:94:
                    f3:3f:bc:28:c8:b4:ce:b7:b1:12:e2:e6:a1:24:c2:
                    4e:7b:2c:78:e1:07:60:e6:eb:f0:d5:51:28:4f:f1:
                    6d:a6:e3:3b:84:d3:7f:32:06:d8:be:0e:32:42:8a:
                    c5:11:05:ef:39:ea:0c:90:17:72:b7:f6:97:89:4b:
                    f9:12:ec:eb:fc:6e:3b:58:e4:0f:9e:18:79:13:28:
                    fd:22:60:68:16:39:1a:5f:95:2a:58:31:77:06:92:
                    14:08:8e:14:75:91:b9:83:5a:bc:7a:30:78:1c:5e:
                    9c:0b:6d:72:2c:fb:7b:43:dc:73:04:c1:0a:ec:c3:
                    f3:b3:8c:02:f5:86:f1:de:e8:f1:5f:d7:06:57:4c:
                    c6:e3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
```

```
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                BE:0C:E8:66:E1:F8:7E:DE:50:38:07:4A:A0:14:39:62:AE:5D:00:E1
            X509v3 Authority Key Identifier:
                keyid:91:1A:8E:67:B6:C4:71:CB:63:62:9C:61:A9:44:54:DE:AC:23:9D:D2

    Signature Algorithm: sha1WithRSAEncryption
         49:d0:ab:29:5f:61:bc:b4:e7:2a:41:ff:93:6e:ab:cb:c8:a8:
         2a:91:d8:10:66:da:9e:83:c2:84:18:03:75:8c:c7:16:49:0d:
         49:35:52:5a:fa:98:8f:20:da:79:34:17:00:1c:74:c0:d1:26:
         0e:13:a4:2b:52:34:b8:99:45:67:20:42:9c:15:36:8a:e0:14:
         63:ff:b1:00:94:bc:bf:86:3d:24:67:6c:39:d1:c8:8f:3d:a6:
         3b:88:12:1b:99:e1:6d:c2:d7:2b:0d:8f:57:44:47:09:05:ae:
         ee:55:ab:2d:54:ef:6e:11:7c:be:a8:7d:21:1a:50:b3:c5:d6:
         fd:40:72:7d:55:e8:32:b8:83:00:dd:14:86:f1:95:4a:37:80:
         a0:f5:1e:66:c3:c3:7c:78:e2:1c:0a:39:5c:60:2a:80:04:49:
         2e:4f:38:cb:13:e9:26:c7:1f:85:b3:01:a0:40:d2:d6:58:4b:
         bd:7c:3a:16:59:14:95:ca:4a:7e:b5:f4:72:ee:98:af:09:1d:
         5a:8c:34:8a:55:af:c3:ac:88:5b:d9:d0:69:10:a0:91:9f:ce:
         c3:fe:7a:0c:cc:6d:78:8e:9a:57:2e:0c:64:e6:d5:4f:05:9a:
         2f:4e:35:9a:92:d2:2b:fe:a8:bc:78:d1:83:b0:64:e7:c6:83:
         67:72:da:31

Hit return to continue...
CAC/PKI Menu

Please choose a menu item from the following list:

0)  Return to previous menu
1)  Create CSR
2)  Self-Sign CSR
3)  List Certificates
4)  Import Certificate
5)  Display Certificate
6)  Validate Certificate
7)  Remove Certificate

Please input your choice [0]: 3
CTPView_CA.crt    ctpview_server.crt
```

```
Hit return to continue...
```

4. Follow the onscreen instructions and configure the options as described inTable 3 on page 56.

Table 3: Creating a Certificate Signed Request

Field	Function	Your Action
Enter encryption key size(1024 or 2048)(Only <ENTER> to abort):	Specifies the encryption key size of the CSR file.	Specify `1024` or `2048`. If you enter a different value, you are prompted to enter the key size again. You can press `Enter` to terminate the process of creating the CSR.
Enter Common Name, i.e. IP or FQDN (Only <ENTER> to abort):	Specifies the common name to be used for the CSR file.	Specify the IP address or the fully-qualified domain name, which is the common name that is used in the distinguished name. The FQDN or any other CN values must be specified during the certificate request procedure. You can press `Enter` to terminate the process of creating the CSR.
Enter Organization Name (Only <ENTER> to abort):	Specifies the organization name of the CSR.	Enter the organization name to be used in the CSR. This name is a component in the distinguished name. You can press `Enter` to terminate the process of creating the CSR.
Enter Organizational Unit Name #1 (optional):	Specifies the first name of the organizational unit to be used in the CSR file.	Specify the first name of the organizational unit to be used in the CSR. This name is a component in the distinguished name.
Enter Organizational Unit Name #2 (optional):	Specifies the second name of the organizational unit to be used in the CSR file.	Specify the second name of the organizational unit to be used in the CSR. This name is a component in the distinguished name. This field is optional. If you not want to specify this value, press `Enter` to skip this entry and proceed to the next field.

Table 3: Creating a Certificate Signed Request *(Continued)*

Field	Function	Your Action
Enter Organizational Unit Name #3 (optional):	Specifies the third name of the organizational unit to be used in the CSR file.	Specify the third name of the organizational unit to be used in the CSR. This name is a component in the distinguished name. This field is optional. If you not want to specify this value, press `Enter` to skip this entry and proceed to the next field.
Enter Country (2 characters):	Specifies the country code, such as IN for India or US for United States of America, to be used in the CSR.	Specify the country code to be used in the CSR. The country code is a parameter in the distinguished name. This field is optional. If you not want to specify this value, press `Enter` to skip this entry and proceed to the next field.
Enter State (optional):	Specifies the name of the state to be used in the CSR.	Specify the name of the state to be used in the CSR. This name is a component in the distinguished name. This field is optional. If you not want to specify this value, press `Enter` to skip this entry and proceed to the next field.
Enter City/Town (optional):	Specifies the name of the town or city to be used in the CSR.	Specify the name of the town or city to be used in the CSR. This name is a component in the distinguished name. This field is optional. If you not want to specify this value, press `Enter` to skip this entry and proceed to the next field.

Table 3: Creating a Certificate Signed Request *(Continued)*

Field	Function	Your Action
CSR Filename	The script will generate a random seed to use when creating the CSR by using the timing of keystrokes on your keyboard. The CSR will be a RSA certificate in ASCII format (i.e. plain text), using either 1024 or 2048 bit encryption depending on your choice when creating the CSR. The CSR name will be <Common Name>.csr and is created in the /tmp directory on the server. If you want to change any of the information you entered when creating the CSR simply create a new CSR. Creating a CSR has no effect on the configuration or operation of the server.	View the CSR filename that is generated is displayed. You are alerted that the CSR needs to be signed by a CA. Also, the path in which the CSR file is stored is displayed.

5. Press `Enter` to continue to the next step. You need to self-sign the CSR after you have created it. The CAC/PKI menu is displayed.
6. In the CAC/PKI Menu, select **2) Self-Sign CSR**.

   While it is preferred that you have your server CSR signed by a Trusted Signing CA, where that is not possible you may generate a self-signed server certificate using the CTPView_CA issued by Juniper Networks. Note that if you use the CTPView_CA certificate, the self-signed certificate will generate an error in client browsers to the effect that the signing certificate authority is unknown and not trusted. However you will be able to successfully complete the connection. To use the CTPView_CA to sign your CSR select Self-Sign CSR from the CAC/PKI Menu.

   Enter the CSR filename and the utility will create a signed server certificate which you can then import into the certificate database. No additional Chain of Trust certificates are required to use the CTPView_CA. As when creating a CSR, repeating the signing process has no effect on the configuration or operation of the server since a separate process is required to import the certificate. When the Trusted Signing CA sends you the signed server certificate you will need to import it into your server's certificate database. You will also need to import all of the certificates that make up the Chain of Trust for your new server certificate. These are available from your Trusted Signing CA. Copy all of the certificates into the /tmp directory of the server. They can have any filename and file extension.
7. Enter answers for each question that is subsequently displayed.

You are required to enter the Encryption Key Size, Common Name, Organization Name and Country. You may also include any combination of these optional fields: Organizational Unit (3 possible fields), State, and City/Town. The script will generate a random seed to use when creating the CSR by using the timing of keystrokes on your keyboard. The CSR will be a RSA certificate in ASCII format (i.e. plain text), using either 1024 or 2048 bit encryption depending on your choice when creating the CSR. The CSR name will be <Common Name>.csr and is created in the /tmp directory on the server. If you want to change any of the information you entered when creating the CSR simply create a new CSR. Creating a CSR has no effect on the configuration or operation of the server. Send the CSR which you created to your Trusted Signing CA. You may be asked to send the CSR as an email attachment or to paste the CSR into a web form. You can do that by opening the CSR file with a text editor, such as WordPad or VI, then use the copy and paste editing functions to transfer the new certificate request to the web form.

> **NOTE**: For **Common Name**, enter the IP address of the server. Otherwise, your users' browsers will report a domain name mismatch when users connect to the server.

8. Follow the onscreen instructions and configure the options as described inTable 4 on page 59.

Table 4: Self-Signing a Certificate Signed Request

Field	Function	Your Action
Enter the CSR filename (Only <ENTER> to abort):	Specify the name of the CSR file. The CSR will be a RSA certificate in ASCII format (i.e. plain text), using either 1024 or 2048 bit encryption depending on your choice when creating the CSR. The CSR name will be <Common Name>.csr and is created in the /tmp directory on the server.	Specify the name of the CSR. Press `Enter` to terminate the operation.
Enter pass phrase for /etc/httpd/alias/demoCA/private/CTPView_CA.key:	Specifies the pass phrase, after which the system checks whether the request matches with the signature.	Specify the pass phrase.
Sign the certificate? [y/n]:	Specifies whether you want to sign the certificate.	Specify `y` or `n`.
1 out of 1 certificate requests certified, commit? [y/n]	Specifies whether you want to commit the signed certificate to the database.	Specify `y` or `n`.

9. Press `Enter` to continue to the next step of importing the certificate. The CAC/PKI menu is displayed.
10. From the CAC/PKI Menu, select **4) Import Certificate** to import the certificate into the database.

    There are two categories of certificates you may import. The first is the returned CSR certificate signed by a Signing CA. The second is the group of certificates which are in the chain
11. Follow the onscreen instructions and configure the options as described inTable 5 on page 60.

    Table 5: Self-Signing a Certificate Signed Request

Field	Function	Your Action
Enter the certificate filename (Only <ENTER> to abort):	Specifies the name of the CSR. The CSR name will be <Common Name>.csr and is created in the /tmp directory on the server. If you want to change any of the information you entered when creating the CSR simply create a new CSR. Creating a CSR has no effect on the configuration or operation of the server.	Specify the name of the CSR file that you previously created. Press `Enter` to terminate the operation.
Is this the signed CSR certificate for this server? [N]	Specifies whether the signed CSR is for the server on which you are configuring it. If you enter `y`, the HTTP daemon is stopped and started. You are asked to enter the pass phrase in the next step.	Specify `y` or `n`.
Enter pass phrase:	Specifies the pass phrase for the private key files that need to be decrypted for security reasons.	Specify the pass phrase for the private key files that are encrypted.

12. Press `Enter` to continue to the next step. The CAC/PKI menu is displayed.
13. From the CAC/PKI Menu, select **5) Display Certificate**. The list of certificates are displayed.

```
Current listing of installed Certificates:
CTPView_CA.crt  ctpview_server.crt
```

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Importing Certificates Issued by a Third-Party CA (CTPView Server Menu)

To import certificates issued by a third-party CA:

1. From the CTPView Configuration Menu, select **9) AAA Functions**.

```
CTPView Configuration Menu

Please choose a menu item from the following list:

0) Exit CTPView Configuration Menu
1) Security Profile
2) System Configuration
3) Port Forwarding
4) Advanced Functions
5) Backup Functions
6) PostgreSQL Functions
7) CTPView Access Functions
8) GRUB Functions
9) AAA Functions

Please input your choice [0]: 9
```

2. From the AAA Menu, select **7) CAC/PKI Configuration**.

```
 AAA Menu

Please choose a menu item from the following list:

0) Return to previous menu
1) SSH(1st) - CAC/PKI:          Disabled
2) SSH(2nd) - RADIUS/RSA:       Disabled, TACACS+:       Disabled
3) SSH(3rd) - Local User/Pass:  Enabled - Loc Acct
4) HTTPS(1st) - CAC/PKI:          Disabled
5) HTTPS(2nd) - RADIUS/RSA:       Disabled, TACACS+:       Disabled
6) HTTPS(3rd) - Local User/Pass:  Enabled - Loc Acct
7) CAC/PKI Configuration
8) RADIUS/RSA SecurID Configuration
9) TACACS+ Configuration
```

```
Please input your choice [0]: 7
```

3. In the CAC/PKI Menu, select **4) Import Certificate**.

```
CAC/PKI Menu

Please choose a menu item from the following list:

0)  Return to previous menu
1)  Create CSR
2)  Self-Sign CSR
3)  List Certificates
4)  Import Certificate
5)  Display Certificate
6)  Validate Certificate
7)  Remove Certificate
8)  List CRL's
9)  Import CRL
10) Display CRL
11) Remove CRL

Please input your choice [0]: 4
```

4. Enter the certificate filename. Make sure that the certificate issued by the third-party CA is placed in the /tmp directory.

```
There are two catagories of certificates you may import.
The first is the returned CSR certificate signed by a Signing CA.
The second is the group of certificates which are in the chain

Place the certificate (and root certificate of signing CA) you wish to import into the /tmp
directory.

Enter the certificate filename (Only <ENTER> to abort):
```

5. Enter **n** if the certificate being imported is not signed by the CTPView CA.

```
Is this the CTPView CA signed certificate for this server? [N] n
```

6. Enter the root certificate filename of signing CA.

```
Enter the root certificate filename of signing CA(Only <ENTER> to abort):
```

7. Press Enter to continue to the next step. The CAC/PKI menu is displayed.
8. From the CAC/PKI Menu, select **5) Display Certificate**. The imported certificate must be displayed in the list.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Configuring Subdomains in Hostnames (CTPView Server Menu)

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.

To enter the hostnames with subdomains and in accordance with the DNS standards:

1. From the CTPView Configuration Menu, select **2) System Configuration** to select the system settings to configure.
2. Select the **Change Hostname/Domain** menu option to make the changes to the hostname and to enter the hostname with subdomains. 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.

CHAPTER 6

Configuring the CTPView Server on Virtual Machines

IN THIS CHAPTER

Guidelines for Configuring Virtual CTPView Servers on WMWare ESX Servers

One of the salient and significant advantages of configuring a CTPView server on a virtual machine is to enable configuration of multiple CTPView server instances for quick access to a variety of server configurations. Also, you can run different OS versions and software releases on the virtualized CTPView server instances. TACACS+ servers, syslog servers, and RADIUS servers, besides serving as a platform for other applications, can be configured on the virtualized CTPView servers. We recommend that you use the VMWare help documentation for assistance in using the vSphere Client software.

Keep the following guidelines in mind when you configure a CTPView server on a VMWare ESX Server:

- Sizing the CTPView drive
  - When building a server, several options are presented to you from the Installation Utility. These choices depend on the version of software you are installing. The procedure illustrated in the section to create a VM instance of CTPView describes the options for CTPView 4.2R1 on CentOS. You can determine what other versions and OS you need by inspecting the code/gui/cdrom/isolinux.cfg file appropriate for the system in question. It also contains some hidden options not shown on the GUI screen.
  - Your most common selection is mostly “ctpview-vmdemo”. The advantage of using this choice is the small storage capacity it requires, with a minimum size is 4 GB. This behavior is achieved, which is also a disadvantage in some test cases, is using a single partition for the OS , data and

applications. The only time you might not want to build a CTPView server in such a manner is when you are conducting a test or a trial, which is dependant on having the same drive partitions as a production server.

- The choices of “ctpview-install” and ctpview-vmware” are identical. The reason for the distinction on the GUI screen is to alert the user that a minimum drive size of 60 GB is required. This classification is because some of the CTPView partitions in a network environment are fixed in size.

- A directory has been created on the ESXi host for storing ISO files that you may upload at **/vmfs/volumes/datastore1/ISO_FILES/**.
- When using a graphical application, such as WinSCP, to upload ISO files to the datastore remember to specify “scp” as the transport protocol. Also, you must disable the “Lookup user groups” option on the scp application to avoid a warning message.
- You need to manage a maximum number of virtual machines that are running at a point in time in such a way that it does not adversely affect total performance. The vSphere client has a variety of tools available to help you monitor the system performance.

CTPView Servers on Virtual Machines Overview

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. However, you must deploy the virtual appliance on a VMWare ESXi or Hyper-V server, which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional. Just as you can install additional physical appliances as CTPView servers to create a fabric to provide scalability and availability, you can deploy multiple virtual appliances to create a fabric that provides the same scalability and high availability as a fabric of physical appliances.

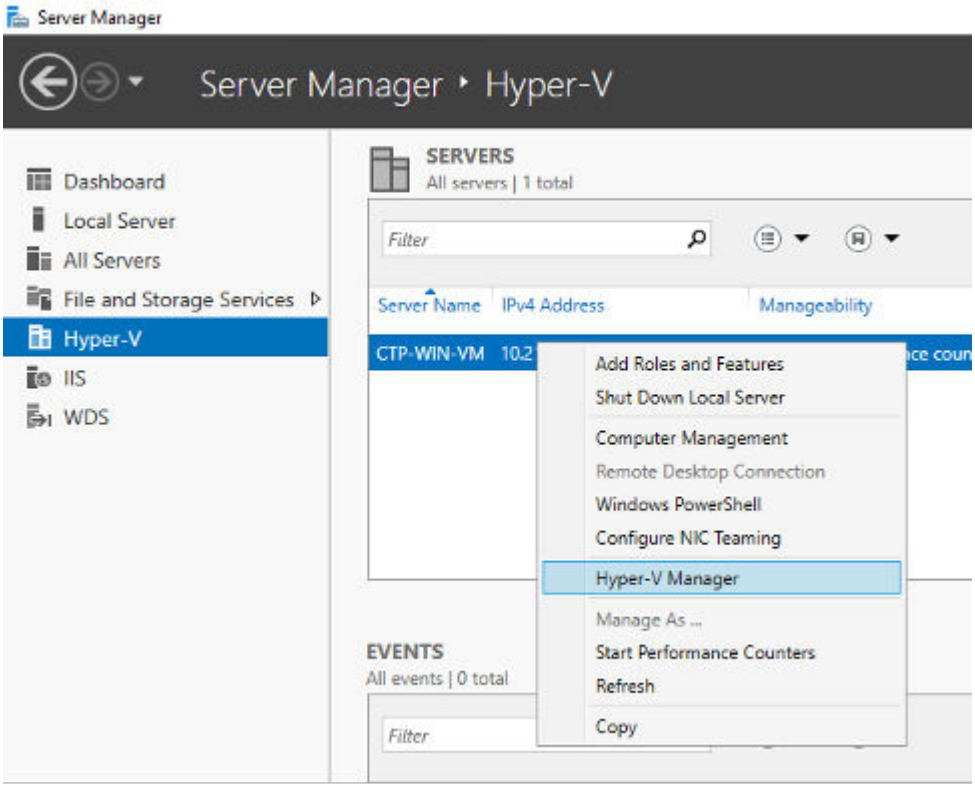
Various layers of abstraction combine to create virtualized environments. Virtualized hardware supports multi-tenancy in which guest virtual machines (VMs) running discrete operating system images share the system resources. Each guest VM runs its own user-space applications. If a physical machine does not directly support virtualization, a software layer called a hypervisor is used to manage the relationship between the guest VMs that run on it and compete for its resources.

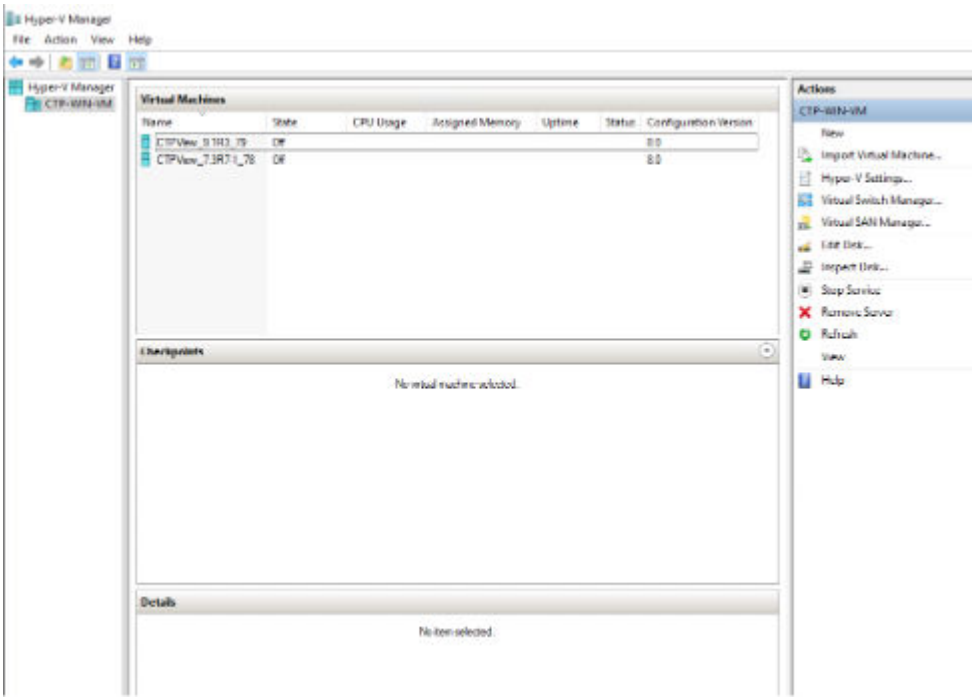
You can configure CTPView servers on a VMWare ESXi Server and a Microsoft Hyper-V Server.

Creating a Virtualized Instance of CTPView Server on a Hyper-V Server

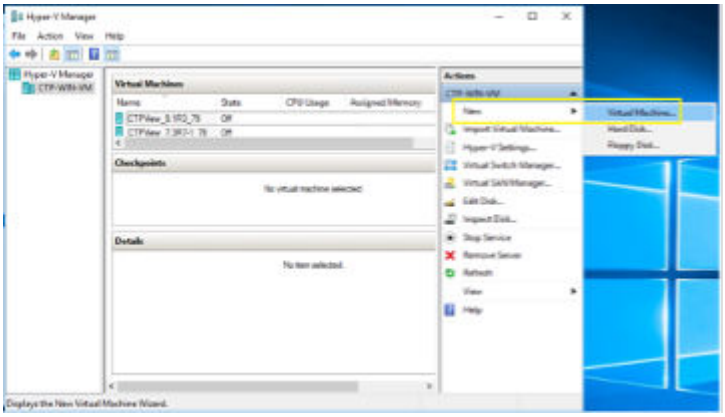
To create a virtualized CTPView server in a Hyper-V environment:

1. Install Hyper-V server on your system. We have taken Windows Server 2016 as the candidate for illustration purpose.
2. Copy the ISO files. For example, you will need *CentOS_CTPView_7.3R7-1_210302_CD.iso for 7.3R7-1 CTPView* and *centOS-7-x86_64-DVD-1804.iso for 9.x CTPView* , at the Hyper-V datastore at the path **C:\Users\Administrator\Downloads**. You can use any other path to store ISO files.
3. To open Hyper-V Manager, click **Hyper-V** in Server Manager.Right click **Hyper-V server**.Click **Hyper-V Manager** as shown, or you can access it by searching with the keyword “Hyper-V Manager” from the start menu.

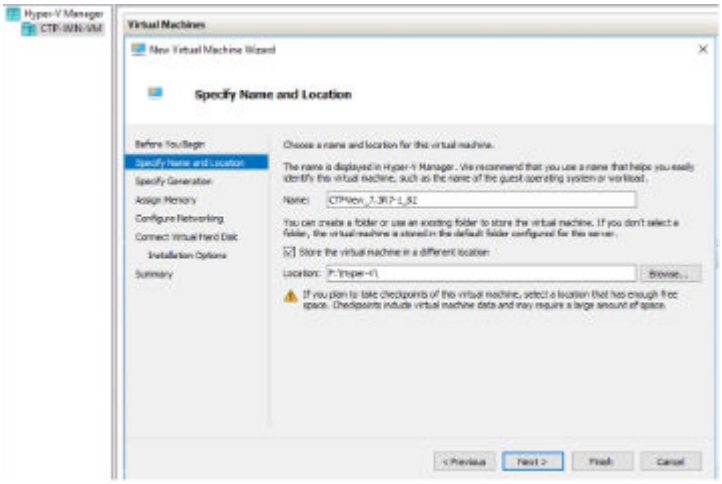




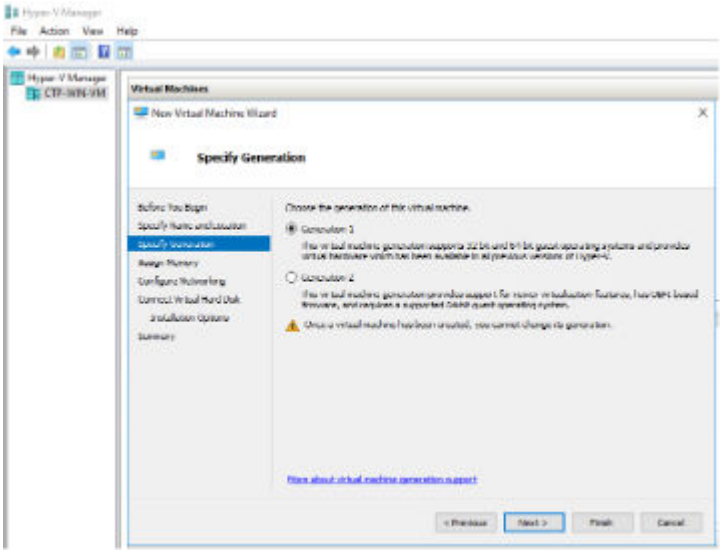
4. Click **New** > **Virtual Machine** in the Actions pane to create a new VM as shown below.



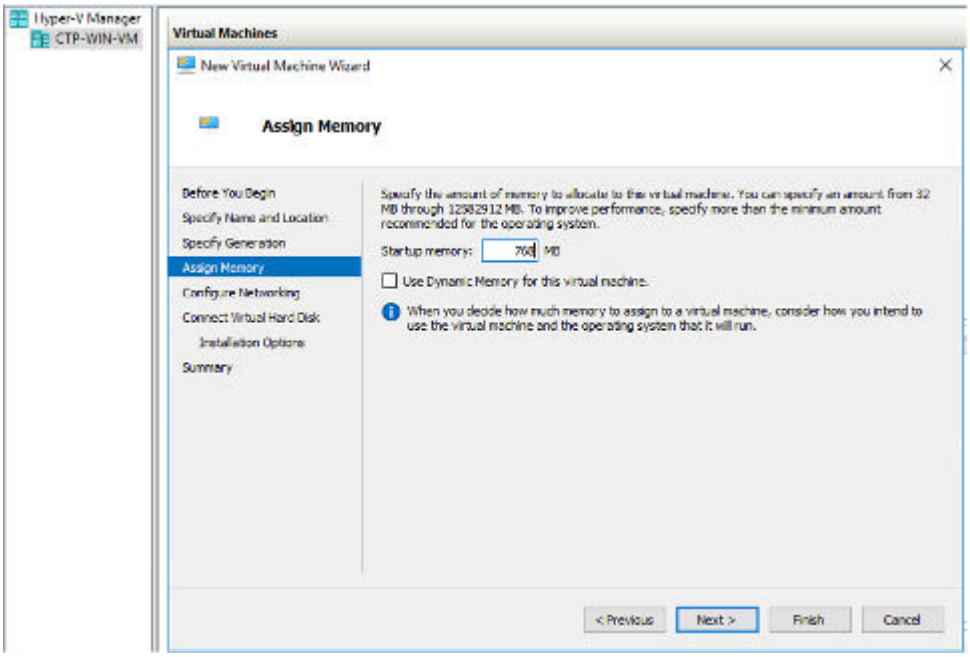
5. Click **Next** to create a VM with a custom configuration.
6. Enter a name and location for this VM. Then click **Next**.



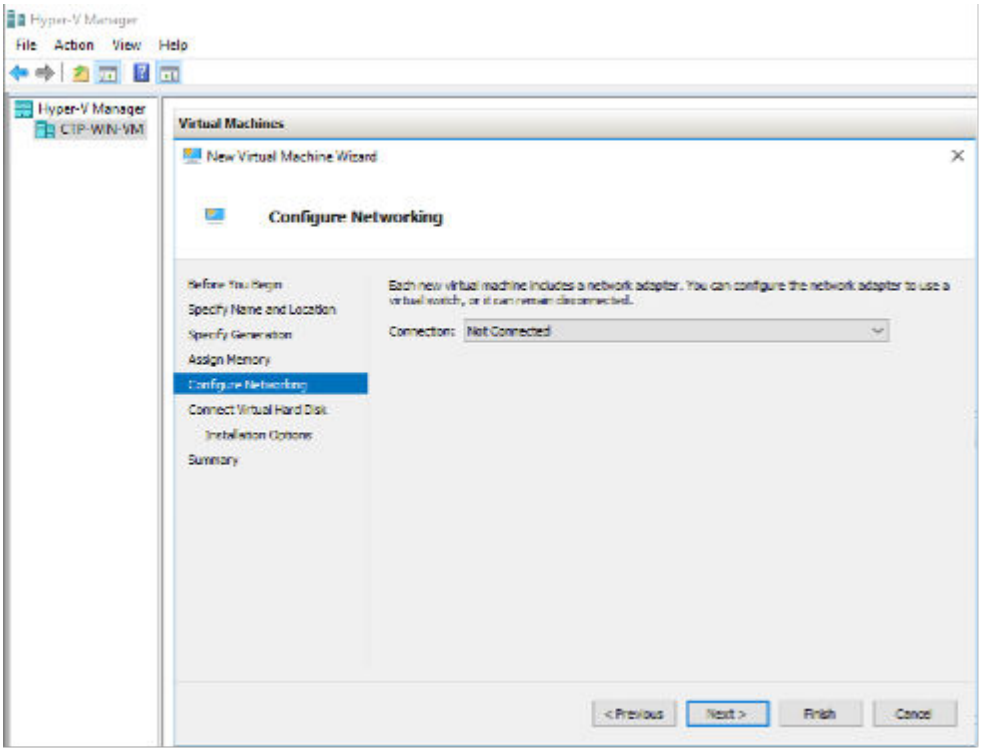
7. Select **Generation 1** as it is suitable for both 32-bit and 64-bit guest operating systems and click **Next**.



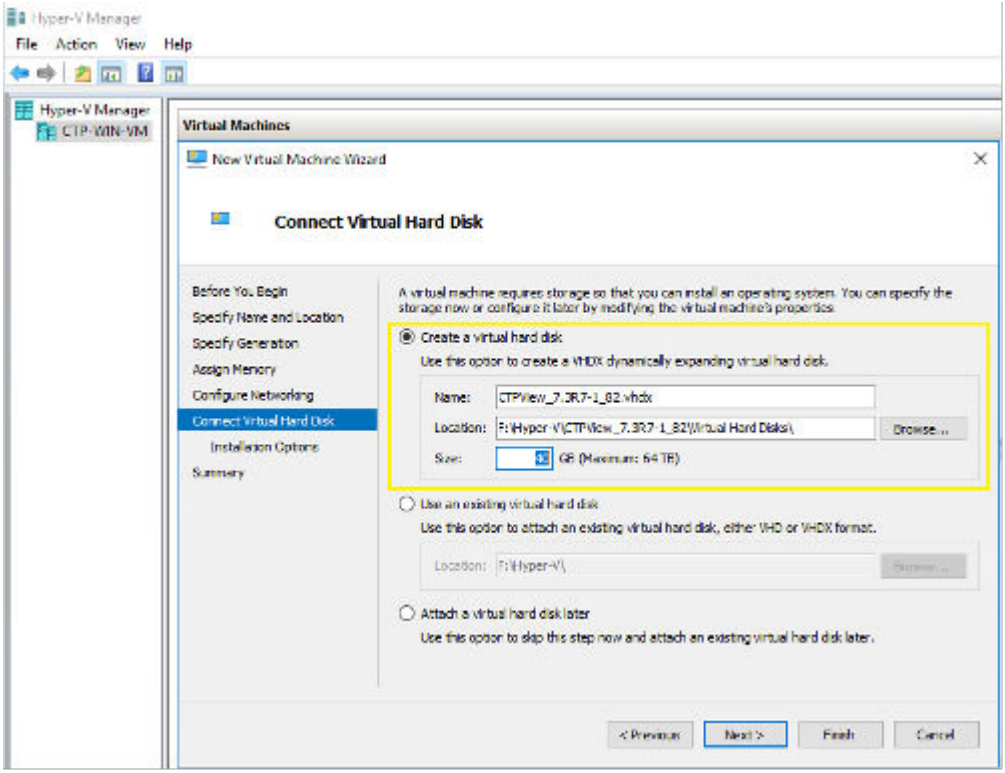
8. Enter memory size as 768 MB for “7.x CTPView” and 4 GB in case of “CentOS 7 (9.x CTPView)” and then click Next. Uncheck “Use Dynamic Memory for this virtual machine” check box if selected. This is applicable only for nested virtualization. Click “Next”.



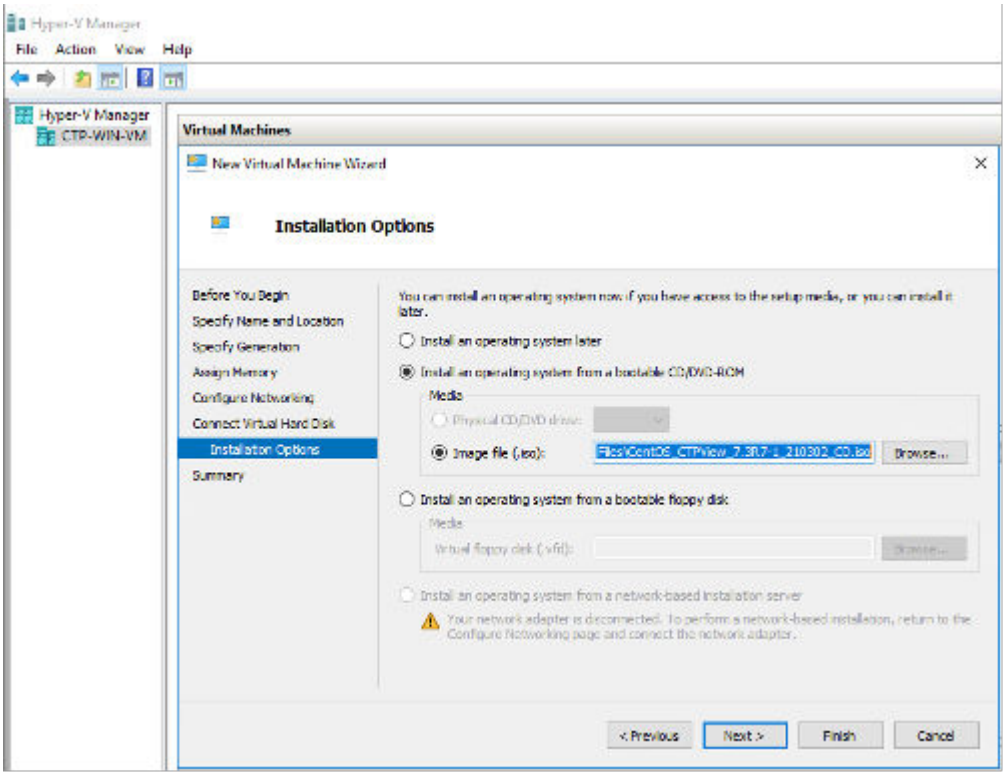
9. Leave Network configuration as “Not Connected”. You need to add Legacy Network Adapter as the default Network Adapter is not supported in CTPView. There is no option to add Legacy Network Adapter at this stage. You can add this after creating the virtual machine. Click “Next”.



10. Choose disk size as 40 GB for “7.x CTPView” and 80 GB in case of “CentOS 7 (9.x CTPView)” and create a virtual hard disk as shown.

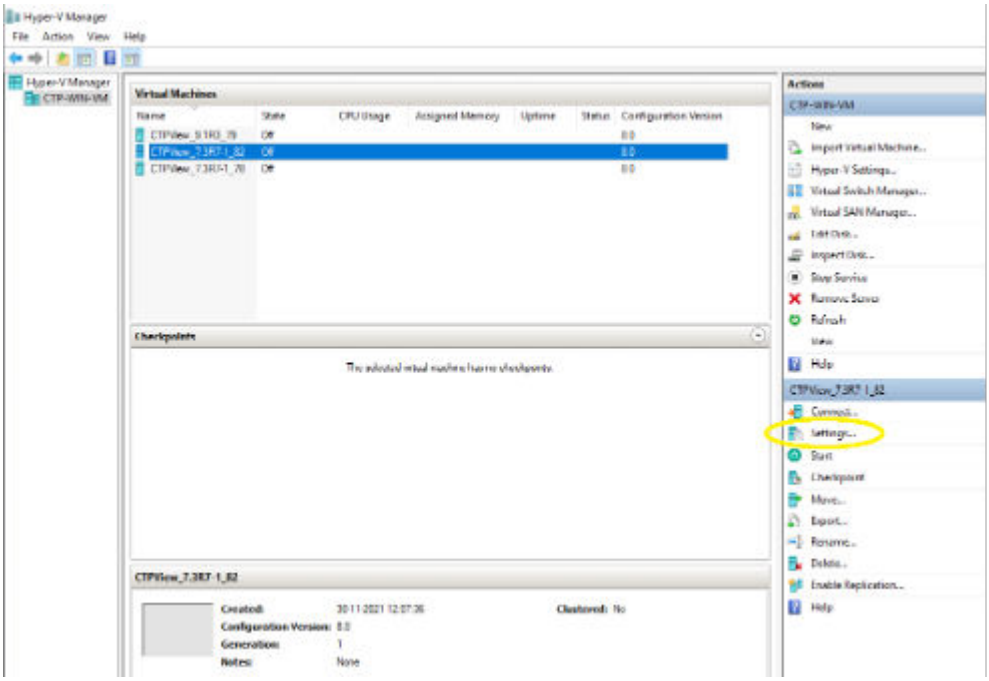


11. Select installation from CD/DVD-ROM and specify the full path of the required installation image file (.iso). Click “Next”.

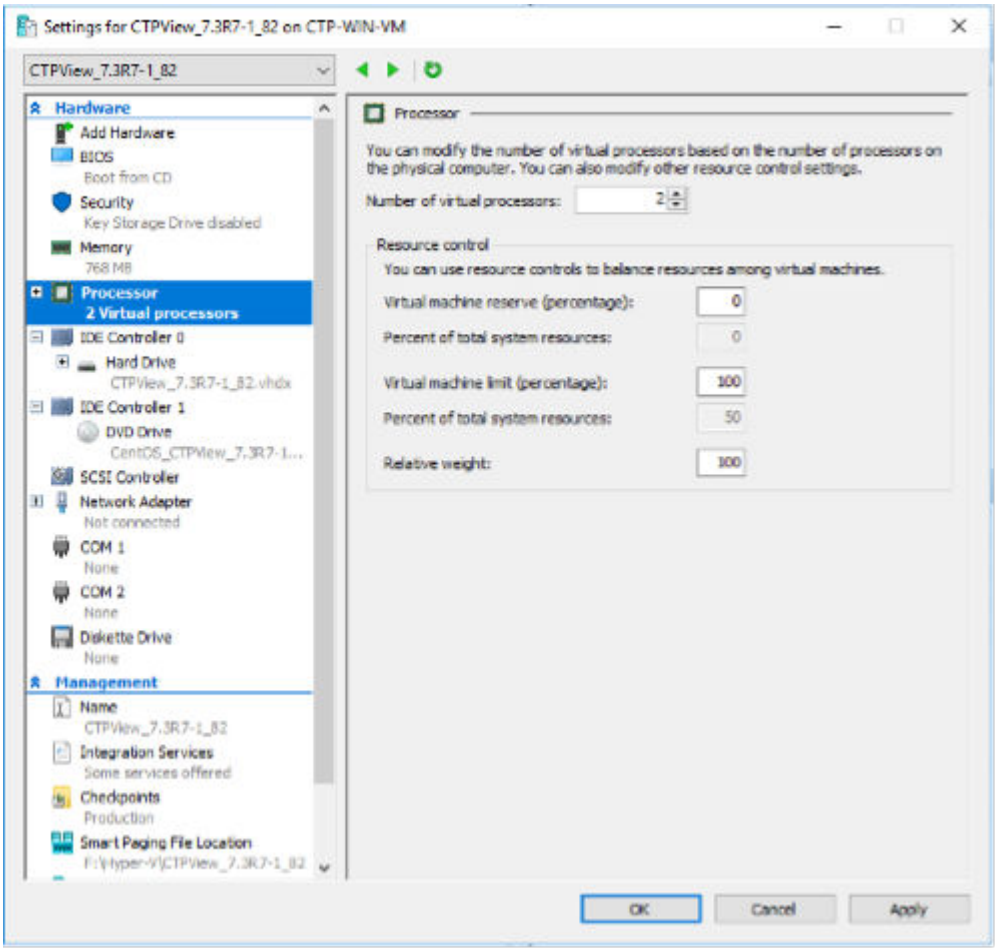


12. Summary of VM configuration will be displayed. Click **Finish** to create the Virtual machine.

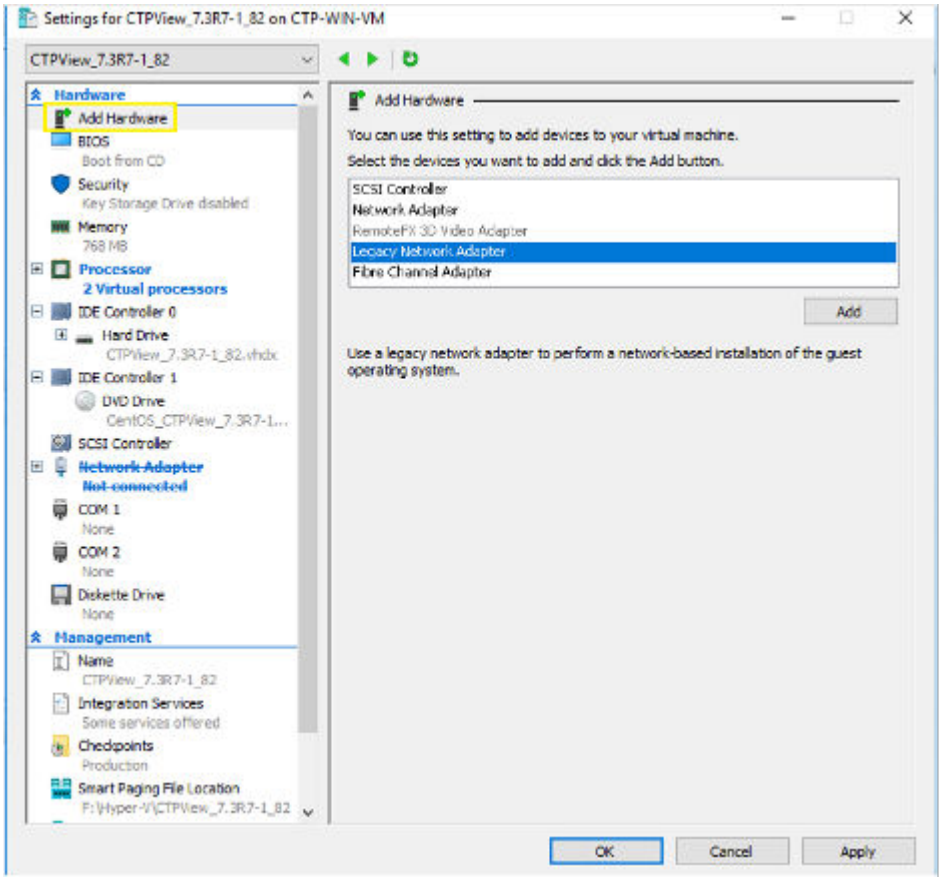
13. Select the VM and click **Settings** in the *Actions* pane.



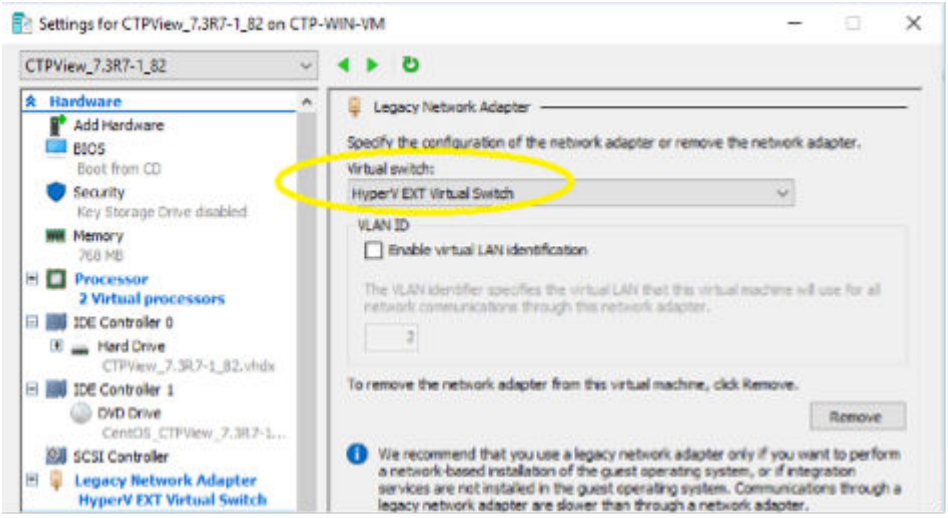
14. Settings window is displayed. Select 2 Virtual processors.



15. Delete the Network Adapter which is present by default, and select **Legacy Network Adapter** option under “Add Hardware” in the “Hardware” pane. Then click **Add**, A popup window is displayed.

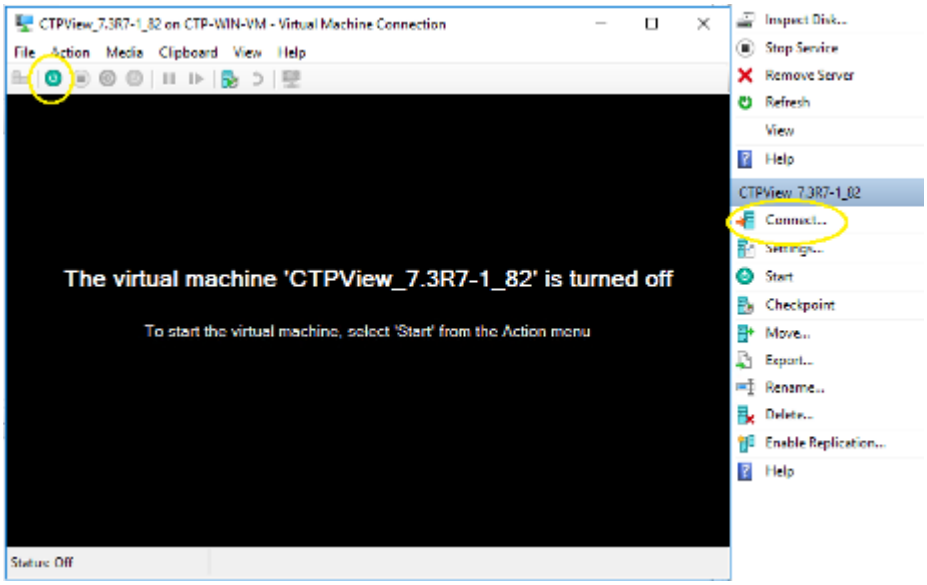


16. Select the Virtual Switch which was created while installing the Hyper-V service. In this case, Virtual Switch name is *HyperV EXT Virtual Switch*.



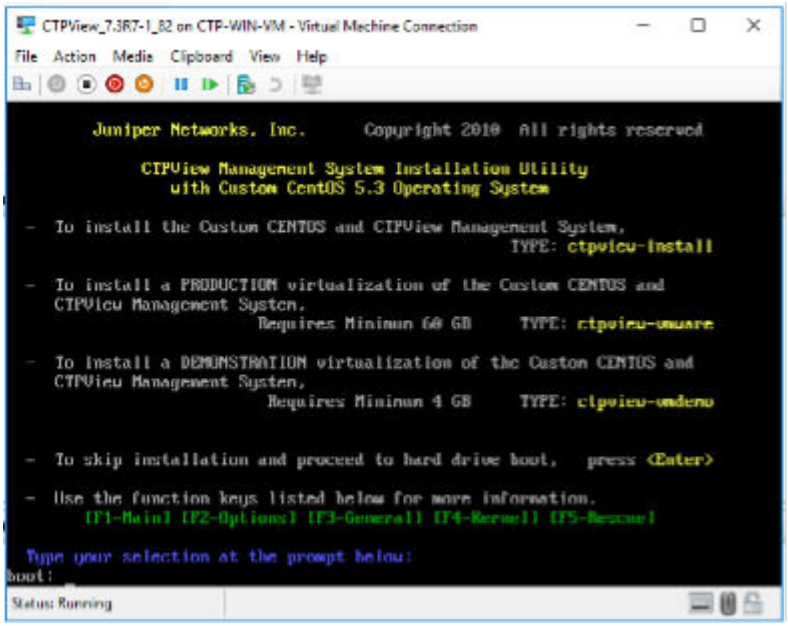
17. For 9.x CTPView, configure 2 Legacy Network Adapters. After changing these hardware settings, click OK.

18. Select the VM and click **Connect** in the Actions pane to open VM console. Then start the virtual machine.



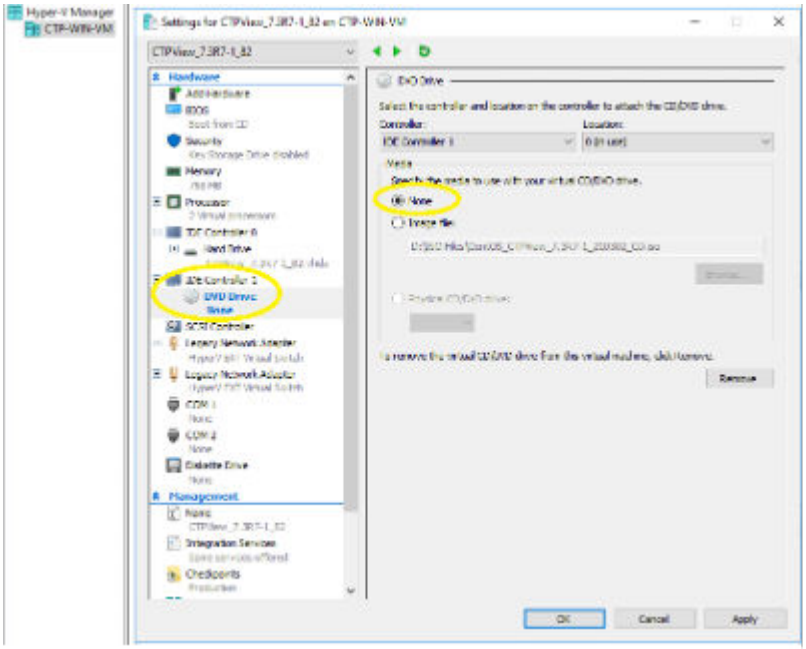
19. In case of CentOS 7 (9.x CTPView) installation, select “Install centOS Linux 7” and complete the installation. See "Creating a Virtualized Instance of CTPView Server on an ESX Server " on page 76 for detailed information on CentOS 7 installation procedure. Install 9.x CTPView RPM on top of CentOS 7.

20. In 7.x CTPView, at the prompt “boot:”, enter your installation choice as “ctpview-install”.



21. VM will reboot after 20~30 minutes. It will display the same boot options. At this stage, turn off the VM and go to “Settings” in the Actions pane.
22. Click on DVD Drive and select None option and apply the settings.

> **NOTE**: This step is not applicable to Centos 7 installation.



23. Start the VM and configure basic settings, such as the IP address and hostname using the CTPView CLI menu.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Creating More Disk Space on the CTPView Server (CTPView) | 17

Creating More Disk Space on the CTPView Server (CTPView Server Menu) | 18

Creating a Virtualized Instance of CTPView Server on an ESX Server

Before you begin:

- Make sure that vSphere client is installed on you 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.

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_9.0R1.
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.

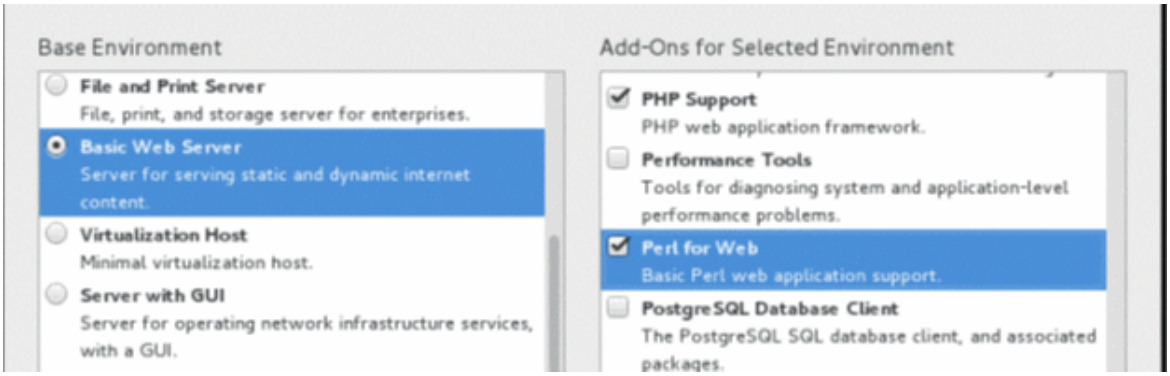
18. Select the **Install CentOS Linux 7** option with the Up Arrow key and press **Enter**.

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**.

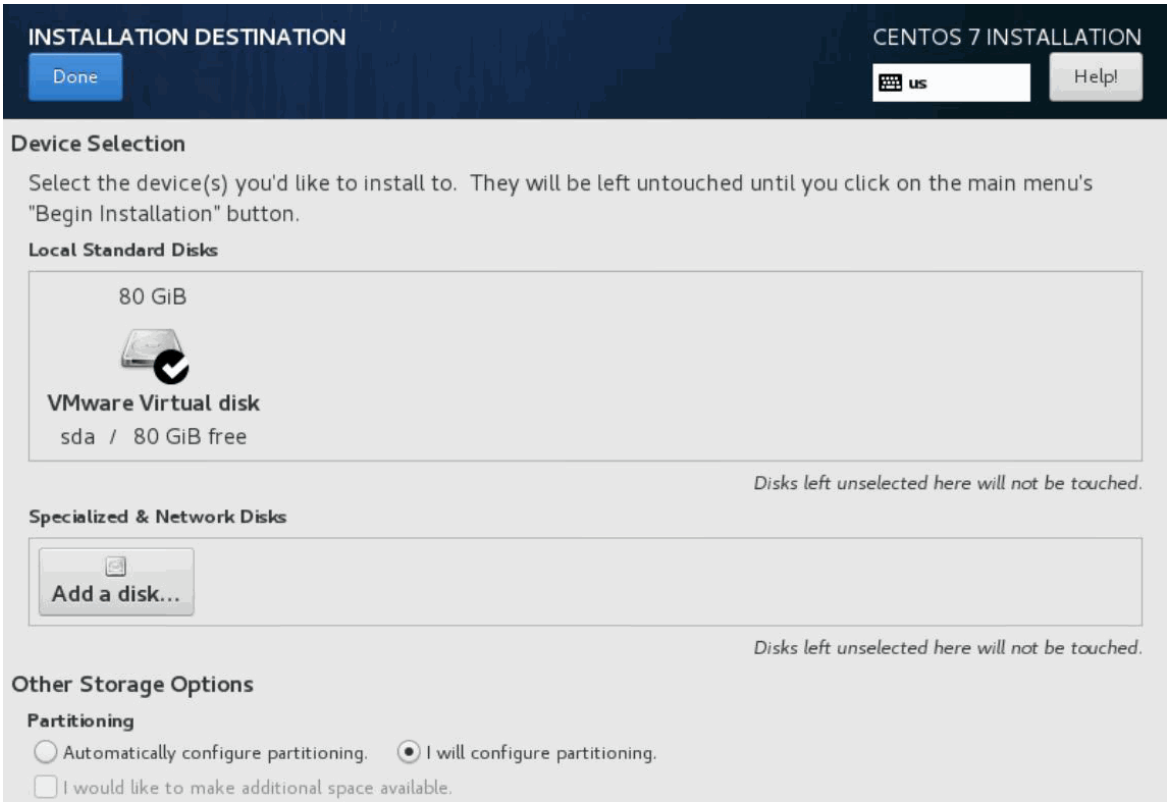
21. Click the **SOFTWARE SELECTION** option.

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**.

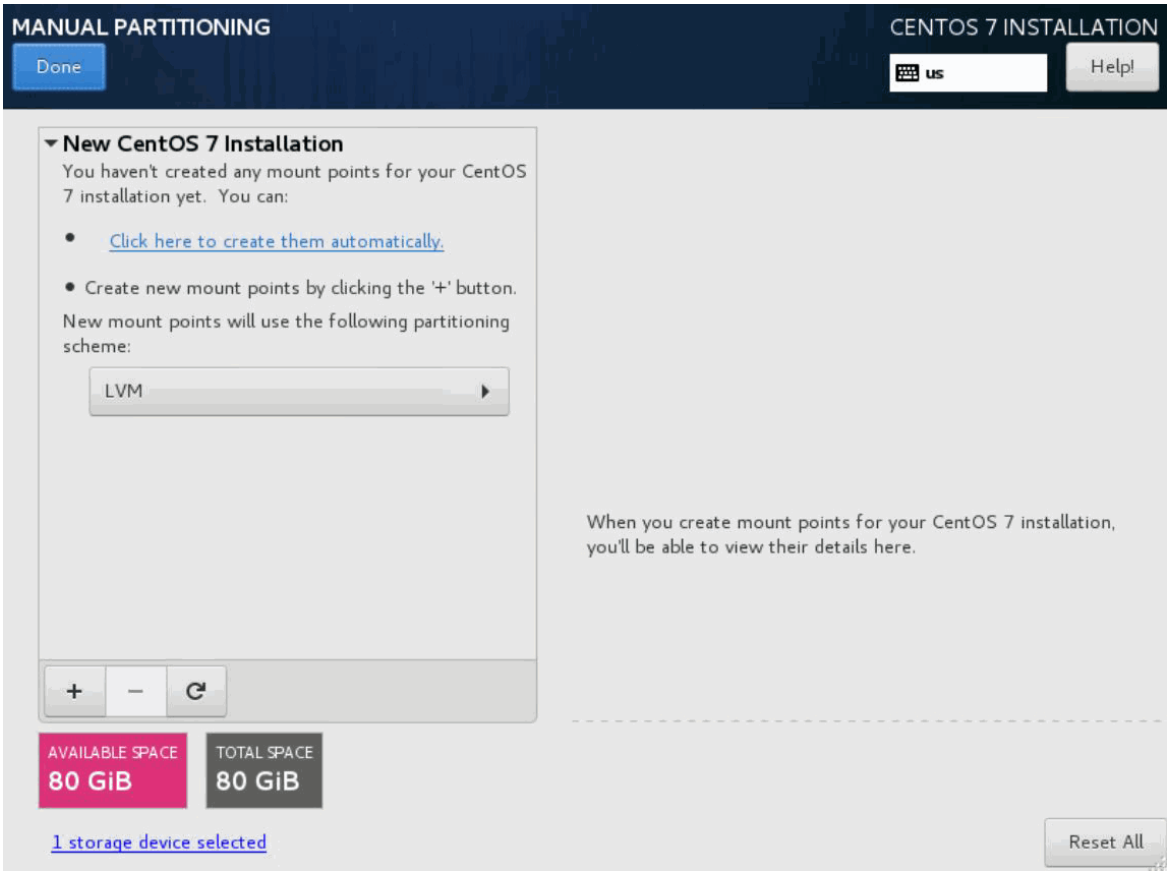


23. Click **INSTALLATION DESTINATION** and verify that the **VMware Virtual disk** (80 GB) is selected.

24. In the **Other Storage Options** section, select the **I will configure a partitioning** option button.

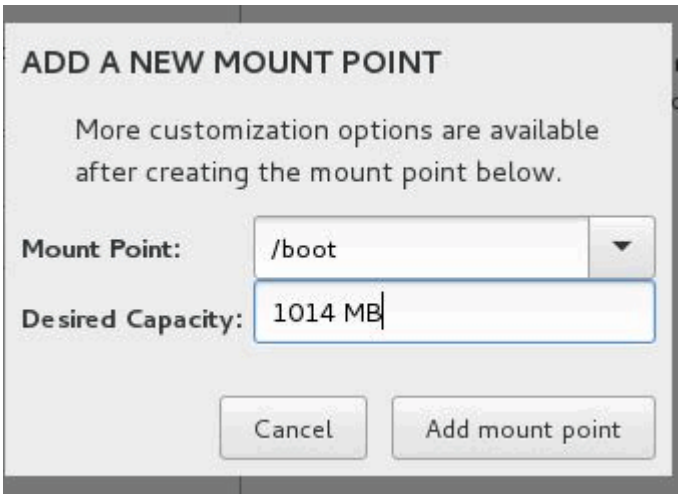


25. Click **Done**. The **MANUAL PARTITIONING** page appears.

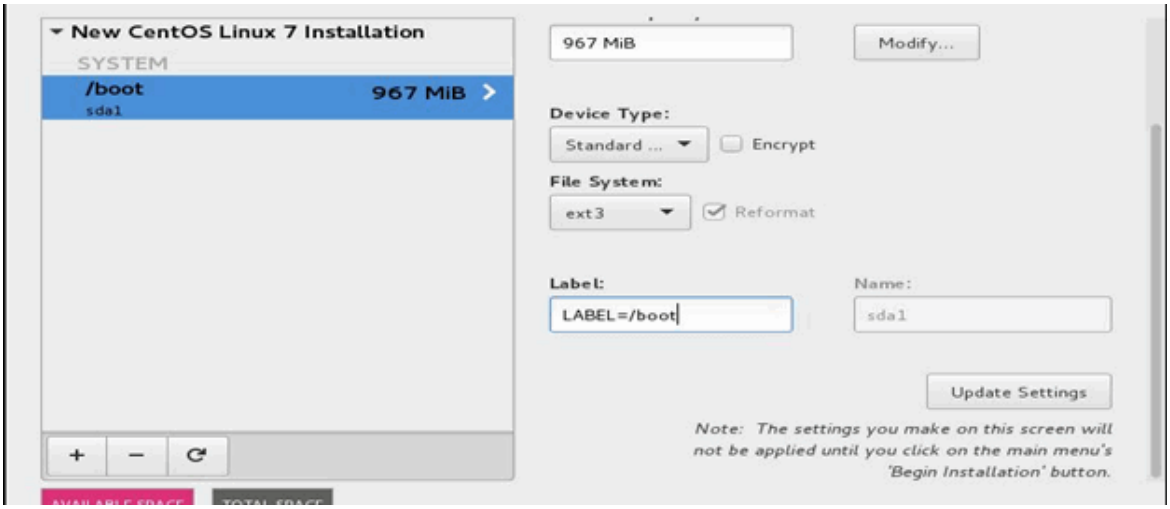


26. Click the **+** button. The **ADD A NEW MOUNT POINT** dialog box appears.

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**.



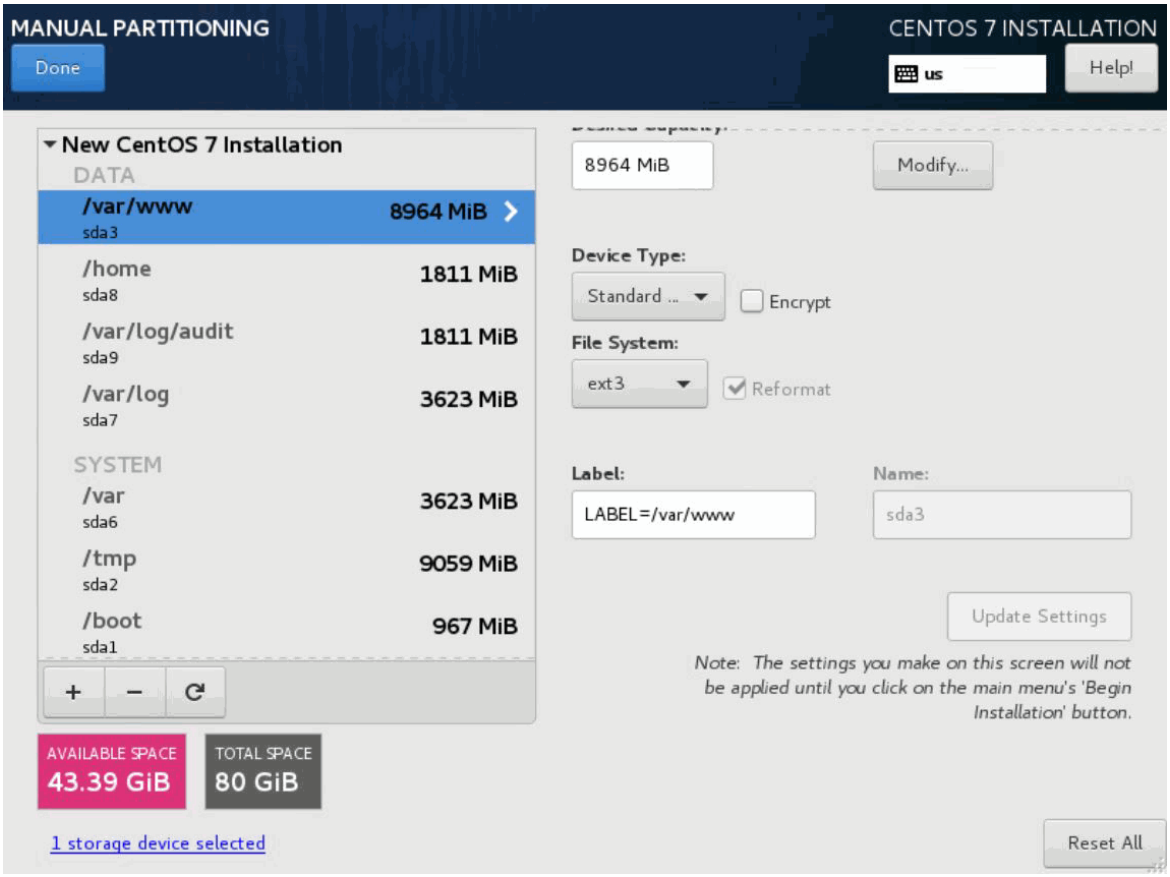
28. Select **Standard Partition** from the **Device Type** list and select **ext3** from the **File System** list. Enter **LABEL=/boot** in the **Label** field and then click **Update Settings**.



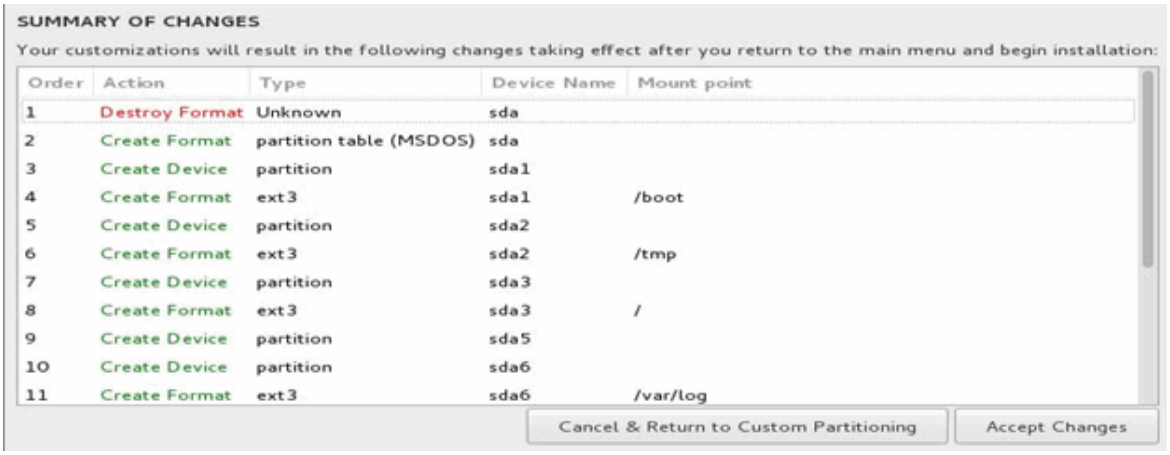
29. Similarly, repeat the steps "26" on page 79 through "28" on page 79 to create partitions for the following mount points with the provided settings.

Table 6: 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

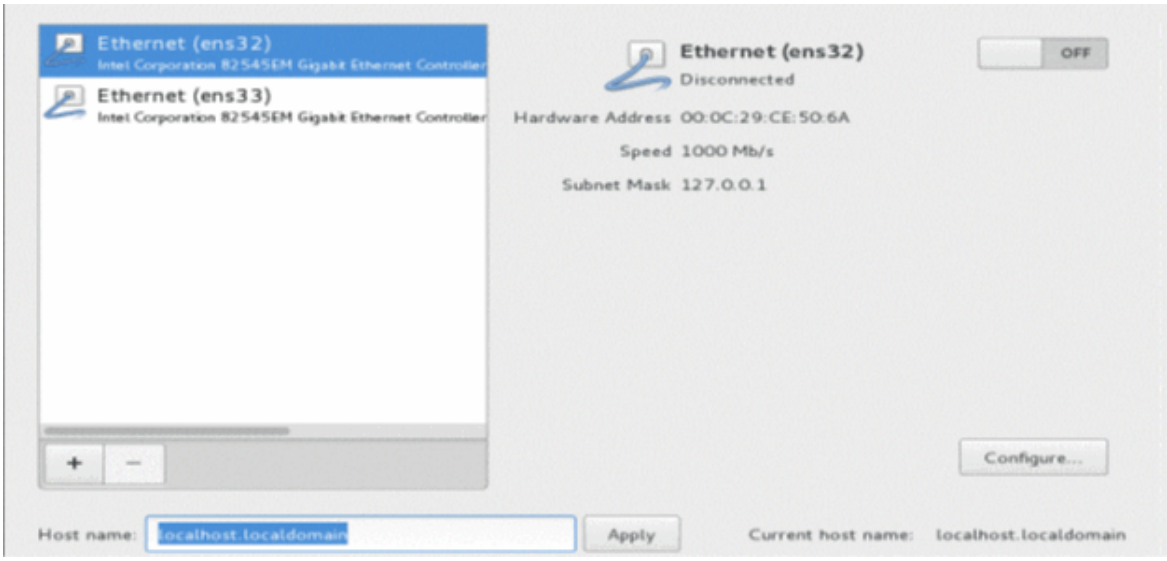


30. Click **Done** twice and then click **Accept Changes**.

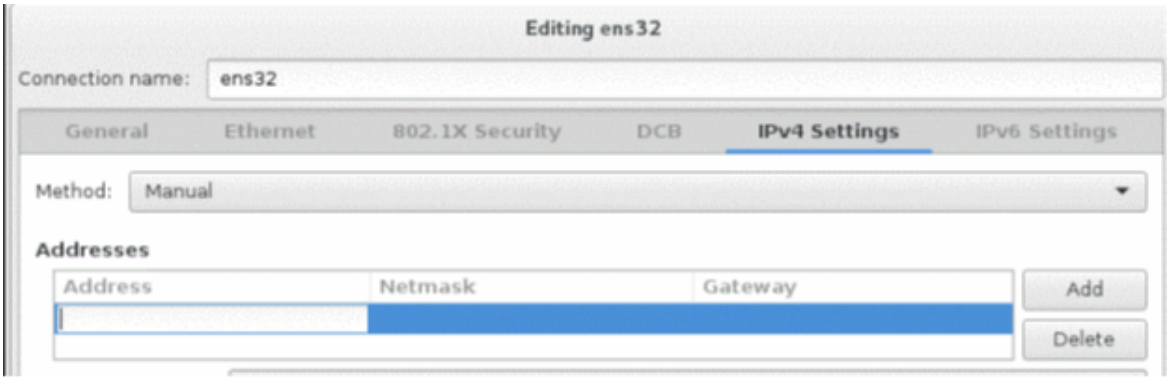


31. Click **NETWORK & HOST NAME**.

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.



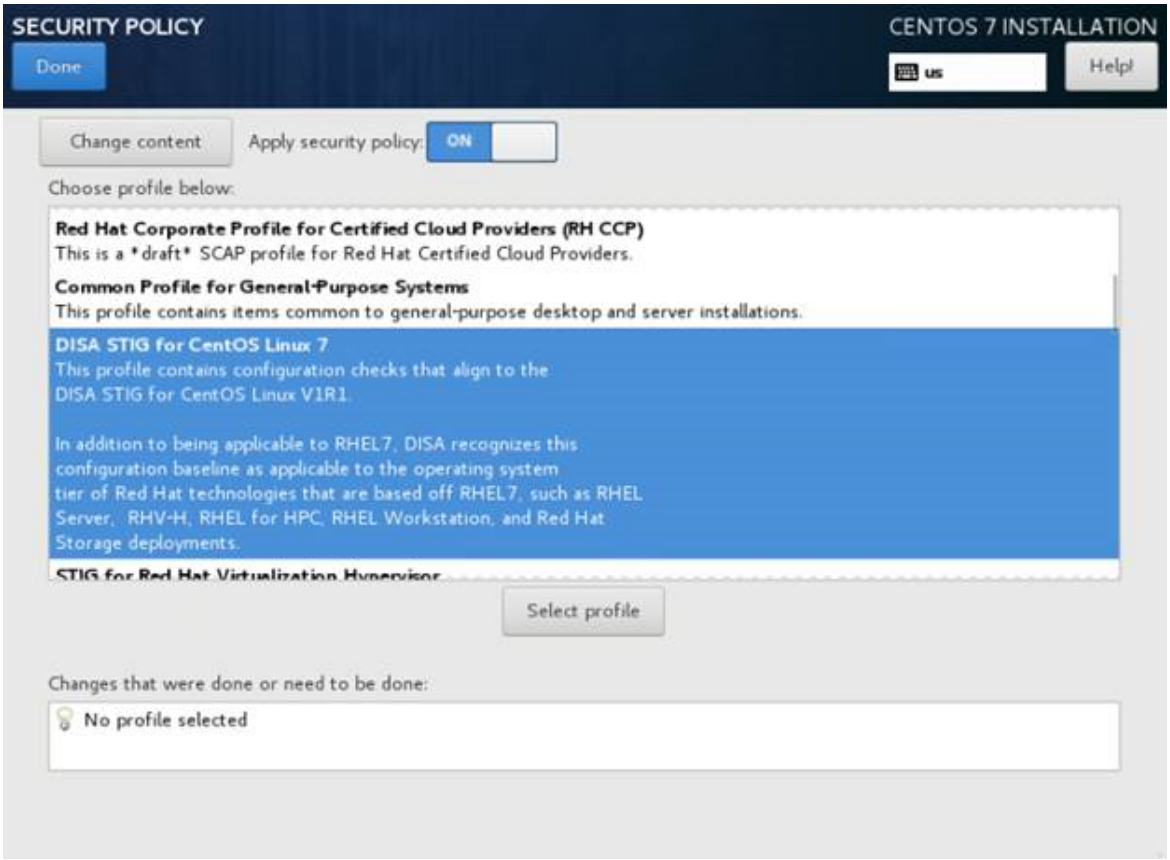
34. Select **Manual** from the **Method** list and click **Add**.

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**.

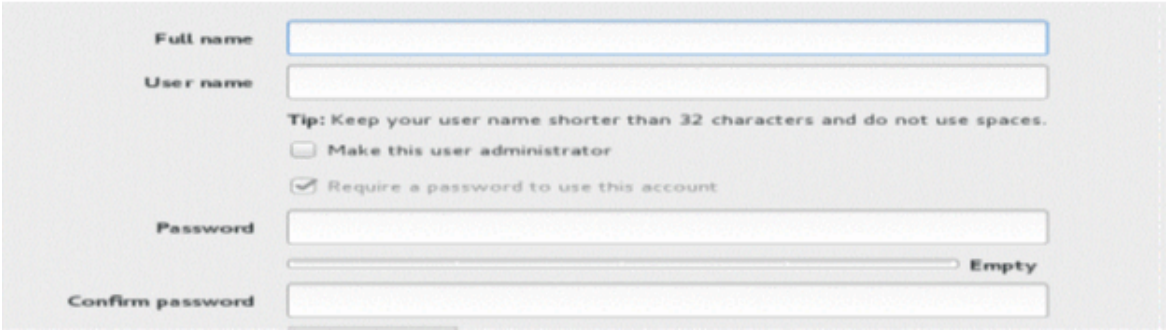
38. Select the **DISA STIG for CentOS Linux 7 Server** option and click **Select Profile**. Then, click **Done**.



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** and enter the username as "admin" and enter a password. Do Not use the username "juniper_sa".

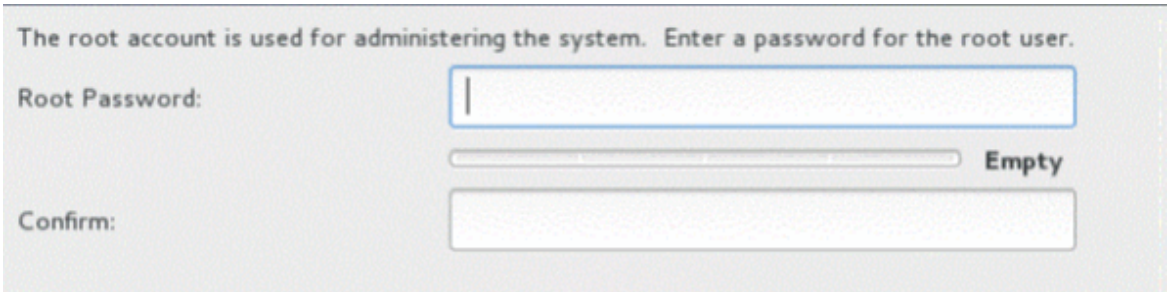


41. Select the **Make this user administrator** check box and click **Done**.

42. In the **USER SETTINGS** page, click **ROOT PASSWORD**, enter a password for the root account and click **Done**.

    Remember the passwords. Password recovery is not a simple process and is service affecting. It requires console access to the CTPView and requires rebooting of CTPView (possibly even a system re-power).

> **NOTE**: If unique passwords are not required, use the password as “CTPView-2-2”.



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

> **NOTE**: By default, USB mass storage device will not be detected on CentOS 7 server as it is blacklisted due to security requirements.
> To enable USB mass storage device on CentOS 7:
>
> - Comment the line *install usb-storage /bin/true* in the file **/etc/modprobe.d/usb-storage.conf**.
> - Reboot the server.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | **14**

Creating More Disk Space on the CTPView Server (CTPView) | **17**

Creating More Disk Space on the CTPView Server (CTPView Server Menu) | **18**

CHAPTER 7

Upgrade Tasks for CTPOS

IN THIS CHAPTER

Using the CTPView Server Software to Update CTPOS (CTPView)

IN THIS SECTION

You can use the CTPView software to distribute and install CTPOS update archive files on the CTP platforms in your network.

NOTE: Upgrading to CTPOS 7.3R7 on a dual image flash system is not supported.

To update CTPOS:

Installing CTPOS 9.1R3.1 Dual Image on CTP Device using CTPView

1. Access the CTP platform software download page at the Juniper Networks Customer Support site at https://www.juniper.net/customers/csc/software/ctp/#sw.
2. Use a Secure Copy Protocol (SCP) program to copy the web archive file to the **ctp** directory on the CTPView server.

You must be a member of the **server** group to access this directory. The CTPView server automatically checks and modifies the copied file's ownership and permissions as necessary.

3. Log in to the CTPView GUI.
4. In the side pane, select **Node > Maintenance**.
5. Click **Upgrade CTP Software**.

   The Upgrade CTP Software window is displayed.
6. Select the desired archive file from the list.
7. Click the name of the platform you want to update.

   You can select more than one platform by holding down the Ctrl key when you click the platform names. Alternatively, you can click **Select All Hosts** to select all the listed CTP platforms.
8. Click **Upgrade CTP(s)**.

   The selected CTP platforms are upgraded sequentially. A progress window shows the status of the upgrade.

Installing CTPOS 9.1R3.1 Dual Image on CTP Device using CTPView

Starting in CTPOS Release 9.1R3.1, you can upgrade or install your CTP device with dual image.

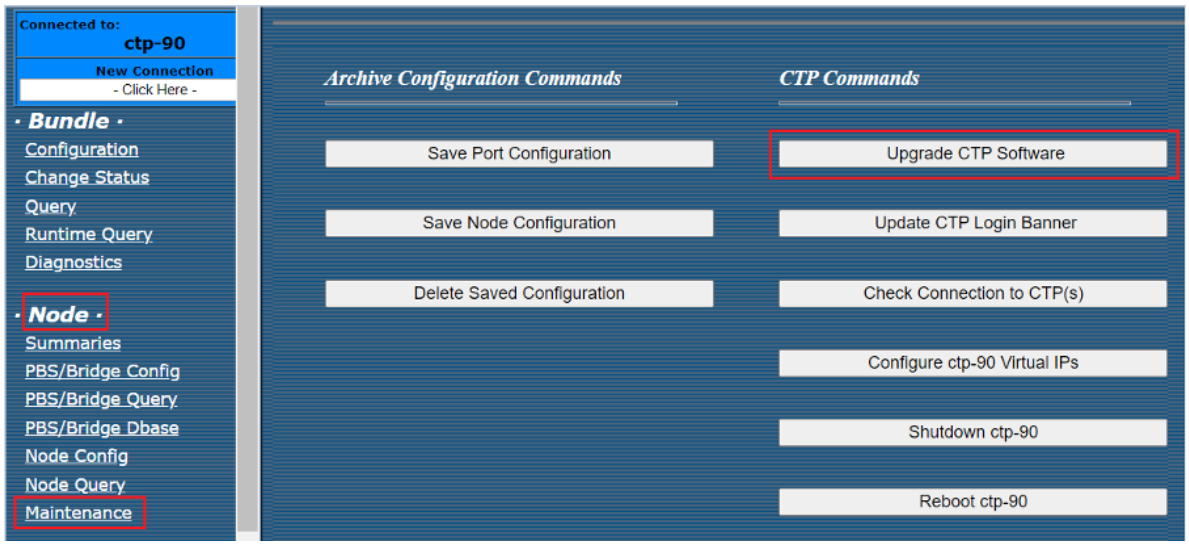
To install dual image using CTPView:

NOTE:

- For CTP2000/CTP150, the figures and illustrations are similar. So, we have used only CTP2000 device as a reference.
- The steps for upgrading CTP151 are the same. The only difference being the 'image archive' to be used.
- You may manage a CTP device running CTPOS 7.3R7 or higher version using CTPView 9.1R3.1. However, upgrading to a higher version of CTPOS 7.3 is not supported using CTPView 9.1R3.1. In such a scenario, to upgrade the CTP device, use the corresponding version of CTPView.

1. Launch CTPView software in your CTP device and ensure that a valid CTPOS is running.

2. After connecting the host In the CTPView GUI, go to **Node > Maintenance** and click **Upgrade CTP Software** under CTP commands head.

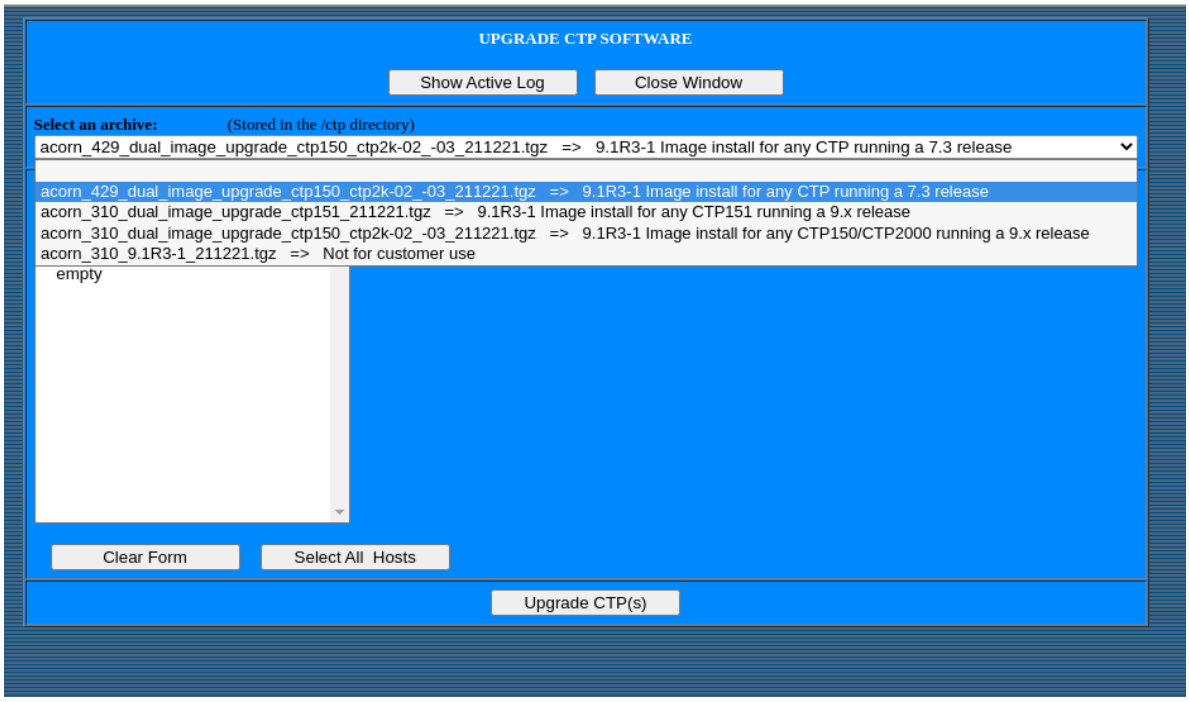


The Upgrade CTP Software screen is displayed.

3. Select an acorn archive from the dropdown list to upgrade as per the running release of the CTP node

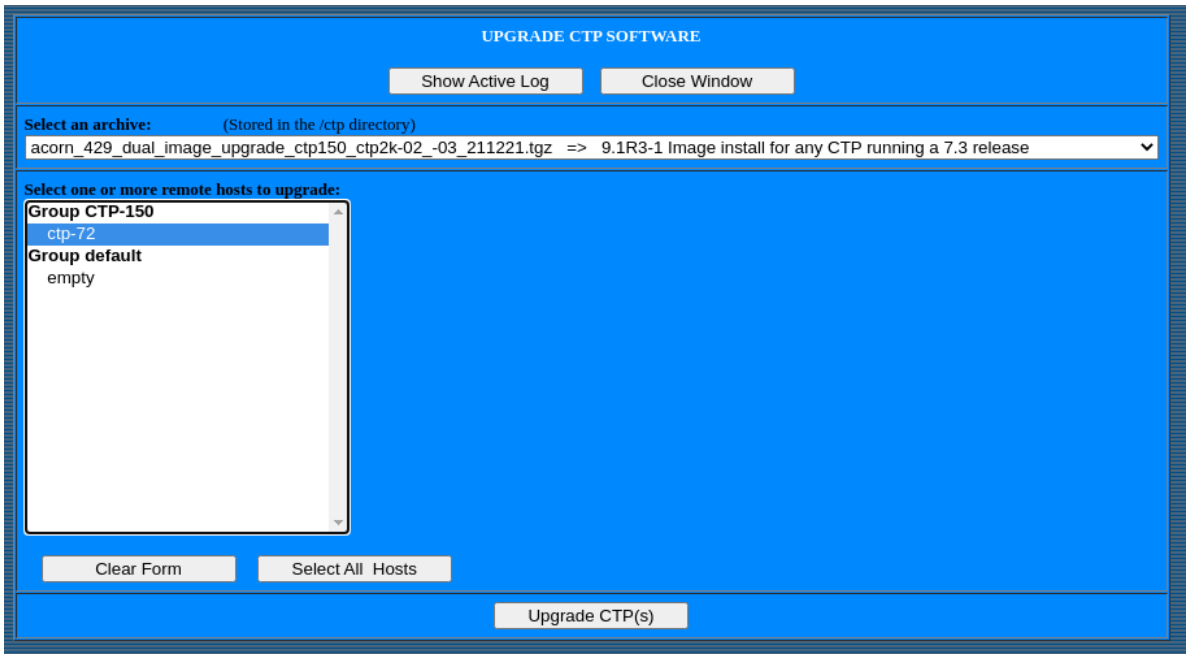
   - In case of CTP-150 and CTP-2000 running with 9.x release, archive to be used for upgrading would be “acorn_310_dual_image_upgrade_ctp150_ctp2k-02_-03_211221.tgz”.
   - In case of CTP-151 running with 9.1R1 or 9.1R2 release, archive to be used for upgrading would be “acorn_310_dual_image_upgrade_ctp151_211221.tgz”.
   - In case of CTP-150 and CTP-2000 running with 7.3 release, archive to be used for upgrading would be “acorn_429_dual_image_upgrade_ctp150_ctp2k-02_-03_211221.tgz”.

Figure 4: For CTP150 or CTP2000 Series Device



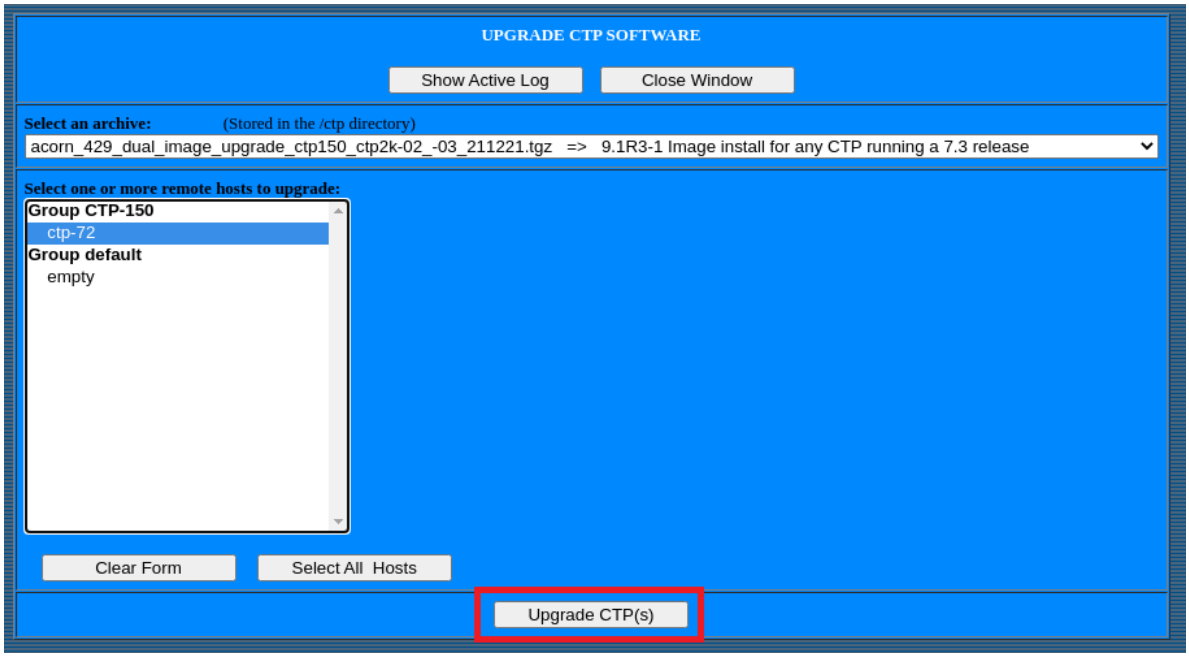
4. Select the host for the upgrade from the dropdown list.

Figure 5: For CTP150 or CTP2000 Series Device



5. Click **Upgrade CTP(s)** to start the upgrade.

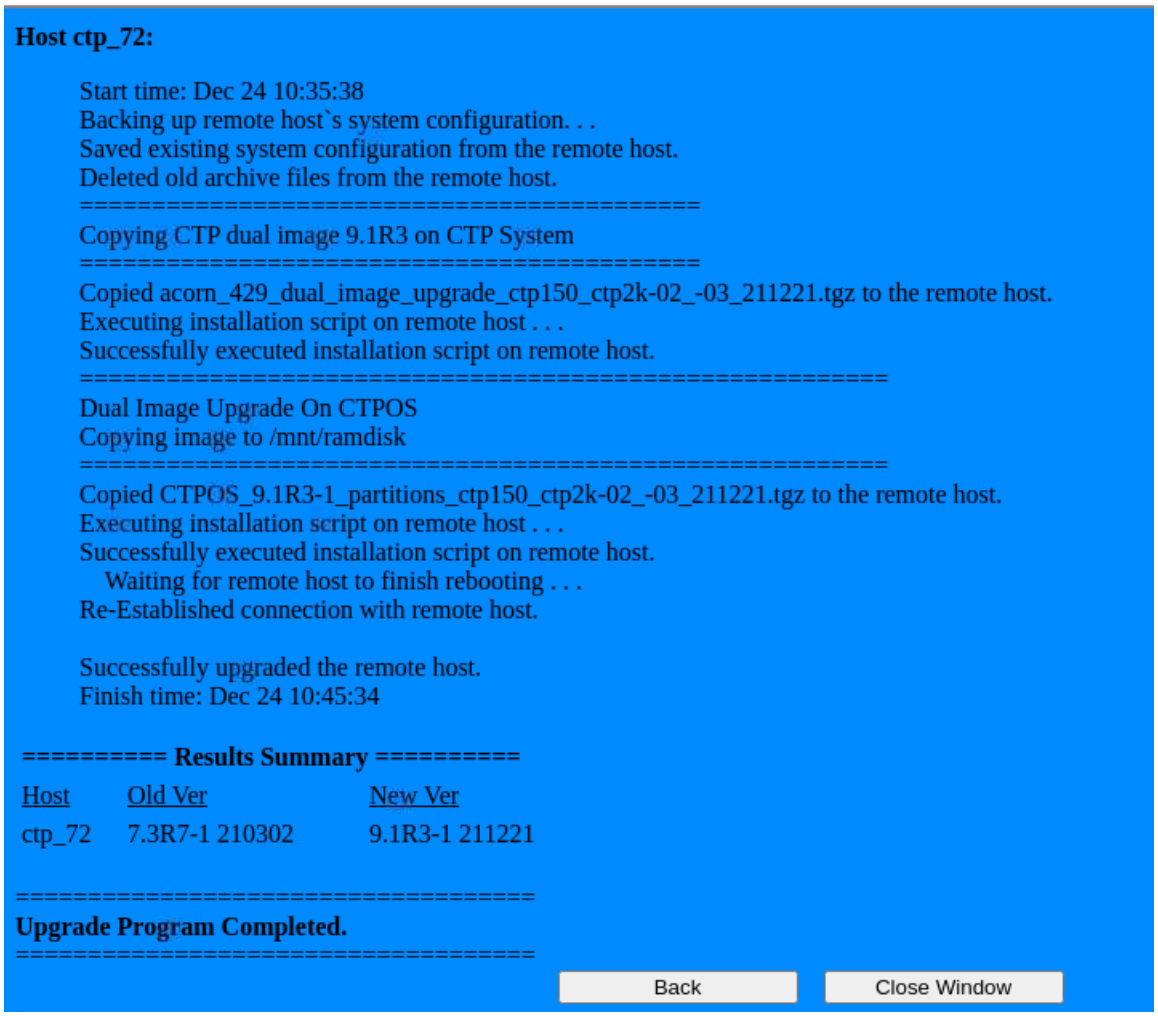
Figure 6: For CTP150 or CTP2000 Series Device



6. When upgrade starts, a new window will open which will populate all upgrade logs and different stages of upgrade.

> **NOTE**: Do not close this window while upgrade is in-progress. Closing this window will terminate the upgrade process.

Figure 7: For CTP150 or CTP2000 Series Device



Upgrade logs are displayed on CTPView web page.

The upgrade process is complete.

RELATED DOCUMENTATION

Default CTPOS and CTPView Accounts and Passwords | 94

Burning CTPOS Images to a CompactFlash Card (CTPView Server CLI)

Before using CTPView to burn CTP software images onto CompactFlash cards, you must copy the appropriate CTP image files to the proper directory on the CTPView server. Released versions of CTP operating system software images are available for download from the Juniper Networks Customer Support site at https://www.juniper.net/customers/csc/software/ctp/#sw. You need your customer support username and password to access this site.

Place the CTP flash image file on the CTPView server in the **/var/www/html/flash/** directory. To copy software into this directory, you must be a root user or a member of the UNIX group *server*, such as the default user *juniper*. You do not need to modify the file's ownership and permissions after you copy it into the **/flash** directory.

You must have physical access to the CTPView server to perform this procedure.

To burn a CTPOS image to a CompactFlash card:

1. Place the new CompactFlash card into a USB CompactFlash card adapter, and insert the adapter into one of the USB ports on the CTPView server.

   The CTPView server automatically mounts the adapter.
2. Log in to the CTPView server and switch to the root account.

   Use a directly connected monitor and keyboard or use SSH from a remote computer to log in to the server.
3. Change directories to**/var/www/html/flash**.
4. Enter **./burn flash_*version***.

   The image filename is **flash_*version***. If you fail to include the version when you enter the command, the CTPView server displays usage instructions and a list of available flash images.
5. Answer the screen prompts to complete the process.
6. Log out of the server and remove the USB CompactFlash card adapter.

RELATED DOCUMENTATION

Burning an Image of CTPOS to a CompactFlash Card (CTPView Server Menu) | 93

Burning an Image of CTPOS to a CompactFlash Card (CTPView Server Menu)

You can burn CTPOS images to a CompactFlash Card either from the CTPView Server Menu or from the CTPView Server CLI. This section describes how to burn an image of CTPOS from the CTPView Server Menu.

Before using CTPView to burn CTP software images onto CompactFlash cards, you must copy the appropriate CTP image files to the proper directory on the CTPView server. Released versions of CTP operating system software images are available for download from the Juniper Networks Customer Support site at https://www.juniper.net/customers/csc/software/ctp/#sw. You need your customer support username and password to access this site.

Place the CTP flash image file on the CTPView server in the **/var/www/html/flash/** directory. To copy software into this directory, you must be a root user or a member of the UNIX group *server*, such as the default user *juniper*. You do not need to modify the file's ownership and permissions after you copy it into the **/flash** directory.

Before you begin, log in to the CTPView server and access the CTPView Server Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To burn an image of the CTPOS:

1. From the CTPView Server Configuration Menu, select **4) Advanced Functions**.
2. Select **8) Burn CTPOS Flash Image**.

RELATED DOCUMENTATION

Burning CTPOS Images to a CompactFlash Card (CTPView Server CLI) | **92**

CHAPTER 8

Default Accounts and Passwords

IN THIS CHAPTER

Default CTPOS and CTPView Accounts and Passwords

This topic lists the default accounts and passwords for the CTP Series platforms and the CTPView server.

Table 7 on page 94 lists the default accounts and passwords to access the CTPView server.

Table 7: CTPView Server Default Accounts and Passwords

Application	Account	Default Username	Default Password
Server (CLI)	BIOS menu	Not applicable	CTPView-2-2
Server (CLI)	GRUB boot loader	Not applicable	CTPView-2-2
Server (CLI)	user account	juniper_sa (lowercase *j*)	Not applicable
Server (CLI)	root account	root	Not applicable
CTPView (browser)	Global_Admin account	Juniper (uppercase *J*)	Not applicable
PostgreSQL (CLI)	Administrator account	postgres	CTPView-2-2
PostgreSQL (CLI)	Apache account	ctpview_pgsql	Not applicable

NOTE: Upgrading from a CTPView software version lower than 2.2 to the current software does not change the existing server passwords or accounts except to add the *juniper* user account. However, all the user accounts that existed in the lower version of the CTPView software are removed. In the higher versions, browser access to the CTPView server is through a login interface, which requires that an administrator create new usernames and passwords.

Table 8 on page 95 lists the default accounts and passwords to access CTPOS on the CTP Series platforms.

Table 8: CTPOS Default Account and Password

Application	Account	Default Username	Default Password
CTP platform	CLI menu	ctp	Not applicable
CTP platform	System administrator—Member of the system administrator class. Certain tasks require a user in this class when the CTPOS security level is set to high.	ctp_sa	Not applicable
CTP platform	System auditor—Enables the user to view logs for the platform when the CTPOS security level is set to high.	ctp_aud	Not applicable

RELATED DOCUMENTATION

Updating the CTPView Server Operating System and CTPView Network Management System Software | **11**

Installing or Upgrading the CTPView Server OS | **14**

Upgrading Only the CTPView Software | **25**

Setting a New Password for a Nonroot User Account (CTPView Server CLI) | **256**

Setting a New Password for a Root User Account (CTPView Server CLI) | **257**

CTPOS and CTPView Software Password Requirements

Certain requirements apply to passwords for the following:

- CTPOS
- CTPView server shell access accounts
- CTPView GUI access accounts
- PostgreSQL accounts
- GRUB Boot loader

New passwords must include the following:

- At least one lowercase letter
- At least one uppercase letter
- At least one numeral
- At least one of the following nonalphanumeric characters: ~ ! @ # % & - _ = { } [ ] ,

NOTE: Follow the onscreen instructions for the character range.

New passwords must not include either of the following:

- The username as part of the password.
- More than two adjacent repeated characters.

RELATED DOCUMENTATION

CTPView Network Management System Administration
Managing CTPView Users with the CTPView Admin Center | 102
Adding New CTPView Users (CTPView) | 104
Changing the PostgreSQL Apache Account Password (CTPView Server Menu) | 38
Changing the PostgreSQL Administrator Account Password (CTPView Server Menu) | 39

Changing the GRUB Boot Loader Password (CTPView Server Menu) | 37

Changing the User Password (CTP Menu) | 45

Setting a New Password for a Nonroot User Account (CTPView Server CLI) | 256

Setting a New Password for a Root User Account (CTPView Server CLI) | 257

Default CTPOS and CTPView Accounts and Passwords | 94

CHAPTER 9

Understanding CTPView Upgrade Files

IN THIS CHAPTER

Understanding CTPView Software Upgrade Files

The CTPView software upgrade file that you download from the Juniper Networks Customer Support site at https://www.juniper.net/customers/csc/software/ctp/#sw depends on the CTPView server's operating system (OS), the version of CTPView software currently installed on the server, and the CTPView software release that you want to upgrade to. Table 9 on page 98 lists the combinations of OS and CTPView software and the associated upgrade file. The *CTPView Release Notes* for the version you are upgrading to also describes the upgrade files required for various combinations of currently installed CTPView server OS and CTPView software.

Table 9: CTPView Software Upgrade Files

CTPView Server OS	Installed CTPView Release	Upgrade to CTPView Release	Archive File for Upgrade	Server Reboots During Upgrade?
CentOS 5.3	4.2 or later	4.4R1	web_update_4.4R1_120731.tgz	No
	4.1 or earlier	4.4R1	ctpview_complete_centos_4.4R1_120731.tgz	Yes
FC9	3.4R2 or later	4.4R1	web_update_4.4R1_120731.tgz	No
	3.4R1 or earlier	4.4R1	ctpview_complete_fc9_4.4R1_120731.tgz	Yes
FC9	3.3Rx	3.4R1	ctpview_fc9_complete_3.4R1_090715.tgz	No

Table 9: CTPView Software Upgrade Files *(Continued)*

CTPView Server OS	Installed CTPView Release	Upgrade to CTPView Release	Archive File for Upgrade	Server Reboots During Upgrade?
FC9	3.2Rx	3.4R1	ctpview_fc9_complete_3.4R1_090715.tgz	Yes
FC9	3.2R3 or higher	3.3R2	web_fcX_3.3R2_090616.tgz	No
FC9	3.2R3 or higher	3.2R4	web_fcX_3.2R4_090903.tgz	No
FC9	3.2R3 or higher	3.2R3	web_fcX_3.2R3_090402.tgz	No
FC9	3.2R1 or 3.2R2	3.3R2	ctpview_fc9_complete_3.3R2_090616.tgz	Yes
FC9	3.2R1 or 3.2R2	3.2R4	ctpview_fc9_complete_3.2R4_090903.tgz	Yes
FC9	3.2R1 or 3.2R2	3.2R3	ctpview_fc9_complete_3.2R3_090402.tgz	Yes
FC9	3.2R1	3.2R2	ctpview_fc9_complete_3.2R2_090112.tgz	Yes
FC4	2.2R2 or higher	3.4R1	web_fcX_3.4R1_090715.tgz	No
FC4	2.2R2 or higher	3.3R2	web_fcX_3.3R2_090616.tgz	No
FC4	2.2R2 or higher	3.2R4	web_fcX_3.2R4_090903.tgz	No
FC4	2.2R2 or higher	3.2R3	web_fcX_3.2R3_090402.tgz	No
FC4	2.2R2 or higher	3.2R2	web_fcX_3.2R2_090112.tgz	No
FC4	2.2R1 or lower	3.4R1	ctpview_fc4_complete_3.4R1_090715.tgz	Yes

Table 9: CTPView Software Upgrade Files *(Continued)*

CTPView Server OS	Installed CTPView Release	Upgrade to CTPView Release	Archive File for Upgrade	Server Reboots During Upgrade?
FC4	2.2R1 or lower	3.3R2	ctpview_fc4_complete_3.3R2_090616.tgz	Yes
FC4	2.2R1 or lower	3.2R4	ctpview_fc4_complete_3.2R4_090903.tgz	Yes
FC4	2.2R1 or lower	3.2R3	ctpview_fc4_complete_3.2R3_090402.tgz	Yes
FC4	2.2R1 or lower	3.2R2	ctpview_fc4_complete_3.2R2_090112.tgz	No
FC4	2.5Rx	2.5R4	web_fc4_2.5R4_090105.tgz	No
FC4	2.4Rx or lower	2.5R4	ctpview_fc4_complete_2.5R4_090105.tgz	No
FC1		3.2R2	Refer to 3.2 manuals	
FC1		2.5R4	refer to 2.5 manuals	

RELATED DOCUMENTATION

Upgrading Only the CTPView Software | 25

3

PART

Administration

CHAPTER 10

Managing and Displaying Users (CTPView)

IN THIS CHAPTER

Managing CTPView Users with the CTPView Admin Center

The CTPView Admin Center provides a central location for managing users, passwords, groups, and access for CTPView users. Only Global_Admin users can create, modify, and delete CTPView user accounts.

You can perform the following tasks in the Admin Center:

- "Accessing the CTPView Admin Center (CTPView)" on page 103

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | **96**

Accessing the CTPView Admin Center (CTPView)

The CTPView Admin Center provides a central location for managing users, passwords, groups, and access for CTPView users. Only Global_Admin users can create, modify, and delete CTPView user accounts.

To access the CTPView Admin Center:

- On the CTPView Login Page, click **Admin Center**. The CTPView Login Administration page is displayed. This documentation refers to this page as the CTPView Admin Center.

To display all configuration choices available in the CTPView Admin Center:

- From the Admin Center, click **Display All**.

Although all configuration choices are listed, clicking the button to make any configuration change returns you to the Admin Center display for only that configuration choice.

To block global access to the CTPView Admin Center:

1. From the Admin Center, click **Access To CTPView is ALLOWED**.
2. Confirm your decision when prompted.

To reinstate global access to the CTPView Admin Center:

1. From the Admin Center, click **ALL ACCESS To CTPView Is BLOCKED**.
2. Confirm your decision when prompted.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Monitoring CTPView Users (CTPView)

To display all CTPView users that are currently logged in to the server through the CTPView GUI:

- From the Admin Center, select **Users > Active Users** to display all users that are currently logged in.

A view-only table lists the username, the user browser's IP address, the time the browser session began, the time of last activity, and the current period of inactivity. Users logged in through an SSH connection to the CTPView server are not displayed; see "Managing CTPView Users (CTPView Server Menu)" on page 198 for information about viewing these users.

To display all CTPView users regardless of login status:

- From the Admin Center, select **Users > All Users**.

This view-only table displays all users who are in the CTPView user database, as well as each user's group affiliation, user level, and the time of last login.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Adding New CTPView Users (CTPView)

To add a new CTPView user:

1. From the Admin Center, select **Users > Add New User**.
2. Type a username for the new user.

   The username must be at least 6 characters and no more than 30 characters in length. The name can include alphanumeric characters and the following nonalphanumeric characters:
   ~ ! @ # % & - _ = { } [ ] ,
3. Select a group for the new user from the list.

   The new user is assigned the properties associated with this group.
4. Type a password for the user in both fields.

   Click **Password Help** to display the password requirements. The user is forced to change this password at the first login.
5. Click **Add User**.

   The new user is immediately added to the **All Users** table.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

CTPOS and CTPView Software Password Requirements | 96

Modifying CTPView User Properties (CTPView)

CTPView users are assigned to a group when created, and inherit the properties associated with that user group. You can override these properties for any or all members of a group.

To modify CTPView user properties:

1. From the Admin Center, select **Users > Modify User Properties**.
2. Select a username from the list to display the user's current properties.
3. (Optional) Select a new user level.
4. (Optional) Select the maximum number of days allowed between logins.
5. (Optional) Select the minimum number of days allowed between password changes.
6. (Optional) Select the number of days a new password is valid.
7. (Optional) Select the number of days before password expiration that a warning is first provided.
8. (Optional) Select the number of days the user can still log in after a password expires before access is blocked.
9. (Optional) Type a date on which access is blocked from that date forward.

   This field overrides all other properties.
10. Click **Update User Properties**.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Monitoring CTPView Groups (CTPView)

To display all CTPView user groups:

From the Admin Center, select **Groups > All Groups**.

The view-only table displays all groups that are currently configured. The table also lists the default user properties configured for the group. You can configure individual user properties to override the group defaults.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Modifying CTPView User Group Affiliation (CTPView)

CTPView users are assigned to a group when created. Typically, groups are used to group users that share a common set of user properties. However, shared properties are not a requirement. If desired, user groups can simply label a set of users without regard to their individual user properties.

NOTE: Changing a user's group affiliation does not alter the user's current properties.

To modify CTPView user properties:

1. From the Admin Center, select **Users > Modify User's Group Affiliation**.
2. Select a username from the list to display the user's current group affiliation.
3. Select a new group from the list.
4. Click **Update Group**.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Adding a New CTPView User Group (CTPView)

To add a new CTPView user group:

1. From the Admin Center, select **Groups > Add New Group**.
2. Enter a group name.

   The group name must be at least 6 characters and no more than 30 characters in length. The name can include alphanumeric characters and the following nonalphanumeric characters:
   ~ ! @ # % & - _ = { } [ ] ,
3. Select a default user level for members of the group.
4. Click **Add Group**.

Modifying CTPView User Group Default Properties (CTPView)

CTPView users are assigned to a user group when created and by default inherit the properties associated with the group. You can override these properties for any or all members of a group.

To modify CTPView user properties:

1. From the Admin Center, select **Groups > Modify Group Properties**.
2. Select a group name from the list to display the group's current properties.
3. (Optional) Select a default user level.
4. (Optional) Select the maximum number of days allowed between logins.

   The default is 30 days.
5. (Optional) Select the minimum number of days allowed between password changes.

   The default is 1 day.
6. (Optional) Select the number of days a new password is valid.

   The default is 60 days.
7. (Optional) Select the number of days before password expiration that a warning is first provided.

   The default is 7 days.
8. (Optional) Select the number of days the user can still log in after a password expires before access is blocked.

   The default is 14 days.
9. (Optional) Type a date on which access is blocked from that date forward.

   This field overrides all other properties.
10. (Optional) Select **Update current members** to apply these changes to all members of the group.

    If you do not select this option, the group changes do not affect any current member of the group.

11. Click **Update Group Properties**.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Prohibiting and Reinstating CTPView Access by Users (CTPView)

IN THIS SECTION

You can prevent individual users from accessing the CTPView software until you reinstate that access.

Displaying Prohibited CTPView Users (CTPView)

To display currently prohibited CTPView users:

- From the Admin Center, select **Prohibit > Current Prohibited Users**.

The view-only table displays all prohibited users, the time each was prohibited, who prohibited the user, and the last time the user access the CTPView software.

Prohibiting User Access to CTPView (CTPView)

To prohibit a CTPView user:

1. From the Admin Center, select **Prohibit > Designate Prohibited User**.
2. Select the user from the list.
3. Click **Submit Prohibited User**.

Reinstating Prohibited CTPView Users (CTPView)

To reinstate a currently prohibited CTPView user:

1. From the Admin Center, select **Prohibit > Reinstate Prohibited User**.

2. Select the user from the list.
3. Click **Reinstate Prohibited User**.

SEE ALSO

Deleting Users and Groups (CTPView) | 109

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Deleting Users and Groups (CTPView)

IN THIS SECTION

You can delete active and inactive CTPView users from the user database. Inactive users are those who have not logged in within a specified number of days; the default is 365 days. Active users have logged in more recently than the default. You can also delete user groups.

Deleting Active CTPView Users (CTPView)

To delete an active CTPView user:

1. From the Admin Center, select **Delete > Delete User**.
2. Select the user from the list.

   NOTE: Prohibited and inactive users do not appear on the list and must be deleted separately.

3. Click **Delete User**.

Deleting Inactive CTPView Users (CTPView)

To delete an inactive CTPView user:

1. From the Admin Center, select **Delete > Inactive User**.
2. Select the number of days without a login to designate inactive users.
3. Click **Delete Inactive Users**.

Deleting Prohibited CTPView Users (CTPView)

To delete a currently prohibited CTPView user from the database:

1. From the Admin Center, select **Prohibit > Delete Prohibited User**.
2. Select the user from the list.
3. Click **Delete Prohibited User**.

Deleting CTPView Groups (CTPView)

To delete a CTPView user group and all its members:

1. From the Admin Center, select **Delete > Delete Group**.
2. Select the group from the list.
3. Click **Delete Group**.

SEE ALSO

Prohibiting and Reinstating CTPView Access by Users (CTPView) | **108**

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | **102**

Managing User Passwords (CTPView)

IN THIS SECTION

You can limit how frequently a user can reuse a password, exclude passwords, reinstate excluded passwords, and specify the rules for forming passwords.

Limiting Password Reuse (CTPView)

To limit how frequently a password can be reused:

1. From the Admin Center, select **Passwords > Re-Use Password Limit**.
2. Select the number of new passwords a user must create before a given password can be re-used.
3. Click **Set Password Re-Use Limit**.

Excluding Passwords from Use (CTPView)

To exclude certain passwords from use:

1. From the Admin Center, select **Passwords > Excluded Passwords**.
2. Type a password to add to the list of excluded passwords.
3. Click **Add Password to List**.

Reinstating Excluded Passwords (CTPView)

To reinstate a previously excluded password for use:

1. From the Admin Center, select **Passwords > Excluded Passwords**.
2. Select the password from the list of excluded passwords.
3. Click **Reinstate Selected Passwords**.

Changing Requirements for New Passwords (CTPView)

To change the requirements for new passwords (current passwords are not affected):

1. From the Admin Center, select **Passwords > Modify Password Requirements**.
2. (Optional) Select the minimum password length, in the range 15 through 56.
3. (Optional) Select the maximum password length, in the range 15 through 56.

   The default is 56 characters.
4. (Optional) Select the minimum number of lowercase letters, in the range 1 through 56.

5. (Optional) Select the minimum number of uppercase letters, in the range 1 through 56.
6. (Optional) Select the minimum number of numerals, in the range 1 through 56.
7. (Optional) Select the minimum number of nonalphanumeric characters, in the range 1 through 56.
8. Click **Update Password Properties**.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

CTPOS and CTPView Software Password Requirements | 96

Configuring User Login Properties (CTPView)

IN THIS SECTION

You can configure a number of properties that affect how users log in to and log out of the CTPView software.

Logging Out a CTPView User (CTPView)

To log out a CTPView user:

1. From the Admin Center, select **Login/Logout > Logout Users**.
2. Select the user from the list.
3. Click **Logout Selected Users**.

Configuring Automatic Logout for a CTPView User (CTPView)

To specify that a CTPView user is automatically logged out after a certain period:

1. From the Admin Center, select **Login/Logout > Auto Logout**.
2. Select the inactivity period from the list.
3. Click **Set Auto Logout Period**.

Configuring the Number of Login Attempts Allowed Before Lockout (CTPView)

To specify how many times a CTPView user can attempt to log in before the login is considered to have failed and the user is locked out:

1. From the Admin Center, select **Login/Logout > Login Limit** .
2. Select the number of attempts allowed from the list.
3. Click **Set Failed Login Limit**.

Configuring a Lockout Period for CTPView Users (CTPView)

When a user exceeds the allowed number of failed login attempts or tries to open multiple CTPView sessions from unique IP addresses, the user is prevented from accessing CTPView for a lockout period.

To specify a CTPView user's lockout period:

1. From the Admin Center, select **Login/Logout > Lockout Period**.
2. Select the lockout period from the list.
3. Click **Set Lockout Period**.

Clearing CTPView User Counters (CTPView)

Two counters are associated with each CTPView user. One counter tracks the number of failed login attempts. This counter is automatically reset to zero after a successful login. The other counter tracks the number of reminders that a user receives to change the user password. This counter is automatically reset after the user has selected a new password. When either counter exceeds the allowed limit, the user is locked out of CTPView access.

To clear a user's counters:

1. From the Admin Center, select **Login/Logout > Clear Counters**.
2. Select the user from the list.
3. Click **Clear Counters**.

Reinstating Locked-Out IP Addresses (CTPView)

When a user attempts to access the CTPView software from a second IP address with a currently active username, the username and both IP addresses are locked.

To reinstate an IP address that has been locked from CTPView access:

1. From the Admin Center, select **Login/Logout > Unlock IP**.
2. Select the IP address from the list.
3. Click **Reinstate Locked IP**.

Creating an Access Filter to Allow or Deny IP Addresses (CTPView)

IP access filters enable you to specify whether users from an IP address or range of IP addresses are allowed or denied access to the CTPView software.

To create an IP access filter:

1. From the Admin Center, select **Login/Logout > IP Access Filter**.
2. Type an IP address or range of IP addresses.
3. Select whether to allow or deny that address or range access to the CTPView software.

   In the case of conflict between multiple filters, a rule to deny an address or range overrides a rule that allows access.
4. Click **Add IP Range to List**.

Removing an IP Access Filter (CTPView)

To remove an IP filter:

1. From the Admin Center, select **Login/Logout > IP Access Filter**.
2. Select the IP address from the list.
3. Click **Remove IP Range From List**.

RELATED DOCUMENTATION

Managing CTPView Users with the CTPView Admin Center | 102

Understanding CTPView GUI User Levels

This topic describes the user security levels available in the CTPView GUI.

Three user levels are provided to enhance the security of CTPView GUI logins:

- Net_View—Users in this class are restricted to query-only access to CTP platforms. Early versions of the CTPView software referred to this class as query-only users. Net_View users can change their own passwords.

- Net_Admin—Users in this class can configure CTP platforms. They do not have permission to create or modify CTPView user accounts. Early versions of the CTPView software referred to this class as administrators. Net_Admin users can change their own passwords.
- Global_Admin—Users in this class have all the privileges of the Net_Admin class. They are also able to create and modify user accounts. Only members of the Global_Admin user class have access to the CTPView Admin Center, where CTPView user and password profiles are managed.

Each CTPView user has a profile that describes user properties, including user privileges and restrictions. All users are assigned to user groups. Each user group has a set of default user properties that are transferred to new users created in or assigned to that group. Global_Admin users can modify any of the user properties on a per-user basis.

CTPOS and CTPView Software Password Requirements

Certain requirements apply to passwords for the following:

- CTPOS
- CTPView server shell access accounts
- CTPView GUI access accounts
- PostgreSQL accounts
- GRUB Boot loader

New passwords must include the following:

- At least one lowercase letter
- At least one uppercase letter
- At least one numeral
- At least one of the following nonalphanumeric characters: ~ ! @ # % & - _ = { } [ ] ,

NOTE: Follow the onscreen instructions for the character range.

New passwords must not include either of the following:

- The username as part of the password.
- More than two adjacent repeated characters.

RELATED DOCUMENTATION

CTPView Network Management System Administration

Managing CTPView Users with the CTPView Admin Center | 102

Adding New CTPView Users (CTPView) | 104

Changing the PostgreSQL Apache Account Password (CTPView Server Menu) | 38

Changing the PostgreSQL Administrator Account Password (CTPView Server Menu) | 39

Changing the GRUB Boot Loader Password (CTPView Server Menu) | 37

Changing the User Password (CTP Menu) | 45

Setting a New Password for a Nonroot User Account (CTPView Server CLI) | 256

Setting a New Password for a Root User Account (CTPView Server CLI) | 257

Default CTPOS and CTPView Accounts and Passwords | 94

Unlocking a User Account (CTP Menu)

Every user created in the CTP system expires after a specified time limit. If there is no user activity for a specified number of days after the expiry of the password, the user is locked out of the system. Such users can access the system only after their account is unlocked by a system administrator.

> **NOTE**: The menu option, `Unlock user account` is displayed only if you log in as a system administrator.

This topic describes how to unlock a user account that has been locked out because of prolonged inactivity.

To unlock a user from the CTP Menu:

From the Main Menu, select **5) Node Operations** > **15) Unlock user account** and specify the user account to be unlocked.

```
==========================================================================
= (ctp_87 04/08/14 15:29:21  UTC) | Node Operations Menu
==========================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
```

```
 1) Change Node Date/Time/TimeZone
 2) Display network settings
 3) Configure network settings
 4) Initialize Database
 5) Ping IP address
 6) Traceroute IP address
 7) ssh to another host
 8) System descriptor field:
 9) Reboot Node
10) Powerdown Node
11) Display ethernet media
12) Config ethernet media
13) Set your password
14) Config security profile
15) Unlock user account
------------ Your choice [0]: 15

Enter the user to be unlocked:

Usage: chage [-l] [-m min_days] [-M max_days] [-W warn]
        [-I inactive] [-E expire] [-d last_day] user
```

chage Sets the password expiry information for a user.

-l Sets the expiry information for an account.

-m Sets the minimum number of days that must pass before the password can be changed again. This is calculated from the date when the password was last changed.

-M Sets the maximum number of days after which password must be changed. This is calculated from the date when the password was last changed.

-W Sets the number of days before the expiry of the current password to issue password change warning. before

-I Sets the number of days after password expiry when the account will be locked.

-E Sets the password expiry date for a user. Specify date in the format MM/DD/YYYY or YYYY-MM-DD.

-d Sets the last day for the user to change password.

user User account

Unlocking User Accounts for Which Password Has Expired

IN THIS SECTION

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 accounts after a 35-day period of account inactivity. This requirement- standard denotes that the passwords 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.

All the users authorized to access the syslog file can view the lockout warning messages. The lockout warning messages are started to be sent from 10 days before the date on which the account is bound to be locked. For example, when an account is due to be locked because of not having been accessed for the last 25 days, the first warning message is sent on 25th day, the second warning message is sent on the 26th day, and so on, until the 35th day is reached and the account is locked. All the users whose accounts are locked can request the system administrators or root access-privileged users to unlock the accounts for them.

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.

Script to Monitor the Duration of Inactivity of 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. Currently, this file is used to lock the user accounts after a 35-day period of account inactivity.

The following sequence of events occur with the “activity_check” script that is used for sending the lockout warning messages.

1. If the user account is not already locked, then the script identifies the date on which the user was logged in. If the user has not logged in for the last 25 days, and if the user is a system administrator, then a warning message is generated and transmitted to the syslog with the severity level of the log greater than 8.

2. If the user account is not already locked, then the script determines the date on which the user account was created. If the user has not logged in for the last 25 days, and if the user is a system administrator, then a warning message is generated and transmitted to the syslog with the severity level of the log greater than 8.

Script to Reset the Expired User Accounts

The reset_pw_lock script is added to the CTP device CTP Box and CTPView server in the /bin folder. This script can also be run in shell or CLI mode. With locked user accounts (in which the user cannot log in to shell), the user needs to manually change to single-user mode to run this script. The script can be run by entering the reset_pw_lock <user> command. The script unlocks the password of only the user specified in the command. With multiple users, you can enter the command as reset_pw_lock <user1> <user2> .... When you run this script, it unlocks the password of the specified user account, performs the mounting operations, and reboots the system. The activity_check script file is modified to send the lockout warning message to the network syslog. The reset_pw_lock script is added to unlock the password of disabled user accounts.

CHAPTER 11

Managing the CTPView Server (CTPView)

IN THIS CHAPTER

Adding and Removing CTP Platforms Managed by CTPView Software (CTPView)

Before you can use CTPView to manage the CTP platforms in your network, you must configure the platform information in the CTPView software. In the context of the network, the CTP platforms are often referred to as remote hosts, nodes, and remote platforms.

To add a CTP platform to your network:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Enter a unique name for the remote host.
3. Enter a management IP address for the host.

   This address is used for the CTPView management connection to the host.
4. If the host is running CTPOS 4.1 or lower, select the checkbox.
5. Enter a password to be used by the CTPView software when accessing the host.
6. Select a group to associate with the host; only the **default** group is available if no other groups have been configured.
7. Select the model number for the host.
8. Include or exclude the host from monitoring by the CTPView software by selecting **Yes** or **No**.
9. Select how the CTPView software accesses the host when the host has been including for network monitoring.
10. Select the SNMP community associated with the host.
11. Click **Add New Remote Host**.

To remove a CTP platform from your network:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click the **Remove Remote Host** field, select the group to which the host belongs, and then select the remote host.
3. Click **Remove Remote Host**.

Adding and Removing Host Groups (CTPView)

CTPView software enables you to create host groups. Subsequently you assign one or more CTP platforms to each host group. The host groups enable easier connection and monitoring of CTP

platforms, especially as your network becomes large and complex. Host groups are displayed at the top of the CTPView side pane. There you can choose a group and then connect to a host that is a member of that group.

Host groups and names are often configured based on geography or application type. If you do not define a group, then the CTP platforms are placed in the default group.

To add a host group:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Enter a unique name for the host group.

   Group names can include from 3 to 20 characters consisting of letters, numbers, hyphens, and underscores.
3. Click **Add New Group**.

To remove a host group:

> **NOTE**: Removing a host group automatically deletes all host that are members of that group. If that is not your intention, move those hosts to another group before you perform the following steps.

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click the **Remove Host Group** field and select the group.
3. Click **Remove Group**.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | 123

Adding and Removing SNMP Communities (CTPView)

You can configure SNMP communities for management of CTP platforms in your network.

To add an SNMP community:

1. In the side pane, select **Server > Administration**.

The Administrative Functions pane is displayed.

2. Enter a unique name for the community.
3. Click **Add New Community**.

To remove an SNMP community:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.

2. Select the community.
3. Click **Remove Community**.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | 123

Managing CTP Platforms in the Network (CTPView)

When CTP platforms have already been configured in the CTPView software, you can subsequently change many aspects of that configuration.

To manage a CTP platform (remote host) in your network:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.

2. Click **Manage Network Hosts**.

   The Manage Network pane is displayed.

3. Select a host group and click **Show Selected Groups**.

   A table listing all CTP platforms in the network is displayed.

   > **NOTE**: If the management and data Ethernet segregation feature is disabled for the selected host group, the Manage Network pane displays the default IP in the **Mgmt/Default IP** column and "N/A" in the **Data IP** column.

4. (Optional) Select a different **Group Name** to change the host's group affiliation.
5. (Optional) Make a selection in the **Monitor** column to change whether CTPView monitors the host.
6. (Optional) Make a selection in the **Connect Type** column to change how CTPView accesses a monitored host.

7. (Optional) Make a selection in the **SNMP Community** column to change the SNMP community associated with the host.
8. Click **Submit Changes**. If you do not want to submit your changes, then click **Reset**.

Alternatively, you can perform the following steps to access CTP platform management:

1. In the side pane, select **Network > Monitoring**.

   The Administrative Functions pane is displayed.

2. Click **Manage Network Hosts**.

   The Network Monitoring pane is displayed.

3. Click **Manage Network**.

   The Manage Network pane is displayed.

4. Perform steps 3 through 8 as described above.

RELATED DOCUMENTATION

Monitoring the Network with the CTPView Software (CTPView) | **178**
Changing the Display Settings for CTPView Network Monitoring (CTPView) | **180**
Checking the CTPView Server Connection to CTP Platforms in the Network (CTPView) | **181**

Configuring Email Notifications (CTPView)

You can configure the CTPView software to send email notifications to a distribution list when certain events take place on the CTP platform. Table 10 on page 124 lists the events for which you can configure email notification.

Table 10: CTP Platform Events for Email Notifications

Event
CTP platform state is Unreachable.
CTP platform state is Check Host.

CTP port state is Active-Down.
CTP port state is Assessing.
CTP port state is Active-Up.
CTP port state is Disabled.

To configure email notifications for CTP platform events:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **Email Notifications**.

   The Email Notifications window is displayed.
3. Enter the name or IP address of a qualified mail server.
4. Click **Change Mail Server**.
5. Click **Send Test Email** to verify email connectivity.
6. Type an email address in the **Add Recipient to List** field.
7. (Optional) Check **Add Recipient to all Lists** if you want the recipient to receive notification for all events.
8. Click **Add Email Address** to add the recipient to the primary list of email recipients.
9. For any event listed in Table 10 on page 124, select a recipient for notification and click **Add Recipient**.
10. Click **Close Window** when finished.

To remove recipients from a notification list:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **Email Notifications**.

   The Email Notifications window is displayed.
3. Do either of the following:

   - Select a recipient from the primary list, and click **Remove Email Address** to remove the recipient from all notifications.

- Select a recipient from any of the event lists, and click **Remove Recipient** to remove the recipient from that list.

4. Click **Close Window** when finished.

RELATED DOCUMENTATION

Monitoring the Network with the CTPView Software (CTPView) | 178

Setting the CTPView Server Start-Up Banner (CTPView)

When you log in to the CTPView server, a log-in or start-up banner presents a message. This banner is displayed whether you log in through the CTPView GUI or through an SSH connection. You can change the banner to display the desired message.

To set the start-up banner:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **Set Start-up Banner**.

   The Modify Start-Up Banner Content window is displayed.
3. Type your message in the field.
4. Click **Submit Changes**. If you do not want to submit your changes, then click **Undo Changes**.

RELATED DOCUMENTATION

Setting the CTP Platforms Login Banner (CTPView) | 126

Setting the CTP Platforms Login Banner (CTPView)

When you log in to the CTP platforms through an SSH connection, a banner presents a message. You can change the banner to display the desired message. You can also configure different banners for different CTP platforms.

To set the platform login banner:

1. In the side pane, select **Node > Maintenance**.

The Node Maintenance pane is displayed.

2. Click **Update CTP Login Banner**.

   The Upgrade CTP Banner window opens and displays the current CTPView software start-up banner and a list of platform groups and their members.

3. Skip to step 8 if you want to copy the current banner to the CTP platforms.
4. Click **Change Banner** to use a message different than the current banner.

   The Modify Start-Up Banner Content window is displayed.

5. Type your message in the field.
6. Click **Submit Changes**. This action changes the start-up banner for CTPView itself. If you do not want to submit your changes, then click **Undo Changes**.
7. Click **Return to CTP Banner Upgrade**.
8. Click the name of a platform. You can select more than one platform by holding down the Ctrl key when you click the platform names.
9. Click **Upgrade Banner on CTP(s)**.

   The banner is pushed to each selected CTP platform. The new login banner is displayed in your terminal window when you create an SSH connection to the platform. It is also displayed when you log in to the CTPView server through the CTPView GUI or through an SSH connection.

RELATED DOCUMENTATION

Setting the CTPView Server Start-Up Banner (CTPView) | 126

Configuring an SSH Connection to a CTP Platform that Persists Through the Session (CTPView)

This topic describes how to configure CTP platforms so that an SSH connection remains established for the entire session when the CTPView server connects to the platform.

SSH port forwarding creates an encrypted and protected connection between the CTPView software and a remote CTP platform, that remains up as long as the server connection to the platform is up. It must be enabled on both the CTP platform and the CTPView software; it is enabled on both by default. When this feature is not enabled, the CTPView server creates a separate SSH connection to the platform for each command and configuration change. This feature reduces overhead and increases performance of the CTPView software. You can choose to disable this feature or reenable it.

To disable SSH port forwarding on the connected CTP platform:

1. In the side pane, select **Server > Administration**.

The Administrative Functions pane is displayed.

2. Click **Do not use persistent CTP SSH connections** and confirm the action when prompted.

   The button text changes to **Use persistent CTP SSH connections (if available)**.

To enable SSH port forwarding on the connected CTP platform:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.

2. Click **Use persistent CTP SSH connections (if available)** and confirm the action when prompted.

   The button text changes to **Do not use persistent CTP SSH connections**.

You can also change the state of this feature by selecting **System > Configuration** in the side pane and clicking **SysMon**. You can then select **Enabled** or **Disabled** for the feature.

When the SSH port forwarding connection is successfully made to a connected CTP platform, Port Forwarding is displayed at the top of the side pane immediately under the name of the connected CTP platform.

RELATED DOCUMENTATION

Configuring an SSH Connection to a CTP Platform That Persists Through the Session (CTPView Server Menu) | 226

Setting the CTPView Server Clock (CTPView)

The date and time configured on the CTPView server is displayed in the heading section of the CTPView GUI, regardless of which pane is currently displayed. You can change the time zone, date, and time for the server.

> **NOTE**: We strongly recommend that you set the time zone to Coordinated Universal Time (UTC) on all CTPView servers and CTP platforms in your network. This practice is necessary to enable the statistics graphs of CTP network behavior to accurately represent when particular events occurred. CTP platform time is set when you first power up the device.

To set the date and time on the CTPView server clock:

1. In the heading section, click the globe icon to the right of the current time display.

   The Clock CTPView window is displayed.

2. (Optional) Select a different time zone and click **Submit New Timezone**.

> **NOTE**: Changing the time zone reboots the CTPView server.

3. If you want only to adjust the time and not change the time zone, click **Cancel**.

   The Clock CTPView window now displays the current time and fields for the new time.

4. Select new values to adjust any or all of the day, month, year, hour, minute, or second, and click **Submit Changes**.

   The current time displayed in the CTPView GUI does not update automatically. When you navigate to any other pane in the software, the time display updates.

RELATED DOCUMENTATION

Powering On the CTP Platform

Managing NTP Servers for the CTPView Network (CTPView) | **129**

Managing NTP Servers for the CTPView Network (CTPView)

IN THIS SECTION

NTP servers are used to synchronize system clocks over an IP network. You can manage your NTP peers and clients from the NTP Server Settings window. This window displays the results of a query of the configured NTP peers. Table 11 on page 130 describes the information provided in the results. From this

window you can stop the NTP daemon, add and remove NTP peers, and synchronize to a particular peer. For more information about the information displayed in the summary, consult a reference on NTP.

Table 11: Summary Information for NTP Server Peers

Field	Description
remote	Hostname or IP address of the reference clock source. LOCAL refers to the system time on the NTP server. Table 12 on page 130 describes the meaning of a prefix to the name or address.
refid	Reference ID that identifies the type of the reference clock. Typically this is the primary clock to which that NTP server peer is synchronized. When the primary clock is unknown, 0.0.0.0 is displayed.
st	Stratum number of the NTP server peer.
t	Remote peer type: broadcast, local, multicast, or unicast.
when	Time since the last packet was received, in seconds. When this value matches the poll value, the reference clock is queried, and when is reset to zero.
poll	Polling interval, in seconds.
reach	Reachability register, displayed in octal format. Indicates whether data was readable from the NTP server peer at the last poll, and whether the peer was synchronized to another time source.
delay	Current estimated round-trip time for queries to the remote peer.
offset	Difference between the reference time value and the CTPView server clock.
jitter	Magnitude of the jitter between several time queries.

A prefix to the peer name or IP address indicates the fate of the peer in the clock selection process. Table 12 on page 130 describes the possible values.

Table 12: Prefixes Designating Peer Clock Selection Status

Prefix	Meaning

space	The peer is discarded as unreachable, synchronized to this server (I a synchronization loop), or having a very large synchronization distance.
x	Peer is discarded by the intersection algorithm as a false ticker.
-	Peer is discarded by the clustering algorithm as an outlier.
+	Peer is a survivor and a candidate for the combining algorithm.
#	Peer is a survivor, but is not one of the first six peers sorted by synchronization distance. If the association is ephemeral, it may be demobilized to conserve resources.
*	Peer has been declared the system peer and lends its variables to the system variables.
o	Peer has been declared the system peer and lends its variables to the system variables. However, the actual system synchronization is derived from a pulse-per-second (PPS) signal, either indirectly by means of the PPS reference clock drive or directly by means of the kernel interface.

A summary of NTP network client access lists the IP address and netmask for each network client. You can add and remove network clients and modify client netmasks.

Accessing the NTP Server Settings Window (CTPView)

To configure NTP servers:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **NTP Server Configuration**.

   The NTP Server Settings window is displayed.

Stopping the NTP Daemon (CTPView)

To stop the NTP sever daemon:

- In the NTP Server Settings window, click **Stop NTP Daemon**.

  The connection to the listed NTP server peers is brought down, and the Summary of NTP Server Pairs table is cleared.

Adding an NTP Peer (CTPView)

To add an NTP peer to the summary table:

1. In the NTP Server Settings window, type an IP address or fully qualified domain name in the Manage NTP Peers section.
2. Click **Add New NTP Peer**.

   The peer address or name and information appear in the summary table.

Removing an NTP Peer (CTPView)

To remove an NTP peer from the list of configured peers:

1. In the NTP Server Settings window, select a peer to remove in the Manage NTP Peers section.
2. Click **Remove Selected Peer**.

   The peer is removed from the table, and the NTP daemon is restarted if it was running.

Synchronizing the CTPView Server to an NTP Peer (CTPView)

To manually synchronize the server to an NTP peer:

1. In the NTP Server Settings window, select a peer for synchronization in the Manage NTP Peers section.
2. Click **Sync to Selected Peer**.

Adding NTP Network Clients (CTPView)

To add a new network client:

1. In the NTP Server Settings window, type an IP address or fully qualified domain name in the Manage NTP Client Access section.
2. Click **Add New Network Client**.

   The client address or name and netmask appear in the summary table.

Removing an NTP Network Client (CTPView)

To remove an NTP network client from the list of configured clients:

1. In the NTP Server Settings window, select a client to remove in the Manage NTP Client Access section.
2. Click **Remove Selected Network Client**.

   The client is removed from the table, and the NTP daemon is restarted if it was running.

Modifying the Netmask of an NTP Network Client (CTPView)

To modify a client netmask:

1. In the NTP Server Settings window, select a client in the Manage NTP Client Access section.
2. Select a new netmask.
3. Click **Modify Client Netmask**.

SEE ALSO

Setting the CTPView Server Clock (CTPView) | **128**

NTP Authentication Overview on CTP Devices

IN THIS SECTION

Network Time Protocol (NTP) is a UDP protocol for IP networks. It is a protocol designed to synchronize the clock on client machines with the clock on NTP servers. NTP uses Coordinated Universal Time (UTC) as the reference time.

The implementation of NTP requires separate client and server applications. Superficially, NTP is a software daemon operating in a client mode and server mode. Using NTP packets, the client and server exchange time stamp data, ultimately setting the clock on the client machine similar to that of the NTP server. Starting with CTPOS Release 7.2R1, NTP authentication is supported. NTP authentication checks the authenticity of NTP server before synchronizing local time with server. This phenomenon helps you to identify secure servers from unauthorized or illegal servers. NTP authentication works with a symmetric key configured by user. The key is shared by the client and an external NTP server. The servers and clients must agree on the key to authenticate NTP packets. Currently NTP is already supported in CTP devices but NTP authentication is not supported. Authentication support allows the NTP client to verify that the server is in fact known and trusted and not an intruder intending accidentally or on purpose to masquerade as that server.

The following are the different operating modes used by NTP:

- Client/Server—In a common client/server model, a client sends an NTP message to one or more servers and processes the replies as received. The server interchanges addresses and ports, overwrites certain fields in the message, recalculates the checksum, and returns the message immediately. Information included in the NTP message allows the client to determine the server time with respect to local time and adjust the local clock.

- Symmetric Active/Passive—Configuring a peer in symmetric-active mode indicates remote server that one wish to obtain time from the remote server and that one is also willing to supply time to the remote server if necessary. This mode is appropriate in configurations involving a number of redundant time servers interconnected through diverse network paths. Symmetric modes are most often used between two or more servers operating as a mutually redundant group.

- Broadcast—The advantage is that clients do not need to be configured for a specific server, as this mode is intended for configurations involving one or a few servers and a possibly very large client population. Broadcast mode requires a broadcast server on the same subnet. Since broadcast messages are not propagated by routers, only broadcast servers on the same subnet are used. Since an intruder can impersonate a broadcast server and inject false time values, this mode should always be authenticated.

In the CTPView server, the Client/Server mode is implemented, which is the use case of the CTP device and CTPView or any other Linux machine within the same network as that of the CTP device will act as NTP servers for authentication.

Although you can configure NTP using the CTPView server in CTPView releases earlier than Release 7.2, you can configure NTP authentication starting from CTPView Release 7.2R1. NTP can only be configured from the CTPView server by using the **System Configuration > Node Settings** page of the CTPView server. NTP authentication allows the NTP client to verify that servers are known and trusted. Symmetric key authentication will be used to authenticate the packets. It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. The client then adds the required key id and shared secret key to their configuration and keys files through CTPView or through syscfg commands. The **Key ID** and **Key Value** fields must be left blank in CTPView to disable NTP authentication.

NTP Authentication Procedure

It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. Also, the “trustedkey keyid” attribute must be mentioned in the server’s ntp.conf file and the NTP process (ntpd) must be started in the server side for successful authentication.

The user provides the communicated key id and key values through the CTPView server or syscfg commands. The CTPView server adds the key value and key id to the conf and keys files of the CTP device and starts the NTP daemon. The NTP servers and clients involved must agree on the key, key ID, and key type to authenticate the NTP packets.

When the NTP daemon is started, it reads the key file specified by the keys command and installs the keys in the key cache. It then exchanges packets with its configured servers at poll intervals. The NTP authentication packet adds the key ID and the MAC address in its header, and the packets are accepted by the server only if the key ID matches a trusted key and the message digest is verified with this key.

After authentication is successful, the NTP server stores its own timestamp and a transmit timestamp into the packet and send it back to the client. In the case of authentication failure, time is not synchronized.

The following is the example of NTP authentication assuming that the key received from NTP server is 12345 and the key number and corresponding key value is added to the conf and key files of the CTP device.

```
Command - ntpdate -d –a <Key Id> -k /etc/ntp/keys <Server Ip>

Example - ntpdate -d –a 12345 -k /etc/ntp/keys 10.216.118.101



[root@ctp_74 ctp_cmd 36]# ntpdate -d -a 12345 -k /etc/ntp/keys 10.216.118.101
27 May 16:13:41 ntpdate[11935]: ntpdate 4.2.8@1.3265-o Tue Jan  6 05:50:59 UTC 2015 (3)
Looking for host 10.216.118.101 and service ntp
host found : 10.216.118.101
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
transmit(10.216.118.101)
receive(10.216.118.101)
receive: authentication passed
server 10.216.118.101, port 123
stratum 11, precision -21, leap 00, trust 000
refid [10.216.118.101], delay 0.02577, dispersion 0.00006
transmitted 4, in filter 4
reference time:    d9101e66.08f2fe3d  Wed, May 27 2015 10:43:50.034
originate timestamp: d9101e68.fbd8b5c6  Wed, May 27 2015 10:43:52.983
transmit timestamp:  d9106bbb.82aca793  Wed, May 27 2015 16:13:47.510
filter delay:  0.02580  0.02579  0.02577  0.02579
         0.00000  0.00000  0.00000  0.00000
filter offset: -19794.5 -19794.5 -19794.5 -19794.5
         0.000000 0.000000 0.000000 0.000000
delay 0.02577, dispersion 0.00006
```

```
offset -19794.526903

27 May 16:13:47 ntpdate[11935]: step time server 10.216.118.101 offset -19794.526903 sec
```

The preceding command, when run without “-d” option, synchronizes the time of CTP device with the NTP server. The “-d” option runs in debug mode, prints the intermediate results, and does not adjust the clock. If the key number or key value are not correct, then the message “authentication passed” is replaced with “authentication failed” and time is not synchronized.

Configuring NTP Authentication Using the System Query Page (CTPView)

NTP authentication enables the CTP device, which functions as the NTP client, to verify that servers are known and trusted. Symmetric key authentication will be used to authenticate the packets. It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. The client then adds the required key id and shared secret key to their configuration and keys files through CTPView or through syscfg commands. The **Key ID** and **Key Value** fields must be left blank in CTPView to disable NTP authentication.

To configure NTP authentication using the System Query page of CTPView:

1. In the side pane, select **System** > **Query**.

   > **TIP**: Alternatively, you can specify the key ID and key value for NTP authentication from the System Configuration page by selecting **System** > **Configuration** in the side pane.

2. Click **Node Settings** tab.

   The NTP Settings page is displayed. The hostname and IP address of the CTP device are displayed under the Device table, which is shown to the left of the NTP Settings table.

3. Configure the parameters described in Table 13 on page 137 and click **Submit Settings**.
4. (Optional) Click **System** > **Query** > **Node Settings** to verify the NTP configuration details.

Table 13: NTP Server Authentication Settings on the System Query Page in CTPView

Field	Function	Your Action
Server IP	Specifies the IPv4 or IPV6 address of the NTP server. Adds NTP servers to the server list (IP addresses or hostnames). You can configure a maximum of two NTP servers. NTP authentication is started from the first server in the list and if the first server fails or becomes unavailable, the second server in the list is used.	Enter the IPv4 or IPv6 address of the NTP server to be used for authentication.
Key ID	Specifies the key ID to authenticate the NTP packets received from the server by the NTP client. The servers and clients involved must agree on the key and key identifier to authenticate NTP packets. Keys and related information are specified in a key file. Key ID is used to prove authenticity of data received over the network. During the synchronization of time, the client requests the key ID with the “NTP Client” packet and server sends the response with the “NTP Server” packet. If the key ID differs in both the packets, then the time does not synchronize. The time is synchronized and modified for the client only when the two key IDs are the same. The IP address with the secret key is configured in the “/etc/ntp.conf” NTP configuration file on the CTP device. The following is the example for the ntp.conf file: ‘server x.x.x.x key 123’ where: x.x.x.x is the NTP server IP address Key is the secret key id which is shared by both the client and server.	Enter a 32-bit integer in the range of 1 through 65534.

Table 13: NTP Server Authentication Settings on the System Query Page in CTPView *(Continued)*

Field	Function	Your Action
Key Value	Specifies the value of the NTP key used for NTP authentication between the NTP server and the NTP client. NTP uses keys to implement authentication. This key is used while exchanging data between the client and server. The following three key types are present: • An A key is just a sequence of up to eight ASCII characters. • An M key is a sequence of up to 31 ASCII characters. • An S key is a 64 bit value with the low order bit of each byte being odd parity. CTP devices support the M key (MD5) for NTP authentication. All the keys must be defined in the "/etc/ntp/keys" file. The following is an example for the keys file: '123 M pass' where: 123 is the key id (range 1 to 65534) M designates the key type (M means MD5 encryption) Pass denotes the key itself	Enter the key value as a sequence of up to 31 ASCII characters.
Status	Specifies whether you want to enable or disable the NTP process on the CTP device.	Select one: • Enabled—Enables the NTP process on the CTP device. • Disabled—Disables the NTP process on the CTP device.

Configuring NTP Authentication Using the System Configuration Page (CTPView)

NTP authentication enables the CTP device, which functions as the NTP client, to verify that servers are known and trusted. Symmetric key authentication will be used to authenticate the packets. It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their configuration and keys files. The client then adds the required key ID and shared secret key to their configuration and keys files through CTPView or through syscfg commands. The **Key ID** and **Key Value** fields must be left blank in CTPView to disable NTP authentication.

To configure NTP authentication using CTPView:

1. In the side pane, select **System** > **Configuration**.

   > **TIP**: Alternatively, you can specify the key ID and key value for NTP authentication from the System Query page by selecting **System** > **Query** in the side pane.

2. Click **Node Settings** tab.

   The NTP Settings page is displayed. The hostname and IP address of the CTP device are displayed under the Device table, which is shown to the left of the NTP Settings table.

3. Configure the parameters described in Table 14 on page 139 and click **Submit Settings**.
4. (Optional) Click **System** > **Configuration** > **Node Settings** to verify the NTP configuration details.

Table 14: NTP Server Authentication Settings on the System Configuration Page in CTPView

Field	Function	Your Action
Server IP	Specifies the IPv4 or IPV6 address of the NTP server. Adds NTP servers to the server list (IP addresses or hostnames). You can configure a maximum of two NTP servers. NTP authentication is started from the first server in the list and if the first server fails or becomes unavailable, the second server in the list is used.	Enter the IPv4 or IPv6 address of the NTP server to be used for authentication.

Table 14: NTP Server Authentication Settings on the System Configuration Page in CTPView *(Continued)*

Field	Function	Your Action
Key ID	Specifies the key ID to authenticate the NTP packets received from the server by the NTP client. The servers and clients involved must agree on the key and key identifier to authenticate NTP packets. Keys and related information are specified in a key file. Key ID is used to prove authenticity of data received over the network. During the synchronization of time, the client requests the key ID with the “NTP Client” packet and server sends the response with the “NTP Server” packet. If the key ID differs in both the packets, then the time does not synchronize. The time is synchronized and modified for the client only when the two key IDs are the same. The IP address with the secret key is configured in the “/etc/ntp.conf” NTP configuration file on the CTP device. The following is the example for the ntp.conf file: ‘server x.x.x.x key 123’ where: x.x.x.x is the NTP server IP address Key is the secret key id which is shared by both the client and server.	Enter a 32-bit integer in the range of 1 through 65534.

Table 14: NTP Server Authentication Settings on the System Configuration Page in CTPView *(Continued)*

Field	Function	Your Action
Key Value	Specifies the value of the NTP key used for NTP authentication between the NTP server and the NTP client. NTP uses keys to implement authentication. This key is used while exchanging data between the client and server. The following three key types are present: • An A key is just a sequence of up to eight ASCII characters. • An M key is a sequence of up to 31 ASCII characters. • An S key is a 64 bit value with the low order bit of each byte being odd parity. CTP devices support the M key (MD5) for NTP authentication. All the keys must be defined in the "/etc/ntp/keys" file. The following is an example for the keys file: '123 M pass' where: 123 is the key id (range 1 to 65534) M designates the key type (M means MD5 encryption) Pass denotes the key itself	Enter the key value as a sequence of up to 31 ASCII characters.
Status	Specifies whether you want to enable or disable the NTP process on the CTP device.	Select one: • Enabled—Enables the NTP process on the CTP device. • Disabled—Disables the NTP process on the CTP device.

You can also configure the RADIUS and TACACS+ settings from the System Configuration page.

To configure TACACS+ from the CTPView web interface:

1. In the side pane, select **System** > **Configuration**.

2. Click **Node Settings** > **TACACS+ Settings** tab.

   The TACACS+ Settings page is displayed.

3. Configure the parameters described in Table 15 on page 142 and click **Submit Settings**.

4. (Optional) Click **System** > **Query** > **Node Settings** to verify the TACACS+ configuration details.

Table 15: TACACS+ Settings for the CTPView Web Interface

Field	Function	Your Action
Status	Specifies whether TACACS+ is enabled or disabled. TACACS+ is disabled by default.	Select one. • Enabled • Disabled
Dest Port	TACACS+ uses the TCP port for sending and receiving data. Port 49 is reserved for TACACS+ and is the default port.	Enter the destination port number.
Timeout	Time in seconds that the TACACS+ client should wait for a response from the TACACS+ server after sending the authentication and authorization request. Timeout value applies to all the TACACS+ servers that are configured. The default timeout value is 5 seconds.	Specify a value.
Off-Line-Failover	You can use the local authentication credentials if the configured TACACS+ servers are unavailable or no response is received from the TACACS+ servers. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct
Reject-Failover	You can use the local authentication credentials if the TACACS+ server rejects the attempt to authenticate. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct

Table 15: TACACS+ Settings for the CTPView Web Interface *(Continued)*

Field	Function	Your Action
Servers	You can configure up to 10 TACACS+ servers each for CTPOS and CTPView users for authentication and authorization. CTP tries to authenticate the user from the first server in the list. If the first server is unavailable or fails to authenticate, then it tries to authenticate from the second server in the list, and so on. Authorization is done on the server that successfully authenticates the user.	Enter the IP address of the server, and specify a shared secret.
Shared Secret	Shared secret is the secret key that TACACS+ servers use to encrypt and decrypt packets that are sent and received from the server. TACACS+ clients use the same secret key to encrypt and decrypt packets.	Specify the shared secret.

To configure RADIUS from the CTPView web interface:

1. In the side pane, select **System** > **Configuration**.
2. Click **Node Settings** > **RADIUS Settings** tab.

   The RADIUS Settings page is displayed.
3. Configure the parameters described in Table 16 on page 143 and click **Submit Settings**.
4. (Optional) Click **System** > **Query** > **Node Settings** to verify the RADIUS configuration details.

   Table 16: RADIUS Settings for the CTPView Web Interface

Field	Function	Your Action
Status	Specifies whether RADIUS is enabled or disabled. RADIUS is disabled by default.	Select one. • Enabled • Disabled

Table 16: RADIUS Settings for the CTPView Web Interface *(Continued)*

Field	Function	Your Action
Dest Port	RADIUS uses the TCP port for sending and receiving data. Port 49 is reserved for RADIUS and is the default port.	Enter the destination port number.
Timeout	Time in seconds that the RADIUS client should wait for a response from the RADIUS server after sending the authentication and authorization request. Timeout value applies to all the RADIUS servers that are configured. The default timeout value is 5 seconds.	Specify a value.
Off-Line-Failover	You can use the local authentication credentials if the configured RADIUS servers are unavailable or no response is received from the RADIUS servers. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct
Reject-Failover	You can use the local authentication credentials if the RADIUS server rejects the attempt to authenticate. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct
Servers	You can configure up to 10 RADIUS servers each for CTPOS and CTPView users for authentication and authorization. CTP tries to authenticate the user from the first server in the list. If the first server is unavailable or fails to authenticate, then it tries to authenticate from the second server in the list, and so on. Authorization is done on the server that successfully authenticates the user.	Enter the IP address of the server, and specify a shared secret.
Shared Secret	Shared secret is the secret key that RADIUS servers use to encrypt and decrypt packets that are sent and received from the server. RADIUS clients use the same secret key to encrypt and decrypt packets.	Specify the shared secret.

Configuring NTP and Syslog over IPv6 on CTP Node (CTPView)

IN THIS SECTION

Following are the pre-requirements for configuring NTP and Syslog over IPv6 on CTP node:

- CTP should be configured to either “IPv6 only” or “IPv4 and IPv6” protocol as shown below:

```
Hostname: ctp_90

Protocols supported:   IPV4 & IPV6

Default network device (eth0: 10/100/1000 Copper (right back)) IPV4 parameters:
        ipaddress:  10.216.118.90
        netmask:    255.255.254.0
        default gw: 10.216.119.254
        mtu:        1500 bytes

Default network device (eth0: 10/100/1000 Copper (right back)) IPV6 parameters:
        ip6addr:    2001:418:9802:ffee::90/48
        ip6mtu:     1500 bytes
        ipv6gw:     2001:418:9802:ffee::1
```

- The NTP or Syslog server should be configured with an IPv6 address.

Configuring NTP (without Authentication) over IPv6 on CTP Node

To configure NTP (without authentication) over IPv6 on CTP node using CTPView:

1. In the side pane, select **System** > **Configuration**. The **System Configuration** page appears.
2. Click the **Node Settings** tab.
3. Under the **NTP Settings** section, enter the first IPv6 server address in the **1st** field. If required, enter the second IPv6 server address in the **2nd** field.

4. Leave the **Key ID** and **Key Value** fields blank.

5. Change the Status to **Enabled**, and then click **Submit Settings**.

   After submitting the NTP settings, CTP node tries to synchronize with the first NTP server. Upon successful synchronization, the date or time of CTP node is changed to the respective date or time of the first NTP server. If the CTP node is unable to synchronize with the first server, it tries to synchronize with the second NTP server. Upon successful synchronization with the second NTP server, the date or time of the CTP node is changed to the respective date or time of the second NTP server.

Configuring NTP (with Authentication) over IPv6 on CTP Node

It is assumed that the shared secret key is already being communicated between client and server and it is the responsibility of the server to have the shared secret keys already configured in their conf and keys files.

If CTPView acts as NTP server, make sure that the line “trustedkey 1” (here 1 is key ID, some other key ID can also be used) is added in the **/etc/ntp.conf** of CTPView server. The line “1 M juniper” (here 1 is key ID and juniper is key, some other key and key ID can also be used) should be mentioned in the **/etc/ntp/keys**, and ntpd should be started in CTPView server.

To configure NTP with authentication over IPv6 on CTP node using CTPView:

1. In the side pane, select **System** > **Configuration**. The **System Configuration** page appears.
2. Click the **Node Settings** tab.
3. Under the **NTP Settings** section, enter the first IPv6 server address in the **1st** field. If required, enter the second IPv6 server address in the **2nd** field.
4. Enter key ID and key values in the **Key ID** and **Key Value** fields, respectively. The key ID should be unique for both NTP servers.
5. Change the Status to **Enabled**, and then click **Submit Settings**.

   4. After submitting the NTP settings, CTP node tries to synchronize with the first NTP server. Upon successful synchronization, the date or time of CTP node is changed to the respective date or time of the first NTP server. If the CTP node is unable to synchronize with the first server, it tries to synchronize with the second NTP server. Upon successful synchronization with the second NTP server, the date or time of the CTP node is changed to the respective date or time of the second NTP server.

Configuring Syslog over IPv6 on CTP Node

To configure Syslog over IPv6 on CTP Node:

1. In the side pane, select **System** > **Configuration**. The **System Configuration** page appears.
2. Click the **Node Settings** tab.

3. Under the **Syslog Settings** section, enter the first IPv6 server address in the **1st** field. If required, enter the second IPv6 server address in the **2nd** field.
4. Change the Status to **Enabled**, and then click **Submit Settings**.
5. After submitting the Syslog settings, monitor the **/var/log/messages** of both the syslog servers. The CTP logs should be displayed in syslog servers as shown below:

```
[root@ctp_90 /tmp 19]# t
Jun 22 18:23:33 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: RUNNING to DISABLD
Jun 22 18:23:34 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: DISABLD to NoSYNC
Jun 22 18:23:35 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: NoSYNC to InSYNC
Jun 22 18:23:36 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: InSYNC to RUNNING

Logs in Syslog Servers
[juniper_sa@ctpview log 30]$ tail -f /var/log/messages
Jun 22 18:23:33 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: RUNNING to DISABLD
Jun 22 18:23:34 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: DISABLD to NoSYNC
Jun 22 18:23:35 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: NoSYNC to InSYNC
Jun 22 18:23:36 ctp_90 ctpd: 7      util_prt_psc: se-0/2  B4 St Chg: InSYNC to RUNNING
```

Configuring NTP over IPv6 on CTPView Server (CTPView)

IN THIS SECTION

Following are the pre-requirements for configuring NTP over IPv6 on CTPView:

- CTPView should be configured to either “IPv6 only” or “IPv4 and IPv6” protocol as shown below:

```
Hostname: ctpview

Domain: (none)

Protocols supported:   IPV4 & IPV6
```

```
Default network device (eth0: ) IPV4 parameters:
        ipaddress:  10.216.118.98
        netmask:    255.255.254.0
        default gw: 10.216.119.254
        mtu:        1500 bytes

Default network device (eth0: ) IPV6 parameters:
        ip6addr:    2001:418:9802:ffee::98/48
        ip6mtu:     1500 bytes
        ipv6gw:     2001:418:9802:ffee::1
```

- The NTP server should be configured with an IPv6 address.

Configuring NTP over IPv6 on CTPView

To configure NTP over IPv6 on CTPView:

1. In the side pane, select **Server** > **Administration**. The Administrative Functions pane is displayed.
2. Click **NTP Server Configuration**. The NTP Server Settings window is displayed.
3. Under the **Manage NTP Peers** section, enter the IPv6 address of NTP server, and then click **Add New NTP Peer**.

   A popup of “Successfully added peer” is displayed.
4. Click **OK** and wait for 3 to 5 minutes. Then, click **Refresh Page**.

   Under the **Summary of NTP Servers Peers** section, verify that the CTPView server is synchronized successfully with the added NTP server.
5. You can also manually synchronize CTPView server with NTP server by selecting the already added NTP peer from the **Select a peer to manually sync to:** list and then clicking the **Sync to Selected Peer** button.

   After clicking **Sync to Selected Peer**, a popup of “The CTPView server clock has been manually synchronized to peer” should be displayed. Wait for 3 to 5 minutes, and then click the **Refresh Page** button. Under the **Summary of NTP Servers Peers** section, verify that CTPView server is synchronized successfully with the added NTP server.

Configuring NetRef Settings (CTPView)

NetRef primary backup operation involves a new packet flow from the primary node to all the backup nodes. These timing packets are sent at a rate of approximately 4.5 packets per second.

NOTE: In this topic, the terms *Primary* and *Backup* refer to primary and client operations or nodes, respectively.

To configure network node reference with primary and backup operation using the Node Configuration page of CTPView:

1. In the side pane, select **Node** > **Node Config**.
2. Configure the parameters described in Table 17 on page 149 and click **Submit Configuration**.
3. (Optional) Click **Node** > **Node Query** to verify the NetRef primary and backup node configuration details.

Table 17: Node Configuration Settings Page in CTPView

Field	Function	Your Action
Port Providing Reference	Specifies whether you want to enable or disable the NetRef primary node to function as the reference port providing frequency for clock synchronization. You need to specify this value for the **1st Priority Reference 0**, **2nd Priority Reference 1**, **3rd Priority Reference 2**, **4th Priority Reference 3**, and **5th Priority Reference 4** fields to specify the reference clocks for the primary nodes with corresponding priorities.	Select **Yes** or **No** to enable or disable the primary node to function as the reference clock.
Reference Frequency	Specifies the frequency to be used for the reference clock or the primary node. You need to specify this value for the **1st Priority Reference 0**, **2nd Priority Reference 1**, **3rd Priority Reference 2**, **4th Priority Reference 3**, and **5th Priority Reference 4** fields to specify the reference clocks for the primary nodes with corresponding priorities.	Select a reference frequency in the range from 32 Khz through 4096 KHz. You can configure the CTP systems by using the menu interface to provide multiple prioritized node clock references. An external reference input and any of the serial interfaces may be used for the node reference clock. Reference frequencies must be 32 KHz, n x 64 KHz, or 1,544 KHz up to a maximum of 4096 KHz (2048 KHz maximum on the CTP1002).

Table 17: Node Configuration Settings Page in CTPView *(Continued)*

Field	Function	Your Action
NetRef: Slave	Specifies the client node for which multiple primary nodes are associated for receiving clock synchronization information.	Select the client node to be locked to the different primary nodes.
Master IP (Priority # 1)	Specifies the IP address of the primary node with priority 1.	Enter the IP address of the primary node with priority 1.
Master IP (Priority # 2)	Specifies the IP address of the primary node with priority 2.	Enter the IP address of the primary node with priority 2.
Master IP (Priority # 3)	Specifies the IP address of the primary node with priority 3.	Enter the IP address of the primary node with priority 3.
Master IP (Priority # 4)	Specifies the IP address of the primary node with priority 4.	Enter the IP address of the primary node with priority 4.
32 kHz Reference Output	Specifies whether you want to enable the reference output signal.	Select the **Enable** check box if it is already disabled.
Clock Main RTM	Specifies the clock rear transition module (RTM) used to input a reference clock into the CTP2000 platform.	Select a value from the Port DB25 drop-down list to use clock module RTM.

Configuring Automatic Monitoring of CTP Platforms (CTPView)

IN THIS SECTION

You can configure certain monitoring operations to be automatically performed on the CTP platforms in the network. You manage these operations in the CTPView Automatic Functions window. This window displays a summary table of the currently configured automatic settings for the connected CTP platform. Table 18 on page 151 describes the information provided in the table. From this window you can add and remove automatic operations for the CTP platform, and configure the monitoring details.

Table 18: Current CTPView Automatic Settings

Field	Description
Action	One of the following monitoring operations: • Backup Current PostgreSQL Database. • Gather Remote Host Statistical Data—Retrieves the data used to create the plots of IP Buffer Usage, Delay Jitter, Round Trip Delay, and Missing Packets. • Update Network Interface Device Information—Collects network interface device information. Use this automatic function if you configure virtual IP addresses using the CLI or if you use multiple CTPView servers to configure CTP platforms and virtual IP addresses. • Remove Outdated Files—Removes older files (typically CTP platform statistical data) based on the age of the data. The age criterion can be set to 6, 9, or 12 months. We recommend that you configure this automatic function to ensure that the file system does not become filled. • Synchronize Secondary Servers—Copies information from the primary server to each secondary server. The information includes SSH keys, archived port configurations, email notifications, port forwarding settings, trigger point for hard drive usage warning level, and CTP platform identification information (IP address, hostname, group name). • Synchronize Secondary Servers and Remote Hosts—Copies information from the primary server to each secondary server and CTP platform. The information transferred to the secondary servers includes SSH keys, archived port configurations, email notifications, port forwarding settings, trigger point for hard drive warning usage level, CTP identification information (IP address, hostname, group name), and CTP statistical data. The function copied from the primary server to CTP platforms includes each secondary server's SSH key. • Save Current CTP Host System Configuration—Saves every CTP platform configuration at the specified time interval. CTPView will save the 10 most recent configurations.

Minute	Minute of the hour when the operation is scheduled to take place.
Hour	Hour of the day when the operation is scheduled to take place.
Day	Date when the operation is scheduled to take place.
Month	Month when the operation is scheduled to take place.
Day of Week	Day of the week when the operation is scheduled to take place.

Accessing the CTPView Automatic Functions Window (CTPView)

To configure automatic functions:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **Automatic Functions**.

   The CTPView Automatic Functions window is displayed.

Adding an Automatic Monitoring Operation (CTPView)

To add an automatic monitoring operation:

1. In the CTPView Automatic Functions window, select an action.
2. Select when you want the operation to take place.

   The numbers you select represent a specific time, not an interval of time. For example, the default setting of [0,1,ANY,ANY,ANY] means that action occurs at the 0 minute (on the hour) of the first hour (1 AM) every day (any day of any month, landing on any day of the week). A setting of [30,16,8,ANY,ANY] causes the action to occur at 4:30 PM on the 8th of every month.
3. Click **Add New Entry**; the operation appears in the summary table.

   If you decide not to add the entry, click **Reset**.

To have the same function performed at different times, add a new entry for that operation for each time.

Removing an Automatic Monitoring Operation (CTPView)

To remove an automatic monitoring operation:

1. In the summary table in the CTPView Automatic Functions window, click the **Remove** checkbox for each action you want to remove.

2. Click **Remove Selected Lines**; the operation disappears from the summary table.

Backing Up MySQL Database and Restoring in PostgreSQL (CTPView Server CLI)

Starting from CTPView 7.3R6 release, CTPView server uses PostgreSQL database and does not support MySQL database. You can backup the current MySQL database data and restore it in the PostgreSQL database while migrating from CTPView 7.3R5 or earlier release to CTPView 7.3R6 or later release.

To backup the current MySQL database data and restore it in the PostgreSQL database:

1. Log in to the CTPView Server of release 7.3R5 or earlier.
2. Copy the **backup_mysql_db.tcsh** script which is located at **/data/archive/gui/GUI_7.3R6** to the **/tmp** directory.
3. Go to the **/tmp** directory and run the script.

   You need to provide the password of MySQL Apache user account as an argument to run this script. If no password argument is provided, the script automatically takes the default password "CTPView-2-2".

```
[juniper_sa@ctpview /tmp 40]$ sudo ./backup_mysql_db.tcsh "CTPView-1-1"

>>>>>>   MySQL Backup Complete.   <<<<<<

    Backup file is present at the following path
  /var/www/html/acorn/backup_files/backup_mysql.sql
```

   The created backup file is stored at **/var/www/html/acorn/backup_files/backup_mysql.sql**.
4. Copy the created backup file to the **/tmp** directory of CTPView server release 7.3R6 or later.
5. Log in to the CTPView server of release 7.3R6 or later and access the CTPView Configuration Menu.
6. Select **PostgreSQL Functions**, and then select **Restore Backup in PostgreSQL**.
7. Select **Restore MySQL Backup**. An error message will be displayed if the backup file is not available in the **/tmp** directory.

```
************************************************************
     CTPView version 7.3R6_RC2 190725
     Server: ctpview    Date: Fri Aug  9 19:25:19 2019
     Release: CentOS release 5.11 (Final)
     Kernel: 2.6.18-419.el5
     User root logged in from 10.212.174.83 as root
     +++++  ALL  ACTIONS  ARE  LOGGED  +++++
************************************************************
```

```
Restore Function Menu

Please choose a menu item from the following list:

0) Return to previous menu
1) Restore PostgreSQL Backup
2) Restore MySQL Backup

Please input your choice [0]: 2
backup_mysql.sql
is present

You will now be asked for the password of the PostgreSQL Apache account:

Password for user ctpview_psql:
UPDATE 1
SET
SET
UPDATE 1
SET
SET
UPDATE 1
SET
SET
UPDATE 1

.
.
.
Restoration successful.

Hit return to continue...
```

After successful restoration, you can log in to the CTPView GUI and verify the database entries under the CTPView Admin Centre.

Backing Up and Restoring PostgreSQL Database (CTPView)

To backup and restore the current PostgreSQL database data:

NOTE: Starting from CTPView 7.3R6 release, CTPView server uses PostgreSQL database and does not support MySQL database.

1. Log in to the CTPView GUI.
2. In the CTPView Automatic Functions window, select the action **Backup Current PostgreSQL Database**.
3. Select the date and time when you want the operation to take place.

   The numbers you select represent a specific time, not an interval of time. For example, the default setting of [0,1,ANY,ANY,ANY] means that action occurs at the 0 minute (on the hour) of the first hour (1 AM) every day (any day of any month, landing on any day of the week). A setting of [30,16,8,ANY,ANY] causes the action to occur at 4:30 PM on the 8th of every month.
4. Click **Add New Entry**; the backup operation appears in the summary table. After the backup operation is complete, verify that the backup file is created in **/var/www/html/acorn/backup_files**.

   In the following example, **pgsql_0** is the created backup file.

```
[juniper_sa@ctpview backup_files 45]$ pwd
/var/www/html/acorn/backup_files

[juniper_sa@ctpview backup_files 46]$ ls
index.html  pgsql_0
```

5. Log in to the CTPView server and access the CTPView Configuration Menu.
6. Select **PostgreSQL Functions**, and then select **Restore Backup in PostgreSQL**.
7. Select **Restore PostgreSQL Backup**. This lists the available PostgreSQL backup files.
8. Select the PostgreSQL backup file you want to restore.

```
************************************************************
     CTPView version 7.3R6_RC2 190725
     Server: ctpview    Date: Fri Aug  9 19:15:42 2019
     Release: CentOS release 5.11 (Final)
     Kernel: 2.6.18-419.el5
     User root logged in from 10.212.174.83 as root
     +++++  ALL  ACTIONS  ARE  LOGGED  +++++
************************************************************

Restore Function Menu

Please choose a menu item from the following list:
```

```
0) Return to previous menu
1) Restore PostgreSQL Backup
2) Restore MySQL Backup

Please input your choice [0]: 1

Following are the available PostgreSQL backup directories:
pgsql_0

Please choose one of the backup directory from the above list to restore the PostgreSQL DB:
pgsql_0
pgsql_0
is present

Restoration successful

Hit return to continue...
```

After successful restoration, you can log in to the CTPView GUI and verify the database entries under the CTPView Admin Centre.

RELATED DOCUMENTATION

Setting a Limit on File Transfer Bandwidth Between the CTPView Server and CTP Platforms (CTPView) | **156**

Synchronizing Multiple CTPView Servers (CTPView) | **159**

Setting a Limit on File Transfer Bandwidth Between the CTPView Server and CTP Platforms (CTPView)

You can specify a limit on the bandwidth used for file transfers between the CTPView server and the CTP platforms in the network. The maximum throttle rate allowed on the server's Ethernet port is 100,000 Kbps. By default, the *bandwidth throttling* value is set to 800 Kbps. Throttling the bandwidth is typically not necessary and may be required only when the local LAN segment experiences significant load and bandwidth limitations.

The following functions are affected by bandwidth throttling:

- Gathering statistical data for plots

- Synchronizing secondary CTPView servers
- Saving CTP platform configurations
- Modifying CTP platform login banners
- Upgrading the CTP operating system software
- Network monitoring

> **NOTE**: The bandwidth throttling configuration has no effect on data packet throttling.

To configure the bandwidth limit:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **Automatic Functions**.

   The CTPView Automatic Functions window is displayed, and shows the current value for bandwidth throttling for the CTPView server.
3. Select a new throttling value.

   Valid values are: 100, 200, 500, 800, 1000, 2000, 5000, 8000, 10000, 20000, 50000, 80000, and 100000 Kbps.
4. Click **Modify Throttle Value**.

RELATED DOCUMENTATION

Configuring Automatic Monitoring of CTP Platforms (CTPView) | **150**

Restoring CTPView Software Configuration Settings and Data (CTPView)

This topic lists two methods to restore the CTPView software configuration settings and data. Typically you restore this information only after one of the following events has occurred:

- An installation of the latest version of the CTPView server operating system, which reformats the server's hard drives.
- In the unlikely event of a data loss.

Use one of the following methods to restore saved CTPView information:

- Use the CTPView restore utility in the CTPView server menu. You must use this method when you have only a single CTPView server.

  See "Restoring CTPView Software Configuration Settings and Data with the Restore Utility (CTPView Server Menu)" on page 20.

- Synchronize the server. This method is available only when you have two or more CTPView servers in your network.

  See "Restoring CTPView Software Data by Manually Synchronizing the CTPView Server (CTPView)" on page 21.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Data by Manually Synchronizing the CTPView Server (CTPView)

This topic describes how to use CTPView server synchronization to restore the CTPView software configuration settings and data.

To restore your saved information by synchronizing the CTPView server with another server:

1. Log in to the CTPView GUI on the server for which you are restoring the data.
2. In the side pane, select **Server > Administration** to display the Administrative Functions pane.
3. Click **Server Synchronization**.
4. Verify that the server is either not listed or its Server Type is set to Not Selected.
5. Log in to the CTPView GUI on the server from which you are restoring the data.
6. In the side pane, select **Server > Administration** to display the Administrative Functions pane.
7. Click **Server Synchronization**.
8. Ensure that the Server Type is set to Primary Server for this server, Secondary Server for the server being updated, and Not Selected for all other CTPView servers listed.
9. Click **Manually Synchronize Network**.

   The Synchronize Secondary Servers window opens.
10. Click **Select All Hosts**, and then click **Synchronize Servers**.
11. When the synchronization is completed, restore the Server Type for all CTPView servers to the values that you normally use for your network.

Using CTPView server synchronization, you can restore the following CTPView configuration settings and data:

- AutoSwitch configuration for CTP devices
- Configuration of CTP devices on CTPview (addition of CTP devices in groups)
- Configuration of remote bundles (CTP, SAToP, and CESoPSN)
- Network monitoring configuration on CTPView
- NTP configuration for CTP devices
- RADIUS configuration for CTP devices
- Syslog configuration for CTP devices
- SNMP and SNMP trap configurations for CTP devices

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Configuration Settings and Data (CTPView) | 20

Synchronizing Multiple CTPView Servers (CTPView)

IN THIS SECTION

When you have more than one CTPView server in your network, you can synchronize some or all of the servers to the same configuration. You must designate one server as the primary server and the others as secondary servers. When you add a secondary server, the primary server sets up SSH authorization keys with the secondary server so it can communicate without requiring the login password again. The server configuration settings apply only to the server you are logged in to. These settings do not affect the other CTPView servers in the network.

The primary server has a 15-second period to establish contact with a remote CTP platform. If the period times out, the primary server skips to the next remote CTP platform and continues executing the program. This information is displayed in the screen output and logs. When you add a new remote CTP platform to a primary server, the new platform's SSH RSA keys are also exchanged with each secondary server. You can disable this feature in the Administrative Functions pane when you add the new remote platform.

The following definitions are restricted in scope to the server that you are logged in to. Each server maintains its own file of server designations that it refers to when performing a server synchronization. You do not need to configure settings on a remote secondary server for that server to be updated by the primary server that is performing the synchronization.

- Primary server—You can designate any server running the correct CTPView software version as a primary server. The primary server runs the synchronization program and distributes data to the secondary servers. Regardless of how any other server is configured, the data on a primary server cannot be overwritten by any other server running the server synchronization program.
- Secondary server—On the primary server, you can designate any server running the correct CTPView software version as a secondary server. Synchronization updates the data files on the secondary server to match the files on the primary server.
- Data files—Synchronization applies to statistical history archived from the CTP platforms and the information needed to communicate with the platforms: IP addresses, hostnames, host menus, and SSH authorization keys.

NOTE: Server synchronization is supported only on CTPView 1.4.2 or higher releases.

Configuring a CTPView Server Synchronization Network (CTPView)

You must identify a primary server and one or more secondary servers as members of a synchronization network.

To configure your synchronization network:

1. Log in to the CTPView server selected to be the primary server.
2. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
3. Click **Server Synchronization**.

   The Server Synchronization pane is displayed.
4. In the Add Network Server section, type the information required for the primary server: IP address, name, admin login name, and login password, and click **Add New Server**.

   The primary server information is displayed in the Current Server Synchronization Settings table. The server name is used for display purposes only and does not need to be the server's UNIX hostname.

5. Add the same information to the table for each of the additional CTPView servers in your network that you want to synchronize with the primary server.
6. In the Current Server Synchronization Settings table, select a server type for each server: **Primary Server** for the primary CTPView server, and **Secondary Server** for each of the secondary servers.

   The primary server must be the server you are currently logged in to.
7. (Optional) Set the server type to **Not Selected** when you want to temporarily remove a server from the synchronization process.

   To add this server back to the synchronization network, select **Secondary Server** for the server type.
8. (Optional) Click the **Remove** box to remove a server from the synchronization network.

   The server is deleted from the table. If you later want this server to be part of the synchronization network, you must add it back to the table.
9. Click **Commit Changes** to save this configuration.

   If you want to restore the original settings in the table, click **Reset** instead of **Commit Changes**.

Synchronizing the CTPView Server Network Automatically (CTPView)

To automatically synchronize your network:

1. In the Server Synchronization pane, click **Set Automatic Functions**.

   The CTPView Automatic Functions pane is displayed.
2. Select **Synchronize Secondary Servers and Remote Hosts** or **Synchronize Secondary Servers**.

   When the secondary servers and the CTP platforms are synchronized, the CTPView software copies the necessary SSH keys to each secondary server so that it can communicate with the CTP platforms without requiring the login password to be entered. When only the secondary servers are synchronized, only server-specific information Is synchronized.
3. Select when you want the operation to take place.

   The optimal configuration runs the synchronization shortly after the statistical data is obtained from the CTP platforms. The numbers you select represent a specific time, not an interval of time. For example, the default setting of [0,1,ANY,ANY,ANY] means that synchronization occurs at the 0 minute (on the hour) of the first hour (1 AM) every day (any day of any month, landing on any day of the week). A setting of [30,16,8,ANY,ANY] causes the synchronization to occur at 4:30 PM on the 8th of every month.
4. Click **Add New Entry**; the operation appears in the summary table.

   If you decide not to add the entry, click **Reset**.

To have the same function performed at different times, add a new entry for that operation for each time.

Synchronizing the CTPView Server Network Manually (CTPView)

To manually synchronize your network:

1. In the Server Synchronization pane, click **Manually Synchronize Network**.

   The Synchronize Secondary Servers window is displayed.
2. (Optional) Click the name of the CTP platform on which you want to check the SSH RSA keys during synchronization.

   You can select more than one platform by holding down the Ctrl key when you click the platform names. Alternatively, you can click **Select All Hosts** to select all the listed CTP platforms.
3. Click **Synchronize Servers**.

SEE ALSO

Configuring Automatic Monitoring of CTP Platforms (CTPView) | **150**

Restoring CTPView Software Data by Manually Synchronizing the CTPView Server (CTPView) | **21**

Establishing an SSH Connection (CTP Menu)

You can establish a secure connection to any CTP device to administer and maintain it remotely over the network. You can establish an SSH connection to a remote host from the CTPMenu by specifying the IP address of the remote host. You can also use the CTPView Node Maintenance window to establish an SSH session to a host. This topic describes how to establish a secure connection to a remote host from the CTPMenu.

NOTE: Only system administrators are allowed to establish SSH connections to other devices.

To establish an SSH connection to a remote host from the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **7) ssh to another host**.
3. When prompted, enter the IP address of the host to connect to that host.

Adding a VLAN Interface to a Node (CTP Menu)

IN THIS SECTION

This topic describes how add a VLAN interface to a node. Adding VLAN interfaces to a node comprises two steps:

Adding a VLAN ID to the System

When you add a VLAN to a node, the network and CTP devices are restarted to update the network parameters. The node is not restarted.

> **NOTE**: For VLAN failover to function correctly, VLANs must be configured on the primary Ethernet interface (for example, eth1) that has IPv4 configured and Ethernet failover enabled.

To add a VLAN ID to the system from the CTP Menu:

1. From the Main Menu, select **5) Node Operations** > **3) Configure network settings** > **8) VLAN Configuration**.

```
==========================================================================
= (ctp_90 05/08/14 23:03:48 WST) | Network Configuration Menu
==========================================================================
Please select a number from the following list:
-------------------------------------
0) Back to Previous Menu
1) Supported Protocols: IPv4 only
2) IPv4 Configuration
3) IPv6 Configuration
4) Virtual IP addresses
5) OAM port (IPv4): 16
6) CTP Bndl Data pkt protocol: 47
7) CTP Bndl OAM port (IPv6): 32
8) VLAN Configuration
```

```
9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [0]: 8
***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
*** system may not be reachable via the network
*** after the network restarts.
***
Are you sure? y[n]: y
Exsisting VLAN interfaces :
No VLAN is configured yet
How do you want to change VLANs (add/delete/quit) ? (rtn for show): add
Which ethernet port the new VLAN will be added on? (0-3)[0] 1
What is the new VLAN id? (0-4095)[0] 111
Exsisting VLAN interfaces :
eth1.111: Vlan ID 111 on ethernet port 1
How do you want to change VLANs (add/delete/quit) ? (rtn for show): quit
```

2. Follow the onscreen instructions and configure the options as described in Table 19 on page 164.

Table 19: Configuring a VLAN Interface

Field	Function	Your Action
How do you want to change VLANs ?	Enter `add` to add a new VLAN, `delete` to remove a VLAN, and `rtn` to show existing VLANs.	Enter `add` to create a new VLAN.

Table 19: Configuring a VLAN Interface *(Continued)*

Field	Function	Your Action
Which ethernet port the new VLAN will be added on ?		Specify the ethernet port number. The default value is 0 (zero).
What is the new VLAN id ?		Assign the VLAN ID for the newly created VLAN in the range 0–4095. The default value is 0 (zero).

Configuring VLAN Interface by Using the VLAN ID

1. From the Main Menu, select **5) Node Operations** > **3) Configure network settings** > **2) IPv4 Configuration** to assign an IP address for the VLAN.

```
==========================================================================
= (ctp_90 05/08/14 23:09:40 WST) | Network Configuration Menu
==========================================================================
Please select a number from the following list:
-------------------------------------
0) Back to Previous Menu
1) Supported Protocols: IPv4 only
2) IPv4 Configuration
3) IPv6 Configuration
4) Virtual IP addresses
5) OAM port (IPv4): 16
6) CTP Bndl Data pkt protocol: 47
7) CTP Bndl OAM port (IPv6): 32
8) VLAN Configuration
9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [8]: 2
***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
```

```
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
*** system may not be reachable via the network
*** after the network restarts.
***
Are you sure? y[n]: y
There are 2 ethernet devices available for use. The default device
is the device through which the default gateway can be accessed.
Ctp circuits can run over any ethernet device, default or not.
A default device must be configured, other devices may be configured
and enabled, or disabled. Here is a list ot the available devices
and their descriptions:
Copyright © 2014, Juniper Networks, Inc. 3
eth0: 10/100/1000 Copper (right back)
eth1: 10/100/1000 Copper (left back)
List of VLAN interface :
eth1.111: Vlan ID 111 on ehternet port 1
What device would you like to make the IPV4 default device? (rtn for eth1):
OK, eth1 (10/100/1000 Copper (left back)) will be configured as IPV4 default
device.
Please input the hostname (return for ctp_90):
===== Configuration for eth0:
Activate IPV4 interface eth0 on boot [n]
===== Configuration for eth1 (default device):
Please input the ip (return for 10.216.118.90):
Please input the netmask (return for 255.255.254.0):
Please input the gateway (return for 10.216.119.254):
Please input the mtu in bytes (return for 1500):
Add route to interface eth1 [n]
IPV4 configuration for VLAN interfaces :
===== Configuration for eth1.111:
Activate IPV4 interface eth1.111 on boot [n] y
Please input the ip (return for 10.0.0.1): 1.1.1.1
Please input the netmask (return for 255.255.255.0):
Please input the mtu in bytes (return for 1500):
Add route to interface eth1.111 [n]
```

2. Follow the onscreen instructions and configure the options as described in Table 20 on page 167.

Table 20: IP Parameters for Configuring a VLAN

Field	Your Action
What device would you like to make the IPv4 default device ?	Select the default Ethernet device.
Please input the hostname.	Specify the host name. Press **Enter** to select the default hostname. **NOTE**: 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 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.
Activate the IPv4 interface eth0 on boot.	Enter `n`. Ethernet failover may not work correctly if multiple Ethernet interfaces are activated or the active Ethernet interface is configured as the secondary interface.
Configuration for eth1 (default device)	Enter the IP address, network mask, gateway, and MTU for eth1.
Activate the IPv4 interface eth1.111 on boot.	Enter `y`.
Configuration for eth1.111	Enter the IP address, network mask, and MTU for eth1.111.

Separate Interfaces for Management and Circuit Traffic Overview

IN THIS SECTION

Until CTPOS and CTPView Release 7.1, only one network device (the default device) is used for both management and circuit data. In certain network topologies, a segregation is required between the circuit or Ethernet traffic and management traffic. Therefore, separate interfaces need to be used for the management and circuit networks so that traffic segregation can be achieved at the physical interface level. Starting with CTPOS Release 7.2, support for configuring two default gateways, one for management traffic and the other for circuit device, is available, which enables circuit and management traffic to be segregated.

The functionality to segregate management and circuit traffic requires at least two Ethernet devices—one for circuit traffic and the other for management traffic. When this feature is enabled, both management and circuit interfaces are required to be configured. Segregation of traffic is performed on the basis of the management and circuit device or interface. CTP devices that support two default gateways are required—one for management device and other for circuit device. Each interface replies to incoming packets via its own default gateway. All incoming and outgoing packets in the circuit network traverse through the circuit device gateway (main default gateway). All incoming and outgoing packets in the management network traverse through the management device gateway.

For having two default gateways, policy-based routing is required. Policy-based routing enables the creation of multiple routing tables, one for each interface. Policy-based routing provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator. This capability enables you to implement policies that selectively cause packets to take different paths. For circuit traffic, the main routing table, inet.0 is referred and for management traffic, the newly-created policy-based routing table is referred. The policy-based routing table is used, based on a set of rules. Using the main routing table for circuit device enables any IP table-related changes for the SAToP and CESoPSN bundles to be avoided. An entry of this newly created policy-based routing table is stored at **/etc/iproute2/rt_tables**.

The “IPV4 configuration” under “Config Network Settings” menu is modified to enable the configuration of different interfaces for management traffic and circuit or Ethernet traffic. The Display network settings menu is modified to display the circuit and management network devices. A separate conf file is implemented to indicate the status of this feature (whether it is enabled or not). Apart from feature status, this configuration file also stores information related to circuit and management device. With this feature to distinguish management and circuit traffic, Ethernet failover is supported only on the circuit

interface and not on the management interface. This feature cannot be activated during the first boot process.

After the management device is selected, a new policy based routing table is created for this device. For example, if the routine table is named 10 tab-eth0, 10 denotes the route table number and tab-eth0 signifies the route table name created for management device eth0. This table is referred according to the rule specified in the rule-eth0 file.

The following command displays the main route table and the newly created policy based route table “tab-eth0”:

```
[root@ctp_90 ctp_cmd 2]# ip route show  tab main
1.1.1.0/24 dev eth0  scope link
10.216.118.0/23 dev eth1  scope link
169.254.0.0/16 dev eth1  scope link
127.0.0.0/8 dev lo  scope link
default via 10.216.119.254 dev eth1
```

```
[root@ctp_90 ctp_cmd 3]# ip route show  tab tab-eth0
1.1.1.0/24 dev eth0 scope link
default via 1.1.1.3 dev eth0
```

The following command displays the rules added for the policy-based route table:

```
[root@ctp_90 ctp_cmd 4]# ip rule show
0:      from all lookup local
32764:  from all to 1.1.1.1 lookup tab-eth0
32765:  from 1.1.1.1 lookup tab-eth0
32766:  from all lookup main
32767:  from all lookup 253
```

When this feature is disabled, the IP config/query section in the CTP Menu does not display the option for segregating management and circuit traffic.

Operations Performed When Management and Circuit Traffic Are Segregated

When you activate the feature to separate management and circuit traffic, you are prompted to enter the default circuit and default management device. If you enter the same device for both management

and circuit devices, an error message is displayed stating that you need to define different devices for circuit and management traffic. When you enter a correct management device (say ethX), a reference for the policy-based routing table is created for management device. An entry of its route-table number and route-table name is added in /etc/iproute2/rt_tables. This route table is referred for the management device according to the rule specified by its rule file (rule-ethX).

After you configure the management device, a route entry for its own subnet and a default gateway route for that device is added to the route- ethX file. Rules are added to rule-ethX file to handle the inbound and outbound packets through this network. The rule-ethX file contains the rules such that if any packet arrives for the management network or if any packet is originated from the management network IP address, then such a packet is transmitted through the management device gateway. An existing configuration file, **/etc/sysconfig/ctp**, is used to store this feature configuration. The configuration of this feature contains the status of this feature, circuit device name, and management device name.

The following example illustrates the contents of the **/etc/sysconfig/ctp** file:

```
[root@ctp_90 ctp_cmd 5]# cat /etc/sysconfig/ctp
CTP=yes
TARGET=yes
CTP_IP_PROTO=0
status=1
ckt_dev=eth0
mgmt_dev=eth1
```

When you disable this feature, the policy-based route table and the rules corresponding to that route table are deleted from the system and the system is configured as it was configured previously (with one default gateway). The route-ethX file and rule-ethX files are also be deleted from the system after the feature is disabled.

This feature is not supported with IPv6-only or independent IPv6 (and not a combination of IPv4 and IPv6) configuration. This limitation denotes that with IPv6 configuration settings specified on a CTP device, the option to separate management and circuit traffic is not available for configuration. If this feature is enabled on CTP150 devices, Ethernet failover cannot be activated because CTP150 devices contain only two Ethernet devices and the PCI mezzanine card (PMC) is not supported on such devices.

Configuring Separate Interfaces for Management and Circuit Traffic (CTP Menu)

In certain network topologies, a segregation is required between the circuit or Ethernet traffic and management traffic. Therefore, separate interfaces need to be used for the management and circuit

networks so that traffic segregation can be achieved at the physical interface level. Starting with CTPOS Release 7.2, support for configuring two default gateways, one for management traffic and the other for circuit device, is available, which enables circuit and management traffic to be segregated.

> **NOTE**: This feature is not supported with IPv6-only or independent IPv6 (and not a combination of IPv4 and IPv6) configuration. This limitation denotes that with IPv6 configuration settings specified on a CTP device, the option to separate management and circuit traffic is not available for configuration. If this feature is enabled on CTP150 devices, Ethernet failover cannot be activated because CTP150 devices contain only two Ethernet devices and the PCI mezzanine card (PMC) is not supported on such devices.

To configure separate interfaces for management traffic and circuit traffic on a CTP device using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **3) Configure network settings** to specify the network configuration parameters.
3. Select **2) IPv4 Configuration** to define the IPv4 attributes.
4. A message is displayed stating that you are about to modify a system parameter that requires a network restart when the configuration settings are modified. If you proceed with the configuration settings, the network automatically restarts after you complete specifying the parameters, the existing menu session is terminated, and active circuits undergo traffic drops. You must reopen a new CTP Menu session to perform additional configuration changes.

   The message alerts you that if the parameters are incorrectly defined, the system might be unreachable over the network after the system restarts. Therefore, you must exercise caution while entering the attributes. Enter **y** to proceed with defining the interfaces for management and circuit traffic.

```
Please select a number from the following list:
-------------------------------------
 0) Exit to Shell
 1) Bundle Operations
 2) Node Synchronization
 3) Node Summary
 4) Node Diagnostics
 5) Node Operations
 6) Save Running Database to Flash
------------ Your choice [3]: 5



==========================================================================
```

```
= (ctp_90 06/29/16 23:04:38  UTC) | Node Operations Menu
==========================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) Change Node Date/Time/TimeZone
 2) Display network settings
 3) Configure network settings
 4) Initialize Database
 5) Ping IP address
 6) Traceroute IP address
 8) System descriptor field:
 9) Reboot Node
10) Powerdown Node
11) Display ethernet media
12) Config ethernet media
13) Set your password
14) Config security profile
------------ Your choice [0]: 3


==========================================================================
= (ctp_90 06/29/16 23:04:38  UTC) | Network Configuration Menu
==========================================================================

Please select a number from the following list:
-------------------------------------
 0) Back to Previous Menu
 1) Supported Protocols:        IPv4 only
 2) IPv4 Configuration
 3) IPv6 Configuration
 4) Virtual IP addresses
 5) OAM port (IPv4):            16
 6) CTP Bndl Data pkt protocol: 47
 7) CTP Bndl OAM port (IPv6):   32
 8) VLAN Configuration
 9) Current Configuration (active on reboot)
10) Port operations (PBS/bridge)
11) Config port operational mode (CE/PBS/bridge)
12) Config access ip filtering
13) SNMP Configuration
------------ Your choice [0]: 2
```

```
***
*** You are about to modify a system parameter that will require
*** a network restart when complete.
***
*** If you decide to continue, the network will automatically
*** restart upon leaving the menu, existing menu session will be
*** terminated and active circuits will take traffic hits. For
*** further configuration re-initiate the menu session.
***
*** Note: If these parameters are changed incorrectly,
***       system may not be reachable via the network
***       after the network restarts.
***
        Are you sure? y[n]: y

There are 4 ethernet devices available for use. The default device
is the device through which the default gateway can be accessed.
Ctp circuits can run over any ethernet device, default or not.
A default device must be configured, other devices may be configured
and enabled, or disabled. Here is a list ot the available devices
and their descriptions:

        eth0: 10/100/1000 Copper (right back)
        eth1: 10/100/1000 Copper (left back)
        eth2: 1000 Fiber (left)
        eth3: 1000 Fiber (right)

Do you want to segregate circuit and management traffic (y/n)? [n]  y

Which device would you like to make the IPV4 default circuit device? (rtn for eth1):
OK, eth1 (10/100/1000 Copper (left back)) will be configured as IPV4 default circuit device.

Which device would you like to make the IPV4 default management device? (rtn for eth0): eth1
**** Management and Circuit Device cannot be same ****
You will be asked to enter management and circuit devices again

Which device would you like to make the IPV4 default circuit device? (rtn for eth1):
OK, eth1 (10/100/1000 Copper (left back)) will be configured as IPV4 default circuit device.

Which device would you like to make the IPV4 default management device? (rtn for eth0):
OK, eth0 (10/100/1000 Copper (right back)) will be configured as IPV4 default management
device.
```

```
Please input the hostname (return for ctp_90):

===== Configuration for eth0 (default management device):
Please input the ip (return for 127.0.0.1): 1.1.1.1
Please input the netmask (return for 255.255.255.0):
Please input the gateway (return for 127.0.0.1): 1.1.1.3
Please input the mtu in bytes (return for 1500):

Add route to interface eth0 [n]

===== Configuration for eth1 (default circuit device):
Please input the ip (return for 10.216.118.90):
Please input the netmask (return for 255.255.254.0):
Please input the gateway (return for 10.216.119.254):
Please input the mtu in bytes (return for 1500):

Add route to interface eth1 [n]

===== Configuration for eth2:

Activate IPV4 interface eth2 on boot [n]

===== Configuration for eth3:

Activate IPV4 interface eth3 on boot [n]
```

Follow the onscreen instructions and configure the options as described inTable 21 on page 175.

Table 21: Configuring Separate Interfaces for Management and Circuit Traffic

Field	Function	Your Action
Do you want to segregate circuit and management traffic (y/n)?	Specifies whether you want to enable the capability to configure separate interfaces for management and circuit traffic. Lists the previously configured Ethernet devices that are available for use in the system. The default device is the device through which the default gateway can be accessed. CTP circuits can run over any Ethernet device, such as the default or non-default devices. A default device must be configured, while other devices might be configured and enabled or disabled.	Specify `y` or `n`.
Which device would you like to make the IPV4 default circuit device?	Specifies the device or interface that you want to configure as the default circuit device for IPv4.	Specify an interface from the list of available interfaces that were previously displayed in the CTP Menu as the default circuit interface. Specify `rtn` to set the interface that is prompted by the system to be specified as the default IPv4 circuit device. For example, if the prompt displays (`rtn for eth1`), and if you specify `rtn`, `eth1` is set as the default circuit device.

Table 21: Configuring Separate Interfaces for Management and Circuit Traffic *(Continued)*

Field	Function	Your Action
Which device would you like to make the IPV4 default management device?	Specifies the device or interface that you want to configure as the default management device for IPv4.	Specify an interface from the list of available interfaces that were previously displayed in the CTP Menu as the default management interface. Specify `rtn` to set the interface that is prompted by the system to be specified as the default IPv4 management device. For example, if the system prompt displays (`rtn for eth0`), and if you specify `rtn`, `eth0` is set as the default management device. **NOTE**: You must not specify the same device for both management and circuit traffic. Otherwise, the system prompts you to enter the default circuit device and default management device again. For example, if you specify `eth1` as the default interface for both circuit and management traffic, the system prompts you to enter the settings again.
Please input the hostname	Specifies the hostname of the CTP device.	Enter the hostname of the CTP device. Press `Enter` to specify the default hostname.
Please input the ip	Specifies the IP address of the Ethernet interface.	Enter an IP address.
Please input the netmask	For IPv4 interfaces, specifies the network mask.	Enter the network mask.
Please input the gateway	Specifies the IP address of the next-hop gateway (the router).	Enter an IP address.
Please input the mtu in bytes	Specifies the maximum transmission unit (MTU) for the Ethernet interface.	For IPv4 networks, enter a number from 64 through 1500.

Table 21: Configuring Separate Interfaces for Management and Circuit Traffic *(Continued)*

Field	Function	Your Action
Add route to interface eth	Specifies whether or not to add static routes to the Ethernet configuration.	Specify `yes`.
Activate IPV4 interface eth on boot	Specifies whether you want to activate the particular IPv4 interface during the boot operation.	Enter `y` or `n`.

CHAPTER 12

Monitoring CTP Platforms (CTPView)

IN THIS CHAPTER

Monitoring the Network with the CTPView Software (CTPView)

You can enable network monitoring so that the CTPView software can periodically check the status of CTP platforms in your network. You can modify the network monitoring settings from the CTPView web interface. Before you can use network monitoring, you need to add your CTP devices (hosts) to the CTPView configuration and enable the device for network monitoring. To do so, use one of the following topics:

- "Adding and Removing CTP Platforms Managed by CTPView Software (CTPView)" on page 121
- "Adding and Removing Host Groups (CTPView)" on page 121

To enable CTPView network monitoring:

1. In the side pane, select **Network > Monitoring**.

   The Network Monitoring pane is displayed. A Network Monitoring box displays the status of monitoring, **Running** or **Stopped**.

2. Click the button for the group of CTP devices you want to monitor.
3. Click **Click to Start** to initiate monitoring of the selected group.

   The operation or alarm status of each device in the group, and of each bundle on the device, is displayed. Table 22 on page 179 lists the status options. A color key in the pane indicates the bundle state. The highest alarm level on a CTP device percolates up to the button for its group.

Table 22: Platform Group and Bundle Status

Status	Description
Active-Down	The bundle is configured as active, but the bundle state is Down, meaning that no circuit is established to the bundle.
Active-Up	The bundle is configured as active, and the bundle state is Up, meaning that a circuit is established to the bundle.
Assessing	The problem is being assessed, and a user has placed the CTP platform into the Assessing state.
Check Host	The CTP platform is reachable across the network, but the CTPView software is unable to communicate with the platform to obtain the status of the bundles.
Disabled	The circuit is configured as disabled. Ports not attached to bundles are marked Disabled.
No Data	No data can be obtained from the CTP platform. You must investigate further to determine the cause.
Unreachable	The CTPView server cannot reach the CTP host. This alarm can be due to an IP network problem, a site problem (such as a power outage), or a CTP equipment or configuration issue.

You can click on a CTP platform button or a bundle or port button to perform additional monitoring operations, such as checking the host connection, displaying the runtime query results, or overriding the network status.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | 123
Changing the Display Settings for CTPView Network Monitoring (CTPView) | 180
Checking the CTPView Server Connection to CTP Platforms in the Network (CTPView) | 181
Displaying Runtime Query Results for a CTP Platform (CTPView) | 183
Overriding CTP Platform Network Status and Adding Comments (CTPView) | 183
Configuring Email Notifications (CTPView) | 124

Changing the Display Settings for CTPView Network Monitoring (CTPView)

You can change several settings to customize the look of CTPView network monitoring.

To change the display settings:

1. In the side pane, select **Network > Monitoring**.

   The Network Monitoring pane is displayed.
2. Click **Display Settings**.

   The Display Options window opens.

   You can change the following display options:

   - Number of platform group buttons in a row.
   - Width of each group button, in pixels.
   - Text size of each group button, in pixels.
   - Text size of each bundle or port button, in pixels.
   - Level of debugging information.
   - Audible notification by the browser each time status is reported as UNREACHABLE, CHECKHOST, or ACTIVE-DOWN.
3. Select the setting values you want to change. Click **Submit Choices** to accept your changes, or click **Undo Changes** to restore the current value.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | 123

Checking the CTPView Server Connection to CTP Platforms in the Network (CTPView)

IN THIS SECTION

You can determine whether the CTPView server is currently able to reach one or more of the CTP platforms in your network. This is a one-time, immediate check rather than ongoing network monitoring. You can check the connection status from the Network Monitoring pane or from the Node Maintenance pane.

Checking Connections from the Network Monitoring Pane (CTPView)

To check the current reachability of CTP platforms:

1. In the side pane, select **Network > Monitoring**.

   The Network Monitoring pane is displayed.
2. Click **Check Connections**.

   The Check Connections to CTPs window opens and displays a list of platform groups and their members.
3. Click the name of the platform you want to check.

   You can select more than one platform by holding down the Ctrl key when you click the platform names. Alternatively, you can click **Select All Hosts** to select all the listed CTP platforms.
4. Click **Check Connection to Selected CTPs**.

   The CTPView software checks the connection to each selected CTP device in turn and displays the results.

Checking Connections from the Node Maintenance Pane (CTPView)

You can also check CTP platform connections from the Node Maintenance pane.

1. In the side pane, select **Node > Maintenance**.

   The Node Maintenance pane is displayed.
2. Click **Check Connection to CTP(s)**.

   The Check Connections to CTPs window opens and displays a list of platform groups and their members.
3. Click the name of the platform you want to check.

   You can select more than one platform by holding down the Ctrl key when you click the platform names. Alternatively, you can click **Select All Hosts** to select all the listed CTP platforms.
4. Click **Check Connection to Selected CTPs**.

   The CTPView software checks the connection to each selected CTP device in turn and displays the results.

Displaying Previously Logged Connection Status (CTPView)

To display logs of previous connection checks:

1. In the Check Connections to CTPs window, click **Show Active Log**.
2. (Optional) Click **Archive This Log** to archive the current results summary tables.
3. (Optional) Click **View All Summaries** to display previously archived results summary tables.

Checking Connections in the Remote Host Options Window (CTPView)

The CTPView software provides another way to check CTP platform connections starting from the Network Monitoring pane.

1. Perform the steps listed in "Monitoring the Network with the CTPView Software (CTPView)" on page 178.

   Monitoring is started for the selected bundle or platform.
2. Click the button for a platform or bundle being monitored.

   The Remote Host Options window is displayed.
3. Click **Check Host Connection**.

   A new window displays the SSH query and response and the SNMP query and response.

> **NOTE**: To receive a response for an SNMP query, you need to configure and enable SNMP on the target CTP device.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | 123

Monitoring the Network with the CTPView Software (CTPView) | 178

Changing the Display Settings for CTPView Network Monitoring (CTPView) | 180

Displaying Runtime Query Results for a CTP Platform (CTPView)

You can quickly access the runtime query results for a CTP platform or bundle from the Network Monitoring pane.

To display the runtime query results:

1. Perform the steps listed in "Monitoring the Network with the CTPView Software (CTPView)" on page 178.

   The Network Monitoring pane is displayed.
2. Click the button for a platform or bundle being monitored.

   The Remote Host Options window is displayed.
3. Click **Open Bundle Runtime Query Page** for all bundles or, if you selected an individual bundle, for that bundle.

   The Bundle Runtime Information page appears.
4. Select a row and click **Display Selected Bundles**.

   Runtime query results for the selected bundle are displayed.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | 123

Monitoring the Network with the CTPView Software (CTPView) | 178

Changing the Display Settings for CTPView Network Monitoring (CTPView) | 180

Displaying Running CTP Bundle Configuration, State, and Counters (CTPView)

Overriding CTP Platform Network Status and Adding Comments (CTPView)

You can manually override the status of CTP platforms. You can also add comments that appear in the Remote Host Options window for a CTP platform that is currently being monitored.

To override the status of a platform:

1. Perform the steps listed in "Monitoring the Network with the CTPView Software (CTPView)" on page 178.

   The Network Monitoring pane is displayed.
2. Click the button for a platform being monitored.

   The Remote Host Options window is displayed.
3. Click **Modify Host Status/Comments**.

   The Modify Host Comments window is displayed.
4. Select **Yes** to set the status to Assessing.

   If the status was previously overriden and set to Assessing, you can select **No** to remove the override.
5. Click **Submit Changes**.

   A magnifying glass icon appears in the button for the platform, its group, and its network. The status color of only the platform button is set to orange for Assessing. The group and network buttons display only the most severe status reported for a platform that has not been manually overridden.

To add a comment:

1. Perform the steps listed in "Monitoring the Network with the CTPView Software (CTPView)" on page 178.

   The Network Monitoring pane is displayed.
2. Click the button for a platform being monitored.

   The Remote Host Options window is displayed.
3. Click **Modify Host Status/Comments**.

   The Modify Host Comments window is displayed.
4. Type a comment of up to 125 characters in the comment field.
5. Click **Submit Changes** to apply your text to the Remote Host Options window.

   Alternatively, click **Delete Comments** to remove a current comment (and if applied, the Assessing status), or **Undo Changes** to cancel your comment change. A time stamp indicates when the comment was last modified.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | **123**

Monitoring the Network with the CTPView Software (CTPView) | **178**

Saving CTP Platform Configurations (CTPView)

You can set an automatic function to save the CTPView configuration for the CTP platforms in your network automatically. The automatic function stores up to the 10 most recent configuration files. You can also save the configuration manually. Manually saved configurations are stored in addition to any automatically saved configurations. You can also save previously stored configurations for any CTP platform.

To configure automatic file saving:

1. In the side pane, select **Server > Administration**.

   The Administrative Functions pane is displayed.
2. Click **Automatic Functions**.

   The CTPView Automatic Functions window is displayed.
3. In the Action section in the second box, select **Save Current CTP Host System Configurations**.
4. Select when you want the operation to take place.
5. Click **Add New Entry**; the operation appears in the summary table. Or, if you do not want to add the entry, click **Reset**.

To have the configurations saved at additional times, add a new entry for that operation for each time.

To save the configurations manually:

1. In the side pane, select **Node > Maintenance**.

   The Administrative Functions pane is displayed.
2. Click **Save/Restore CTP Configurations**.

   The CTP System Configuration window is displayed.
3. Select the desired host.
4. Click **Save CTP Configuration**.

   The name and IP address of the selected host is displayed.
5. (Optional) Type text for a label associated with the configuration.
6. Click **Click To Save Current CTP Configuration**.

   The configuration is added to the list of saved configurations.

To restore a configuration:

NOTE: Restoring a saved configuration to a CTP platform reboots that device.

1. In the side pane, select **Node > Maintenance**.

   The Administrative Functions pane is displayed.

2. Click **Save/Restore CTP Configurations**.

   The CTP System Configuration window is displayed.

3. Select the desired host.

4. Click **Restore CTP Configuration**.

   The name and IP address of the selected host is displayed.

5. Select a saved configuration from the list.

6. Click **Restore CTP Configuration**.

   The CTP platform is rebooted as part of the restoration process.

To delete a saved configuration:

1. In the side pane, select **Node > Maintenance**.

   The Administrative Functions pane is displayed.

2. Click **Save/Restore CTP Configurations**.

   The CTP System Configuration window is displayed.

3. Select the desired host.

4. Click **Delete Saved CTP Configuration**.

   The name and IP address of the selected host is displayed.

5. Select a saved configuration from the list.

6. Click **Delete CTP Configuration**.

Setting an Audible Alert for CTP Platform Status (CTPView)

You can set an alert that the CTPView browser plays every time it detects a CTP platform status as UNREACHABLE, CHECKHOST, or ACTIVE-DOWN. You can add additional alert sounds to the available choices.

To select an alert sound:

1. In the side pane, select **Network > Monitoring**.

   The Network Monitoring pane is displayed.
2. Click **Display Settings**.

   The Display Options window opens.
3. Select Enabled to set the browser to play an alert.
4. Select an alert sound from the list.
5. Click **Submit Choices** to accept your changes, or click **Undo Changes** to restore the current value.

To add additional alert sounds:

- Copy the sound files to the CTPView server directory **/var/www/html/acorn/sounds/**.

> **NOTE**: Only files in .wav format are supported. The sound filename can include only alphanumeric characters and the underscore (_) character. The filename root is displayed as the label for the sound in the browser. The CTPView software automatically corrects illegal filenames and modifies file permissions as needed to enable the embedded media player to read the file.

The default browser installation for LINUX workstations may not include an embedded media player. An easy-to-install multimedia plug-in is available at http://fredrik.hubbe.net/plugger.html.

RELATED DOCUMENTATION

Managing CTP Platforms in the Network (CTPView) | **123**

Monitoring the Network with the CTPView Software (CTPView) | **178**

Changing the Display Settings for CTPView Network Monitoring (CTPView) | **180**

Displaying CTPView Network Reports (CTPView)

The CTPView software provides the following reports that detail how ports are provisioned on the CTP platforms in your network:

- Channelization Report—Information about all ports on selected CTP platforms.
- Configured Ports Report—Information about only the configured ports on selected CTP platforms.
- Non-configured Ports Report—Information about only ports that are incompletely configured on selected CTP platforms.

To display the desired report:

1. In the side pane, select **Node > Maintenance**.

   The Node Maintenance pane is displayed.
2. Click **View Network Host Reports**.

   The CTPView Network Reports pane is displayed.
3. Select one or more remote hosts (CTP platform), or click **Select All Hosts** to select all listed CTP platforms.
4. Click the button for the desired report.

   The report is displayed in the bottom of the pane. Click **Clear/Reload Page** to remove the report from the pane.
5. (Optional) Click on a column header in the report to sort the data in ascending order for that column.
6. (Optional) Select a different font size for readability.
7. (Optional) Click **Printer Friendly Page** to display the report in a format suitable for printing.

   You can select and copy the printer-friendly information and paste it in a spreadsheet.

The report database is updated whenever you use the CTPView software to provision a CTP platform. You can also save the CTP platform configuration data to the database automatically or manually.

To update the database automatically, see "Configuring Automatic Monitoring of CTP Platforms (CTPView)" on page 150.

1. To update the database manually:
2. In the side pane, select **Node > Maintenance**.

   The Node Maintenance pane is displayed.
3. Click **View Network Host Reports**.

   The CTPView Network Reports pane is displayed.
4. Click **Update Database**.

RELATED DOCUMENTATION

Field Descriptions in CTPView Network Reports (CTPView) | 189

Field Descriptions in CTPView Network Reports (CTPView)

Table 23 on page 189 describes the information provided by the CTPView software in the CTPView network reports.

Table 23: CTPView Network Reports Fields

Field	Description
Source IP Address	IP address of the source CTP platform.
Source Host Name	Name of the source CTP platform.
Source Port Number	Number identifying port on the source CTP platform.
Source CID	Source circuit ID.
Source Bundle Number	Number identifying bundle on the source CTP platform.
Destination IP Address	IP address of the destination CTP platform.
Destination Host Name	Name of the destination CTP platform.
Destination Port/CID Number	Destination port and circuit ID.
Source Interface Type	Type of interface on the source CTP platform: EIA530, EIA530A. RS-232, V.35, T1/E1, fractional T1/E1, or 4WTO analog voice.
Source Port Speed	Clock speed configured for the source CTP platform.
Source Service Type TOS/DSCP	Value of the Type of Service byte in packets sent from the source CTP platform to the IP network.

Source Port Descriptor	Descriptive term or name applied to the port.
Source Bundle Descriptor	Descriptive term or name applied to the bundle.
Source Code Version	CTPOS software version running on the source CTP platform.
Last Update	Date and time report was last updated to the database.

RELATED DOCUMENTATION

Displaying CTPView Network Reports (CTPView) | 188

Displaying Network Statistics (CTPView)

The CTPView software periodically retrieves IP performance information from each CTP platform in the network. The data is retrieved at 1-minute intervals and includes the following observation:

- Minimum, maximum, and average values for the buffer state
- Calculated IP packet delay variance (jitter)
- Missing packet counts
- Round-trip packet delay

The plots display information for the currently connected CTP platform. You can display plots for a single bundle or all configured bundles on the connected CTP platform. Each plot's Y axis is automatically scaled for convenient viewing. However, for the buffer, packet delay variance, and round-trip delay plots, you can specify different units, minimum values, and maximum values for the Y axis intervals. You can select the period of time for which you want to review the data, from the preceding hour up to the preceding week, or you can set a custom period to review.

NOTE: The Network Statistics pane requires you to select the circuit of interest based on bundle numbers. An expanding table in the pane displays a summary of the current bundle circuits and their attached ports on the connected platform.

To display a plot of IP statistics for the connected CTP platform:

1. In the side pane, select **Statistics > Plots**.

   The Network Statistics pane is displayed.

2. Click on the time period button for which you want data to be plotted.

   The plots are displayed, and the period plotted is indicated. Click any plot to open a larger version in a new window.

   You can click a button for a single bundle or all configured bundles. To plot data for a single bundle, expand the table, follow the directions in the pane to display and select the bundle. Time period buttons are then displayed for that bundle.

To display a plot with different values for the Y axis:

1. In the Network Statistics pane, click **Custom Y-axis Options**.

   The Network Statistics pane is displayed.

2. Select any combination of minimum value, maximum value, or different units for the Y axis.

   You can select these values for the Buffer, IP packet delay variation, or IP one-way packet loss plots. You can click **Reset Custom Y-axis** to restore the default values for all plots.

To display a plot for a custom time period:

1. In the Network Statistics pane, click **Custom Y-axis Options**.

   The Network Statistics pane is displayed.

2. Click **Custom Time Options**.

3. Select a starting and ending year, month, day, hour and minute.

4. Click **Custom Time** for the bundles you want to plot.

   You can click **Reset Custom Time** to restore the default values for all plots.

   The plots are displayed, and the period plotted is indicated. Click any plot to open a larger version in a new window.

Displaying the Management and Circuit Interface Settings (CTP Menu)

To display the configured network settings using the CTP Menu:

1. From the CTP Main Menu, select **5) Node Operations**.

2. Select **2) Display network settings**.

```
Hostname: ctp_90

Protocols supported:   IPV4 ONLY

Segregation between management and circuit traffic: ON

Default management device (eth0: 10/100/1000 Copper (right back)) IPV4 parameters:
        ipaddress:  1.1.1.1
        netmask:    255.255.255.0
        gw:              1.1.1.3
        mtu:        1500 bytes

Default circuit device (eth1: 10/100/1000 Copper (left back)) IPV4 parameters:
        ipaddress:  10.216.118.90
        netmask:    255.255.254.0
        default gw: 10.216.119.254
        mtu:        1500 bytes
```

Table 24 on page 192 describes the fields corresponding to the configured network settings, including the status of the capability to segregate management and circuit traffic, displayed in the output.

Table 24: CTP Network Settings Display in the CTP Menu

Field Name	Field Description
Hostname	Hostname of the CTP device.
Protocols supported	Displays the protocols supported on the CTP device, such as IPv4 or IPv6.
Segregation between management and circuit traffic	Displays whether the functionality to segregate management and circuit traffic is configured (**ON**) or not (**OFF**).
Default management device (eth) IPV4 parameters	

Table 24: CTP Network Settings Display in the CTP Menu *(Continued)*

Field Name	Field Description
ipaddress	Displays the IP address of the Ethernet interface set as the default management interface.
netmask	Displays the network mask of the Ethernet interface set as the default management interface.
gw	Displays the IP address of the next-hop gateway for the Ethernet interface set as the default management interface.
mtu	Displays the maximum transmission unit (MTU) of the Ethernet interface set as the default management interface.
Default circuit device (eth) IPV4 parameters	
ipaddress	Displays the IP address of the Ethernet interface set as the default circuit interface.
netmask	Displays the network mask of the Ethernet interface set as the default circuit interface.
gw	Displays the IP address of the next-hop gateway for the Ethernet interface set as the default circuit interface.
mtu	Displays the maximum transmission unit (MTU) of the Ethernet interface set as the default circuit interface.

CHAPTER 13

Changing CTPView GUI Settings

IN THIS CHAPTER

Configuring CTPView Software for Tabbed or Nontabbed Browsers (CTPView)

You can configure the CTPView software to be displayed properly in a tabbed browser or a nontabbed browser. By default, the software is set to classic, which supports a nontabbed browser. You must separately configure each browser that you use.

To set the browser preference for tabs:

1. In the side pane, select **Server > GUI Settings**.

   The GUI Settings pane is displayed.
2. Select **Classic** for nontabbed browsers or **Tab** for tabbed browsers.
3. Click **Change CTPView Style**.

   The viewing style is displayed in the side pane under **Server**.

To open a CTPView window in a new tab in your browser:

- In the side pane, select **Server > New Window**.

The current tabbed browsers do not support dynamically changing the tab's title after a page has been loaded onto the screen. The CTPView software uses frames to open new content in the viewing window without reloading the entire page, so the tab titles cannot describe the current content. The CTPView software adds a bracketed sequencing number to the tab title to differentiate the tabs for easier browser, and keeps track of the number of tabs that you have opened.

To reset the tab count:

1. In the side pane, select **Server > GUI Settings**.

   The GUI Settings pane is displayed.

2. Click **Reset Browser Tab Index**.

   The count resets to 1. The next tab you open will have the sequence number 1. The counter is automatically reset when you close all the browser windows.

Changing the CTPView Display Settings (CTPView)

You can modify the appearance of text, and the background color of tables and some buttons in the CTPView software. By default, text is displayed in 3-point Verdana.

To change the text appearance:

1. In the side pane, select **Server > GUI Settings**.
   The GUI Settings pane is displayed.
2. Select a font style.
3. Select a base text size.
4. Click **Submit Changes**.

To change the background color of certain tables and buttons:

1. In the side pane, select **Server > GUI Settings**.

   The GUI Settings pane is displayed.

2. Type the hexadecimal code for the new color in the field for the table, button, or message type that you want to change.

3. (Optional) Click **Go To Color Chart** to view a table of codes for browser-safe colors, and type the code.

4. Click **Submit Changes**.

   Alternatively, you can restore the default colors by clicking **Use Default Colors**.

The current window refreshes immediately with the text or color changes. However, other windows (or tabs) that are open when you make the change are not automatically refreshed. The changes appear in any windows that you subsequently open.

RELATED DOCUMENTATION

Displaying Help for CTPView GUI Settings (CTPView) | 196

Displaying Help for CTPView GUI Settings (CTPView)

You can display troubleshooting information and tips regarding CTPView GUI settings and browser display.

To display GUI help:

1. In the side pane, select **Server > GUI Settings**.

   The GUI Settings pane is displayed.
2. Click **Troubleshooting and Tips**.

   The Troubleshooting and Tips pane is displayed.

RELATED DOCUMENTATION

Changing the CTPView Display Settings (CTPView) | 195

CHAPTER 14

Managing and Displaying Users (CTPView Server Menu)

IN THIS CHAPTER

Accessing the CTPView Server Configuration Menu (CTPView Server Menu)

To access the CTPView server CLI menu:

1. Using an SSH application, log in to the CTPView server.

   NOTE: If you do not successfully log in within 60 seconds, the session is closed.

   Alternatively, you can log in directly to the CTPView server if you connect a keyboard and monitor to the server. Using an SSH application requires that the CTP server already be configured in your network with an assigned IP address.
2. Enter **menu**.
3. Enter the root password.

The CTPView Configuration Menu is displayed.

RELATED DOCUMENTATION

Default CTPOS and CTPView Accounts and Passwords | 94

Managing CTPView Users (CTPView Server Menu)

IN THIS SECTION

You can view currently active shell account users, and add or delete administrator shell accounts. Shell accounts provide access to the CTPView server by means of an SSH application.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To manage user passwords, you must first access the User Management Menu:

1. From the CTPView Configuration Menu, select **1) Security Profile**.
2. Select **1) User Management**.

   The User Management Menu is displayed.

> **NOTE**: The Security Profile Configuration Menu has an idle timeout period of 10 minutes. If no action is performed for 10 minutes, the user is logged out of the Security Profile Configuration Menu, and is brought back to the Node Operations Menu.

Monitoring CTPView Users (CTPView Server Menu)

To display all CTPView users that are currently logged in to the server through SSH:

- From the User Management Menu, select **1) List users currently logged on**.

Only users logged in to the server through a secure shell (not through the CTPView GUI) are listed. The table lists the username, whether the user logged in remotely or locally, the time the session began, and the user's IP address. Local user connections are indicated by *tty*; remote SSH connections are indicated by *pts*.

Listing Admin Shell Accounts (CTPView Server Menu)

You use a shell account to access the CTPView server with an SSH application.

To list all administrator shell accounts:

- From the User Management Menu, select **2) List admin shell accounts**.

The usernames for the shell accounts are listed according to their classification, Administrator or User.

Adding Admin Shell Accounts (CTPView Server Menu)

To add an administrator shell account:

1. From the User Management Menu, select **3) Add admin shell accounts**.
2. Enter the username for the account.

   Only alphanumeric characters, underscores, and periods are allowed in a username.
3. Enter the appropriate number to classify the user as an Administrator or User.
4. Enter a new password for the user.

   The password requirements are displayed to assist you in choosing an appropriate password.

Starting with CTPOS Release 7.1R1, 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 CLI menu is accessible after a user in JITC mode logs in to the device. Until Release 7.0R1, for shell account users (System Administrator and Auditor users), the shell prompt was displayed after logging in and for menu users (CTP Administrator and Query-Only users), the CLI menu was accessible after logging in for all security levels.

SEE ALSO

CTPOS and CTPView Software Password Requirements | **96**

Deleting Admin Shell Accounts (CTPView Server Menu)

To delete an administrator shell account:

1. From the User Management Menu, select **4) Delete admin shell accounts**.
2. Enter the username for the account.

RELATED DOCUMENTATION

Classification of CTPView Shell Account Users

Users that access the CTPView server running FC OS through a shell account are classified into one of the following classes:

- Administrator—Can configure the CTP platform, configure loops and BERTs, and query the status of ports and clocking.
- User—Can issue commands only to query the status of ports and clocking.

Starting with CTPOS Release 7.1R1, 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 CLI menu is accessible after a user in JITC mode logs in to the device. Until Release 7.0R1, for shell account users (System Administrator and Auditor users), the shell prompt was displayed after logging in and for menu users (CTP Administrator and Query-Only users), the CLI menu was accessible after logging in for all security levels.

Managing User Passwords (CTPView Server Menu)

IN THIS SECTION

You can display user accounts and password settings, configure various aging criteria for user passwords, and specify the rules for forming passwords.

Before you begin, log in to the CTPView server, and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To manage user passwords, you must first access the Password Management Menu:

1. From the CTPView Configuration Menu, select **1) Security Profile**.
2. Select **2) Password Management**.

   The Password Management Menu is displayed.

Listing User Accounts (CTPView Server Menu)

The usernames for the accounts are listed according to their classification, Administrator or User..

To list the usernames for CTPView server accounts:

- From the Password Management Menu, select **1) List user & admin accounts**.

Displaying Password Expiration Settings (CTPView Server Menu)

To display the current password expiration settings for a user account:

- From the Password Management Menu, select **2) Display password expiration details**.

Table 25 on page 201 describes the information listed in the output.

Table 25: CTPView User Password Expiration Settings

Field	Description
Account is/is not locked	Status of the account. Locked accounts cannot access CTPView server.
Minimum	Minimum number of days that must elapse before the user can change this password, in the range 1 through 60.
Maximum	Maximum number of days that this password is valid.
Warning	Number of days before password expiration that the user is warned of the impending expiration.
Inactive	Number of days of inactivity after the password expires before the account is locked out (unable to access CTPView server)
Last Change	Date that this password was last changed.

Password Expires	Date that this password expires. Calculated by counting the Maximum value from the Last Change date.
Password Inactive	Date that this password becomes inactive. Calculated by counting the Inactive value from the Password Expires date.
Account Expires	Date that the account expires.

Changing Password Expiration Settings (CTPView Server Menu)

To change the password expiration settings for a user account:

1. From the Password Management Menu, select **3) Manage password requirements**.
2. Enter the password expiration values when prompted.

   Each prompt provides a description and range for the value.

Displaying Password Requirements (CTPView Server Menu)

To display the current requirements for forming a password:

- From the Password Management Menu, select **4) Show password requirements**.

The output lists the minimum password length, the minimum number of lowercase letters, uppercase letters, numerals, and nonalphanumeric characters; and the number of times a user can attempt to enter the correct password before being blocked.

SEE ALSO

CTPOS and CTPView Software Password Requirements | 96

Changing Password Requirements (CTPView Server Menu)

User passwords have strict criteria. You must include a nonzero minimum of lowercase letters, uppercase letters, numerals, and certain nonalphanumeric characters. You must also set the number of times a user can enter the password incorrectly before being blocked from access.

To change the requirements for forming a password:

1. From the Password Management Menu, select **5) Manage password requirements**.
2. Enter values for the password requirements when prompted.

   Each prompt provides a description and range for the value.

SEE ALSO

CTPOS and CTPView Software Password Requirements | 96

RELATED DOCUMENTATION

Default CTPOS and CTPView Accounts and Passwords | 94

CTPOS and CTPView Software Password Requirements | 96

Accessing the Security Profile Configuration Menu (CTP Menu)

You can monitor and manage CTPOS and CTPView users by accessing the Main Security Profile Configuration Menu in CTPOS or the CTPView Server Menu. This section describes how to access the Main Security Profile Configuration Menu from CTPOS. To access Security Profile Configuration Menu from the CTPView Server Menu and manage users, see "Managing CTPView Users (CTPView Server Menu)" on page 198. The options in the Security Profile Configuration Menu are the same whether you access it from the CTPView Server Menu or from CTPOS.

To access the Main Security Profile Configuration Menu from CTPOS:

1. From the Main Menu, select **5) Node Operations** > **14) Config security profile**.
2. When prompted, enter the root password.

```
In order to configure the security profile you will need the
password for root. Would you like to continue? y[n]: y
Password:
************************************************************
****         CTP Security Profile Menu V 2.0          ****
****   Host nova_70: Sat Jan  4 04:21:27 2014
****   User root logged in from 10.215.146.80 as root
**** **** ****     All actions are logged     **** **** ****
************************************************************

Main Security Profile Configuration Menu

Please choose a menu item from the following list:
0) Exit Security Profile Menu
1) User Management
2) Password Management
3) Secure Log Management
```

```
4) Change login banner
5) Modify Security Level
6) Set Management Port Forwarding
```

NOTE: The Security Profile Configuration Menu has an idle timeout period of 10 minutes. If no action is performed for 10 minutes, the user is logged out of the Security Profile Configuration Menu and is brought back to the Node Operations Menu.

RELATED DOCUMENTATION

- Managing CTPView Users (CTPView Server Menu) | **198**
- Managing User Passwords (CTPView Server Menu) | **200**
- Managing CTPView Server Secure Logs (CTPView Server Menu) | **221**
- Setting the CTPView Server Start-Up Banner (CTPView Server Menu) | **223**
- Managing Access Security for the CTPView Server (CTPView Server Menu) | **224**
- Configuring an SSH Connection to a CTP Platform that Persists Through the Session (CTPView) | **127**

Changing the User Password (CTP Menu)

You can change your password by logging in to the CTP system. The new password must meet the requirements that are specified in the Configuration Security Profile menu.

To change your password by using the CTP Menu:

1. From the Main Menu, select **5) Node Operations**.
2. Select **13) Set your password**.

   The CTP system displays the password requirements based on your security profile. Table 26 on page 205 lists the security profiles and their password requirements.

```
##########################################################################
##########################################################################
##########################################################################
                  PLEASE REMEMBER THESE PASSWORDS!!!
```

```
Password recovery is not a simple process:
- It is service affecting.
- It requires console access to the CTP
- It requires rebooting of the device
##########################################################################
##########################################################################
##########################################################################

The new password must be alphanumeric or the characters

           @ { } # % ~ [ ] = & , - _ !


The new password must also be at least 6 characters long, with

1 lowercase, 1 uppercase, 1 digits and 1 other characters.

Enter New Password for ctp

Retype New Password for ctp

Changing password for user ctp.
passwd: all authentication tokens updated successfully.
Backing up /etc to nonvolatile storage..
```

Follow the onscreen instructions to set the new password.

The following message is displayed if you do not have the permissions required to change password:

```
This user does not have privileges to do this.
```

Table 26: Requirements for New Password

Password Attributes	Units	Security Profiles and Their Attribute Range in CTPView		Security Profiles and Their Attribute Range in CTPOS	
		High	Low	High	Low/Very Low
Minimum length	char	15–64	5–64	15–256	15–256

Table 26: Requirements for New Password *(Continued)*

Password Attributes	Units	Security Profiles and Their Attribute Range in CTPView		Security Profiles and Their Attribute Range in CTPOS	
		High	Low	High	Low/Very Low
Maximum length	char	15–64	5–64	256	256
Minimum lowercase characters	char	1–10	0–10	1–15	0–15
Minimum uppercase characters	char	1–10	0–10	1–15	0–15
Minimum digits	char	1–10	0–10	1–15	0–15
Minimum other characters	char	1–10	0–10	1–15	0–15
Contains username	–	no	no	no	no
Checked with cracklib library	–	yes	no	yes	yes
Min required new characters	number	5	0	5	5
Allowed authentication retries	–	1–3	1–3	1–3	1–3
Lockout after login failure	seconds	60-indefinite	60-indefinite	900	900

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Default CTPOS and CTPView Accounts and Passwords | 94

Managing User Passwords (CTPView Server Menu) | 200

Configuring CTPView User Authentication with Steel-Belted RADIUS

IN THIS SECTION

Starting with CTPView Release 4.1, you can provide RADIUS authentication to both HTTPS and SSH users. Earlier releases of CTPView supported RADIUS authentication only for HTTPS users. Enabling RADIUS authentication for SSH users ensures that both HTTPS and SSH users have a common authentication method without requiring separate user-specific configuration.

Starting with CTPView Release 4.1, users do not require a local user account on the CTPView server. For CTPView 4.0 and earlier, a user must have an account on the CTPView server. You can add a user or verify whether a user account exists from the CTPView CLI menu. The username for the CTPView account must match the username that is configured on the RADIUS server.

You can enable or disable RADIUS authentication for both SSH and HTTPS users. You can block a specific user by disbaling that user from the RADIUS server.

To provide RADIUS authentication, use an independent Steel-Belted RADIUS (SBR) server or an RSA SecurID appliance with your CTPView server running FC9 or Centos OS and CTPView 3.4R1 or later. The RSA SecurID appliance incorporates an SBR server, making the configuration very similar to that of an independent SBR server.

Users are authenticated in the following order:

1. By the SBR server.

2. By the local CTPView application.

You can configure the SBR server to use native user authentication or pass-through authentication with RSA SecurID.

- Native user authentication references user accounts stored on the SBR server. When trying the native user method, the SBR software searches its database for an entry whose User-Type is Native User and whose username matches the User-Name in the Access-Request.
- Pass-through authentication (two-factor authentication) enables the SBR server to pass authentication requests through to RSA Authentication Manager (RSA SecurID). RSA SecurID is then responsible for validating the username and password found in the Access-Request.

The order of authentication between these two categories of users is set on the SBR server. You can add the same user (that is, the same user ID) to both the SBR server and the local CTPView application.

Configuring RADIUS Settings on the CTPView Server

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To configure RADIUS settings on the CTPView server:

1. From the CTPView Configuration Menu, select `9) AAA Functions`.

   The RADIUS Menu is displayed.
2. Select `8) RADIUS/RSA SecurID Configuration`. Configure the parameters described in Table 27 on page 208.

   Table 27: RADIUS Menu Options

Field	Function	Your Action
Servers	Displays the RADIUS servers configured on CTPView. You can add up to 10 RADIUS servers. If you define multiple servers, the order in which they are tried differs on the basis of whether the user is trying to access CTPView via SSH or HTTPS. For access via SSH, the servers are tried in order. For HTTPS access, the servers are tried in a round-robin fashion. In both cases, the process continues until the system receives a response from a server or until the maximum number of retries is reached for all servers.	Specify a RADIUS server. Make sure you specify an IPv4 address if you are configuring RADIUS authentication for HTTPS. IPv6 addresses are supported for RADIUS authentication for SSH.

Table 27: RADIUS Menu Options *(Continued)*

Field	Function	Your Action
Destination Port	Specifies the RADIUS destination port.	The default value is 1812.
Retry Attempts	Specifies the number of attempts that the CTPView server makes to contact the listed RADIUS server.	Specify a value in the range of 0 through 9.
Off-Line-Failover	Determines whether the login credentials are passed to the local account login function when no RADIUS server responds to the login request.	Select one: • Allowed to Loc Acct—User credentials are passed to the local account login function. • Not Allowed—User is denied access and the session is terminated.
Reject-Failover	Determines whether the login credentials are passed to the local account login function. The user credentials are not passed if the login information is incorrect or if the user does not have an account for the RADIUS server.	Select one: • Allowed to Loc Acct—User credentials are passed to the local account login function. • Not Allowed—User is denied access and the session is terminated.

3. Select `6) Initialize Web UI Template Accounts`.
4. Enter the PostgreSQL administrator account password when prompted.
5. Select `1) Servers`.

   The system displays the RADIUS servers that are configured currently.
6. Enter `y` to add, remove, or modify a server from the list.

   NOTE: Whenever you make changes to the server list, you must reenter all RADIUS servers.
7. When prompted, enter the following information:
   - Shared secret

- Timeout period
- Number of retries

> **NOTE**: For shared secret, only alphanumeric characters and special characters such as “at” sign (@), curly braces ({}), pound sign (#), percent sign (%), tilde (~), square brackets ([]), equal sign (=), comma (,), em dash (–), and underscore (_) are supported.

Configuring 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
VALUE Juniper-CTP-Group Auditor 4
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
VALUE Juniper-CTPView-APP-Group NET_DIAG 4
ATTRIBUTE Juniper-CTPView-OS-Group Juniper-VSA(23, integer) r
VALUE Juniper-CTPView-OS-Group Web_Manager 1
VALUE Juniper-CTPView-OS-Group System_Admin 2
VALUE Juniper-CTPView-OS-Group Auditor 3
##################################################################
# CTP Specific Attributes
##################################################################
```

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

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

4. Add the following text after that block.

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

> **NOTE**: SBR Enterprise Release 6.1.4 and SBR Carrier Release 7.2.4 supports the RADIUS attributes required for CTP Series. This step is required only if you are using an earlier version of SBR and the `Juniper CTP Series` attribute is not listed.

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

Configuring the SBR Server's Active Authentication Method

To configure the SBR server's active authentication method:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by entering the address http://*SBR-server-IP-address*:1812.
2. Click **Launch**.
3. Select **Steel-Belted RADIUS** > **Authentication Policies** > **Order of Methods**.

   Ensure that your chosen method, Native User or SecurID User, is listed under the section Active Authentication Methods.

Adding the CTPView Server as a RADIUS Client on an SBR Server

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

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by entering the address http://*SBR-server-IP-address*:1812.
2. Click **Launch**.
3. Select **Steel-Belted RADIUS > RADIUS Clients**.
4. Add your CTPView server as a client. In the Make or model field, select **Juniper CTP Series**.

Adding 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 entering the address http://*SBR-server-IP-address*:1812.
2. Click **Launch**.

3. Select the user type.
   - For native users, select **Steel-Belted RADIUS** > **Users**> **Native**.
   - For RSA SecurID users, select **Steel-Belted RADIUS** > **Users** > **SecurID**.
4. Add a user with the Add Native User dialog box or the Add SecurID dialog box, depending on your choice in the previous step.
5. In the Attributes section, click the **Return List** tab and then click **Add**. The Add Return List Attribute dialog box opens.
6. In the Attributes section select **Juniper-CTPView_APP-Group**.
7. In the Value section select one of the following authorization levels for the user you are adding:
   - Global_Admin
   - Net_Admin
   - Net_View
   - Net_Diag

Assigning SecurID Tokens to CTPView Users

SecurID authentication requires that you issue a SecurID token to each user and assign it to them on the RSA SecurID appliance. The first time a new user logs in to the CTPView software, the *token code* displayed on the SecurID token is the password. The user is then prompted to create a PIN. On subsequent logins, the user's PIN followed immediately by the token code displayed on the SecurID token is the password.

To assign SecurID tokens:

1. On the RSA SecurID appliance, launch the RSA Authentication Manager Host Mode application.
2. Select **User** > **Add User**.
3. Complete at least the following required fields:
   - Last Name
   - Default Login
   - Required to Create a PIN
   - Assign Token

Configuring CTPOS and CTPView User Authentication with TACACS+

IN THIS SECTION

The TACACS+ protocol provides access control (authentication, authorization, and accounting services) for routers and network access servers through one or more centralized TACACS+ servers. Unlike RADIUS, TACACS+ provides separate handling of authentication, authorization, and accounting services. CTPOS and CTPView use only authentication and authorization services, and do not use the accounting service.

CTP devices act as TACACS+ clients, which send request for authentication and authorization from the centralized TACACS+ servers that have separate user databases for CTPOS CLI users, CTPView CLI users, and CTPView Web UI users.

TACACS+ is supported only on CTPOS Release 6.4 and later and CTPView Release 4.4 and later. In earlier releases, RADIUS is used for remote authentication and authorization. Effective from CTPOS Release 6.4 and CTPView Release 4.4, both RADIUS and TACACS+ are supported.

CTP uses TACACS+ authentication to authenticate users based on the login credentials that are configured on the centralized TACACS+ servers and provides the privileges to the TACACS+ clients. The user is logged in to the device with the privileges that TACACS+ server returns after successful authentication and authorization.

Configuring TACACS+ Settings from the CTPView Server

You can configure TACACS+ for CTPView CLI and CTPView HTTPS users only from CTPView menu. You cannot enable both RADIUS and TACACS+ at the same time. You can enable TACACS+ only after disabling RADIUS.

To configure TACACS+ settings on the CTPView server:

1. From the AAA Menu, select **2) SSH(2nd) - RADIUS/RSA** > **2) TACACS+**.

   The current status of TACACS+ is displayed.

```
Currently, SSH - TACACS+ is set to Disabled.

Please choose a menu item from the following list:
```

```
0) Return to previous menu
1) Enable
2) Disable
Enter your selection for SSH - TACACS+
Please input an integer between 0 and 2 [0]:
```

2. Select **1) Enable** to enable TACACS+.

```
Please choose a menu item from the following list:
0) Return to previous menu
1) RADIUS/RSA: Disabled
2) TACACS+: Enabled
Please input your choice [0]:
```

3. Return to the AAA Menu, and select **9) TACACS+ Configuration** > **1) Servers** to configure the TACACS+ servers.
4. Follow the onscreen instructions and configure the parameters as described in Table 28 on page 214.

Table 28: TACACS+ Settings for CTPView Server

Field	Function	Your Action
Servers	You can configure up to 10 TACACS+ servers each for CTPOS and CTPView users for authentication and authorization. The CTP device tries to authenticate the user from the first server in the list. If the first server is unavailable or fails to authenticate, then it tries to authenticate from the second server in the list, and so on. Authorization is done on the server that successfully authenticates the user.	Enter the IP address of the server and specify the shared secret. Shared secret is the secret key used to encrypt and decrypt packets that are sent and received from the server. The same secret key is used to encrypt and decrypt packets that are sent to and received from the TACACS+ clients.
Destination Port	TACACS+ uses the TCP port for sending and receiving data. Port 49 is reserved for TACACS+ and is the default port.	Enter the destination port number.

Table 28: TACACS+ Settings for CTPView Server *(Continued)*

Field	Function	Your Action
Timeout	Time in seconds that the TACACS+ client should wait for a response from the TACACS+ server after sending the authentication and authorization request. Timeout value applies to all the TACACS+ servers that are configured. The default timeout value is 5 seconds.	Specify a value in the range 1–60.
Off-Line-Failover	You can use the local authentication credentials if the configured TACACS+ servers are unavailable or no response is received from the TACACS+ servers. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct
Reject-Failover	You can use the local authentication credentials if the TACACS+ server rejects the attempt to authenticate. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct

5. From the TACACS+ Menu, select **6) Initialize Web UI Template Accounts**.
6. Enter the PostgreSQL administrator account password when prompted.

   The required template accounts are added to CTPView. These accounts are not configurable. This step is performed as part of the initial configuration of CTPView as a TACACS+ client. However, repeating this step has no detrimental effect on the TACACS+ configuration.

Configuring TACACS+ Settings from the CTPView Web Interface

You can configure TACACS+ for CTPOS users from the CTPView web interface.

To configure TACACS+ from the CTPView web interface:

1. In the side pane, select **System** > **Configuration**.
2. Click **Node Settings** > **TACACS+ Settings** tab.

   The TACACS+ Settings page is displayed.
3. Configure the parameters described in Table 29 on page 216 and click **Submit Settings**.
4. (Optional) Click **System** > **Query** > **Node Settings** to verify the TACACS+ configuration details.

Table 29: TACACS+ Settings for the CTPView Web Interface

Field	Function	Your Action
Status	Specifies whether TACACS+ is enabled or disabled. TACACS+ is disabled by default.	Select one. • Enabled • Disabled
Dest Port	TACACS+ uses the TCP port for sending and receiving data. Port 49 is reserved for TACACS+ and is the default port.	Enter the destination port number.
Timeout	Time in seconds that the TACACS+ client should wait for a response from the TACACS+ server after sending the authentication and authorization request. Timeout value applies to all the TACACS+ servers that are configured. The default timeout value is 5 seconds.	Specify a value.
Off-Line-Failover	You can use the local authentication credentials if the configured TACACS+ servers are unavailable or no response is received from the TACACS+ servers. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct
Reject-Failover	You can use the local authentication credentials if the TACACS+ server rejects the attempt to authenticate. The default option is **Allowed to Loc Acct**.	Select one. • Not Allowed • Allowed to Loc Acct
Servers	You can configure up to 10 TACACS+ servers each for CTPOS and CTPView users for authentication and authorization. CTP tries to authenticate the user from the first server in the list. If the first server is unavailable or fails to authenticate, then it tries to authenticate from the second server in the list, and so on. Authorization is done on the server that successfully authenticates the user.	Enter the IP address of the server, and specify a shared secret.

Table 29: TACACS+ Settings for the CTPView Web Interface *(Continued)*

Field	Function	Your Action
Shared Secret	Shared secret is the secret key that TACACS+ servers use to encrypt and decrypt packets that are sent and received from the server. TACACS+ clients use the same secret key to encrypt and decrypt packets.	Specify the shared secret.

RELATED DOCUMENTATION

Configuring the TACACS+ Server | 217

Configuring the TACACS+ Server

IN THIS SECTION

When installed on a server that uses the CentOS operating system, CTPview allows the TACACS+ authenticated user to log in through SSH and HTTPS.

Users are authenticated in the following order:

- By the TACACS+ server
- By the local user account

You can add the same user to the TACACS+ server and the local CTPView system.

Configuring the TACACS+ Server's Configuration Files

You can use any TACACS+ server that complies with the TACACs+ RFC "The TACACs+ Protocol" (January 1997). You can download the TACACs+ server that we refer to here (v1.2) from the TACACs.net website at http://tacacs.net/download.asp. This version contains four configuration files. To modify the configuration files, you must log in to the TACACs+ server as an administrator.

- Authentication.xml—Modify this file to add a new user on the TACACS+ server. To add a new user, you must a add new user group and the user under the <UserGroups> tag.

```
<UserGroups>
<UserGroup>
<Name>TACACS_User1</Name>
<AuthenticationType>File</AuthenticationType>
<Users>
<User>
<Name> TACACS_User1</Name>
<LoginPassword ClearText="PASSWORD" DES="">
</LoginPassword>
<EnablePassword ClearText="" DES=""></EnablePassword>
<CHAPPassword ClearText="" DES=""> </CHAPPassword>
<OutboundPassword ClearText="" DES="">
</OutboundPassword>
</User>
</Users>
</UserGroup>
</UserGroups>
```

- Authorization.xml—Modify this file to define the authorization level for the user. To define authorization levels, you must add the user group added in **Authentication.xml** file to this file under the <Authorization> tag.

```
<Authorization>
<UserGroups>
<UserGroup>TACACS_User1</UserGroup>
</UserGroups>
<Services>
<Service>
<Set>service=juniper_ctp_srvc</Set>
<Set>protocol=unknown</Set>
<Set>juniper_ctpview_https=1</Set>
</Service>
</Services>
</Authorization>
```

The CTP device uses the **juniper_ctp_srvc** service to access TACACS+ . This service is used only to access TACACS+ and cannot be changed in the **Authorization.xml** file.

To define the authorization level, you can assign a user to any or all of the following groups:

- CTP Device CLI–SSH
- CTPView CLI–SSH
- CTPView Web–HTTPS

The level of authorization for each user is specified in the <Set> tag under the <Service> tag.

Use the attributes and values shown in Table 30 on page 219 for HTTPS access to CTPView.

Table 30: Attributes and Values for HTTPS Access

Attribute	Value
Global_Admin	juniper_ctpview_https=1
Net_Admin	juniper_ctpview_https=2
Net_View	juniper_ctpview_https=3
Net_Diag	juniper_ctpview_https=4

Use the attributes and values shown in Table 31 on page 219 for SSH access to CTPView.

Table 31: Attributes and Values for SSH Access to CTPView

Attribute	Value
Web Manager	juniper_ctpview_cli=1
System Admin	juniper_ctpview_cli=2
Auditor	juniper_ctpview_cli=3

Use the attributes and values shown in Table 32 on page 220 for SSH access to CTP devices.

Table 32: Attributes and Values for SSH Access to CTP Devices

Attribute	Value
Read_Only	juniper_ctp_cli=1
Admin	juniper_ctp_cli=2
Privileged_admin	juniper_ctp_cli=3
Auditor	juniper_ctp_cli=4

On the TACAS+ server, you can also modify these files:

- Clients.xml—Modify this file to add the secret key and the domains that can use the TACACS+ server.
- Tacplus.xml—Modify this file to add the remote port number and the IPV4 or IPv6 addresses assigned to the TACACS+ server.

```
<Port>49</Port>
<LocalIP>Write your TACACS+ machine's IP here</LocalIP>
```

Modify the parameters specified in Table 33 on page 220 if required.

Table 33: Attributes for Configuring Tacplus.xml File

Parameter	Function
Port	The default port number is 49.
LocalIP	Specify the IP address of the TACACS+ server. You can enter an IPV4 or IPV6 address. Before you enter an IPv6 address, ensure that both the TACACS+ server and CTPView server or the CTP device supports IPV6.

SEE ALSO

Configuring CTPOS and CTPView User Authentication with TACACS+ | 213

CHAPTER 15

Managing the CTPView Server (CTPView Server Menu)

IN THIS CHAPTER

Managing CTPView Server Secure Logs (CTPView Server Menu)

IN THIS SECTION

This topic describes management of the **/var/log/secure** and **/var/log/secure.*ext*** logs stored on the CTPView server. The secure log provides an audit trail of user and administrator activity on the CTPView server. All actions performed on the CTPView server through the menu are logged and viewable. These logs do not record actions taken through the CTPView GUI.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To manage event logs, you must first access the Secure Log Management Menu:

1. From the CTPView Configuration Menu, select **1) Security Profile**.

   The Main Security Profile Configuration Menu is displayed.

2. Select **3) Secure Log Management**.

   The Secure Log Management Menu is displayed.

Viewing Secure Logs (CTPView Server Menu)

To display all secure logs:

1. From the Secure Log Management Menu, select **1) Scan/view log entries**.
2. Follow the displayed instructions to navigate through the logs.

Copying Secure Logs to a Remote Host (CTPView Server Menu)

Before you perform this operation, you must have the IP address, username, and path to the directory in the user's account where the files will be copied.

To copy the logs to a remote host using secure copy (scp):

1. From the Secure Log Management Menu, select **2) Copy logs to remote host**.
2. Enter the information for the remote host as prompted.

Configuring Remote Logging Options (CTPView Server Menu)

You can enable the secure logs to be automatically logged to one or more remote servers.

To configure remote logging options:

1. From the Secure Log Management Menu, select **3) Configure remote logging options**.
2. Enable or disable remote logging.
3. If you have enabled remote logging, enter the IP address as prompted for each remote log server.

When you enable or disable remote logging, the system logger is shut down and then restarted to either send or stop sending subsequent logs to the remote servers.

Displaying the Remote Logging Configuration (CTPView Server Menu)

To display the remote logging configuration:

- From the Secure Log Management Menu, select **4) Show remote logging configuration**.

The status of remote logging is displayed. When remote logging is enabled, the IP address of the remote logging servers is also displayed.

Setting the CTPView Server Start-Up Banner (CTPView Server Menu)

When you log in to the CTPView server, a log-in or start-up banner presents a message. You can change the banner to provide an appropriate message.

To set the start-up banner:

1. From the CTPView Configuration Menu, select **1) Security Profile**.

   The Main Security Profile Configuration Menu is displayed.
2. Select **4) Change login banner**.

   The current banner is displayed.
3. Enter **y** to continue.
4. Enter your message in the field, up to 80 characters per line.

   Only alphanumeric characters, commas, and underscores are allowed in the text.
5. Enter a blank line to end the message.

   The new message is displayed.
6. Enter **y** to accept the new message.

> **NOTE**: The log in banner is pushed to all CTP platforms on the network. You see the banner when you log in to CTPView whether by the GUI or by secure shell to the server.

RELATED DOCUMENTATION

Setting the CTP Platforms Login Banner (CTPView) | 126

Managing Access Security for the CTPView Server (CTPView Server Menu)

IN THIS SECTION

You can control access to the CTPView server by setting security levels for access to the CTPView server through the CTPView GUI or though an SSH connection. The security levels determine the severity of password restrictions, installation or removal of certain utilities, control of root log in, and so on.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To manage security access levels, you must first access the Security Level Menu:

1. From the CTPView Configuration Menu, select **1) Security Profile**.
2. Select **5) Modify Security Level**.

   The Security Level Menu is displayed.

Viewing the Access Security Level for the CTPView Server (CTPView Server Menu)

To display the current settings for access to the CTPView server:

- From the Security Level Menu, select **1) View current security level**.

The security level for access through an SSH connection and to the CTPView GUI are displayed.

Setting Access Security for the CTPView Server (CTPView Server Menu)

To set the security level for access to the CTPView server:

1. From the Security Level Menu, select one of the following options to set the SSH access level: **3) Set OS level to 'very-low'**, **4) Set OS level to 'low'**, **5) Set OS level to 'high'**.

   Table 34 on page 225 describes these security levels.
2. Select one of the following options to set the CTPView GUI access level: **6) Set GUI level to 'low'** or **7) Set GUI level to 'high'**.

Table 35 on page 225 describes these security levels.

The **sshd** process is stopped and restarted whenever you change the security level.

Table 34: Access Security Levels for SSH Connections

Access Security Level	Description
very-low	• Enables root login. • Disables session inactivity timeout. • Enables Fedora Core OS default username/password restrictions. • Enables single-user mode login for password recovery. • Installs **tcpdump** and **hdparm** utilities. These files must exist in the **/tmp** directory.
low	• Disables root login. • Disables session inactivity timeout. • Enables Fedora Core OS default username/password restrictions. • Enables single-user mode login for password recovery. • Installs **tcpdump** and **hdparm** utilities. These files must exist in the **/tmp** directory.
high	• Disables root login. • Enables session inactivity timeout. • Enables elevated username/password restrictions. • Disables single-user mode login. • Removes **tcpdump** and **hdparm** utilities.

Table 35: Access Security Levels for CTPView GUI

Access Security Level	Description
low	Enables permissive username/password restrictions.

high	Enables elevated username/password restrictions.

Configuring an SSH Connection to a CTP Platform That Persists Through the Session (CTPView Server Menu)

IN THIS SECTION

This topic describes how to configure the CTPView server so that an SSH connection remains established for the entire session when the CTPView server connects to a CTP platform.

SSH port forwarding creates an encrypted and protected connection between the CTPView software and a remote CTP platform, that remains up as long as the server connection to the platform is up. It must be enabled on both the CTP platform and the CTPView software; it is enabled on both by default. When this feature is not enabled, the CTPView server creates a separate SSH connection to the platform for each command and configuration change. This feature reduces overhead and increases performance of the CTPView software. You can choose to disable this feature or reenable it.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To configure the CTPView server for port forwarding, you must first access the Port Forwarding Menu:

- From the CTPView Configuration Menu, select **3) Port Forwarding**.

  The Port Forwarding Menu is displayed.

Viewing the Current State of Port Forwarding (CTPView Server Menu)

To display the current state of port forwarding on the CTPView server:

- From the Port Forwarding Menu, select **1) View Current State**.

The state is displayed, Allowed or Prohibited.

Setting Port Forwarding Permissions (CTPView Server Menu)

To set the permissions for port forwarding on the CTPView server:

1. From the Port Forwarding Menu, select **2) Set Port Forwarding Permissions**.
2. Select **1) Allow** or **2) Prohibit**.

   The new state is displayed.

Closing Port Forwarding Sockets (CTPView Server Menu)

To close all open port forwarding sockets on the CTPView server:

- From the Port Forwarding Menu, select **3) Close Port Forwarding Sockets**.

Clearing Open Sockets by Restarting the Apache Daemon (CTPView Server Menu)

When you configure port forwarding, you may want to clear all the open sockets that were used for the previous port forwarding configuration. You can do so by restarting the Apache daemon.

To restart the Apache daemon on the CTPView server:

- From the Port Forwarding Menu, select **4) Restart Apache Daemon**.

You can also restart the Apache daemon elsewhere in the server menus. From the CTPView Configuration Menu, select **7) CTPView Access Functions > 2) Restart Apache Daemon**.

RELATED DOCUMENTATION

Configuring an SSH Connection to a CTP Platform that Persists Through the Session (CTPView) | 127

Saving the CTPView Configuration Settings and Data (CTPView Server Menu)

This topic describes how to save the current configuration settings and data for the CTPView software. Although you can perform this task at any time, it is typically performed before you upgrade the CTPView server OS and the CTPView software.

You can use the backup utility in the CTPView server menu to save the information into an archive (`.tgz`) file and, if desired, move the archive to an external storage device. If you do not use the utility to move the archive, you can later copy or move it manually from outside the CTPView server menu.

> **NOTE**: If you do not move the archive file to an external storage device, you are not protected from loss of the backed-up data. If you are upgrading the software, you must move the file to an appropriate location.

Alternatively, when you have more than one CTPView server, you can use the CTPView software GUI to synchronize the server with another server to save the settings and data. See "Synchronizing Multiple CTPView Servers (CTPView)" on page 159 for the synchronization procedure.

> **NOTE**: We recommend that you use the CTPView server backup utility to save your current information.

Before you use the CTPView server backup utility:

- Confirm that the external storage device is running a UNIX-like operating system and is enabled for SSH connections.

  > **NOTE**: Although the external storage device can use any operating system, the CTPView backup utility can automatically transfer the backup file only to a device that is running a UNIX-like operating system. If the device is running a different kind of OS, you must transfer the backup file with a copy utility that is compatible with that OS.

- Confirm that a network path exists between the CTPView server and the external storage device used for storing the backup file.
- Confirm that the hard drive on the CTPView server that you are backing up has at least 25 percent free space. If you attempt to run the backup utility when less than 25 percent free space is available, the utility prompts you to delete more old data files before you continue. See "Creating More Disk Space on the CTPView Server (CTPView)" on page 17.
- Log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To back up your current information with the CTPView server backup utility:

1. From the CTPView Configuration Menu, select **5) Backup Functions**.

   The Backup Functions Menu is displayed.

2. Select **1) Save Current Settings and Data**.

   If an archive file already exists in the `/var/www/html/acorn/data` directory on the server, the utility prompts you to delete or move the archive.
3. (Optional) From outside the menu (for example, in another terminal window), manually move the old archive to an external storage device if you want to save the information.
4. Enter **y** to delete the old archive.

   The utility deletes the old archive file and creates the new archive file.
5. Enter **y** to move the new archive to an external location.
6. Follow the prompts to enter the IP address, username, and absolute path to the external device.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | **14**

Creating More Disk Space on the CTPView Server (CTPView) | **17**

Creating More Disk Space on the CTPView Server (CTPView Server Menu) | **18**

Creating More Disk Space on the CTPView Server (CTPView Server Menu)

This topic describes how to create free space by removing redundant data files from the server.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To delete old files to create more free disk space:

1. From the CTPView Configuration Menu, select **5) Backup Functions**.

   The Backup Functions menu is displayed.
2. Select **3) Remove Redundant Binary Data Files**.

RELATED DOCUMENTATION

Saving the CTPView Configuration Settings and Data (CTPView Server Menu) | **16**

Installing or Upgrading the CTPView Server OS | **14**

Restoring CTPView Software Configuration Settings and Data with the Restore Utility (CTPView Server Menu)

This topic describes how to use the CTPView restore utility to restore the CTPView software configuration settings and data from a previously saved archive file.

Before you begin:

- Copy the backup (archive) file from its externally saved location to the `/var/www/html/acorn/data` directory on the server. The filename is in the format `ctpview_data_`*`server-name_date`*`.tgz`.
- Log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To restore your saved information with the CTPView restore utility:

1. From the CTPView Configuration Menu, select **5) Backup Functions**.

   The Backup Functions menu is displayed.
2. Select **2) Restore Settings and Data**.

   You are prompted to use the archive file. After the restore script runs, you are prompted to run it again.

Using the restore utility, you can restore the following CTPView configuration settings and data:

- Server synchronization on CTPView
- AutoSwitch configuration for CTP devices
- Configuration of CTP devices on CTPview (addition of CTP devices in groups)
- Configuration of remote bundles (CTP, SAToP, and CESoPSN)
- Network monitoring configuration on CTPView
- NTP configuration for CTP devices
- RADIUS configuration for CTP devices
- Syslog configuration for CTP devices
- SNMP and SNMP trap configurations for CTP devices

NOTE: We recommend that you use CTPView server synchronization to restore your data.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

Restoring CTPView Software Configuration Settings and Data (CTPView) | 20

Restarting the PostgreSQL Server (CTPView Server Menu)

NOTE: Restart the PostgreSQL server only under the guidance of the Juniper Networks Technical Assistance Center (JTAC).

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To restart the PostgreSQL server on the CTPView server:

1. From the CTPView Configuration Menu, select **6) PostgreSQL Functions**.
2. Select **3) Restart PostgreSQL Server**.

   The PostgreSQL server is stopped and then restarted.

Setting the Logging Level (CTPView Server Menu)

You can specify the logging level, which determines what events are logged The log output is placed in the **/var/log/acorngui.log** file.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To set the logging level:

1. From the CTPView Configuration Menu, select **4) Advanced Functions**.
2. Select **7) Set Logging Level**.
3. Enter one of the following:
   - **1) Normal (Most commands, All errors)**
   - **2) Debug Level 1 (All commands, All errors)**
   - **3) Debug Level 2 (All commands, All output)**

NOTE: Starting with CTPView Release 7.2R1, that occur, attempts to log in that are unsuccessful and failed login attempts to access-denied functionalites are recorded in the log file.

CHAPTER 16

Restoring Default Values on the CTPView Server

IN THIS CHAPTER

Resetting the Default System Administrator Account (CTPView Server Menu)

You can remove the configured values for the CTPView System Administrator account and restore the default values.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To reset the System Administrator account and password to the new values:

1. From the CTPView Configuration Menu, select **4) Advanced Functions**.
2. Select **6) Reset account for default System Administrator**.

Resetting the Data File Permissions (CTPView Server Menu)

You can remove all configured permissions for the CTPView server data files.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To reset the data file permission values:

1. From the CTPView Configuration Menu, select **4) Advanced Functions**.

2. Select **5) Reset Data File Permissions**.
3. Enter **1) Yes** when prompted to continue.

Resetting the CTPView System Files to the Default Values (CTPView Server Menu)

You can remove all configured values for the CTPView server system files and restore the default values.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To reset the CTPView system files to the default values:

1. From the CTPView Configuration Menu, select **4) Advanced Functions**.
2. Select **3) Reset System Files to default CTPView values**.
3. Enter **1) Yes** when prompted to continue.

CTPView displays information about the actions taken, as shown in the following sample output.

```
***************************************************************************
  Modifying the system files on this server to Juniper CTPView default values . . .

===== Refreshing log directory  =====
===== setting log file permissions =====
=====  Verifying default umask  =====
=====  Updated runtime level in /etc/inittab file =====
=====  Serial console access already set in /etc/inittab file =====
=====  Added ttyS0 to /etc/securetty file =====
=====  Serial parameters already set in /boot/grub/grub.conf file  =====
=====  Timeout parameters already set in /boot/grub/grub.conf file  =====
=====  CTPView title already set in /boot/grub/grub.conf file  =====
=====  Disabling pool.ntp.org servers in /etc/ntp.conf file  =====
=====  Enabling 127.127.1.0 as local clock in /etc/ntp.conf file  =====
Shutting down ntpd:                        [  OK  ]
Starting ntpd:                             [  OK  ]
=====  Setting status of system services  =====
  == set httpd on
Stopping httpd:                            [  OK  ]
Closing CTPView sockets:                   [  OK  ]
Starting httpd:                            [  OK  ]
```

```
  == set ntpd on
Shutting down ntpd:                    [  OK  ]
Starting ntpd:                         [  OK  ]
  == set sendmail on
Shutting down sm-client:               [  OK  ]
Shutting down sendmail:                [  OK  ]
Starting sendmail:                     [  OK  ]
Starting sm-client:                    [  OK  ]
  == set sshd on
Stopping sshd:                         [  OK  ]
Starting sshd:                         [  OK  ]
  == set PostgreSQLd on
Stopping PostgreSQL:                       [  OK  ]
Starting PostgreSQL:                       [  OK  ]
  == set network on
Shutting down interface eth0:              [  OK  ]
Shutting down loopback interface:          [  OK  ]
Bringing up loopback interface:              [  OK  ]
Bringing up interface eth0:                 [  OK  ]
  == set auditd on
Stopping auditd:                       [  OK  ]
Error deleting rule (Operation not permitted)
Starting auditd:                       [  OK  ]
Error deleting rule (Operation not permitted)
There was an error in line 7 of /etc/audit/audit.rules
  == set anacron off
  == set atd off
  == set netfs off
  == set nfslock off
  == set NetworkManager off
===== File /etc/cron.daily/00-logwatch did not exist
===== Directory /mnt/usbhd already exists
===== Directory /mnt/flash already exists
===== Directory /mnt/cdrom already exists
===== Cleared /etc/resolv.conf file
===== Restarting network daemon =====
Shutting down interface eth0:              [  OK  ]
Shutting down loopback interface:          [  OK  ]
Bringing up loopback interface:              [  OK  ]
Bringing up interface eth0:                 [  OK  ]
=====  nullok option already disabled in /etc/pam.d/system-auth file  =====
=====  Setting credit options in /etc/pam.d/system-auth file  =====
=====  Setting remember options in /etc/pam.d/system-auth file  =====
```

```
=====  Setting configuration in /etc/ssh/sshd_config file  =====
=====  Setting configuration in /etc/ssh/ssh_config file  =====
=====  Setting single user login configuration  =====
=====  Setting login.def parameters  =====
=====  Setting man file permissions  =====
=====  Setting access.conf parameters  =====
=====  Disable <Ctrl><Alt><Del>  =====
=====  Setting root directory file permissions  =====
=====  Setting nosuid in fstab file  =====
=====  Setting allowable cron access  =====
=====  Setting cron permissions  =====
=====  Setting httpd permissions  =====
=====  Setting logwatch.pl permissions  =====
=====  Setting denied at access  =====
=====  Setting sysctl parameters  =====
=====  Setting traceroute permissions  =====
=====  Disable decode alias  =====
=====  Setting snmpd permissions  =====
=====  Setting rsyslog permissions  =====
=====  Setting encryption parameters  =====
=====  Setting security tools permissions  =====
=====  Rotating logs  =====
=====  Removing non-owned files =====
find: /proc/4297/task/4297/fd/4: No such file or directory
find: /proc/4297/task/4297/fd/4: No such file or directory
find: /proc/4297/task/4297/fdinfo/4: No such file or directory
find: /proc/4297/task/4297/fdinfo/4: No such file or directory
find: /proc/4297/fd/4: No such file or directory
find: /proc/4297/fd/4: No such file or directory
find: /proc/4297/fdinfo/4: No such file or directory
find: /proc/4297/fdinfo/4: No such file or directory
=====  Restarting sshd =====
Stopping sshd:                          [  OK  ]
Starting sshd:                          [  OK  ]
=====  Disabling welcome page  =====
=====  Disabling browser access to manual  =====
=====  Setting KeepAlive to On  =====
=====  Setting StartServers to 8  =====
=====  Setting MaxSpareServers to 10  =====
=====  Setting -ExecCGI Option  =====
=====  Setting -FollowSymLinks Option  =====
=====  Setting -IncludesNOEXEC Option  =====
=====  Setting -MultiViews Option  =====
```

```
=====  Setting -Indexes Option  =====
=====  Setting LimitRequestBody Option  =====
===== Restarting httpd daemon =====
Stopping httpd:                          [  OK  ]
Closing CTPView sockets:                 [ NONE ]
Starting httpd:                          [  OK  ]
=====  Setting cgi-bin permissions  =====
=====  Setting htpasswd permissions  =====
===== Removing application/x-shell mime types =====

>>>>>>   JUNIPER  SERVER  MODIFICATIONS  COMPLETE.   <<<<<<
```

NOTE: 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.

Resetting the Default Firewall Settings (CTPView Server Menu)

You can remove all configured values for the CTPView server firewall and restore the default values.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To reset the CTPView server firewall settings to the default values:

1. From the CTPView Configuration Menu, select **4) Advanced Functions**.
2. Select **1) Reset Default Firewall Settings**.
3. Enter **1) Yes** when prompted to continue.

   The default firewall values are restored in **/etc/sysconfig/iptables**. The NTP daemon is started, and the SSH daemon is stopped and then restarted.

CHAPTER 17

Changing Administrative Passwords to Improve Access Security

IN THIS CHAPTER

Changing Passwords to Improve Access Security

A number of administrative passwords must be changed when you install a new CTPView server or upgrade the software. Juniper Networks also recommends that you change the following administrative passwords at least on an annual basis, and whenever CTP network administrators are changed.

To change administrative passwords:

- Change the BIOS menu password.

  See "Changing the BIOS Menu Password (CTPView Server CLI)" on page 35.

- Change the CTPView server’s root account password.

  See "Changing the Server's Root Account Password (CTPView Server CLI)" on page 36.

- Change the GRUB Boot Loader password.

  See "Changing the GRUB Boot Loader Password (CTPView Server Menu)" on page 37.

- Change the PostgreSQL Apache account password.

  See "Changing the PostgreSQL Apache Account Password (CTPView Server Menu)" on page 38.

- Change the PostgreSQL Administrator account password.

  See "Changing the PostgreSQL Administrator Account Password (CTPView Server Menu)" on page 39.

Changing the BIOS Menu Password (CTPView Server CLI)

For security purposes, change the default password for BIOS menu access. This account has no username associated with it. The BIOS menu password should conform to your local password requirements.

> **BEST PRACTICE**: Change the BIOS menu password at least yearly and whenever administrators change.

To change the BIOS menu password:

1. Power on or reboot the server.
2. During the boot process, press F2 while the Dell logo is displayed on the monitor. The boot process continues and displays several messages in turn on the screen.
3. Enter the default password when the process pauses and displays “Enter Setup Password.”

   For the default BIOS menu password, see "Default CTPOS and CTPView Accounts and Passwords" on page 94.
4. At the BIOS menu, select **System Security** and press Enter.
5. Highlight **Setup Password**—be sure that you have not selected **System Password**—and press Enter.
6. Enter your new BIOS password, reenter it, and then Press Enter to continue.
7. Press Esc.
8. In the window that opens, select **Save Changes and Exit** and press Enter.

   The server restarts.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

Changing the Server's Root Account Password (CTPView Server CLI)

For security purposes, change the password for the server's root user account at regular intervals. The root account password should conform to your local password requirements.

> **BEST PRACTICE**: Change the root account password at least yearly and whenever administrators change.

To change the root account password:

1. Log in to the CTPView server as a non-root user, using either a directly connected keyboard and monitor or an SSH application over your network.

   > **NOTE**: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

2. Enter **su -** to switch to the root account.
3. Enter the root password that you have set.

   You cannot log in using the root account.
4. Enter **passwd**.
5. Enter your new password.

RELATED DOCUMENTATION

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

Changing the GRUB Boot Loader Password (CTPView Server Menu)

For security purposes, change the default password for the GRUB Boot Loader menu.

> **BEST PRACTICE**: Change the GRUB Boot Loader password at least yearly and whenever administrators change.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

> **NOTE**: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To change the GRUB Boot Loader password:

1. From the CTPView Configuration Menu, select **Option 8 (GRUB Functions)**.
2. Select **1) Change GRUB password**.
3. Follow the prompts to complete changing the password.

RELATED DOCUMENTATION

- CTPOS and CTPView Software Password Requirements | **96**
- Configuring the CTPView Administrative Settings | **32**
- Changing Passwords to Improve Access Security | **238**

Changing the PostgreSQL Apache Account Password (CTPView Server Menu)

For security purposes, change the password for the PostgreSQL server Apache user account at regular intervals.

> **BEST PRACTICE**: Change the PostgreSQL Apache password at least yearly and whenever administrators change.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

NOTE: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To change the PostgreSQL Apache password:

1. From the CTPView Configuration Menu, select **6) PostgreSQL Functions**.
2. Select **2) Change PostgreSQL Apache password**.
3. Follow the prompts to complete changing the password.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | **96**

Configuring the CTPView Administrative Settings | **32**

Changing Passwords to Improve Access Security | **238**

Changing the PostgreSQL Administrator Account Password (CTPView Server Menu)

For security purposes, change the default password for the PostgreSQL server administrator user account.

BEST PRACTICE: Change the PostgreSQL administrator account password at least yearly and whenever administrators change.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

NOTE: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To change the PostgreSQL administrator account password:

1. From the CTPView Configuration Menu, select **6) PostgreSQL Functions**.
2. Select **1) Change PostgreSQL Administrator password**.
3. Follow the prompts to complete changing the password.

RELATED DOCUMENTATION

- CTPOS and CTPView Software Password Requirements | **96**
- Configuring the CTPView Administrative Settings | **32**
- Changing Passwords to Improve Access Security | **238**

CHAPTER 18

Configuring Access Control and Privileges

IN THIS CHAPTER

Configuring IP ACLs for Restricting Access to Resources (CTPView Server Menu)

An access control list (ACL) is a sequential collection of permit and deny conditions that you can use to filter inbound or outbound routes. You can use different kinds of access lists to filter routes based on The router compares each route's IP address against the conditions in the list, one-by-one. If the first match is for a permit condition, the route is accepted or passed. If the first match is for a deny condition, the route is rejected or blocked. The order of conditions is critical because testing stops with the first match. If no conditions match, the router rejects or blocks the address; that is, the last action of any list is an implicit deny condition for all routes.

You can define an access list to permit or deny routes on the basis of the IP address or the range of IP addresses. Each access list is a set of permit or deny conditions (based on how they match a route's address) for a route. A zero in the wildcard mask means that the corresponding bit in the address must be exactly matched by the route. A one in the wildcard mask means that the corresponding bit in the address does not have to be matched by the route. You can also specify a range of IP addresses, by entering the starting IP address and the ending IP address in the range separated by a hyphen (-), if you want to enable or disallow traffic from a set of IP addresses.

> **BEST PRACTICE**: We recommend that you modify the IP ACLs during periods of relatively low traffic to minimize network disruptions and outages in processing packets.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

NOTE: You cannot use an SSH application to access the CTPView server until you have configured the server in your network and assigned it an IP address. See "Configuring the Network Access (CTPView Server Menu)" on page 40.

To add, remove, or display IP ACLs:

1. From the CTPView Configuration Menu, select **6) PostgreSQL Functions**.
2. Select **6) IP ACL Function**. The IP ACL Function menu is displayed, which enables you to create a new ACL, delete a previously configured ACL, and view all the ACLs configured on your CTP device.

```
CTPView Configuration Menu

Please choose a menu item from the following list:

0) Exit CTPView Configuration Menu
1) Security Profile
2) System Configuration
3) Port Forwarding
4) Advanced Functions
5) Backup Functions
6) PostgreSQL Functions
7) CTPView Access Functions
8) GRUB Functions
9) AAA Functions

Please input your choice [0]: 6
************************************************************
     CTPView version 7.2R1-rc3 151120
     Server: ctpview    Date: Mon Dec  7 06:00:20 2015
     Release: CentOS release 5.11 (Final)
     Kernel: 2.6.18-406.el5
     User root logged in from 10.215.150.11 as root
     +++++  ALL  ACTIONS  ARE  LOGGED  +++++
************************************************************

PostgreSQL Menu

Please choose a menu item from the following list:

0) Return to previous menu
```

```
1) Change PostgreSQL Administrator password
2) Change PostgreSQL Apache password
3) Restart PostgreSQL Server
4) Initialize Web UI Template Accounts
5) IP ACL Function
6) Upgrade Database Structures

Please input your choice [0]: 5
************************************************************
     CTPView version 7.2R1-rc3 151120
     Server: ctpview    Date: Mon Dec  7 06:00:23 2015
     Release: CentOS release 5.11 (Final)
     Kernel: 2.6.18-406.el5
     User root logged in from 10.215.150.11 as root
     +++++  ALL  ACTIONS  ARE  LOGGED  +++++
************************************************************

IP ACL Function Menu

Please choose a menu item from the following list:

0) Return to previous menu
1) Add
2) Remove
3) Show

Please input your choice [0]: 1

Enter the IP or IP range[e.g 10.0.1-23.*]: 1.2.3.4

Specify the permission
0) Deny
1) Allow
Please input your choice [0]: 0
IP range/ IP address added successfully...

Hit return to continue...
```

3. Select **1) Add**
4. Follow the onscreen instructions and configure the options as described inTable 36 on page 247.

Table 36: Creating an IP ACL

Field	Function	Your Action
Enter the IP or IP range [e.g 10.0.1-23.*]	Specifies the IP address or a pool of IP addresses from which you want to enable or disallow traffic.	Specify an IP address in the format a.b.c.d/xx, where xx is the subnet prefix, or an IP address range in the format of *starting-address - ending -address*, with the starting and ending IP addresses separated by a hyphen (-).
Specify the permission	Specifies whether you want to enable or deny traffic from the specified IP address or range of addresses.	Select **0) Deny** to cause the CTP device to drop traffic arriving from the specified IP address. Select **1) Allow** to cause the CTP device to allow traffic arriving from the specified IP address. Specify `rtn` to set the interface that is prompted by the system to be specified as the default IPv4 circuit device. For example, if the prompt displays (`rtn for eth1`), and if you specify `rtn`, `eth1` is set as the default circuit device.

5. Press `Enter` to proceed to the next step of removing any of the configured IP ACLs. The IP ACL Function menu is displayed.
6. Select **2) Remove**. The IP address ranges or IP addresses for which you previously configured ACLs are displayed.

```
************************************************************
     CTPView version 7.2R1-rc3 151120
     Server: ctpview    Date: Mon Dec  7 06:01:04 2015
     Release: CentOS release 5.11 (Final)
     Kernel: 2.6.18-406.el5
     User root logged in from 10.215.150.11 as root
     +++++  ALL  ACTIONS  ARE  LOGGED  +++++
************************************************************

IP ACL Function Menu

Please choose a menu item from the following list:

0) Return to previous menu
1) Add
2) Remove
3) Show
```

```
Please input your choice [0]: 2
Current listing of IP range :
0) Return to previous menu
1) *.*.*.*
2) 1.2.3.4
3) 78.34.3.2
Please input your choice [0]:2
IP range/ IP address removed successfully...

Hit return to continue...
```

7. From the list of IP addresses displayed, select a number pertaining to your choice. Enter the number next to the `Please input your choice [0]` field. If you select **0**, you are returned to the previous menu.

   After you enter a number pertaining to your choice in the menu, a confirmation message is displayed stating that the selected IP address or range is successfully deleted.
8. Press `Enter` to proceed to the next step of viewing all the configured IP ACLs. The IP ACL Function menu is displayed.
9. Select **3) Show**. All the configured IP addresses and their corresponding permissions are displayed. The access modifier or permission of 1 denotes permit, and 0 denotes deny.

```
************************************************************
     CTPView version 7.2R1-rc3 151120
     Server: ctpview    Date: Mon Dec  7 06:01:14 2015
     Release: CentOS release 5.11 (Final)
     Kernel: 2.6.18-406.el5
     User root logged in from 10.215.150.11 as root
     +++++  ALL  ACTIONS  ARE  LOGGED  +++++
************************************************************
IP ACL Function Menu

Please choose a menu item from the following list:

0) Return to previous menu
1) Add
2) Remove
3) Show

Please input your choice [0]: 3
All database entries:
+-----------+------------+
 | iprange   | permission |
```

```
 +-----------+------------+
 | *.*.*.*   |          1 |
 | 78.34.3.2 |          0 |
 +-----------+------------+


Hit return to continue...
```

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Configuring the CTPView Administrative Settings | 32

Changing Passwords to Improve Access Security | 238

CHAPTER 19

Using Third-Party Software on CTPView Servers

IN THIS CHAPTER

Third-Party Software on CTPView Servers

You may choose to use third-party software on your CTPView server.

> **NOTE**: Third-party software installed on the CTPView server is not supported by Juniper Networks.

Typical third-party software is one of the following types:

- System file monitoring and management software

  Tripwire third-party software is preloaded onto the CTPView server. Tripwire facilitates security, intrusion detection, damage evaluation, and recovery. You can use this software to generate a baseline of system files and directories after you have configured your server to a known secure state. Tripwire subsequently monitors the system files and directories and compares them with the baseline, enabling you to identify any changes that have been made.

  Refer to the Tripwire documentation for more information. Complete documentation is located on the CTPView server in the **/usr/share/doc/tripwire-<*current-version-number*>** directory.

- Antivirus software

  McAfee VirusScan for UNIX, version 5.10.0, is the only antivirus application from a DOD-approved vendor that is compatible with CTPView server software.

The CTPView server includes a dedicated directory, **/var/av**, for installation of antivirus software. You must be a member of the **server** group to install the antivirus software directly into the **/var/av** directory. After the software archive is in the **/var/av** directory, follow the installation directions in the McAfee

product guide. We recommend that you select the default choices offered when installing the antivirus software. Refer to the antivirus documentation for more information about this software.

4

PART

Troubleshooting

CHAPTER 20

Validating the CTPView Server System Configuration

IN THIS CHAPTER

Validating the CTPView Server Configuration (CTPView)

This topic describes how to validate the CTPView server system configuration. Examining the system configuration information is a useful first step in troubleshooting many issues. Validate the configuration after installing or upgrading the CTPView software or server OS to determine whether the operation completed successfully.

The validation utility reports on a long list of configuration details that are critical or desirable for proper operation of the CTPView software. Instructions are provided for correcting items that are out of compliance.

To validate the system configuration:

1. Log in to the CTPView GUI.
2. In the side pane, select **Server > Diagnostics**.

   The System Information pane is displayed.
3. Click **Validate Server Configuration**.

   The Server Configuration Validation pane is displayed.
4. Confirm that all fields are set to their default values.

   The display indicates whether each item is valid or noncompliant. A highlighted field indicates a problem. Follow the displayed instructions to correct the problem.

RELATED DOCUMENTATION

Installing or Upgrading the CTPView Server OS | 14

CHAPTER 21

Restoring CLI Access to the CTPView Server

IN THIS CHAPTER

Restoring Access to a CTPView Server

You must use a nonroot password to log in to the CTPView server. If you lose all the nonroot passwords, then you cannot access the CTPView server.

To perform tasks on the server as a root user, you must first log in using an existing nonroot account. You then switch to the root account with the command **su -** and enter the root password.

This topic describes how to restore access to the CTPView server in any of the following events:

- You lose the passwords to all nonroot user accounts.
- You lose the root password.
- You lose the all nonroot user passwords and the root password.

Before you begin, you must have the GRUB Boot Loader password and physical access to the server with a connected monitor and keyboard.

If you have do not have the GRUB Boot Loader password, you must use the system motherboard jumpers to disable the password protection feature before proceeding. You can find details about how to perform this task on the Dell PowerEdge Documentation CD, which was included with the original packing material for the CTPView server.

To restore access to the CTPView server when you have lost all nonroot user passwords:

1. Access a shell.

See "Accessing a Shell on the CTPView Server (CTPView Server CLI)" on page 255.

2. Set a new password for a nonroot user account.

   See "Setting a New Password for a Nonroot User Account (CTPView Server CLI)" on page 256.

3. Create a temporary nonroot user account and password, access the root account, and create a new permanent nonroot user.

   See "Creating a Nonroot User Account and Password (CTPView Server CLI)" on page 257.

To restore access to the CTPView server when you have lost the root password:

1. Access a shell.

   See "Accessing a Shell on the CTPView Server (CTPView Server CLI)" on page 255.

2. Set a new password for a root user account.

   See "Setting a New Password for a Root User Account (CTPView Server CLI)" on page 257.

To restore access to the CTPView server when you have lost all nonroot user passwords and the root password:

1. Access a shell.

   See "Accessing a Shell on the CTPView Server (CTPView Server CLI)" on page 255.

2. Set a new password for a root user account.

   See "Setting a New Password for a Root User Account (CTPView Server CLI)" on page 257.

3. Set a new password for a nonroot user account.

   See "Setting a New Password for a Nonroot User Account (CTPView Server CLI)" on page 256.

4. Create a temporary nonroot user account and password, access the root account, and create a new permanent nonroot user account.

   See "Creating a Nonroot User Account and Password (CTPView Server CLI)" on page 257.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Accessing a Shell on the CTPView Server (CTPView Server CLI)

Before you begin, you must have physical access to the server with a connected monitor and keyboard.

To gain access to a shell:

1. Use the power switch on the server to turn off the power.
2. Turn on the server power.
3. When the blue GNU GRUB screen appears, enter the letter **p**. You have only a few seconds to do this.
4. Enter the GRUB Boot Loader password.
5. Enter the letter **e**.
6. Use the keyboard arrows to highlight the line that begins with the word **kernel**.
7. Enter the letter **e**.
8. Enter the following code at the end of the highlighted line:

   init=/bin/bash
9. Enter the letter **b**.

   The system boots and displays the **bash-3.00#** shell prompt.
10. Enter the following command:

    /bin/mount /dev/md2 -o remount,rw

RELATED DOCUMENTATION

Restoring Access to a CTPView Server | 254

Setting a New Password for a Nonroot User Account (CTPView Server CLI)

Before you begin, prepare the server by accessing the shell. See "Accessing a Shell on the CTPView Server (CTPView Server CLI)" on page 255.

To set a new password for a nonroot user account:

1. Enter the following command:

   /usr/bin/passwd *username*
2. Enter the new password for the nonroot user when prompted.
3. Enter the following command:

   /bin/mount /dev/md2 -o remount,ro
4. Enter the command **reboot**.

   Wait for the server to reboot.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Restoring Access to a CTPView Server | 254

Setting a New Password for a Root User Account (CTPView Server CLI)

Ensure that the new root account password conforms to your local password requirements.

Before you begin, prepare the server by accessing the shell. See "Accessing a Shell on the CTPView Server (CTPView Server CLI)" on page 255.

To set a new password for a root user account:

1. Enter the following command:

   /usr/bin/passwd
2. Enter the new password when prompted.
3. Enter the following command:

   /bin/mount /dev/md2 -o remount,ro
4. Enter the command **reboot**.

   Wait for the server to reboot.

RELATED DOCUMENTATION

Restoring Access to a CTPView Server | 254

Creating a Nonroot User Account and Password (CTPView Server CLI)

Before you begin, prepare the server by accessing the shell. See "Accessing a Shell on the CTPView Server (CTPView Server CLI)" on page 255.

To create a new account and password for a nonroot user:

1. Enter the following command:

   /usr/sbin/useradd *username*
2. Enter the following command:

   /usr/bin/passwd *username*
3. Enter the new password for the nonroot user when prompted.

4. Enter the following command:

   /bin/mount /dev/md2 -o remount,ro

5. Enter the command **reboot**.

   Wait for the server to reboot.

6. Log in as the new temporary user.
7. Enter the command **su -** to switch to the root account and display the CTPView Configuration Menu utility.
8. Create a new permanent nonroot user account.
9. Exit the utility, the root account, and then the temporary user account.
10. Log in as the new permanent nonroot user.
11. Enter the command **su -** to switch to the root account.
12. Enter the following command to delete the temporary user account:

    /usr/bin/userdel -r *username*

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

Restoring Access to a CTPView Server | 254

CHAPTER 22

Restoring Browser Access to a CTPView Server

IN THIS CHAPTER

Restoring Browser Access to a CTPView Server (CTPView Server Menu)

You cannot recover lost usernames and passwords. If you lose access to the CTPView GUI as a Global_Admin user, you can use the following procedure to restore the default Global_Admin user account *Juniper*, select a new password for user *Juniper*, and assign the user to the default user group *TempGroup*.

Before you begin, log in to the CTPView server and access the CTPView Configuration Menu. See "Accessing the CTPView Server Configuration Menu (CTPView Server Menu)" on page 197.

To restore browser access to the CTPView server:

1. From the CTPView Configuration Menu, select **7) CTPView Access Functions**.
2. Select **1) Reset password for default user Juniper**.
3. Follow the prompts to assign user *Juniper* to user group *TempGroup*. The user is given default user properties.
4. Log in to the CTPView GUI with the restored user password, and review the default user values in CTPView Admin Center. Make any appropriate changes.

CHAPTER 23

Changing a CTPOS User Password

IN THIS CHAPTER

Changing a User Password for a CTP Platform

The CTPOS software is installed on a CompactFlash card that normally operates in a read-only state. You must make the card writable in order to change a user password. Only the root user is allowed to make the CompactFlash card writable.

To change a CTP platform user's password:

1. Log in to the CTP platform as a nonroot user.
2. Enter the command **su -** to switch to the root account.
3. Enter the following command to make the CompactFlash card writable:

   mfw
4. Open a new SSH window and log in with the username whose password you want to change.
5. Follow the prompts to change the password.
6. Enter the command **su -** to switch to the root account.
7. Enter the following command to return the CompactFlash card to read-only:

   mfr

NOTE: For users who employ the utility SecureCRT for SSH to access the CTP platform, you must change the Authentication method on SecureCRT from the default setting of Password to Keyboard Interactive. If you fail to do so, the password prompts originating at the CTP platform are prevented from reaching your display, and the password update procedure fails.

RELATED DOCUMENTATION

CTPOS and CTPView Software Password Requirements | 96

CHAPTER 24

Booting the CTPView Server from the CD-ROM Drive

IN THIS CHAPTER

Booting the CTPView Server from the CD Drive

For security purposes, booting from the CD drive is disabled in the system BIOS settings. If you need to boot from a CD, you must reconfigure the BIOS. You must also have physical access to the server and have the BIOS Menu password.

If you have forgotten the BIOS Menu password, use the system motherboard jumpers to disable the password protection feature before proceeding. Details about how to perform this task are found on the Dell PowerEdge Documentation CD, which was included with the original CTPView server packing material.

To boot the CTPView server from the CD drive:

1. Connect a monitor, keyboard, and mouse to the server.
2. Power on the server and press F2 while the Dell logo is displayed.

   The phrase **Entering Setup** appears in the top right corner of the screen, and then the BIOS setup screen loads. If you miss pressing F2 at the proper time, press Ctrl+Alt+Delete to reboot the system so you can repeat this step.

   The bottom line on the screen contains help for navigating and modifying this menu.
3. Insert the CD boot disk into the CD drive.
4. Enter the BIOS Menu password, and press Enter to continue.
5. Highlight **Boot Sequence**, press Enter, and select **IDE CD-ROM device**. Press Enter to continue.
6. Press Esc. In the pop-up window highlight **Save Changes and Exit**, and press Enter.

   The server restarts and boots from the CD.

NOTE: For security considerations, it is important that you subsequently disable booting from a CD.

To disable booting from the CD drive:

1. Repeat Steps 1 through 4 above.
2. Highlight **Boot Sequence**, press Enter, and clear **IDE CD-ROM device**. Press Enter to continue.
3. Press Esc. In the pop-up window highlight **Save Changes and Exit**, and press Enter.

   The server restarts and boots from CompactFlash memory.

CHAPTER 25

Restarting the Apache Daemon In the Event of Browser Issues

IN THIS CHAPTER

Restarting the Apache Daemon (CTPView Server Menu)

If you are having problems viewing or accessing the CTPView GUI in your browser, you might want to restart the Apache daemon on the CTPView server.

To restore browser access to the CTPView server:

1. From the CTPView Configuration Menu, select **7) CTPView Access Functions**.
2. Select **2) Restart Apache Daemon**.

CHAPTER 26

Displaying Jitter Statistics in MIBs and Supporting Acorn MIB for Daemon Model

IN THIS CHAPTER

Support for Display of Jitter and Latency in the CTP Bundle Query Output on MIB Browser

IN THIS SECTION

Until CTPOS Release 7.1, the CTP bundle query does not provide statistics for jitter and latency. Starting with CTPOS and CTPView Release 7.2R1, jitter and latency values are displayed in the command used to query the CTP bundles. Latency is computed as follows:

Latency = RoundTripDelay / 2

where:

RoundTripDelay is the sum of the amount of time taken for a signal to be sent and the amount of time taken for an acknowledgment of that signal to be received.

Jitter is calculated as follows:

Jitter = (double) Span/ CTP_OSC_FREQ

where:

CTP_OSC_FREQ = 0x8000 or 32MHz

Span = Largest Buffer – Smallest Buffer

Two additional values are appended at the end of the following command to support bundle jitter and bundle latency.

```
[root@ctp_87 ctp_cmd 3]# cmd bndl 0 qry snmp v1;B;0;1;this is ctp bundle description of maximum length on te-0.0
port.;te-0/0;1;-1;10.216.118.88;0;0;0;10.0.0.1;1024;16.000;12.000;8.000;0;255;0x40;-1;-
1;3;20206060;20208183;0;24;88;86;0;1;10189;10089;6045;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;-1;4.145;
150;
```

Similarly, MIB objects for bundleJitter and bundleLatency are added in ACORN-MIB used by the MIB Browser.

Jitter and latency fields are added for the CTP, SAToP, CESoPSN, and VComp bundles. However, for VComp bundles, this value is always –1, and for SAToP and CESoPSN bundles, the latency field is always –1.

Enhanced snmpAcorn.pl to Support the Daemon Model

Until CTPOS Release 7.1, all SNMP requests for the Acorn MIB are rendered to the snmpAcorn.pl script, which computes the results and returns them to the requestor. It is observed that snmpAcorn.pl is causing high CPU usage for the complete SNMP walk of Acorn MIB. Starting with CTPOS and CTPView Release 7.2R1, the snmpAcorn.pl script is run in daemon mode. All the SNMP requests arrive first at the snmpAcorn client, which in turn sends an interprocess communication message (IPC) to the daemon. The daemon processes the request and sends it back to the snmpAcorn client. To enable this functionality of the daemon processing the SNMP requests, the snmpAcorn.pl has been enhanced to support the daemon model.

CHAPTER 27

CHAPTER 28

Knowledge Base