



Avaya Call Management System
CMS Upgrade Express for
Sun computers

Release 17.0
June 2014

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

<http://www.avaya.com/support>

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, <http://support.avaya.com/LicenseInfo/> ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at:

<http://support.avaya.com/ThirdPartyLicense/>

You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://www.avaya.com/support>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

<http://www.avaya.com/support>

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction	9
Purpose.	9
Intended audience	9
Related resources	9
Documentation.	9
Avaya Mentor videos	10
Documentation websites	11
Support.	11
Chapter 2: Preparing for the upgrade	13
Who must do upgrades	14
Verifying that the customer has prepared their system for an upgrade	14
Required hardware accessories	14
Remote support	15
Troubleshooting and escalation	15
Firmware updates	15
Switch software and link compatibility.	16
Hardware additions	16
Software considerations	16
Customization issues	17
Parts list	17
Checking for ACD 1	18
Recording storage interval data	19
Checking for a symbolic link between <code>/etc/hosts</code> and <code>/etc/inet/hosts</code>	19
Preserving the CMS authentication file	21
Checking the system battery	22
Chapter 3: Configuring the data extraction device	23
Extracting data to tape	23
Extracting data to a USB storage device.	24
Verifying the USB storage device is recognized by the CMS system	24
Extracting data to a network mount point	32
Configuring a NFS server	33
Solaris 10 NFS server configuration	34
Linux NFS server configuration.	35
Upgrading the system's firmware	37
Extracting customer administration and options	39
Determining if a RAID hardware controller is installed	50

Chapter 4: Replacing disk drives and adding RAID controller cards	53
Prerequisites	53
Upgrade procedures.	53
Labeling the old disk drives.	54
T5120 4-core front panel.	54
T5120 8-core front panel.	55
T5220 front panel	56
Netra X4270 front panel	56
T4-1 front panel	57
Removing the disk drives	57
Installing new disk drives	58
Installing the RAID hardware controller	59
Installing the T5120 4-core RAID hardware controller.	59
Installing the T5120 8-core RAID hardware controller.	60
Installing the T5220 RAID hardware controller	61
Installing the CUE flash image	63
Installing the CUE flash image on SPARC-based T5120, T5220, or T4-1 platforms	63
Installing the CUE flash image on an x4270 platform	71
Verifying the system recognizes the logical disk drive	75
Mounting an extract device	77
Mounting a USB storage device	78
Mounting a network server	79
Checking the status of the extract device	81
Verifying that the upgrade can continue	82
Performing a manual boot to the CUE Bootable DVD	83
Chapter 5: Copying and activating the customer's administration and options	87
Upgrading the CMS load (optional).	88
Installing Solaris patches	89
Removing the current CMS load	91
Installing CMS	92
Installing CMS patches	94
Copying customer data	96
Checking file differences between the old system and the new system.	98
Verifying files using pkgchk	99
Comparing directory and file permissions.	99
Linking the /etc/hosts file	100
Checking for installed Feature Packages and pseudo ACDs.	101
Checking the setup.out file	101

Activating customer options	103
Recovering from failed installation scripts	107
Scripts that can be skipped and installed later	107
Failures that require escalation to support	108
Failures that occur when adding features	109
Removing temporary ACD 1	109
Restoring the cms.install file	110
Turning on CMS	111
Starting CMS WebClient.	112
Certificate Management	112
Signing in.	112
Configuring Access Security Gateway.	113
Verifying that CMS is operating.	114
Verifying unmeasured trunks	114
Updating storage interval data	115
Checking manual merge discrepancies	115
Updating unmeasured trunks.	116
Updating the switch setup	116
Removing the upgrade files.	117
Authorizing ODBC Connections	118
Migrating customer data	119
Migrating system administration data	119
Migrating agent and call center administration data	121
Verifying that the CONSOLE parameter is set properly.	122
Verifying auto-boot is set to true	122
Replacing the customer's tapes	123
Turning the upgraded system over to the customer	123
Configuring alarming options.	123

Chapter 1: Introduction

Purpose

The document describes how to upgrade a Sun workstation from R15 to Avaya Call Management System (CMS) R17 or R16.x to CMS R17.

Intended audience

This document is intended for implementation engineers and system administrators.

Related resources

Documentation

See the following documents.

Table 1: Related documents

Title	Use this document to:	Audience
Implementing		
<i>Avaya Call Management System Upgrade Express Customer Requirements</i>	Upgrade from an earlier version without change in platform hardware.	Implementation engineers and system administrators

Table 1: Related documents

Title	Use this document to:	Audience
<i>Avaya Call Management System Sun T5120 / T5220 Computer Hardware Installation, Maintenance, and Troubleshooting</i>	Install, maintain, and troubleshoot Sun T5120/T5220.	Implementation engineers and system administrators
<i>Avaya Call Management System Sun Netra X4270 Computer Hardware Installation, Maintenance, and Troubleshooting</i>	Install, maintain, and troubleshoot Sun Netra X4270.	Implementation engineers and system administrators
<i>Avaya Call Management System Sun SPARC T4-1 Computer Hardware Installation, Maintenance, and Troubleshooting</i>	Install, maintain, and troubleshoot Sun SPARC T4-1.	Implementation engineers and system administrators

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to <http://www.youtube.com/AvayaMentor> and perform one of the following actions:

- Enter a key word in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Documentation websites

All CMS documentation can be found at <http://www.support.avaya.com>. New issues of CMS documentation will be placed on this website when available.

Use the following websites to view related support documentation:

- Information about Avaya products and services

<http://www.avaya.com>

- Sun hardware documentation

<http://docs.sun.com>

Support

Visit the Avaya website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Preparing for the upgrade

Before you start a CUE upgrade, use the following checklist of topics to prepare for the upgrade:

Topic	✓
Who must do upgrades on page 14	
Verifying that the customer has prepared their system for an upgrade on page 14	
Required hardware accessories on page 14	
Remote support on page 15	
Troubleshooting and escalation on page 15	
Firmware updates on page 15	
Switch software and link compatibility on page 16	
Hardware additions on page 16	
Software considerations on page 16	
Customization issues on page 17	
Parts list on page 17	
Checking for ACD 1 on page 18	
Recording storage interval data on page 19	
Checking for a symbolic link between /etc/hosts and /etc/inet/hosts on page 19	
Preserving the CMS authentication file on page 21	
Checking the system battery on page 22	

Who must do upgrades

Avaya-approved business partners, with Avaya Support Professional Specialist (ASPS) certification, are authorized to perform CMS implementation and upgrades. Only Avaya-authorized personnel can enable CMS licenses.



Important:

If these procedures are performed by nonauthorized personnel, the following consequences might occur:

- You might permanently lose data.
- The CMS system might be put in a nonfunctioning state for some time.
- You might be billed additional time and material expenses by Avaya.

Verifying that the customer has prepared their system for an upgrade

Before starting a CUE upgrade, customers must do maintenance backups and a CMSADM backup. If the customer has not done these backups, the upgrade cannot start. For more information, see *Avaya Call Management System Upgrade Express (CUE) Customer Requirements*. Verify that the backups were done as described in the *Customer Requirements* document before you start the upgrade.

Required hardware accessories

You must connect the following hardware to the system and make it operational before you start the upgrade:

- Monitor
- Keyboard
- Mouse
- Remote access device (Modem, SAL)

Remote support

All upgrade procedures are done at the customer site. However, when remote personnel such as CMS Provisioning are supporting the upgrade, the system commands used in this document are done by the remote personnel so they can monitor the progress of the upgrade. Run the commands from the local console only when there is no remote support or when you are instructed to run the commands.

Troubleshooting and escalation

If problems occur during the upgrade procedure:

1. Escalate the problem through normal channels.
2. Inspect the upgrade log file that is located at `/var/log/cvuelog`.
3. If the problem persists, shut down the system, reinstall the customer's old disk configuration, and bring the system back up under the old CMS load.

Firmware updates

Use this procedure for the T5120, T5220, and T4-1 platforms only.

This procedure determines if the firmware version of the system is compatible with the latest Solaris kernel patches.

1. Verify that you are logged in to the system as **root**.
2. Enter:

```
prtdiag -v | grep Firmware
```

```
Sun System Firmware 7.1.6.j <timestamp>
```

The minimum firmware version that supports the latest Solaris kernel patches is Sun System Firmware 7.2.0.

- If the system is a T5120 or T5220 platform and the firmware version is not at least 7.2.0, *do not* upgrade the system at this time. Contact Avaya Services to have a new firmware update applied through the Sun's Integrated Lights Out Manager (ILOM) interface.

- If the system is a T4-1 platform and the firmware version is not at least 8.3.0, make a note that you must perform the steps in [Upgrading the system's firmware](#) on page 37.
3. Continue with [Switch software and link compatibility](#) on page 16.

Switch software and link compatibility

CMS R15 or later does not support switch releases CM 1.0 or earlier. The upgrade extract tool recognizes the incompatibility. The tool requires you to enter a host name or IP address and TCP port before the upgrade can continue. Determine the host name or IP address and TCP port before you start the upgrade.



Important:

If the host name or IP address and TCP port information is not known during the CUE upgrade, you can enter fictitious information to get through the upgrade. The switch links do not become active until you update the switch setup information with accurate information.

Hardware additions

Do not perform hardware additions during an upgrade. For example, add RAM only after verifying that the upgrade was successful. Install the RAM as described in the maintenance and troubleshooting document for the computer.

Note:

This does not refer to disk drives or RAID HBAs. The Avaya CUE upgrade includes the proper number of supported disk drives, and all drives should be used for the upgrade.

Software considerations

The following software, at one time separate purchasable items, are now part of the standard CUE package:

- Expanded AUX

CMS Authorizations: All features that require authorization will need to be reauthorized as part of the CUE upgrade. You must also go through authorization to adjust any capacity values.

Customization issues

The upgrade process does not preserve third-party software packages and customizations, such as pseudo-ACDs. The customer or Avaya Professional services must collect, reinstall, recompile, and reconfigure any nonstandard CMS software after the upgrade is completed and approved.

**CAUTION:**

If Operational Analyst (OA) is installed, you must engage an Avaya resource for reinstallation. OA is a custom application that must be reinstalled after a CUE upgrade.

The customer data that the administrator copies during the upgrade procedure includes the following information:

- License information
- User login IDs and passwords
- System name and IP address
- Serial printer administration
- CMS administration, setup, and authorizations

For a complete list of the files copied during the upgrade, see the `/var/log/cvuelog` file after the upgrade is complete. A copy of the old system's `/etc/vfstab` file is saved in the `cvuelog` file.

Parts list

The following parts are delivered to the customer's site:

- Disk drives for your particular hardware configuration:
 - Four disk drives for the Sun T5120 4-core
 - Eight disk drives for the Sun T5220 and T5120 8-core
 - Eight disk drives for the Sun SPARC T4-1
 - Two disks for the Sun Netra X4270
- Blank labels used to identify the configuration of the old disk drives, for example, which slot is c1t0 or c1t1, and so on.
- RAID Adapter card

Note:

Some CUE kits for disk size upgrades do not include the RAID adapter or cables since those systems already have a RAID adapter installed.

- RAID Cable kit for T5120 and T5220 platforms only.
- CUE upgrade software disk labeled `r17cue1X.N`.
- A complete set of system software on a bootable disc. The CUE bootable software disc contains an image of a CUE system built with CMS software.

Note:

The CMS software disc ships with the CUE kit and contains the following software packages:

- Solaris 10
- Informix IDS
- Informix ILS
- Hardware drivers

Checking for ACD 1

You cannot upgrade a system when the administrator does not administer ACD 1. To determine whether the system has ACD 1 administered:

1. Log on to CMS.
2. Select **System Setup > Switch Setup > List All** to display a list of the administered ACDs. This list shows whether ACD 1 is administered.
 - If ACD1 exists, continue with [Recording storage interval data](#) on page 19.
 - If ACD1 does not exist, continue with [Step 3](#).
3. To add temporary ACD 1:
 - a. Enter:
`cmsadm`
 - b. Select the number that corresponds to the `acd_create` option.
This command adds the first unassigned ACD, which is ACD 1.
 - c. Enter the switch name and switch model. Enable vectoring and disconnect supervision. Enter **1** for the local port and enter **1** for the remote port.
 - d. Select TCP/IP for the link device and use an invalid IP address, it is acceptable to assign an invalid IP address since the temporary ACD will be deleted after the upgrade.

- e. For the remaining options, use the defaults or minimum values.

Recording storage interval data

During a CUE upgrade, not all storage interval data is preserved. The majority of the storage interval data is preserved in the `storage.def` file. However, the information for the data summarizing time, switch time zone offset, and master clock ACD are not part of the `storage.def` file.

To record this information so you can readminister it after the upgrade:

1. Log on to CMS.
2. Select **System Setup > CMS State** to display the Master ACD clock information.
3. Record the ACD displayed in the **Master ACD for clock synchronization** field.
4. For each ACD, Select **System Setup > Storage Intervals** to display the storage interval data for the ACD.
5. Record the **Data summarizing time** and the **Switch time zone offset**. You can print the screens to record the data.
6. Repeat Steps 4 and 5 for each ACD.

Checking for a symbolic link between `/etc/hosts` and `/etc/inet/hosts`

If the CUE extract process detects a unique `/etc/hosts` file *and* a unique `/etc/inet/hosts` file, the process cannot merge the differences between the two "hosts" files. The `/etc/hosts` file must be a symbolic link to `/etc/inet/hosts`.

To determine if the `/etc/hosts` file is a symbolic link to the `/etc/inet/hosts` file:

1. Enter:

```
ls -l /etc/hosts
```

The system displays a message similar to the following example showing the symbolic link:

```
lrwxrwxrwx  1 root    root          12 Feb 23  2002 /etc/hosts -> ./inet/hosts
```

2. Perform one of the following actions:

- If the system displays the symbolic link for `/etc/hosts` to `./inet/hosts`, continue with [Preserving the CMS authentication file](#) on page 21.
- If the system does not display a symbolic link for `/etc/hosts` to `./inet/hosts` and the system is operating properly, continue with Step 3.

3. Enter:

```
ifconfig -a
```

A message similar to the following example is displayed:

```
e1000g0: flags=201000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4,CoS> mtu 1500 index 2
inet 192.168.2.1 netmask ffffffff0 broadcast 135.9.94.255
ether 0:21:28:4:a1:e8
```

4. Enter:

```
more /etc/hosts
```

A message similar to the following example is displayed:

```
127.0.0.1      localhost
192.168.2.1    cvue      loghost
```

5. Compare the host network information from the `/etc/hosts` file to the output of the network information displayed with the `ifconfig` command. If the host IP addresses match as highlighted in the examples, the `/etc/hosts` file is probably the correct hosts file. However, since multiple administrators can independently modified either file, both files can contain important information.

After the CUE copy process, you will need to ensure that the `/etc/hosts` file and symbolic link are restored to their proper state. Inform the customer that two independent hosts files exist on the original system. Tell the customer that both files are preserved, but that the customer is responsible for merging any relevant information into the `/etc/inet/hosts` file after the upgrade.

The `/etc/hosts` file from the original system is preserved as `/manual_merge/etc/hosts` on the new system. The `/etc/inet/hosts` file from the original system is preserved as `/etc/inet/hosts` on the new system. Instructions for moving the `/etc/inet/hosts` file to `/etc/inet/hosts.orig` are provided later in this document.

Preserving the CMS authentication file

The upgrade process does not preserve the Avaya Access Security Gateway (ASG) Authentication File System (AFS) file. Avaya recommends that you obtain a new AFS authentication file. To obtain an AFS authentication file, refer to the section *Installing Access Security Gateway and the CMS Authentication File* in the *Avaya CMS Software Installation, Maintenance, and Troubleshooting for Solaris* document. If you obtain a new AFS authentication file prior to the upgrade, then save it to a non-CMS destination.

- If the customer currently uses ASG, perform the steps below to preserve the current AFS authentication file from the original CMS system. However, Avaya recommends that you obtain a new AFS authentication file.
- If the customer does not currently use ASG but plans to use ASG after the upgrade, you must obtain an AFS authentication file prior to configuring ASG. Do not save the AFS authentication file on the current CMS system of the customer. Save the AFS authentication file to a non-CMS destination that is accessible after the `cvue_activate` procedure is executed. Make a note of the destination path where the AFS authentication file is saved.

Note:

ASG can be installed and configured independent of CUE.

- If the customer does not currently use ASG and does not plan to use ASG after the upgrade, continue with [Configuring the data extraction device](#) on page 23.
1. Verify that you are logged in to the system as root.
 2. Copy the AFS authentication file to a destination path that is accessible after the `cvue_activate` procedure has been executed. Enter:

```
cp -p /etc/asg/lacfile <destination_path>/AFS_file.xml
```

Note:

The destination path can be a USB device, a network mount point, or another computer that is accessible from the CMS computer. Depending on the destination path, you may require a secure copy. For example, you may need to use `scp` instead of `cp`.

3. Verify that the AFS authentication file was copied to the destination directory.
4. Verify that the AFS authentication file properties are consistent with the original file.
5. Continue with [Configuring the data extraction device](#) on page 23.

Checking the system battery

Perform a battery check using the following steps prior to an upgrade:

1. Check if any pre-existing battery alarms exist. Enter:

```
/cms/aom/bin/active_alarms
```

- If BATTERY_WRN and BATTERY_ERR alarms exist, continue with Step [2](#).
- If BATTERY_WRN and BATTERY_ERR alarms do not exist, continue with Step [4](#).

2. Clear pre-existing BATTERY_WRN and BATTERY_ERR alarms. Enter:

```
/cms/aom/bin/alarm_resolve -a BATTERY_WRN
```

```
/cms/aom/bin/alarm_resolve -a BATTERY_ERR
```

3. Check if battery alarms exist. Enter:

```
/cms/aom/bin/active_alarms
```

4. Run the command to check the battery for errors. Enter:

```
/olds/chkDisks
```

If there are battery errors, the system logs the battery errors in file `/olds/log`.

5. Check if the system generates a new battery alarm. Enter:

```
/cms/aom/bin/active_alarms
```

Chapter 3: Configuring the data extraction device

To minimize the time that the system is out of service during the upgrade, you can extract the customer's administration and options while the system is operating. Do not allow the customer to make any administration changes once the extract process starts.



Important:

When remote personnel such as CMS Provisioning support the upgrade, stop here and contact the provisioning group. When remote personnel support the upgrade, the remote personnel use the system commands in this section to monitor the progress of the upgrade. Run the commands from the local console only when instructed or when there is no remote support.

- If the extract device is a tape drive, continue with [Extracting data to tape](#) on page 23.
- If the extract device is a USB storage device, continue with [Extracting data to a USB storage device](#) on page 24.
- If the extract device is a network mount point, continue with [Extracting data to a network mount point](#) on page 32.

Extracting data to tape

To extract the customer's administration and options to tape:

1. For the tape being used with the upgrade, check for the following requirements:
 - Ensure that you are using the correct tape.
 - Ensure that the tape is not write-protected.
2. You must read the following Important note before running the command in this step:



Important:

If the system has more than one tape drives, the upgrade program defaults to the tape drive that has a tape installed and that has the lowest SCSI ID. To prevent using the wrong tape drive, remove the tapes from any other tape drives.

Label the blank tape "Upgrade Extract," and insert the tape into the tape drive.

3. Continue with [Extracting customer administration and options](#) on page 39.

Extracting data to a USB storage device

The customer is responsible for the proper configuration of the USB storage device and connectivity to the CMS system. CMS only supports USB Removable Mass Storage devices formatted using the UFS file system. Solaris may detect USB storage devices formatted with other file system types but CMS only supports the UFS file system. If your USB storage device is formatted with any file system type other than UFS you will need to reformat the device using UFS. The USB storage device must be formatted, Solaris will not allow an unformatted USB storage device to be mounted.



Important:

It is the responsibility of the customer to ensure that the CMS system detects the USB storage device and users can perform read and write operations to and from the USB storage device. This document provides information as a reference to aid in troubleshooting USB storage device recognition issues but you should NOT contact Avaya to resolve any issues with your USB storage devices. Instead, contact your system administrator to resolve any USB storage device issues. Ensure you can write to and read from the installed USB storage devices before performing any Maintenance or CMSADM backups.

Verifying the USB storage device is recognized by the CMS system

Output from the `rmformat` command provides information that is needed to mount the USB storage device.

1. Insert the USB storage device.
2. Enter: `rmformat`

Note:

`rmformat` is defined as removable media format.

The output of the `rmformat` command is shown below:

```
Looking for devices...
  1.Volmgt Node: /vol/dev/aliases/cdrom0
    Logical Node: /dev/rdisk/c0t0d0s2
    Physical Node: /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/
storage@2/disk@0,0
    Connected Device: TSSTcorp CD/DVDW TS-T632A 3R03
    Device Type: DVD Reader/Writer
  2.Volmgt Node: /voi/dev/aliases/rmdisk0
    Logical Node: /dev/rdisk/c6t0d0s2
    Physical Node: /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/hub@4/
storage@2/dlsk@0,0
    Connected Device: Kingston DataTraveler 2.0 PMAP
    Device Type: Removable
  3.Volmgt Node: /vol/dev/aliases/rmdisk1
    Logical Node: /dev/rdisk/c7t0d0s2
    Physical Node: /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/
storage@1/disk@0,0
    Connected Device: HDT72252 5DLATSO V440
    Device Type: Removable
```

The Logical Node, Connected Device and Device Type information is used to identify the USB storage devices. Connected Device identifies manufacturer and model information. Device Type identifies the type of device. USB storage devices are identified as "Removable". Locate all devices that are identified as "Removable". Use the Connected Device information to locate the specific USB storage device of interest.

Examine items 2 and 3 from the `rmformat` output above. These items are USB storage devices and are identified as Removable devices. Note that the Logical Node for item 2 is identified as `/dev/rdisk/c6t0d0s2`, which identifies the controller and slot information of the device.

Note:

Mount all USB storage devices used by CMS under the directory `/rmdisk`. This will provide consistency for finding mounted USB storage devices and paths used by CMS.

3. Determine the size and available disk space of a USB storage device. Refer to the *Avaya CMS Administration* document for information on how to determine the amount of space needed for a maintenance backup of data.

Note:

Do not run this command if a backup is running since the device is already under heavy use.

Enter: `df -k1`

Note:

If multiple USB storage devices are installed but some devices are not displayed with the `df -kl` command, then the USB storage device is probably not formatted properly. Contact your system administrator to correctly configure the USB storage device. The following information is for reference only and should only be performed by experienced personnel.

4. Determine the file system type of a USB storage device.

Enter: `fstyp <logical_node_path>`

- If the output of the `fstyp` command is UFS, continue with Step [9](#).
- If the output of the `fstyp` command is ZFS, continue with Step [10](#).
- If the output of the `fstyp` command is not UFS or ZFS, continue with Step [5](#).

5. Format the USB storage device as ZFS.

Note:

UFS was used on SPARC systems with CMS R16.2. The ZFS filesystem works reliably on Solaris x86 systems, so it is preferred that you format all new USB storage devices with ZFS in CMS R17.0.



CAUTION:

Formatting a USB storage device will overwrite all data on the USB storage device and all data will be lost. Be sure you are certain you want to remove all data on the USB storage device. If you do not want to remove the data on the USB storage device, replace the USB storage device with a different USB device that can be formatted, and restart this procedure from Step [2](#).

You must create the ZFS filesystem in the root directory. The ZFS filesystem name or the pool name that you specify in the `zpool create` command must not include any slashes (/) so it can not be a subdirectory. The ZFS filesystem name or pool name must be unique or it will write over any existing directory. Avaya recommends that you create the ZFS mount points in the root directory to prevent problems due to administrators misplacing or forgetting mount point information.

- a. To change to the root directory, enter:

```
cd /
```

```
mkdir /CUE_extract_dir
```

- b. Disable the volfs service since it can interfere with ZFS mounting. Enter:

```
svcadm disable volfs
```

- c. To create the ZFS filesystem on the USB storage device, enter:

```
zpool create -f -o version=22 CUE_extract_dir {device_path}
```

where

`device_path` is the `logical_node_path` from the `rmformat` command, with `rdsk` replaced by `dsk`.

Example:

```
zpool create -f -o version=22 CUE_extract_dir /dev/dsk/  
c3t0d0p0
```



WARNING:

No warnings are given about overwriting old data. Do not run this command unless you are sure you do not want any data from the USB stick. The USB stick is now available at `/CUE_extract_dir`. You can use a different name but ensure that you are not using an existing directory name.

- d. To mount the USB storage device using ZFS, enter:

```
zpool import -a -f
```

- e. To display the ZFS pool name, enter:

```
zpool list
```

Note:

If the USB mount point was created in the root directory, the above command displays the ZFS pool name. Avaya recommends that you create the USB mount points in the root directory to prevent problems due to administrators misplacing or forgetting mount point information.

- f. You may now re-enable volfs using:

```
svcadm enable volfs
```

Note:

If a device format window opens, close the window.

- g. Verify that files can be written to and read from the USB storage device by creating a file on the USB storage device and accessing the file from the USB storage device.

Note:

You may have to update read and write permissions for the backup directories just created so that system and data backups can be performed by any user authorized to run these backups.

- h. Continue with [Extracting customer administration and options](#) on page 39.

6. Format the USB storage device as UFS.

- a. Disable the volfs service since it can interfere with UFS mounting. Enter:

```
svcadm disable volfs
```



CAUTION:

Formatting a USB storage device will overwrite all data on the USB storage device and all data will be lost. Be sure you want to remove all data on the USB storage device. If you do not want to remove the data on the USB storage device, replace the USB storage device with a different USB device that can be formatted, and restart this procedure from Step 2.

- b. Identify the Logical Node of the device you want to be format.

Enter: `fdisk <logical_node_path>`

Example: `fdisk /dev/rdsk/c6t0d0s2`

In the above example the Logical Node path of the USB storage device is `/dev/rdsk/c6t0d0s2`.

The system displays messages similar to the following:

```
Total disk size is 30515 cylinders
Cylinder size is 16065 (512 byte) blocks

          Cylinders
Partition Status Type Start End Length %
=====
1          IFS: NTFS 0  30514  30515 100

SELECT ONE OF THE FOLLOWING:
1. Create a partition
2. Specify the active partition
3. Delete a partition
4. Change between Solaris and Solaris2 Partition IDs
5. Exit (update disk configuration and exit)
6. Cancel (exit without updating disk configuration)
Enter Selection:
```

- c. Select the option to **Delete a partition**.

```
Specify the partition number to delete (or enter 6 to exit):
```

Enter the appropriate Partition number.

The system displays messages similar to the following:

```
Are you sure you want to delete partition X? This will make all
files and programs in this partition inaccessible (type "y" or
"n").
```

Enter: **y**

- d. Repeat Step 5.b until you have deleted all current partitions.

The system displays messages similar to the following:

```

Total disk size is 30515 cylinders
      Cylinder size is 16065 (512 byte) blocks

      Cylinders
Partition  Status  Type  Start End    Length  %
=====  =====  =====  =====  =====  ==

SELECT ONE OF THE FOLLOWING:
  1. Create a partition
  2. Specify the active partition
  3. Delete a partition
  4. Change between Solaris and Solaris2 Partition IDs
  5. Exit (update disk configuration and exit)
  6. Cancel (exit without updating disk configuration)
Enter Selection:

```

- e. Select the option to **Create a partition**.

The system displays messages similar to the following:

```

Select the partition type to create:
1=SOLARIS2  2=UNIX      3=PCIXOS      4=Other
5=DOS12     6=DOS16     7=DOSEXT     8=DOSBIG
9=DOS16LBA  A=x86 Boot   B=Diagnostic C=FAT32
D=FAT32LBA  E=DOSEXTLBA F=EFI        0=Exit?

```

- f. Select the option for **UNIX**.

The system displays messages similar to the following:

```

Specify the percentage of disk to use for this partition
(or type "c" to specify the size in cylinders).

```

- g. Partition 100% of the disk:

Enter: 100

The system displays messages similar to the following:

```
Should this become the active partition? If yes, it will be
activated each time the computer is reset or turned on.
Please type "y" or "n".
```

Enter: n

The system displays messages similar to the following:

```

Total disk size is 30515 cylinders
Cylinder size is 16065 (512 byte) blocks

Partition  Status      Type      Start    End    Length  %
=====  =====  =====  =====  =====  =====  ==
      1              Unix system  1      30514  30514    100

SELECT ONE OF THE FOLLOWING:
  1. Create a partition
  2. Specify the active partition
  3. Delete a partition
  4. Change between Solaris and Solaris2 Partition IDs
  5. Exit (update disk configuration and exit)
  6. Cancel (exit without updating disk configuration)
Enter Selection:
```

Select the option to "Exit (update disk configuration and exit)".

7. Create the UFS file system on the USB storage device.

Note:

Formatting the disk may take a long time depending on the speed and size of the disk.

Enter: `newfs <logical_node_path>`

The system displays messages similar to the following:

```
newfs: construct a new file system /dev/rdisk/c7t0d0s2: (y/n)?
```

Enter: **y** to continue.

The system displays messages similar to the following:

```
Warning: 142 sector(s) in last cylinder unallocated
/dev/rdisk/c10t0d0s2: 490223474 sectors in 79789 cylinders of 48 tracks,
128 sectors
239366.9MB in 4987 cyl groups (16 c/g, 48.00MB/g, 5824 i/g)
super-block backups (for fsck -F ufs -o b=#) at:
32, 98464, 196896, 295328, 393760, 492192, 590624, 689056, 787488,
885920,
Initializing cylinder groups:
```

8. Verify the file system type for the USB storage device is of type UFS.

Enter: `fstyp <logical_node_path>`

- If the output of the `fstyp` command is UFS, continue with Step [9](#).
- If the output of the `fstyp` command is not UFS, repeat Steps 6-8. If you cannot configure the device properly using the `fstyp` command, use a different USB storage device.

9. Mount the USB storage device. This mount procedure applies to file systems that are of type UFS.

- a. On the CMS server, create the mount point if the mount point does not exist, enter:

```
mkdir /CUE_extract_dir
```

- b. To mount the USB storage device, enter:

```
mount /dev/dsk/c#t#d0s2 /CUE_extract_dir
```

where `c#t#` is the controller and slot assignment.

Example: `mount /dev/dsk/c6t0d0s2 /CUE_extract_dir`

In the above example, the Logical Node is `c6t0d0s2`.

- c. To verify USB storage device is mounted, enter:

```
ls -l /CUE_extract_dir
```

The USB storage device directory should display a message similar to the following:

```
drwx----- 2 root root 8192 Oct 8 15:33 lost+found
```

- d. Turn on volmgt by entering:

```
svcadm enable volfs
```

Note:

If a device format window opens, close the window.

- e. Verify that files can be written to and read from the USB storage device by creating a file on the USB storage device and accessing the file from the USB storage device.

Note:

You may need to update read and write permissions for the backup directories just created so that system and data backups can be performed by any user authorized to run these backups.

10. Continue with [Extracting customer administration and options](#) on page 39.

Extracting data to a network mount point

The customer is responsible for the proper configuration of network mount points and connectivity to the CMS system.



Important:

Contact your system administrator before creating any shared mount points or network mount points. It is the responsibility of the customer to determine if any security violations will be made by creating share points and allowing other systems on the network to access the share points. Creating and sharing mount points should only be performed by experienced personnel.

It is the responsibility of the customer to ensure that the CMS system detects the network mount point and users can perform read and write operations to and from the network mount point. This document provides information as a reference to aid in troubleshooting network mount point recognition issues but you should NOT contact Avaya to resolve any issues with your network mount points. Instead, contact your system administrator to resolve any network mount point issues. Be sure you can write to and read from network mount points before performing a CUE extract to the mount point.

Configuring a NFS server

The customer is responsible for the correct configuration and connectivity between the NFS server and CMS system. Keep in mind the following points when you use NFS mounted directories:

- The NFS mount point must be accessible from the CMS system.
- The NFS server must have sufficient disk space for the backup of data.
- The directory path used when administering an NFS Back Up Device must exist on the NFS server.

The following procedures provide basic information about configuring a NFS server and CMS system to support CUE extracts to NFS servers:

- If the network server is Solaris, continue with [Solaris 10 NFS server configuration](#) on page 34.
- If the network server is Linux, continue with [Linux NFS server configuration](#) on page 35.

Solaris 10 NFS server configuration

Perform the following steps on the Solaris network server.

Note:

These steps are NOT performed on the CMS system. These steps are performed on the NFS server which must be a separate, non CMS, customer provided Solaris computer.

1. On the NFS server, create the network mount point, enter:

```
mkdir /network_server_mt_pt_dir
```

Example:

```
mkdir /CUE_NFS_dir
```

2. Set the permissions for the `network_server_mt_pt_dir`, enter:

```
chmod 755 /network_server_mt_pt_dir
```

```
chown nobody:nobody /network_server_mt_pt_dir
```

Example:

```
chmod 755 /CUE_NFS_dir
```

```
chown nobody:nobody /CUE_NFS_dir
```

Note:

Later, if you are unable to write to the network mount point on the CMS server indicated by a "Permission denied" message on the CMS server, you will need to set the owner and group to `nfsnobody`. Enter:

```
chown nfsnobody:nfsnobody /network_server_mt_pt_dir
```

3. Check if the network service is online, enter:

```
svcs | grep nfs
```

4. If the network service is online, the system displays messages similar to the following:

online	Nov_15	svc:/network/nfs/server:default
--------	--------	---------------------------------

5. If the network service is not online, enable the NFS network server by entering:

```
svcadm -v enable -r network/nfs/server
```

6. To share the Solaris network server, enter the following command at the command line on the Solaris network server:

```
share -F nfs -o rw=<CMS_ip_address> /network_server_mt_pt_dir
```

Example:

```
share -F nfs -o rw=<CMS_ip_address> /CUE_NFS_dir
```

7. To see what mount points are being shared, enter:

```
share
```

8. To unshare a single mount point, enter:

```
unshare /network_server_mt_pt_dir
```

Perform the following steps on the CMS system.

9. On the CMS system, create the network mount point directory, enter:

```
mkdir /CUE_extract_dir
```

10. To mount the Solaris NFS server, enter the following command on a single line:

```
mount -F nfs -o vers=3 <network_server_ip_address>:  
/network_server_mt_pt_dir - /CUE_extract_dir
```

Example:

```
mount -F nfs -o vers=3 xxx.xxx.xxx.xxx:/CUE_NFS_dir -  
/CUE_extract_dir
```

11. To change to the network server mount point directory, enter:

```
cd /CUE_extract_dir
```

12. To list the contents of the network server mount point directory, enter:

```
ls -l
```

Note:

There should be adequate space on the NFS server to extract the CUE data. The `cvue_extract` process displays a message about the amount of space needed for the extracted data after you have collected all the extract information. If there is an insufficient amount of space, the available space value is displayed along with the needed space value.

13. To unmount a network server mount point directory, enter:

```
umount /CUE_extract_dir
```

14. Continue with [Upgrading the system's firmware](#) on page 37.

Linux NFS server configuration

Perform the following steps on the Linux network server.

Note:

These steps are not performed on the CMS system. These steps are performed on the NFS server which must be a separate, non-CMS, customer provided Linux computer.

1. On the NFS server, create the network mount point, enter:

```
mkdir /network_server_mt_pt_dir
```

2. Set the permissions for the `network_server_mt_pt_dir`, enter:

```
chmod 755 /network_server_mt_pt_dir
chown nobody:nobody /network_server_mt_pt_dir
```

Example:

```
chmod 755 /CUE_NFS_dir
chown nobody:nobody /CUE_NFS_dir
```

Note:

Later, if you are unable to write to the network mount point on the CMS server indicated by a "Permission denied" message on the CMS server, you will need to set the owner and group to `nfsnobody`. Enter:

```
chown nfsnobody:nfsnobody /network_server_mt_pt_dir
```

3. To allow other systems to access the `network_server_mt_pt_dir`:
 - a. `vi /etc/exports`
 - b. Append the Linux network mount point information to the bottom of the file:

```
/network_server_mt_pt_dir <CMS_FQDN>(rw, sync)
```

Example: `/CUE_NFS_dir trapper1.dr.avaya.com(rw, sync)`

- c. Write and save the file.
4. To configure NFS and portmap to start on reboot:
 - a. Log in as `root`.
 - b. At the command line, enter: `ntsysv`
 - c. The system starts a GUI interface. Scroll through the list provided and verify that the `nfs` and `portmap` options are selected. These two options should be marked with an `x`.
 - d. Enter **TAB** to highlight **OK**.
 - e. Click **OK**.
5. Starting the NFS service:

Note:

When the `/etc/exports` file is changed, you must stop and start the NFS server.

- a. If the NFS service is not running, enter:

```
/etc/init.d/nfs start
```
 - b. If the NFS service is running, enter:

```
/etc/init.d/nfs restart
```
6. To verify the network service is running, enter:

```
service nfs status
```

Perform the following steps on the CMS system.

7. On the CMS system, create the network mount point directory, enter:

```
mkdir /CUE_extract_dir
```

8. To mount the Linux NFS server, enter the following command on a single line:

```
mount -F nfs -o vers=3 <network_server_ip_address>:  
/network_server_mt_pt_dir /CUE_extract_dir
```

Example:

```
mount -F nfs -o vers=3 xxx.xxx.xxx.xxx:/CUE_NFS_dir  
/CUE_extract_dir
```

9. To change to the network server mount point directory, enter:

```
cd /CUE_extract_dir
```

10. To list the contents of the network server mount point directory, enter:

```
ls -l
```

Note:

There should be adequate space on the NFS server to extract the CUE data. The `cvue_extract` process displays a message showing the amount of space needed for the extracted data after all the extract information has been collected. If there is an insufficient amount of space the available space value will be displayed along with the needed space value.

11. To unmount a network server mount point directory, enter:

```
umount /CUE_extract_dir
```

12. Continue with [Upgrading the system's firmware](#) on page 37.

Upgrading the system's firmware

Use this procedure for the T5120, T5220 and T4-1 platforms only.

1. Verify that you are logged in to the system as **root**.
2. Insert the R17.0 Avaya Call Management System software disc, accompanying the CUE kit, into the disc drive. Ensure that the software disc is correct for the platform, SPARC or x86.

3. Enter:

```
cd /
```

4. Enter:

```
/cdrom/cdrom0/spatches_conf
```

- If the system is a T4-1, continue with Step [5](#).
- If the system is a T5120 or T5220 platform, the system displays one of the following messages:
 - If the system firmware needs to be updated, but the current firmware version is too old to handle the latest Solaris kernel patches, the system displays the following message:

```
WARNING: System FW must be updated to accept latest Solaris patches.  
Contact Avaya Services to have a new FW update applied through the ILOM interface.  
  
WARNING!! Manually bypassing this check and installing the Spatches could leave your  
system unusable.
```



Important:

If the system displays this message, *do not* continue with the CUE procedure. Stop now. Contact Avaya Services to have a new firmware update applied through the ILOM interface as instructed in the message.

- If there are no firmware updates but there are Solaris patches to install, the system displays the following message:

```
Warning: you must close all applications before running this script  
.....  
.....  
.....  
Solaris patches have been spooled to your machine. The patches will  
be installed after rebooting. During the installation of patches  
your server will not be available.  
The estimated time to install all patches is: 15 minutes  
Ready to install Patches. Please leave the CD in the drive.  
You will need to reboot the server for patches to install.  
  
Do you want to reboot now? [y,n,?]
```

Do not update the Solaris patches as the spatches are incorporated in the CUE Bootable DVD.

Enter: **n**

Continue with Step [6](#).

5. If the T4-1 system firmware needs to be updated, the system displays the following message:

```
Warning: you must close all applications before running this script.

Patch configuration started: <timestamp>

WARNING: System FW must be updated to accept latest Solaris patches.
The FW update can be installed now if you wish.
Respond to the below request with y if you wish to install FW now.
This procedure will shutdown the system to apply the FW in ILOM and
could take 20 minutes to complete. After 20-30 minutes press the
Power button to restart the system. Will take ~15 mins. To come up

WARNING!! Manually bypassing this check and installing the Spatches could
leave your system unusable.

WARNING: Host will be powered down for automatic firmware update when download is
completed.

Do you want to continue(yes/no)?
```

Enter **y** to update the firmware version.

The system reboots. Log in to the system as **root**.

6. Remove the Avaya Call Management System software disc and put it in a safe place.
7. Continue with [Extracting customer administration and options](#) on page 39.

Extracting customer administration and options

1. To begin the CUE extract process, perform one of the following actions:
 - If doing the upgrade from the local console, log in as root.
 - If doing the upgrade remotely:
 - a. Log in as **cmssvc**.
 - b. Enter the appropriate password.
 - c. Enter:


```
su - root
```
 - d. Enter the appropriate password.
2. Enter:


```
cd /
```

3. Load the CUE upgrade software disc labeled `r17cue1X.N`.

The system displays the **File Manager** window. Click the cursor in an XTERM window.

4. After 15 seconds, enter `mount` to verify that the system detects the disc.

The system displays a list of devices and file systems that are currently mounted. The final line shows something similar to the following example:

```
.  
.  
/cdrom/Rxx.x cue on /vol/dev/dsk/cNt6d0/Rxx.x cue read only/XX/XX/XX on <time stamp>
```

5. Enter the following commands:

```
cd /cdrom/cdrom0  
./cvue_extract
```

The extract process starts. The system displays a message similar to the following example:

```
Beginning cvue_extract pre-check. Please wait...  
  
Pre-check completed.  
  
Using /var/tmp/new as temporary directory.  
  
CUE VERSION: r17cue1X.N  
  
Current CMS Version is : rlyxx.xl
```

6. The extract process first verifies whether CMS R17 supports the platform you are upgrading. One of the following conditions occur:

- If the platform is supported for CUE upgrades, the system displays the following message and the process continues with Step [7](#).

```
Checking for valid platform (get_server_platform)  
Your system is a(n) Platform_Type.  
This platform is supported by CMS 17.
```

- If the platform is not supported, the system displays a message similar to the following example. You cannot continue with the CUE upgrade:

```
Your system is <a(n) Platform_Type or not supported>. This platform is no longer
supported by CMS 17. Please read the message that follows ...

ERROR:
You have chosen to upgrade to CMS 17 from a CMS platform no longer supported by CMS 17.
Please consult the Avaya CMS Platform Upgrade and Data Migration manual for
instructions on migrating data from unsupported CMS platforms.

Exiting CMS Upgrade Express ...
```

7. The extract process next runs the CMS converter tool. The system displays messages similar to the following example:

```
Continuing with CMS Upgrade Express ...
Admin data will be saved
/var/tmp/new/adminsave/cmsadmin.saved
Converter completed successfully.
Please wait as administration files are extracted ...
```

8. The extract process determines if ACD 1 is administered. One of the following conditions occur:
 - If the system does not display error messages, ACD 1 is administered, and the extract continues with Step [9](#).
 - If the system displays the following error messages, ACD 1 is not administered, and you must temporarily add ACD 1:

```
ERROR:
ACD 1 is currently administered as a skipped ACD.
CUE cannot upgrade when ACD 1 is a skipped ACD.
Please run cmsadm, add a temporary ACD 1, then run
"./cvue_extract" again.
#
```

To add temporary ACD 1:

- a. Enter:
cmsadm
- b. Select the number that corresponds to the **acd_create** option.
This option adds the first unassigned ACD, which is ACD 1 in this example.
- c. Enter the switch name and switch model. Enable vectoring and disconnect supervision. Enter **1** for the local port and enter **1** for the remote port.
- d. When you select a link device, use TCP/IP with an invalid IP address, Since the ACD is deleted after the upgrade, it is acceptable to assign an invalid IP address.

- e. For the remaining options, use the defaults or minimum values.
 - f. Return to Step 5 and start the extract process again.
9. CMS R15 or later supports switch releases Communication Manager 2.0 and later. You might need to upgrade the ACDs when you upgrade CMS. The extract process checks each ACD to determine if any of the ACDs are administered with a switch model of Communication Manager 1.0 or earlier.

One of the following conditions occur:

- If this release of CMS supports all the ACDs, the extract continues with Step [16](#).
- If any ACD is administered using an unsupported switch model, the system displays messages shown in the following example:

```
The switch release <product><release> administered for <acd_name> (ACD <acd_number>)
is no longer supported.

Select the model of switch for this ACD:
  1) Communication Mgr 2
  2) Communication Mgr 3.0
  3) Communication Mgr 3.1
  4) Communication Mgr 4
  5) Communication Mgr 5.2
  6) Communication Mgr 6.x

Enter choice (1-6, or q to quit):
```

10. Enter the upgraded switch model for the ACD.

One of the following conditions occur:

- If another ACD is administered using an unsupported switch model, the extract returns to Step [9](#).
- If no other ACDs are administered using an unsupported switch model, the extract continues with Step [11](#).

11. Enter the host name or IP address of the switch.

The system displays messages similar to the following example:

```
You have entered the following TCP/IP information for <acd_name> (ACD <acd number>):
*****
Host name or IP address: <host_name or IP_address>
*****

If you would like to make changes to the entry above,
please enter "y" for Yes or "n" for No: (default: n)
```

12. Perform one of the following actions:

- If the assignment is correct, press **Enter**. The extract continues with Step [16](#).

- If the assignment is not correct, enter **y**. The following messages are displayed and the extract returns to Step [11](#).

```
CMS Upgrade Express is now returning to TCP/IP information prompts...

Revising TCP/IP Host Name <host_name or IP_address> per user request ...

Enter switch host name or IP Address or q to quit:
```

13. The system displays the following message:

```
Enter switch TCP port number (5001-5999 or q to quit): (default: 5001)
```

14. Enter the switch TCP port number.

The system displays messages similar to the following example:

```
You have entered the following TCP/IP information for <acd_name> (ACD <acd number>):
*****
TCP Port Number: <port_number>
*****

If you would like to make changes to the entry above,
please enter "y" for Yes or "n" for No: (default: n)
```

15. Perform one of the following actions:

- If the assignment is correct, press **Enter**. The system displays the following message.

```
...CMS Upgrade Express is updating <acd_name> (ACD <acd number>) with TCP/IP switch
information.
```

One of the following conditions occur:

- If there are more ACDs that must be converted to TCP/IP, the extract returns to Step [11](#).
- If there are no more ACDs that must be converted to TCP/IP, the extract continues with Step [16](#).
- If the assignment is not correct, enter **y**. The system displays the following messages and the extract returns to Step [14](#).

```
CMS Upgrade Express is now returning to TCP/IP information prompts...

Revising TCP Port Number <port_number> per user request ...

Enter switch TCP port number (5001-5999 or q to quit): (default: 5001)
```

16. Extracting the administration files takes several minutes. When extraction is complete, the system displays the following message:

NOTE: Be sure to review the cvuelog for any files to be merged manually in the upgraded system.

17. You must read the following note before proceeding:

Note:

CMS R17 or later no longer supports Visual Vectors Server software.

The extract process determines if Visual Vectors server software is currently installed on the system. If Visual Vectors server software is detected, the system displays the following message:

INFORMATION:

CUE has detected the existence of the Visual Vectors package.
Visual Vectors is no longer supported for CMS. Files under the
/opt/cc/aas/vector directory will NOT be preserved during this upgrade.

18. The extract process determines if alarm administration data needs to be migrated. If the customer has custom alarms, the administration data is preserved. The system displays the following message:

Alarm admin data will be migrated. Alarm logs will be preserved.

19. The extract process continues and the system displays the following message:

NN blocks
NNNNN blocks

20. The extract process determines if the `/etc/hosts` file is a symbolic link to the `/etc/inet/hosts` file. If it is not a symbolic link, the system displays the following message:

WARNING:

One or more differences were found between
the `/etc/hosts` and the `/etc/inet/hosts` files.
The `/etc/hosts` file has been preserved
and placed in the `/manual_merge` directory.
The `/etc/inet/hosts` file has been preserved
and will be placed in `/etc/inet/hosts` in the upgraded system.

Please review the `/manual_merge/README` file
to see a more detailed report of the difference(s).
IMPORTANT: The customer is responsible for determining
the proper entries in the `/etc/inet/hosts` file
and must link `/etc/hosts` to it for system conformity.

21. The extract process continues and the system displays the following messages:

```
.
.
.
Sendmail permissions will be fixed.

Serial printers will be administered
```

22. The extract process continues and the system displays the following messages:

```
Merging cvue_file_properties with cvuelog

Copying admin data.
Need 141231 KB space to save admin data
```



Important:

The above message displays the amount of available space needed on the extract device for the extract process to successfully write the extract file to the extract device. The extract process fails if there is not sufficient space on the extract device. Verify that the extract device has the amount of space that displayed in the above message.

23. The extract process prompts you to select an extract device type:



Important:

Systems that currently perform CMS Maintenance backups to tape must select the Tape extract device option or the CUE process will fail during the CUE activate process. Customers can convert to USB storage devices and network mount points for CMS Maintenance backups after the CUE process is complete.

```
Choose an extract device:
  1) Tape
  2) Other
Enter choice (1-2):
```

- If the extract device is a USB storage device or a network mount point, enter the number associated with the option `Other`, continue with Step [28](#).
- If the extract device is a tape drive, enter the number associated with the `Tape` option, continue with Step [24](#).

24. The system displays the following message about supported tape drives:

```
##### WARNING #####
Only the following tape drives will be supported in CMS 17:

40+ GB Tape drive

You must use a supported tape drive to continue with the CUE upgrade.

Please enter (q) to quit, any other key to continue:
```

25. Perform one of the following actions:

- If the tape drive you are using is not supported, press **q**. You cannot do a CUE upgrade. You must do a platform upgrade as described in *Avaya CMS Platform Upgrade and Data Migration*.
- If the tape drive you are using is supported, press **Enter** to continue.



Tip:

To track the progress of the extract from a different XTERM window, from a remote terminal, or from a local terminal, use the following command:

```
tail -f /var/tmp/new/var/log/cvuelog
```

26. The extract process checks the tape and the tape drive to determine if the tape is defective, write-protected, or not compatible with the tape drive. The system displays the following message:

```
Testing tape on /dev/rmt/N..
```

27. One of the following conditions occur:

- If the tape and tape drive are operational, the system does not display any error messages and the extract continues with Step [29](#).
- If the tape or tape drive are not operational, the system displays messages similar to the following example:

```
tar: /dev/rmt/N: Permission denied
Tape test failed!! Could not write and then read a file
from the tape at /dev/rmt/N.
Check the following items for possible problems:
  Verify the tape is not write-protected
  Verify the correct type of tape is in the tape drive
  Verify the tape is not defective
/cvue_extract[982]:TAPETESTFAILED:not found
```

Ensure that the tape is not write-protected and the tape is the correct tape for the tape drive. Clean the tape drive or using a different tape and start over with Step [5](#).

28. You must read the following Important note in this step before running the command:

**Important:**

The extract device path must exist on the CMS server and must be mounted.

Enter the extract device path.

29. The extract process writes the Admin data to the extract device. The system displays messages similar to the following example:

```
Admin data will be spooled to /dev/rmt/N
Copy complete.
```

30. Perform one of the following actions:

- If the system is a T5120, T5220 or T4-1 platform, continue with Step [31](#).
- If the system is an x4270 platform, continue with Step [35](#).

31. The extract process determines if the OpenBoot PROM (OBP) must be patched. The system displays the following messages:

**WARNING:**

In very few cases, the OBP is so old that you cannot update it through the normal procedure. Before you perform the CUE procedure, you must check all systems to ensure that the T5120/T5220 Firmware level is 7.2.0 or later. To check the Firmware level, enter:

```
prtdiag -v | grep Firmware
```

If the Firmware level is earlier than 7.2.0, you require a special connection and procedure to update the Firmware. Halt the CUE process and contact Avaya Services to get the Firmware updated.

```
Now checking for the need to update the OBP.
If the OBP is found to be in need of patching, the patch will be installed and the
system WILL be rebooted. You can continue your CUE upgrade after the reboot.
Pausing briefly....
```

32. The system displays the following message when extract process completes:

```
The cvue_extract process is complete.

Warning: you must close all applications before running this script

Patch configuration started: <time stamp>
```

33. No action is required for this step, but depending on your software version and platform, the system displays one of the following messages:

- If OBP is up-to-date, the system displays messages similar to the following example:

```
There are no Solaris patches to install.
```

- If the OBP is not up-to-date, the system displays messages similar to the following example:

**Important:**

You need to monitor the system during the Solaris patch installation process to ensure that the installation of the Solaris patches does not halt. Some Solaris patch updates cause the system to automatically reboot during the Solaris patch installation process. The Solaris patch installation process takes at least the amount of time that was estimated earlier in the procedure. It is possible that the system will power off as part of a Solaris patch installation. If the system powers off, you need to manually power on the system by pressing the power button. In some cases the system can power off before a Solaris patch is actually installed which means that the patch can install during boot up after the power button is pressed. The system can automatically power off again after the patch installs. If this occurs, you need to manually power on the system again. When the Solaris patch installation process completes, the system will automatically reboot into multiuser mode and display the graphical login screen.

**Tip:**

If the extract device is tape and the system needs to be powered on manually, perform Step [34](#).

```
Spooled <patch number>

Solaris patches have been spooled to your machine.  The patches will be
installed after rebooting.  During the installation of patches your
server will not be available.

The estimated time to install all patches is: xx minutes

Ready to install Patches. Please leave the CD in the drive.
Rebooting...

Patch configuration completed: <time stamp>

Shutdown started.      <time stamp>

Changing to init state 6 - please wait

Broadcast Message from root (pts/4) on <hostname> <time stamp>...
THE SYSTEM <hostname> IS BEING SHUT DOWN NOW ! ! !
Log off now or risk your files being damaged
```

34. If the extract device was a tape drive, remove the tape, set the write-protect switch on the tape to read-only, and reinsert the tape.
35. If an OBP update was performed, log into the system as root.
36. Enter the following commands:

```
cd /var/tmp/new/adminsave/init.d
ls -l
```

Verify that the directory contains upgrade scripts. If the scripts *do not* exist, check for free space on the server. Reboot the server and retry the extract. You can run the extract locally instead of remotely. If the scripts do not exist again after rebooting and retrying the extract, escalate to Avaya support.

37. Enter:

```
pg /var/tmp/new/var/log/cvuelog
```

The system displays the temporary upgrade log file. Check for failure messages (FAIL) or other indications that the extract process did not successfully complete. This file also contains a list of files that are copied to the new system. The list of files can be useful for later troubleshooting.

38. Enter:

```
ls -l /var/tmp/new/adminsave/cmsadmin.saved
```

If the files `setup.out`, `fp.out`, and `stor.def` do not exist or have a file size of zero, escalate through normal channels.

39. If the CMS configuration includes data collection by Avaya Operational Analyst (OA), the data forwarders must be turned off. Use the following command to determine if OA is installed:

```
pkginfo | grep AOA
```



Important:

If OA is present, verify that an engineer is engaged to reinstall OA. If an engineer is not engaged to reinstall OA, abort the upgrade and contact the customer and the project manager.

40. Perform one of the following actions:

- If the system displays OA processes, continue with Step [41](#).
- If the system displays OA processes, enter the following commands to turn off the data forwarders:

```
. /opt/BI/.profile
pa stop all
```

For more information about Avaya OA forwarders, see *Avaya OA Maintenance and Troubleshooting*.

41. Perform one of the following actions:
 - If the system is a T5120, T5220 or T4-1 platform, continue with [Determining if a RAID hardware controller is installed](#) on page 50.
 - If the system is an x4270 platform, continue with Step [42](#).
42. To ensure the system boots to the DVD after installing the CUE disks, remove the CUE disc labeled r17cue1X.N and place it to the side.
43. Insert the R17 CUE Bootable disc.
44. Power off the system. Enter:

```
/usr/sbin/shutdown -y -i5 -g0
```

This command shuts down the computer.
45. Turn off the power to any external SCSI disk drives and tape drives.
46. Continue with [Replacing disk drives and adding RAID controller cards](#) on page 53.

Determining if a RAID hardware controller is installed

Determine if you have the AAC or MRSAS RAID adapter in your system.

1. To determine if you have the AAC style RAID adapter, enter:

```
grep aac /etc/path_to_inst
```

- If the system displays a message similar to the following, the system has the AAC style adapter. Make a note of the style of RAID adapter in the system, continue with Step [3](#).

```
"/pci@0/pci@0/pci@9/scsi@0" 0 "aac"
```

- If the system returns the prompt only, continue with Step [2](#).
2. To determine if you have the MRSAS style RAID adapter, enter:

```
grep mr_sas /etc/path_to_inst
```

- If the system displays a message similar to the following, the system has the MRSAS adapter. Make a note of the style of RAID adapter in the system, continue with Step [4](#).

```
"/pci@0/pci@0/pci@9/LSI,mrsas@0" 0 "mr_sas"
```

- If the system returns the prompt only then the system does not have a RAID hardware controller installed. Some information on how to install a RAID hardware controller is provided in the section *Installing the RAID hardware controller*. You must install the

RAID hardware controller during section [Replacing disk drives and adding RAID controller cards](#) on page 53.

3. If you have the AAC style RAID adapter, enter:

```
/opt/StorMan/arcconf getconfig 1 PD | egrep 'State|Device'
```

The following is an example of the command on a T5220:

```
Physical Device information
Device #0
  Device is a Hard drive
  State                               : Online
  Reported Channel,Device             : 0,0
Device #1
  Device is a Hard drive
  State                               : Online
  Reported Channel,Device             : 0,1
Device #2
  Device is a Hard drive
  State                               : Online
  Reported Channel,Device             : 0,2
Device #3
  Device is a Hard drive
  State                               : Failed
  Reported Channel,Device             : 0,3
Device #4
  Device is a Hard drive
  State                               : Online
  Reported Channel,Device             : 0,4
Device #5
  Device is a Hard drive
  State                               : Online
  Reported Channel,Device             : 0,5
Device #6
  Device is an Enclosure services device
  Reported Channel,Device             : 2,0
Device #7
  Device is an Enclosure services device
  Reported Channel,Device             : 2,1
```

Note that the Device #3 is in a Failed State. The yellow light should be on for the drive in slot 3. That is the slot with the bad disk.

You may also see the State "Degraded". This could possibly be a disk that is also causing problems. If no other disk is exhibiting "Failed" and the (blue) light is on for the disk, it may need replacing. The disk status is checked later after the new CUE disks are operational. If there are still problems with any of the disks, you will be instructed what to do at that time.

Continue with step [5](#).

4. If you have the MRSAS style RAID adapter, enter:

```
/opt/MegaRAID/CLI/MegaCli -pdlist -a0 | grep Firmware
```

The following is an example of the command output on a T5120 8-core:

```
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up
```

The following is an example of the command output on a X4270:

```
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up
```

The following is an example of the command output on a T4-1:

```
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up  
Firmware state: Online, Spun Up
```

5. Enter:

```
eeeprom auto-boot?=false
```

This command sets auto-boot? to false.

6. Enter:

```
/usr/sbin/shutdown -y -i5 -g0
```

This command shuts down the computer.

7. Turn off the power to any external SCSI disk drives and tape drives.
8. Continue with [Replacing disk drives and adding RAID controller cards](#) on page 53.

Chapter 4: Replacing disk drives and adding RAID controller cards

This section contains procedures required to upgrade the disk drives to CMS R17. Using these procedures, you can remove the old disk drives in the computer and replace the disk drives with new disk drives that are preloaded with the CMS software.



CAUTION:

Customers *must not* reuse their old disk drives as part of the upgrade procedure. Customers must save these old disk drives to use them for system recovery in case any problems occur during the upgrade procedure.

Prerequisites

Obtain an Electrostatic discharge (ESD) wrist strap before starting this procedure.

Upgrade procedures

To upgrade the disks and add RAID controller hardware, use the following procedures.

Procedure	✓
Labeling the old disk drives on page 54	
Removing the disk drives on page 57	
Installing new disk drives on page 58	
Installing the RAID hardware controller on page 59	
Installing the CUE flash image on page 63	
Verifying the system recognizes the logical disk drive on page 75	

Procedure	✓
Checking the status of the extract device on page 81	
Verifying that the upgrade can continue on page 82	

Labeling the old disk drives



CAUTION:

You must remove all old disk drives from the system and replace with the disk drives from the upgrade kit. Do not leave any old disk drives in the system.

The front panel of the customer's platform is different depending on whether the customers have a Sun T5120, a Sun T5220, a SPARC T4-1, or a Netra X4270. The replacement of disks is the same procedure for all platforms with the exception that the Sun T5120 platform only has 4 disk slots and the Sun T5220 and SPARC T4-1 have 8 disk slots.

Refer to the following diagrams for information about the front panels of the T5120, T5220, SPARC T4-1, and Netra X4270:

- [T5120 4-core front panel](#) on page 54
- [T5120 8-core front panel](#) on page 55
- [T5220 front panel](#) on page 56
- [Netra X4270 front panel](#) on page 56
- [T4-1 front panel](#) on page 57

T5120 4-core front panel

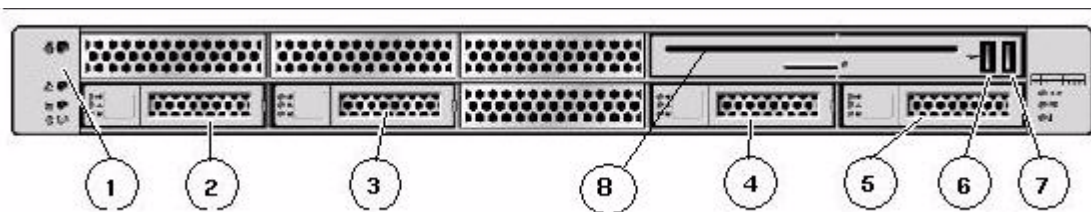


Figure notes:

- | | |
|--|--------------------|
| 1. System status indicators: Top to bottom: Locator LED button, Service Required LED, Power OK LED, Power button | 5. Hard drive HDD3 |
| 2. Hard drive HDD0 | 6. USB port 2 |
| 3. Hard drive HDD1 | 7. USB port 3 |
| 4. Hard drive HDD2 | 8. Disc Drive |

T5120 8-core front panel

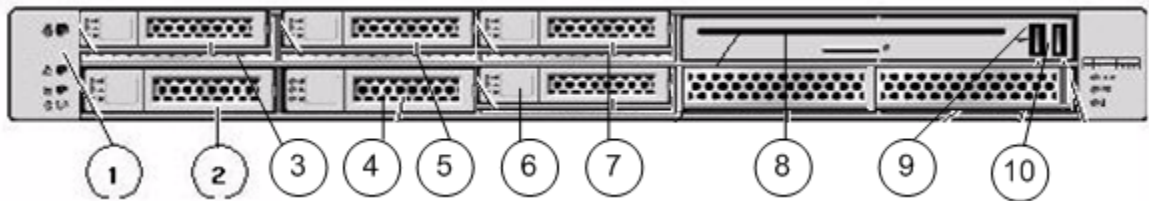
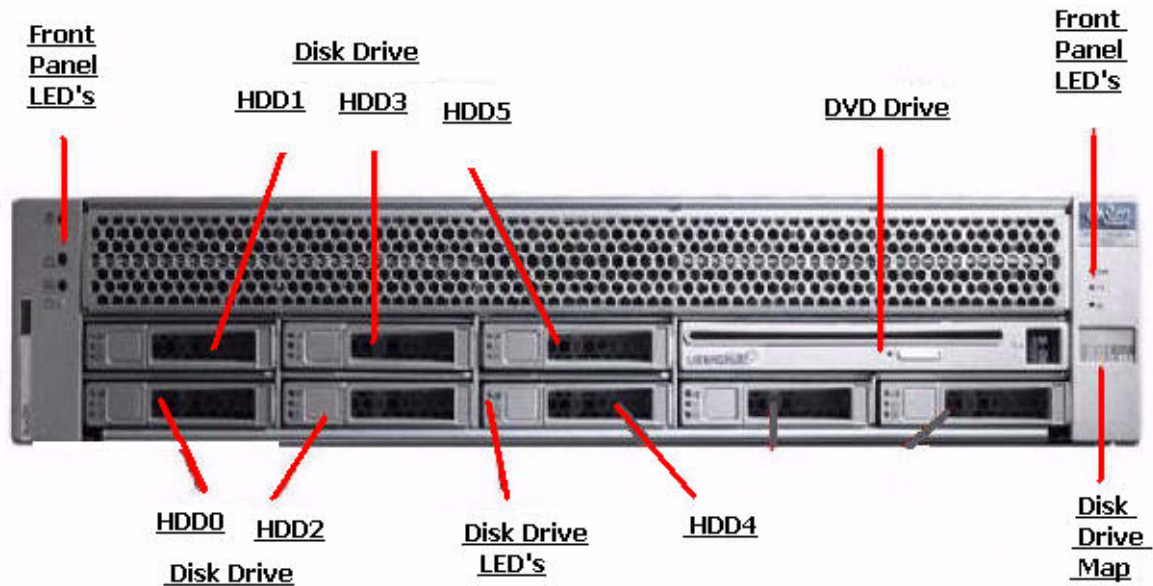


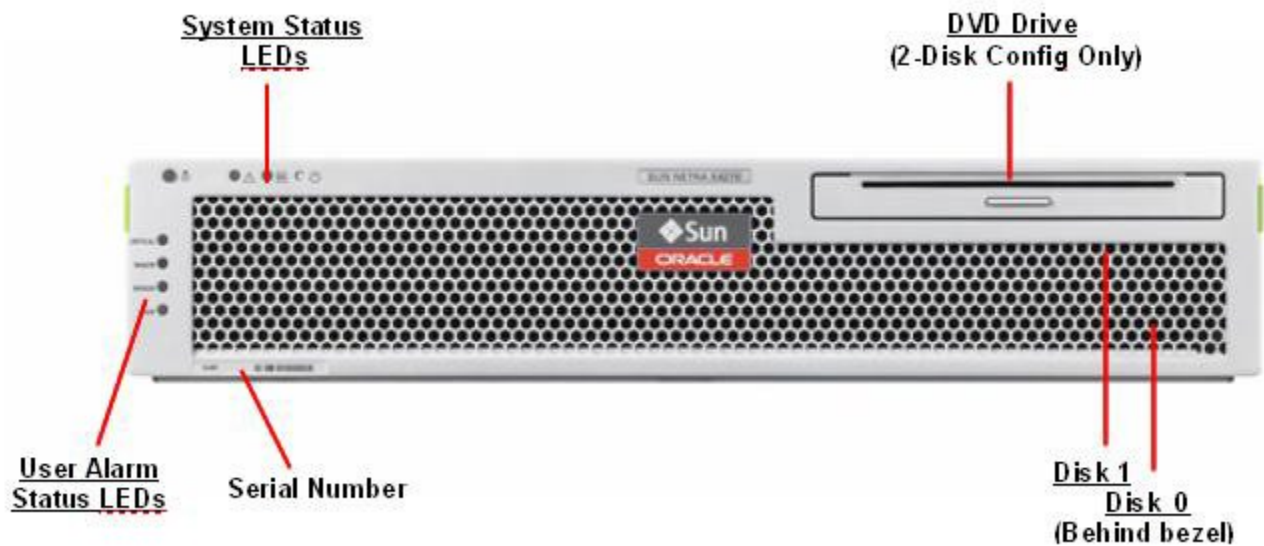
Figure notes:

- | | |
|--|--------------------|
| 1. System status indicators: Top to bottom: Locator LED button, Service Required LED, Power OK LED, Power button | 6. Hard drive HDD4 |
| 2. Hard drive HDD0 | 7. Hard drive HDD5 |
| 3. Hard drive HDD1 | 8. USB port 2 |
| 4. Hard drive HDD2 | 9. USB port 3 |
| 5. Hard drive HDD3 | 10. Disc Drive |

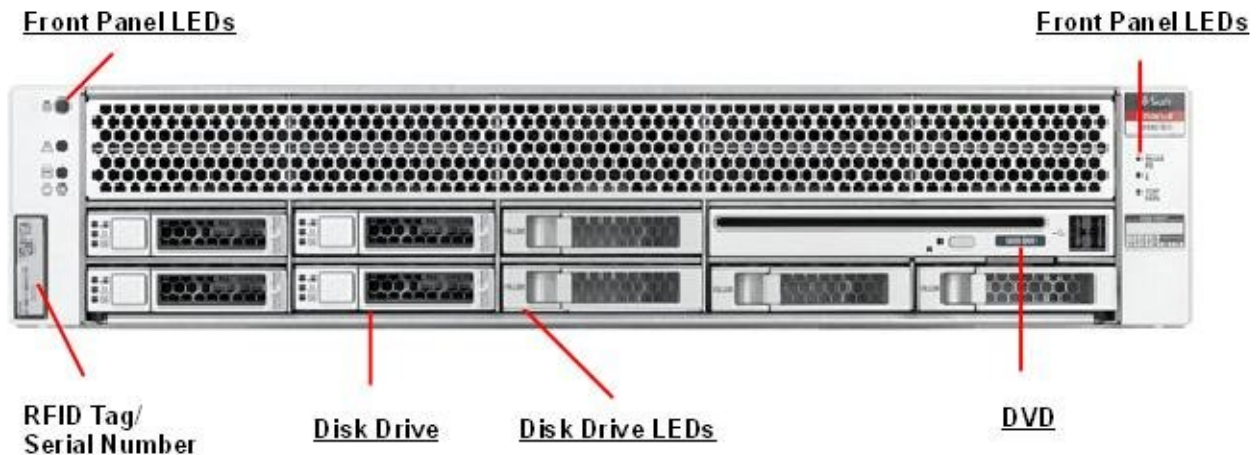
T5220 front panel



Netra X4270 front panel



T4-1 front panel



8-Drive Slot Numbering

-	-	-	-	-
-	-	-	-	-
1	3	5	DVD	
0	2	4	6	7

To label the existing disk drives:

1. If you have not already done so, enter the following command to shut down the computer:
`/usr/sbin/shutdown -y -i5 -g0`
2. For ESD isolation, verify that the AC power cord is plugged in.
3. While the original disk drives are still in the computer, use the colored labels from the upgrade kit to label each disk drive with the slot number. Save the old disk drives in case you have to reinstall the original configuration.
4. Continue with [Removing the disk drives](#) on page 57

Removing the disk drives

This procedure describes how to remove a disk drive. Make sure the original disks have been labeled before removing.

To remove a disk drive:

1. Attach an ESD wrist strap to the metal chassis of the computer and to your wrist.
2. Locate the disk drive you want to remove. A map of drive locations is located on the front right side of the system.
3. Press the drive button to release the drive latch.

4. Pull firmly on the drive latch to slide the drive out of the drive bay.
5. Set the drive aside on an antistatic mat or place in an ESD approved bag.
6. *Remove any USB removable storage devices.*
7. After all the original disks have been removed continue with [Installing new disk drives](#) on page 58.

Installing new disk drives

To install a new disk drive:

1. Remove the replacement hard drive from its shipping container and antistatic packaging.
2. Press the drive button to release the drive latch.
3. Orient the hard drive with the drive latch towards you, and the label facing up.
4. Carefully slide the drive into the drive bay by pressing on the area between the drive button and the drive status LEDs.
5. Set the drive aside on an antistatic mat or place in an ESD approved bag.
6. Press the drive latch so that it closes.
7. Repeat this process until you install all disks. The following table shows the number of disks required for each platform.

Platform	Disk Slots	
T5120 4-core	HDD0	Slot 0
	HDD1	Slot 1
	HDD2	Slot 2
	HDD3	Slot 3
T5220 or T5120 8-core or T4-1	HDD0	Slot 0
	HDD1	Slot 1
	HDD2	Slot 2
	HDD3	Slot 3
	HDD4	Slot 4
	HDD5	Slot 5
	HDD6	Slot 6
	HDD7	Slot 7

Platform	Disk Slots	
X4270		Slot 0
		Slot 1

8. Disconnect the ESD wrist strap.
9. Continue with the following options:
 - If the system is a T4-1 or x86 platform, continue with [Installing the CUE flash image](#) on page 63.
 - If the system is a T5120 or T5220 and a RAID hardware controller is already installed, continue with [Installing the CUE flash image](#) on page 63.
 - If the system is a T5120 or T5220 and a RAID hardware controller is not installed, continue with [Installing the RAID hardware controller](#) on page 59.

Installing the RAID hardware controller

Use this procedure for the T5120 and T5220 platforms only.

Note:

The Cougar "AAC" RAID controller labels its SAS connections as CN0 and CN1. The Niwot (MRSAS) labels its SAS connections as SAS 0 and SAS 1. This document uses the more generic terms of SAS 0 and SAS 1 in all of the sections below. If you have the Cougar RAID adapter, remember that SAS 0 corresponds to the "CN0" label on your RAID card, and SAS 1 corresponds to the "CN1" label on your RAID card.

- If the system is a T5120 4-core, continue with [Installing the T5120 4-core RAID hardware controller](#) on page 59.
- If the system is a T5120 8-core, continue with [Installing the T5120 8-core RAID hardware controller](#) on page 60.
- If the system is a T5220, continue with [Installing the T5220 RAID hardware controller](#) on page 61.

Installing the T5120 4-core RAID hardware controller

To install the RAID 10 hardware controller, refer to the manual that comes with the hardware controller.

The following is a checklist of steps that need to be performed:

1. Verify that the system is powered off. If it is not powered off, enter power-off at the ok prompt.

2. Verify an ESD strap is properly connected.
3. If the system is rack mounted, verify all connections on the back of the system are labeled in the event they are disconnected when the system is pulled out of the rack.
4. Open the hardware controller boxes. One of the boxes will contain 3 cables and a software disc. Locate the cable labeled 530-4119.
5. Locate the hardware controller. You can attach a backup battery to the hardware controller before installing the hardware controller. Follow the directions in the hardware controller manual for instructions on how to attach the battery. You need a Phillips screwdriver and if possible, a small pair of needle nosed pliers.
6. Facing the front of the system, press the release pins located on the front sides of the computer. There are 4 green tabs that need to be compressed. The system might need a push from the back to get the computer to come out.
7. Remove the cover.
8. Press the release button on the cable to remove the old controller cable.
9. Install the new cable. Route the new cable around the old connection point as shown in the hardware controller manual.
10. Remove the long PCI crossbar located at the back of the computer. You will need to remove two screws then lift the crossbar to remove it.
11. Remove the protection tab from the SAS 0 connector.
12. Connect the new cable to the hardware controller before inserting the controller into the PCI slot.
13. Plug the hardware controller into the PCI slot. The PCI card latch must go behind the prong and seat into a notch so the device is level.
14. Replace the PCI cross beam. Tighten the two screws.
15. Replace the cover. There are two sets of release buttons. Pull on the inner white release buttons and push the system into the rack until it will not go any further. Then pull the front green release buttons, located on the sides, to push the system in the remaining distance.
16. Continue with [Installing the CUE flash image](#) on page 63.

Installing the T5120 8-core RAID hardware controller

To install the RAID 10 hardware controller, refer to the manual that comes with the hardware controller.

The following is a checklist of steps that need to be performed:

1. Verify that the system is powered off. If it is not powered off, enter `power-off` at the ok prompt.
2. Verify an ESD strap is properly connected.

3. If the system is rack mounted, verify all connections on the back of the system are labeled in the event they are disconnected when the system is pulled out of the rack.
4. Open the hardware controller boxes. One of the boxes will contain 3 cables and a software disc. Locate the cables labeled 530-4119 and 530-4118.
5. Locate the hardware controller. You need a backup battery to attach to the hardware controller before installing the hardware controller. Follow the directions in the hardware controller manual for instructions on how to attach the battery. You will need a Phillips screwdriver and if possible, a small pair of needle nosed pliers.
6. Facing the front of the system, press the release pins located on the front sides of the computer. There are 4 green tabs that need to be compressed. The system needs a push from the back to get the computer to come out.
7. Remove the cover.
8. Press the release button on the cable to remove the old controller cable.
9. Install the new cable. Route the new cable around the old connection point as shown in the hardware controller manual.
10. Remove the long PCI crossbar located at the back of the computer. You need to remove two screws then lift the crossbar to remove it.
11. Remove the protection tab from the SAS 0 connector. The SAS 0 connector is on the inside and closest to the pin connection.
12. Connect the new cables to the hardware controller before inserting the controller into the PCI slot.
13. Plug the hardware controller into the PCI slot. The PCI card latch must go behind the prong and seat into a notch so that the device is level.
14. Replace the PCI cross beam. Tighten the two screws.
15. Replace the cover. There are two sets of release buttons. Pull on the inner white release buttons and push the system into the rack until it will not go any further. Then pull the front green release buttons, located on the sides, to push the system in the remaining distance.
16. Continue with [Installing the CUE flash image](#) on page 63.

Installing the T5220 RAID hardware controller

To install the RAID 10 hardware controller, refer to the T5220 section of the manual that comes with the hardware controller.

The following is a checklist of steps that need to be performed:

1. Verify that the system is powered off. If it is not powered off, enter power-off at the ok prompt.
2. Verify an ESD strap is properly connected.

3. If the system is rack mounted, verify all connections on the back of the system are labeled in the event they are disconnected when the system is pulled out of the rack.
4. Open the hardware controller boxes. One of the boxes will contain 2 cables and a software disc. You will need both the cables.
5. Locate the hardware controller. You need a backup battery attach to the hardware controller before installing the hardware controller. Follow the directions in the hardware controller manual for instructions on how to attach the battery. You will need a Phillips screwdriver and if possible, a small pair of needle nosed pliers.
6. Facing the front of the system, press the release pins located on the front sides of the computer. There are 4 green tabs that need to be compressed. The system might need a push from the back to get the computer to come out.
7. Remove the cover, air duct, all fans and all fan boards.
 - To remove the air duct, facing the computer, gently push the air duct to the right until the left side can be slipped out of its' round slot then pull the air duct to the left to slip the right side out of it's round slot.
 - To remove the fans simply pull them up out of their slots.
 - To remove the fan boards, remove the screw on the left then gently pull the board to the left until it releases from its' connection on the right.
8. Press the release buttons on the cables to remove the old controller cables.
9. Install the new cables. Route the new cable between the old connection points as shown in the hardware controller manual.
10. Remove the long PCI cross beam located at the back of the computer. You will need to remove two screws then lift the crossbar to remove it.
11. You must move the video card from PCIE Slot 5 to PCIE Slot 1. You need to install the hardware controller in PCIE Slot 2.
12. Remove the protection tab from the SAS 0 and SAS 1 connectors. The hardware controller battery side should face down. The 530-4119 cable should be connected to the SAS 0 connector and the opposite end should be connected to the front left connector. You must connect the 530-3892 cable to the SAS 1 connector. You must connect the opposite end of the 530-3892 cable to the front right connector.

Note:

Connect the new cables to the hardware controller before inserting the controller into the PCI slot.

13. Plug the hardware controller into the PCI slot. The PCI card latch must go behind the prong and seat into a notch so the device is level.
14. Replace the PCI crossbar. Tighten the two screws.

15. Replace the fan boards, fans, air duct and cover. There are two sets of release buttons. Pull on the inner white release buttons and push the system into the rack until you cannot push it any further. Pull the front green release buttons, located on the sides, to push the system in the remaining distance.
16. Continue with [Installing the CUE flash image](#) on page 63.

Installing the CUE flash image

- If the system is a T5120, T5220 or T4-1 platform, continue with [Installing the CUE flash image on SPARC-based T5120, T5220, or T4-1 platforms](#) on page 63.
- If the system is an x4270 platform, continue with [Installing the CUE flash image on an x4270 platform](#) on page 71.

Installing the CUE flash image on SPARC-based T5120, T5220, or T4-1 platforms

Use this procedure for the SPARC-based T5120, T5220, and T4-1 platforms only.

Note:

When remote personnel such as CMS Provisioning are supporting the upgrade, remote personnel use the system commands in this section to monitor the progress of the upgrade. Run the commands from the local console only when instructed or when there is no remote support.



Important:

Remove all USB storage devices. If any USB storage devices are connected to the system, the build process uses the USB storage device for the boot hard drive and the system fails to boot after the build process completes.

1. *Remove any USB storage devices.*
2. Verify all connections on the back of the computer are correct.
3. Turn on all external SCSI devices, starting with the device farthest from the system and working toward the system.
4. Turn on the system monitor.
5. Power on the system.

Note:

The system can take up to 10 minutes to display the ok prompt.

6. Remove the CUE disc labeled r17cue1X.N and place it to the side while the CUE disks are configured.
7. Insert the R17 CUE Bootable disc.

8. The system needs to be reset before you execute the `probe-scsi-all` command to detect the hardware controller and disks. At the `ok` prompt enter:

```
reset-all
```

The screen will turn black. It can take up to 2 minutes for the system to reset and display the `ok` prompt.



Important:

If the `probe-scsi-all` command in the next step displays a prompt to accept the current configuration, you must quickly press **Enter**. If the system is a T4-1 platform, press **F** to accept the current configuration.

9. Execute the `probe-scsi-all` command to detect the new hardware configuration. At the `ok` prompt enter:

```
probe-scsi-all
```

The system displays messages associated with the detection of scsi devices on the screen. Wait for the system to display the `ok` prompt.

- a. If the system responds with messages similar to the following, where the starting text is "Waiting for AAC Controller to start Started", you have an AAC RAID controller.

```
/pci@0/pci@0/pci@9/scsi@0  
  
Waiting for AAC Controller to start .....Started  
  
AAC Kernel Version: 15825  
  
Target 0 Volume 0  
  
Unit 0 Disk Adaptec RAID ASR5805 V1.0 57303401 Blocks, 293 GB  
  
/pci@0/pci@0/pci@8/pci@0/pci@9/pci@0/scsi@8,1  
  
/pci@0/pci@0/pci@8/pci@0/pci@9/pci@0/scsi@8  
  
Target 4  
  
Unit 0 Removeable Tape HP C7438A ZP76  
  
/pci@0/pci@0/pci@2/scsi@0  
  
MPT Version 1.05, Firmware Version 1.22.00.00
```

- b. If the system responds with messages similar to the following, where the starting text is `"/pci@0/pci@0/pci@9/LSI,mrsas@0"`, you have a MRSAS RAID Controller.

```

/pci@0/pci@0/pci@9/LSI,mrsas@0

FW package: 12.9.0-0050

Target 0

Unit 0   Disk           LSIMR9261-8i2.90       17519493312 Blocks, 896 GB

/pci@0/pci@0/pci@8/pci@0/pci@1/LSILogic,sas@0

MPT Version 1.05, Firmware Version 1.29.06.00

Target 4

Unit 0 Removeable Tape HP C7438A ZP76

/pci@0/pci@0/pci@2/scsi@0

MPT Version 1.05, Firmware Version 1.22.00.00

```

10. To determine the current boot-device path, enter:

```
ok> printenv boot-device
```

The system displays the following if you have the AAC style RAID adapter:

```
ok> /pci@0/pci@0/pci@9/scsi@0/disk@0,0
```

The system displays the following if you have the MRSAS style RAID adapter:

```
ok> /pci@0/pci@0/pci@9/LSI,mrsas@0/disk@0,0
```

The system displays the following if you have the MRSAS style RAID adapter and the system is a T4-1:

```
ok> /pci@400/pci@2/pci@0/pci@c/LSI,mrsas@0/disk@0,0
```

- If the boot-device path displayed matches the path shown above, go to Step 13.
- If the boot-device path does not match the above path, then the boot-device path will need to be updated.

11. Use the proper command for your RAID adapter.

Note:

bootdevice2 is not a valid path for CMS R16 or later. Do not include bootdevice2, if it exists.

To update the boot-device path for the AAC style RAID adapter, enter:

```
ok> setenv boot-device /pci@0/pci@0/pci@9/scsi@0/disk@0,0
```

To update the boot-device path for the MRSAS style RAID adapter on a T5120 or T5220 platform, enter:

```
ok> setenv boot-device /pci@0/pci@0/pci@9/LSI,mrsas@0/disk@0,0
```

To update the boot-device path for the MRSAS style RAID adapter on a T4-1 platform, enter the following on a single line:

```
ok> setenv boot-device /pci@400/pci@2/pci@0/pci@c/LSI,mrsas@0
disk@0,0
```

Check the values entered for boot-device:

12. Enter: printenv boot-device

```
ok> /pci@0/pci@0/pci@9/scsi@0/disk@0,0
/pci@0/pci@0/pci@9/LSI,mrsas@0/disk@0,0 or
/pci@400/pci@2/pci@0/pci@c/LSI,mrsas@0/disk@0,0
depending on the RAID adapter.
```

Verify the path entered for boot-device is the path shown above.

- If the path is correct, go to Step [13](#).
- If the path is incorrect, repeat Steps 10 through 12.

13. To start the installation of the flash image, enter the following command at the ok prompt:

```
boot cdrom
```

Note:

The install process can take up to 45 minutes.

The system boots from the R17 CUE Bootable disc and installs the flash image onto the CUE disks. The process will install Solaris, Informix and CMS.

- If the flash image installs onto the CUE disks continue with Step [14](#).
- If the system displays the message “Can’t find boot device” go to [Performing a manual boot to the CUE Bootable DVD](#) on page 83.

14. The flash process checks the correct number of physical disk drives.

- If this process finds the correct number of physical disk drives, the process continues with Step [15](#).
- If the correct number of physical disk drives are not found, the CUE_begin process halts. If the system halts, perform the following steps.

**CAUTION:**

Only perform Steps **a** through **f** if the correct number of physical disk drives were NOT found.

- a. Exit the CUE Bootable disc. Enter:

```
halt
```

- b. At the **ok** prompt enter:

```
power-off
```

- c. Wait for 30 seconds and power on the system.

- d. You need to reset the system. At the **ok** prompt enter:

```
reset-all
```

The system displays a black screen and it can take up to 2 minutes for the system to reset and display the **ok** prompt.

Note:

If the `probe-scsi-all` command in the next step displays a prompt to accept the current configuration, you must quickly press **Enter**. If the system is a T4-1 platform, press **F** to accept the current configuration

- e. The system needs to check if all the new disk drives were recognized. At the **ok** prompt enter:

```
probe-scsi-all
```

The system displays messages associated with the detection of scsi devices on the screen. Wait for the system to display the **ok** prompt.

- f. In some cases the system will not boot to the cdrom if the `eeeprom` variable `fcode-debug?` is not set to true. Make a note of the current `fcode-debug?` value before changing the value. To set `eeeprom` variable `fcode-debug?` to true, enter:

```
setenv fcode-debug? true
```

- g. Boot to the R17 CUE Bootable disc. At the **ok** prompt enter:

```
boot cdrom
```

Note:

If the system halts again, escalate through normal channels.

15. The flash process will check for any logical drives that can exist on the disks. If any logical drives were found the process will delete them and create the logical drive.

The CUE process begins to configure the disks, and the system displays the following information:

```
Extracting Windowing system. Please wait...
```

The system can display the following messages, but you can ignore any ADPT messages:

```
... svc.startd[8] device/ADPTstor_agent: default failed repeatedly: Transitioned to maintenance.
```

Note:

The system can automatically reboot during the CUE build process. If this occurs the system displays a message similar to the following after the reboot, and this message is acceptable:

```
Boot device: /pci@0/pci@0/pci@9/scsi@0/disk@0,0 File and args: - install nowin
```

- If the system reboots properly, continue with Step [17](#).
- If the system fails to reboot and displays a *Can't find boot device message*, continue with Step [16](#).

16. Attempt to restart the CUE process. Enter:

```
boot cdrom - install nowin
```

If the system fails to reboot again and displays the *Can't find boot device* message, continue with [Performing a manual boot to the CUE Bootable DVD](#) on page 83. Then resume from this point, and perform the remaining steps of this procedure.

17. The CUE process begins to build the disks, and the system displays information shown in the following example:

```
Oracle Solaris Install Console
Oracle Solaris Install jumpstart

Starting Solaris installation program...
.
.
.
Processing profile
.
.
.
Extracting archive: CUE xx.x xx.x <platform>
.
.
.
```

**Tip:**

Depending on your system hardware, the remaining portion of the Extracting process can take from 20-60 minutes.

```
Extracted xx.xxMB (x% of xxxx.xxMB archive)
.
.
.
Extracted xxxx.xxMB (100% of xxxx.xxMB archive)
```

18. Near the end of the install process, the system displays a prompt to enter a system serial number.

Note:

The SUN system Serial Number is located on the far left, front side of the computer, and along the edge.

Enter: <SUN system Serial Number>

Enter: y



CAUTION:

The system automatically reboots after the CUE process completes. If the CUE Bootable DVD is in the disc drive when the system reboots, the system attempts to install the CUE image again. Remove the CUE Bootable disc as soon as possible during the reboot.

19. The system automatically reboots when the install process completes.

If after entering the SUN system serial number, the system fails to automatically reboot within 5 minutes, then manually reboot the system. Enter:

```
shutdown -i6 -y -g0
```

Note:

Ignore any messages about **SUNWexplo** or **SUNWexplu** during the boot process.

20. Remove the CUE Bootable DVD from the disc drive during the reboot.

21. Take one the following actions depending on the outcome of the reboot:

- If the system fails to boot, escalate through normal channels.
- If the system boots to the **Welcome to cvue** screen, the CUE image installed properly. Continue with Step [22](#).
- If the system does not display the **Welcome to cvue** screen and you are prompted to open windows, then it is possible that a mouse is not connected to the system. Connect a mouse to the system and then reboot the system. To reboot the system, enter:

```
shutdown -i6 -y -g0
```

22. After the system reboots, perform one of the following actions:

- If you are performing the upgrade from the local console:
 - a. Log in as root.
 - b. If prompted for a password, press **Enter**. At this point in the upgrade, there is no password.
 - c. If prompted for the CDE environment, select Common Desktop Environment.
 - d. If the system displays a java desktop message, select the box **Do not show this message again**. Select **OK**.
- If you are performing the upgrade remotely:
 - a. Dial into the system.
 - b. Log in as **cmssvc**.
 - c. If prompted for a password, use the default Avaya password for cmssvc.
 - d. Enter:

```
su - root
```

- e. If prompted for a password, press **Enter**. At this point in the upgrade, there is no password.
23. Enter:


```
pkginfo -x cms
```
- Note:**
Verify the new CMS load to ensure that it matches the expected upgrade load.
24. Restore the original value for `fcode-debug?`, enter:


```
eepprom fcode-debug?=<orig_fcode-debug?>
```

 where `orig_fcode-debug?` value is the value noted in Step [14f](#) on page 43.
25. Continue with [Verifying the system recognizes the logical disk drive](#) on page 75.

Installing the CUE flash image on an x4270 platform

Use this procedure for the x4270 platform only.

Note:

When remote personnel such as CMS Provisioning are supporting the upgrade, remote personnel use the system commands in this section to monitor the progress of the upgrade. Run the commands from the local console only when instructed or when there is no remote support.

1. Remove any USB storage devices.
2. Verify that all connections on the back of the computer are correct.
3. Turn on all external SCSI devices, starting with the device farthest from the system and working toward the system.
4. Turn on the system monitor.



CAUTION:

The x4270 platform boot up is fast. The CUE Bootable DVD must already be in the disc drive to ensure that the system boots to the CUE Bootable DVD. If the CUE Bootable DVD is not in the disc drive, you need to remove the r17cue1X.N disc and insert the CUE Bootable DVD as soon as possible, then press the **Ctrl**, **Alt**, and **Del** keys simultaneously to reboot the system.



Important:

If the system displays a prompt to accept the current configuration during the power up cycle, you must quickly press **F** to accept the current configuration.

5. Power on the system.

6. The system boots to the CUE Bootable DVD and displays progress messages to the screen, as shown in the following example:

```
.  
.   
.   
Loading Stage 2 .....  
.   
.   
CMS R17 xx.x (Solaris xx) NX4270 Jumpstart  
.   
.
```

The system can display the following messages, but you can ignore any ADPT messages:

```
... svc.startd[8] device/ADPTstor_agent: default failed repeatedly: Transitioned to  
maintenance.
```

7. The flash process checks for any logical drives that can exist on the disks. If any logical drives are found, the process deletes them and creates the logical drive.

The CUE process begins to configure the disks, and the system displays information shown in the following example:

```
SunOS Release x.xx Version Generic...  
.   
.   
Configuring devices.  
Custom Jumpstart  
.   
.   
Attempting to configure interface igbx  
.   
.   
Skipped interface igb0  
Using local console  
Extracting Windowing system. Please wait...  
Beginning system identification  
.   
.
```

8. The system opens and closes various windows and then displays the CUE Extracting progress information.

```
Extracting archive: CUE Rxx
.
.
.
Extracted xx.xxMB (x% of xxxx.xxMB archive)
.
.
.
Extracted xxxx.xxMB (100% of xxxx.xxMB archive)
```

9. Near the end of the install process, the system displays a prompt to enter a system serial number.

Note:

The SUN system Serial Number is located on the far left, front side of the computer, and along the edge.

Enter: <SUN system Serial Number>

Enter: y

**CAUTION:**

The system automatically reboots after the CUE process completes. If the CUE Bootable DVD is in the disc drive when the system reboots, the system attempts to install the CUE image again. Remove the CUE Bootable disc as soon as possible during the reboot.

10. The system automatically reboots when the install process completes.

If after entering the SUN system serial number, the system fails to automatically reboot within 5 minutes then manually reboot the system, enter:

```
shutdown -i6 -y -g0
```

Note:

Ignore any messages about **SUNWexplo** or **SUNWexplu** during the boot process.

11. Remove the CUE Bootable DVD from the disc drive during the reboot.
12. The system displays the Solaris **Welcome to cvue** screen.

Note:

If the system fails to boot, escalate through normal channels.

- If the system boots to the **Welcome to cvue** screen, the CUE image installed properly. Continue with Step [14](#).

- If the system does not display the **Welcome to cvue** screen and you are prompted to open windows, then a mouse is probably not connected to the system. Connect a mouse to the system and then reboot the system. To reboot the system enter:

```
shutdown -i6 -y -g0
```
 - If the system does not boot to the **Welcome to cvue** screen, the CUE image did not install properly. Continue with Step [13](#).
13. Attempt to restart the CUE process. Ensure that the CUE Bootable DVD is in the disc drive. Enter **Ctrl, Alt, and Del** simultaneously.
- If the system fails to install properly again, escalate through normal channels.
14. After the system reboots, perform one of the following actions:
- If you are performing the upgrade from the local console:
 - a. Log in as root.
 - b. If the system prompts for a password, press **Enter**. At this point in the upgrade, there is no password.
 - c. If the system prompts for the CDE environment, select **Common Desktop Environment**.
 - d. If the system displays a java desktop message, select the box **Do not show this message again**. Select **OK**.
 - If you are performing the upgrade remotely:
 - a. Dial in to the system.
 - b. Log in as `cmssvc`.
 - c. If the system prompts for a password, use the default Avaya password for `cmssvc`.
 - d. Enter:

```
su - root
```

If prompted for a password, press **Enter**. At this point in the upgrade, there is no password.
15. Enter:
- ```
pkginfo -x cms
```
- Note:**  
Verify the new CMS load to ensure that it matches the expected upgrade load.
16. Continue with [Verifying the system recognizes the logical disk drive](#) on page 75.

## Verifying the system recognizes the logical disk drive

To verify that the system recognizes the new logical disk drive:

1. Enter:

```
format
```

One logical disk drive 0 should be displayed in the output.

```
Searching for disks...done
AVAILABLE DISK SELECTIONS:
0. clt0d0 <SUN-STKRAIDINT-V1.0 cyl 35667 alt 2 hd 255 sec 63>
 /pci@0/pci@0/pci@9/scsi@0/sd@0,0
Specify disk (enter its number):
```



### Important:

If the logical disk is not on `clt0`, then the disks were not built properly. Start with *Installing the CUE flash image* for the specific platform.

2. Enter: 0
3. Enter: `q`
4. Verify that logical drive 0 was properly created.
  - If the style of the RAID adapter is AAC, continue with Step [5](#).
  - If the style of the RAID adapter is MRSAS, continue with Step [6](#).
5. For AAC style RAID adapter systems, enter

```
/opt/StorMan/arccconf getconfig 1 LD
```

The T5120 system displays messages in the order shown below:

```
Group 0, Segment 0 : Present (0,0)
Group 0, Segment 1 : Present (0,1)
Group 1, Segment 0 : Present (0,2)
Group 1, Segment 1 : Present (0,3)
```

The T5220, T5120 8-core, and T4-1 systems display messages in the order shown below:

```
Group 0, Segment 0 : Present (0,0)
Group 0, Segment 1 : Present (0,1)
Group 1, Segment 0 : Present (0,2)
Group 1, Segment 1 : Present (0,3)
Group 2, Segment 0 : Present (0,4)
Group 2, Segment 1 : Present (0,5)
Group 3, Segment 0 : Present (0,6)
Group 3, Segment 1 : Present (0,7)
```

6. For MRSAS style RAID adapter systems, enter:

```
/opt/MegaRAID/CLI/MegaCli -ldpdinfo -a0 | egrep
"Enclosure|Slot|Span"
```

The T5120 4-core system displays messages in the following order:

```
Span: 0 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 252
Slot Number: 0
PD: 1 Information
Enclosure Device ID: 252
Slot Number: 1
Span: 1 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 252
Slot Number: 2
PD: 1 Information
```

The T5220, T5120 8-core, and T4-1 systems display messages in the following order:

```
Span: 0 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 252
Slot Number: 0
PD: 1 Information
Enclosure Device ID: 252
Slot Number: 1
Span: 1 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 252
Slot Number: 2
PD: 1 Information
Span: 2 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 252
Slot Number: 4
PD: 1 Information
Enclosure Device ID: 252
Slot Number: 5
Span: 3 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 252
Slot Number: 6
PD: 1 Information
Enclosure Device ID: 252
Slot Number: 7
```

The Netra X4270 system displays messages in the following order:

```
Span Depth : 1
Number of Spans: 1
Span: 0 - Number of PDs: 2
Enclosure Device ID: 252
Slot Number: 4
Enclosure Device ID: 252
Slot Number: 5
```

The output must show the correct disk pair configurations. If the system does not meet the criteria, escalate through normal channels.

7. Set the Informix environment by entering:

```
. /opt/informix/bin/setenv
```

8. Initialize the database by entering:

```
/opt/informix/bin/dbinit.sh noprompt
```

9. Verify IDS is Online by entering:

```
onstat -d | egrep "On-Line"
```

- If IDS is Online continue with Step [10](#).
- If IDS is not Online, reboot the system and then repeat Steps 7-9. If IDS is still not Online then escalate through normal channels.

10. Remove the CUE bootable software disc from the disc drive.
11. Verify the CUE extract tape is still in the tape drive.
12. Continue with [Mounting an extract device](#) on page 77.

---

## Mounting an extract device

You must mount the extract device before you can copy the customer data to the new disks.

- If the cvue\_copy is performed from tape, continue with [Checking the status of the extract device](#) on page 81.
- If the cvue\_copy is performed from a USB storage device, continue with [Mounting a USB storage device](#) on page 78.
- If the cvue\_copy is performed from a network server, continue with [Mounting a network server](#) on page 79.

---

## Mounting a USB storage device

Perform the following steps to mount the USB storage device containing the `cvue_extract` data.



### Important:

It is the responsibility of the customer to ensure that the CMS system detects the USB storage device and users can perform read and write operations to and from the USB storage device. This document provides information only as a reference to aid in troubleshooting USB storage device recognition issues. Contact your system administrator to resolve any USB storage device issues.

1. Change to the root directory. Enter:

```
cd /
```

2. On the CMS server, create the USB storage device mount point, enter:

```
mkdir /rmdisk/CUE_extract_dir
```

3. Turn off volmgt before inserting the USB storage device, enter:

```
svcadm disable volfs
```

4. Insert the USB storage device, enter:

- If the fstyp of the USB storage device is ZFS, continue with Step [5](#).
- If the fstyp of the USB storage device is UFS, continue with Step [7](#).

5. To mount the ZFS formatted USB storage device, enter:

```
zpool import -a -f
```

6. To display the ZFS pool name, enter:

```
zpool list
```

Continue with step [10](#).

7. Determine the Logical Node path of the USB device. Enter:

```
rmformat
```

8. The output of the `rmformat` command is similar to the following information:

```
a.Looking for devices...
b.1.Volmgt Node: /vol/dev/aliases/cdrom0
c.Logical Node: /dev/rdisk/c0t0d0s2
d.Physical Node: /pci@0/pci@0/pci@l/pci@0/pci@l/pci@0/usb@0,2/
e.storage@2/disk@0,0
f.Connected Device: TSSTcorp CD/DVDW TS-T632A 3R03
g.Device Type: DVD Reader/Writer
h.2.Volmgt Node: /voi/dev/aliases/rmdisk0
i.Logical Node: /dev/rdisk/c6t0d0s2
j.Physical Node: /pci@0/pci@0/pci@l/pci@0/pci@l/pci@0/usb@0,2/hub@4/
k.storage@2/dlsk@0,0
l.Connected Device: Kingston DataTraveler 2.0 PMAP
m.Device Type: Removable
```

9. Use the Logical Node information from the `rmformat` output to mount the USB storage device, enter:

```
mount /dev/dsk/c#t#d0s2 /CUE_extract_dir
```

where `c#t#` is the controller and slot assignment.

Example:

```
mount /dev/dsk/c6t0d0s2 /CUE_extract_dir
```

10. To verify the USB storage device is mounted, enter:

```
ls -l /CUE_extract_dir
```

The `cvue_extract.tar` file must be listed.

11. To start `volmgt`, enter:

```
svcadm enable volfs
```

**Note:**

If a device format window opens, close the window.

12. Continue with [Checking the status of the extract device](#) on page 81.

---

## Mounting a network server

1. On the CMS server, create the NFS mount point, enter:

```
mkdir /CUE_extract_dir
```

2. Enter:

```
ifconfig network_interface# unplumb
```

where `network_interface#` is `e1000g0` for T5120 and T5220 systems and `igb0` for T4-1 and x86 systems, `CMS_ip` is the ip address of the CMS system and `CMS_netmask` is the netmask of the network for the CMS system.

3. Enter:

```
ifconfig network_interface# plumb
```

4. Enter the following command on a single line:

```
ifconfig network_interface# inet CMS_ip netmask CMS_netmask
broadcast +
```

5. Enter:

```
ifconfig network_interface# up
```

6. Enter:

```
ifconfig -a
```

The system displays the following messages. Search for `network_interface0` and verify the information is correct.

```
network_interface0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 2 inet xxx.xxx.xxx.xxx netmask ffffffff0 broadcast xxx.xxx.xxx.xxx
ether xx:xx:xx:xx:xx:xx
```

7. Enter:

```
route add default route_ip
```

where `route_ip` is the ip address of the network router for the CMS system.

8. Enter:

```
ping route_ip
```

Verify the network router for the CMS system responds.

9. Enter:

```
ping nfs_server_ip_address
```

Verify the network server responds.

10. To mount the network server, enter the following command on a single line:

**⚠ Important:**

The `network_server_mt_pt_dir` must be the same mount point created in the `cvue_extract` procedure.

```
mount -F nfs -o vers=3 <network_server_ip_address>:
/network_server_mt_pt_dir /CUE_extract_dir
```

Example:

```
mount -F nfs -o vers=3
xxx.xxx.xxx.xxx:/CUE_NFS_dir /CUE_extract_dir
```

11. To change to the network server mount point directory, enter:  

```
cd /CUE_extract_dir
```
12. To list the contents of the network server mount point directory, enter:  

```
ls -l
```

The `cvue_extract.tar` file must be listed.
13. Continue with [Checking the status of the extract device](#) on page 81.

---

## Checking the status of the extract device

- If the extract device is a tape drive, continue with Step [1](#).
  - If the extract device is a USB storage device, continue with Step [2](#).
  - If the extract device is a network mount point, continue with Step [3](#).
1. To check the status of the tape drive, verify the tape is write-protected and inserted into the tape drive, enter:  

```
mt -f /dev/rmt/0c status
```

Determine whether the tape drive is available for use.

    - If the tape drive is available for use, continue with [Copying and activating the customer's administration and options](#) on page 87.
    - If the tape drive is not available for use, continue with [Verifying that the upgrade can continue](#) on page 82.
  2. To check the status of a USB storage device:
    - a. Insert the USB storage device
    - b. Mount the USB storage device as defined in [Mounting a USB storage device](#) on page 78.
    - c. Verify data can be written to and read from the USB extract path.

- d. Continue with [Copying and activating the customer's administration and options](#) on page 87.
3. To check the status of a network mount point:
  - a. Mount the network mount point as defined in [Mounting a network server](#) on page 79.
  - b. Verify data can be written to and read from the network mount point extract path.
  - c. Continue with [Copying and activating the customer's administration and options](#) on page 87.

---

## Verifying that the upgrade can continue

Perform this procedure if the extract device is a tape drive and the tape drive is not accessible.

- If the tape drive status is correct, continue with [Copying and activating the customer's administration and options](#) on page 87.
- If the tape drive status is not correct, perform the following procedure:
  1. Enter the following commands. These commands shut down the system and force a reconfiguration the next time that the system boots.

```
cd /
touch /reconfigure
/usr/sbin/shutdown -y -i0 -g0
```
  2. Turn off the system.
  3. Turn off the system monitor.
  4. Turn off any external SCSI devices, starting with the device that is closest to the system and working toward the farthest device.
  5. Check all device cables. Cycle power on all external devices.
  6. Turn on the system monitor.
  7. Turn on the system.
  8. After the system reboots, perform one of the following actions:
    - If you are performing the upgrade from the local console:
      - a. log in as root.
      - b. If prompted for a password, press **Enter**. At this point in the upgrade, there is no password.
      - c. If the system displays a java desktop message, select the box "Do not show this message again." Select **OK**.
      - d. If prompted for the CDE environment, select Common Desktop Environment.

- e. If the system displays a java desktop message, select the box "Do not show this message again." Select **OK**.
- If you are performing the upgrade remotely:
  - a. Dial into the system.
  - b. Log in as **cmsvc**.
  - c. If prompted for a password, press **Enter**. At this point in the upgrade, there is no password.
  - d. Enter:
 

```
su - root
```
  - e. Check the status of the tape drive, enter:
 

```
mt -f /dev/rmt/#c status
```

 where # is the device number for the tape drive.
  - If the tape status is correct, continue with [Copying and activating the customer's administration and options](#) on page 87.
  - If the tape status is still not correct, escalate through normal channels.

---

## Performing a manual boot to the CUE Bootable DVD

- If the CMS system is an x4270 platform and does not boot to the CUE Bootable DVD, escalate through normal channels. The `show-disks` command used in this procedure is not available for the x4270 platform.
- If the CMS system is a T5120, T5220, or T4-1 platform, continue with this procedure.

Perform these steps only if the system failed to boot to the DVD in Step 13 of [Installing the CUE flash image](#) on page 63.

1. Verify the CUE Bootable DVD is in the DVD drive.
2. Remove/disconnect any USB storage devices.
3. At the ok prompt, enter:

```
show-disks
```

- If the CMS system is a T5x20 platform, continue with Step [4](#).
- If the CMS system is a T4-1 platform, continue with Step [11](#).

4. Below is an example of the output from the `show-disks` command for a T5x20 platform:

Example:

```
a) /pci@0/pci@0/pci@9/scsi@0/disk
b) /pci@0/pci@0/pci@1/pci@0/pci@8/scsi@0/disk
c) /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@2/disk
d) /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/hub@4/device@4/storage@0/disk
```

The boot path for the T5x20 platforms contains the word *storage*.

There are two types of DVD drives, SATA and PATA. Typically, older systems have the SATA DVD drive and newer systems have the PATA DVD drive. The boot strings for the two DVD drives shown with the `show-disks` command are:

SATA drive:

```
/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@2/disk
```

PATA drive:

```
/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/hub@4/device@4/
storage@0/disk
```

5. Look through the output from the `show-disks` command to find the letter associated with the DVD drive type for your system. There can be boot options that look similar so be sure to select the option that best aligns with the above paths.
6. Enter the letter associated with the systems DVD drive

Example: Enter the letter **d**.

The system displays the following messages:

```
/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/hub@4/device@4/storage@0/disk has
been selected.
Type ^Y (Control-Y) to insert it in the command line.
e.g. ok nvalias mydev ^Y
 for creating devalias mydev for /pci@0/pci@0/pci@1/pci@0/pci@1/
pci@0/usb@0,2/hub@4/device@4/storage@0/disk
```

### Important:

Do not press the enter key until instructed to do so in Step [9](#).

7. At the `ok` prompt, enter:

```
boot <Ctrl + y>
```

**Note:**

Press the **Ctrl** key and the letter **y** at the same time.

The system appends the boot path option to the command line.

Examples:

```
boot /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@2/disk
```

```
boot /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/hub@4/device@4/storage@0/disk
```

8. Append **@0:f** to the path.

Examples:

```
boot /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@2/disk@0:f
```

```
boot /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/hub@4/device@4/storage@0/
disk@0:f
```

9. Press **Enter**.

10. Continue with step [17](#).

11. Below is an example of the output from the `show-disks` command for a T4-1 platform:

```
a) /pci@400/pci@2/pci@0/pci@f/pci@0/usb@0,2/hub@2/hub@3/storage@2/disk
b) /pci@400/pci@2/pci@0/pci@c/LSI,mrsas@0/disk
c) /pci@400/pci@2/pci@0/pci@4/scsi@0/disk
d) /pci@400/pci@1/pci@0/pci@4/scsi@0/disk
e) /iscsi-hba/disk
```

12. See the output from the `show-disks` command to find the letter associated with the DVD drive type for your system. There can be boot options that look similar so be sure to select the option that best aligns with the above paths.

13. Enter the letter associated with the systems DVD drive.

Example: Enter the letter **c**.

The system displays the following messages:

```
/pci@400/pci@2/pci@0/pci@4/scsi@0/disk has been selected.
Type ^Y (Control-Y) to insert it in the command line.
e.g. ok nvalias mydev ^Y
 for creating devalias mydev for /pci@400/pci@2/pci@0/pci@4/scsi@0/disk
```



### Important:

Do not press the enter key until instructed to do so in Step [16](#).

14. At the `ok` prompt, enter:

```
boot <Ctrl + y>
```

### Note:

Press the **Ctrl** key and the letter **y** at the same time.

The boot path option is appended to the command line.

Example:

```
boot /pci@400/pci@2/pci@0/pci@4/scsi@0/disk
```

15. Append **@p6** to the path.

Example:

```
boot /pci@400/pci@2/pci@0/pci@4/scsi@0/disk@p6
```

16. Press **Enter**.

17. The system should boot to the CUE Bootable DVD.

- If the system boots to the DVD, wait for the CUE flash image to install on the disks, then return to [Installing the CUE flash image](#) on page 63 and execute the remaining steps.
- If the system still fails to boot to the DVD, perform the steps in option a. If you do not get the desired result using option a, perform the steps in option b. If you do not get the desired result using option b, perform the steps in option c. If you do not get the desired result using option c, escalate through normal channels.
  - a. At the `ok` prompt, enter:

```
probe-scsi-all
boot cdrom
```
  - b. Eject the DVD and re-insert the DVD. Enter:

```
boot cdrom
```
  - c. Power the system off and back on. At the `ok` prompt, enter:

```
boot cdrom
```

# Chapter 5: Copying and activating the customer's administration and options

To copy and activate the customer's administration and options, use the following checklist to keep track of each procedure:

| Procedure                                                                                      | ✓ |
|------------------------------------------------------------------------------------------------|---|
| <a href="#">Upgrading the CMS load (optional)</a> on page 88                                   |   |
| <a href="#">Installing CMS patches</a> on page 94                                              |   |
| <a href="#">Copying customer data</a> on page 96                                               |   |
| <a href="#">Checking file differences between the old system and the new system</a> on page 98 |   |
| <a href="#">Linking the /etc/hosts file</a> on page 100                                        |   |
| <a href="#">Checking for installed Feature Packages and pseudo ACDs</a> on page 101            |   |
| <a href="#">Activating customer options</a> on page 103                                        |   |
| <a href="#">Activating customer options</a> on page 103                                        |   |
| <a href="#">Removing temporary ACD 1</a> on page 109                                           |   |
| <a href="#">Turning on CMS</a> on page 111                                                     |   |
| <a href="#">Starting CMS WebClient</a> on page 112                                             |   |
| <a href="#">Configuring Access Security Gateway</a> on page 113                                |   |
| <a href="#">Verifying that CMS is operating</a> on page 114                                    |   |
| <a href="#">Verifying unmeasured trunks</a> on page 114                                        |   |
| <a href="#">Updating storage interval data</a> on page 115                                     |   |
| <a href="#">Checking manual merge discrepancies</a> on page 115                                |   |
| <a href="#">Updating unmeasured trunks</a> on page 116                                         |   |
| <a href="#">Updating the switch setup</a> on page 116                                          |   |
| <a href="#">Removing the upgrade files</a> on page 117                                         |   |

| Procedure                                                                        | ✓ |
|----------------------------------------------------------------------------------|---|
| <a href="#">Migrating customer data</a> on page 119                              |   |
| <a href="#">Verifying that the CONSOLE parameter is set properly</a> on page 122 |   |
| <a href="#">Replacing the customer's tapes</a> on page 123                       |   |
| <a href="#">Turning the upgraded system over to the customer</a> on page 123     |   |

**Note:**

When remote personnel such as CMS Provisioning are supporting the upgrade, remote personnel use the system commands in this section to monitor the progress of the upgrade. Run the commands from the local console only when instructed or when there is no remote support.

## Upgrading the CMS load (optional)

Use this procedure if you are upgrading the CMS load on the CUE disk to a newer version of CMS.

1. If you do not need to upgrade the CMS version, continue with [Copying customer data](#) on page 96.
2. Check the version of CMS on the CUE disc that was shipped with the CUE kit.
3. Check the version of CMS on the CUE flashed system by entering:  
`pkginfo -x cms`
4. Perform one of the following actions:
  - If the version of CMS on the CUE disc matches the version of CMS on the flashed system, CMS does not need to be upgraded to a newer version. Continue with [Installing CMS patches](#) on page 94.
  - If the version of CMS on the CUE disc does NOT match the version of CMS on the flashed system, CMS does need to be upgraded to a newer version. Use the procedures in the following sections before continuing with the CUE upgrade:
    - [Installing Solaris patches](#) on page 89
    - [Removing the current CMS load](#) on page 91
    - [Installing CMS](#) on page 92

## Installing Solaris patches

- If the CMS system is an x4270 platform, continue with [Removing the current CMS load](#) on page 91.
  - If the CMS system is a T5120, T5220, or T4-1 platform, continue with Step [1](#).
1. Load the Avaya Call Management System software disc into the disc drive.

**Note:**

It is safe to reboot the system if the system does not detect the Avaya Call Management System software disc and stopping and restarting volfs does not activate the DVD.

2. Enter:

```
/cdrom/cdrom0/spatches_conf
```

The system displays one of the following messages:

- If there are *no* Solaris patches to install, the system displays the following message:

```
There are no Solaris patches to install
```

- If there are Solaris patches to install, the system displays the following message:

```
Warning: you must close all applications before running this script
.....
.....
.....
Solaris patches have been spooled to your machine. The patches will
be installed after rebooting. During the installation of patches
your server will not be available.

The estimated time to install all patches is: 15 minutes

Ready to install Patches. Please leave the CD in the drive.
You will need to reboot the server for patches to install.

Do you want to reboot now? [y,n,?]
```



**Important:**

The message contains an estimate of the amount of time needed to install the Solaris patches.

3. Exit the spatches installation process.

Enter: **n**

4. The system displays a prompt to confirm that you want to exit and a warning that if you exit the installation of Solaris patches, you must install them before upgrading CMS:

Enter: **y**

5. Choose one of the following steps:

- If there are NOT any Solaris patches to install, continue with [Removing the current CMS load](#) on page 91.
- If there are Solaris patches to install, continue with Step [6](#).

6. Set the IDS environment by entering:

```
. /opt/informix/bin/setenv
```

7. Enter:

```
onmode -yuk
```

8. Ignore any error messages.

9. Enter:

```
/cdrom/cdrom0/spatches_conf
```

10. Install the Solaris patches by entering: **y**

The system boots into single user mode and begins to install the Solaris patches. The Solaris patch installation takes at least the amount of time that was estimated earlier in the procedure. After the Solaris patches are installed, the system reboots into multiuser mode and displays a login prompt.



### CAUTION:

If you cancel the installation of Solaris patches, you must install them before upgrading CMS. To cancel installation of the Solaris patches, enter: **n**

11. Log in to the system as **root**. The `root` password is blank at this time.
12. Verify that all of the Solaris patches have been installed by entering:

```
tail -10 /var/cms/spatches/spatches.log
```

The system displays the following message:

```
All patches installed successfully.
```

**Note:**

If the installation procedure fails for any of the patches, the system displays the following message:

```
Installation failed for one or more Solaris patches.

- Customers in the US should call the CMS Technical Services
 Organization at 1-800-242-2121

- Customers outside the US should contact your Avaya
 representative or distributor.
Patch installation completed: <time stamp>
```

13. If the system displays the message shown in the previous page, continue with the remaining Avaya CUE upgrade procedures. When the upgrade is complete, notify your Avaya CMS support organization as instructed.

---

## Removing the current CMS load

To remove the current CMS load:

1. Enter:

```
cd /
```

2. Enter:

```
eject cdrom
```

3. Enter:

```
pkgrm cms
```

The system checks the package and displays the following message:

```
The following package is currently installed:
cms Avaya(TM) Call Management System
 (sparc) rNNxx.x

Do you want to remove this package? [y,n,?,q]
```

4. Enter: **y**

The system displays the following message:

```
Removing installed package instance <cms>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q]
```

5. Enter: **y**

The system displays the following message:

```
Processing package information.
Executing preremove script.

Do you want to preserve CMS data? [y,n,?]
```



**CAUTION:**

Do *not* preserve CMS data. You must remove the current CMS database.

6. Enter: **n**

The system displays the following message:

```
CMS and associated data will be removed from this machine

Are you sure this is correct? [y,n,?]
```

7. Enter: **y**

The system displays the following message:

```
All file systems should be backed up before continuing.
.
.
.
Have you backed up the file systems? [y,n,?]
```

8. Enter: **y**

**Note:**

If you see a getNextAcd error message during this final step, you can ignore the message and continue with Installing CMS on page 48.

The system removes the current CMS load and displays the following message:

```
>> Removing customer database.
.
.
.
Removal of <cms> was successful.
```

---

## Installing CMS

Upgrade the CMS load to a newer version of CMS after removing the current version:

1. Verify the CMS R17 Standard software disc is in the disc drive.

2. Enter the following command to update the CMS related Informix files.

```
/cdrom/cdrom0/update_ids
```

3. Enter:

```
pkgadd -d /cdrom/cdrom0 cms
```

**Note:**

You must enter **y** several times to continue installing the CMS software.

The system installs the CMS software. The system displays a message similar to the following example:

```
Processing package instance <cms> from </cdrom/rNNxx.x>
. . .
. . .
```

4. If the system displays any messages about conflicting files, setuid/setgid files, or scripts, enter **y** to all questions.
5. Press **Enter**.

The system proceeds to install CMS. When the installation is complete, the program displays the following message:

```
Installation of <cms> was successful.
```

**Note:**

If the installation procedure fails for any reason, the system displays the following message:

```
- Customers in the US should call the CMS Technical Services Organization at
1-800-242-2121

- Customers outside the US should contact your Avaya representative or distributor.
```

If the system displays this message, continue with this procedure and the remaining CMS upgrade procedures. When the upgrade is complete, you will need to perform maintenance on the system.

6. Press **Enter**.

The system returns to the command prompt.

7. Reboot the system. Enter:

```
/usr/sbin/shutdown -y -i6 -g0
```

The system reboots.

8. Log in as **root**.

9. Enter:

```
pkgchk -n cms
```

If the software installation is successful, the system prompt returns to the screen after a few seconds.

Ignore the `pkgchk` error associated with the `sqlhosts` file properties.

10. Continue with [Installing CMS patches](#) on page 94.

---

## Installing CMS patches

If the new CMS load has any patches, those patches must be installed on the system. These patches are on the CMS software disc, not the CUE upgrade software disc. The CMS software disc is included in the upgrade kit.

If there are patches on the CMS software disc, it is labeled similar to “CMS Patch Issue 2.”

To install CMS patches:

1. Perform one of the following actions:

- If you recently upgraded the CMS load, continue with [Step 2](#).
- If the CUE upgrade software disc is in the drive, do the following steps:

- a. Enter:

```
cd /
```

- b. Enter:

```
eject cdrom
```

- c. Remove the CUE upgrade software disc and save the disc for later.

- d. Load the CMS software disc labeled `r17cue1X.N`.

The system displays the **File Manager** window. Click the cursor in an XTERM window.

**Note:**

If the system does not display the **File Manager** window, enter the following commands to start the volume manager:

```
svcadm disable volfs
```

```
svcadm enable volfs
```

The system displays the **File Manager** window. Click the cursor in an XTERM window.

2. After 15 seconds, enter:

**cmssvc**

The system displays the **CMS services** menu.

3. Enter the number that corresponds to the **load\_all** option.
4. One of the following conditions occur:
  - If no patches are on the disc, the system displays the following messages:

No CMS patches found on the CD.  
Please check the CD and try again.

Continue with Step [6](#).

- If patches are on the disc, the system displays a list of the patches.

5. Enter: **y**

The system installs the patches. As the system installs patches, the system displays messages similar to the following example for each patch installed:

```
@(#) installpatch 1.0 <time stamp>
cmspx-s
Generating list of files to be patched...
Creating patch archive area...
Saving a copy of existing files to be patched...
xxxx blocks
 File compression used
Installing patch packages...

Doing pkgadd of cmspx-s package:
Installation of cmspx-s was successful.

Patch packages installed:
 cmspx-s

Patch installation completed.

See /cms/patch/cmspx-s/log for more details
```

6. After the system installs all the patches, or if there are no patches on the disc, enter:
 

**eject cdrom**
7. Continue with [Copying customer data](#) on page 96.

---

## Copying customer data

To copy the customer's data from the upgrade backup device onto the system:

**Note:**

If you used an extract device other than tape for the `cvue_extract` process, then the extract device needs to be mounted and accessible. For more information, refer to [Mounting an extract device](#) on page 77.

1. If the extract device is a tape drive, select **Tape**. Verify that the Upgrade Extract tape of the customer is write-protected and inserted in the correct tape drive. Remove tapes from any other tape drives connected to the system, and continue with Step 4.
2. If the extract device is a USB storage device or a network mount point, select **Other**.
  - The system displays the following message:

Please enter extract path [q]:

3. Enter the path where the extract `cvue_extract.tar` file is located. This must be the path used in the `cvue_extract` process.

Example:

If the extract device is a USB storage device or NFS server mount point, the path can be `/CUE_extract_dir`.

4. If CMS was upgraded, remove the Avaya CMS upgrade software disc from the disc drive and keep the disc in a safe place.
5. Insert the CUE upgrade software disc labeled `r17cue1X.N`.

The system displays the File Manager window. Click the cursor in an XTERM window.

**Note:**

If the File Manager window does not open, enter the following commands to start the volume manager:

```
svcadm disable volfs
```

```
svcadm enable volfs
```

It is safe to reboot the system if the Avaya CUE upgrade software disc is not recognized and stopping and restarting `volfs` does not activate the DVD. If you reboot the system, you need to remount the USB storage device or Network.

6. After 15 seconds, enter:

```
cd /cdrom/cdrom0
```
7. Perform one of the following actions:

- If running the command locally at the console, enter:  
`./cvue_copy`
- You must read the following admonishment before running the command in this step:



**CAUTION:**

If the remote connection is dropped after starting this command with `nohup`, reconnect to the system, but *do not* rerun this command. Use `tail -f /nohup.out` to view the progress of the command. When finished viewing the `nohup.out` file, press **Del** to break out of the command.

Optionally, if running the command remotely on a dial-up line, enter:

```
nohup ./cvue_copy | tee /nohup.out &
```

Depending on the configuration of your system, the system displays the following options:

```
Choose an extract device:
1) Tape
2) Other
Enter choice (1-2):
```

8. The copy process next starts copying files. During the copy process the system displays a list of files being copied:

```
Reading admin data from extract device
.
.
```

9. After the customer's files are copied onto the system, the system displays the messages shown in the following example:

```
.
.
x ./export/home/.geo, 85 bytes, 1 tape blocks
Finished reading admin data from /dev/rmt/X

Finished reading admin data from /dev/rmt/X
```



**Important:**

If the tape copy fails and the extract device is a tape drive, try cleaning the tape drive and restart the copy with Step [7](#). If the tape copy continues to fail, the tape is probably faulty. You must shut down the system, reinstall the original disk drives, boot the system, and restart the extract with a *new* blank tape. See [Configuring the data extraction device](#) on page 23.

10. The `verify_fileproperties` script automatically executes after the customer files are copied from the extract device, and the system displays the following messages:

```
Running verify_fileproperties, any differences will be noted in
/var/log/cvue_file_diff
Verifying file permissions, owner and group, Please wait
see /var/log/cvue_file_diff for differences
The CUE Copy process is complete...<time stamp>
```

11. The system automatically reboots after `cvue_copy` completes, and the system displays the following messages:

```
The system will now be rebooted to clean up configuration changes.
```

12. The system reboots. If the system powers off instead of rebooting, press the power on button.
13. Log into the system as root.
14. Continue with [Checking file differences between the old system and the new system](#) on page 98.

---

## Checking file differences between the old system and the new system

During the upgrade, file properties can be updated with the new version of CMS, Solaris, and other software that is installed. In addition, files used on the old system can be renamed or are not required on the new system. The procedures in this section show you how to check for these differences.



### Important:

It is important to look for file property discrepancies. However, before you change any file properties, you must note that the CUE master disks are created with the correct file properties. Have a person with knowledge regarding properties of files review any changes to file properties to correctly assess the final status of each file.

There are two procedures to check file properties:

- [Verifying files using `pkgchk`](#) on page 99
- [Comparing directory and file permissions](#) on page 99

---

## Verifying files using pkgchk

The **pkgchk** command is a CMS tool that checks specific system files in the new system for discrepancies in the following attributes:

- directory and file permissions
- modes
- ownership
- file size and checksum

Although the system can display error messages when using this tool, error messages do not mean that the system will not function properly.

If you find any permission, mode, and ownership discrepancies between what was expected and what is actually shown, and if you think the discrepancies can cause problems, use the **chmod** and **chown** commands to fix the discrepancies. You can ignore any modtime, file size, and file checksum discrepancies.

To use the **pkgchk** tool:

1. Enter:  

```
pkgchk -n cms
```
2. Determine if the files listed require attention.

---

## Comparing directory and file permissions

The **verify\_fileproperties** command is executed as part of the **cvue\_copy** process and preserves the file permissions and modes from the new system in the file **/var/log/cvue\_file\_properties.post**.

1. To compare the file permissions and modes of the old system to the new system, enter:

```
cd /var/log
diff cvue_file_properties.pre cvue_file_properties.post >
cvue_file_properties.diff
```

The system places any file permissions and mode differences found between the original system and the new system in the **/var/log/cvue\_file\_properties.diff** file.

**Note:**

You can ignore any file differences associated with the **/adminsave** directory.

2. View the file and if any file properties are not appropriate, correct the file properties.
3. Continue with [Linking the /etc/hosts file](#) on page 100.

---

## Linking the `/etc/hosts` file

If the original system displayed a symbolic link for `/etc/hosts` to `/etc/inet/hosts`, this procedure is not needed. Continue with [Checking for installed Feature Packages and pseudo ACDs](#) on page 101.

If the original system did not display a symbolic link for `/etc/hosts` to `./inet/hosts` and the original system was operating properly, you must restore the `/etc/hosts` file temporarily until the customer has time to merge any relevant information into a single "hosts" file.

To restore the `/etc/hosts` file:

1. Enter the following commands:

```
mv /etc/inet/hosts /etc/inet/hosts.orig
cp -p /manual_merge/etc/hosts /etc/inet/hosts
```

2. Enter:

```
ls -l /etc/hosts
```

The system displays a message similar to the following:

```
lrwxrwxrwx 1 root root <time stamp> /etc/hosts -> ./inet/hosts
```

3. Perform one of the following actions:
  - If the system displays a symbolic link for `/etc/hosts` to `./inet/hosts`, continue with Step 6.
  - If the system does not display a symbolic link for `/etc/hosts` to `./inet/hosts` and the original system was operating properly, continue with Step 4.
4. Enter the following commands:

```
cd /etc
ln -s ./inet/hosts /etc/hosts
```
5. Verify that the files are linked by repeating Step 2.
6. Inform the customer they need to merge any relevant information from the `/etc/inet/hosts.orig` file into the `/etc/hosts` file. In the future, the customer must verify that `/etc/hosts` is a symbolic link to `/etc/inet/hosts` before making modifications to the `/etc/hosts` file.
7. Continue with [Checking for installed Feature Packages and pseudo ACDs](#) on page 101.

---

## Checking for installed Feature Packages and pseudo ACDs

If the External Call History (ECH) feature package is installed on the system and pseudo-ACDs are also administered on the system then installation of the ECH feature package fails during the CMS setup process.

To prevent ECH installation from failing during the CMS setup process:

1. Review the `/adminsaver/cmsadmin.saved/fp.install` file.
2. Search for any ACD entries greater than ACD 8. Pseudo ACDs are referenced as **unnamed\_acdx**.
3. If any entries exist, make a copy of the original `/adminsaver/cmsadmin.saved/fp.install` file.
4. Edit the `/adminsaver/cmsadmin.saved/fp.install` file and delete or comment out the **unnamed\_acd** value that is displayed on the line following the **unnamed\_acd** line. In the following example, the value to be commented out is 20000.

```
Number of call segments to buffer for ACD unnamed_acd9:
#20000
```

5. Repeat step 4 for all pseudo ACDs.
6. Save the modified file.
7. Go to [Checking the setup.out file](#) on page 101.

---

## Checking the setup.out file

The CMS setup portion of the CUE activate process fails if the default backup device path in the `/adminsaver/cmsadmin.saved/setup.out` file does not exist or is not accessible.



### Important:

You must check the `/adminsaver/cmsadmin.saved/setup.out` file to ensure that the default backup device path exists and is accessible.

1. To verify that the default backup device in the `/adminsaver/cmsadmin.saved` file is correct, enter:

```
cat /adminsaver/cmsadmin.saved/setup.out | pg
```

```
Enter a name for this UNIX system (up to 256 characters):

Select the type of backup device you are using
1) Tape
2) Other
Enter choice (1-2):
2
Default backup device paths based on device type:
Device Default backup path
Tape /dev/rmt/0c
Other 'none'
Enter the default backup device path:
/CUE_extract_dir/hostname
```

2. Check the accessibility of the default backup device.

- a. If the type of backup device is Tape, enter:

```
mt -f /dev/rmt/x status
```

- If the tape device is detected and the output is correct, continue with [Activating customer options](#) on page 103.
- If the tape device is not detected, resolve the tape device issues then continue with [Activating customer options](#) on page 103.

- b. If the type of backup device is Other, enter:

```
ls -l /CUE_extract_dir/hostname
```

where `/CUE_extract_dir/hostname` is the path of the backup device directory.

- If the backup device path is detected and the output is correct, continue with [Activating customer options](#) on page 103.
- If the backup device path is not detected, continue with Step [3](#).

3. If the system is unable to detect the backup device path, you must either correct the mount problem causing the inaccessibility of the backup device path or you can temporarily change the `/adminsaver/cmsadmin.saved/setup.out` file to complete the CUE Activation process.

To temporarily change the default backup device path:

- a. Make a backup copy of the `/adminsaver/cmsadmin.saved/setup.out` file.  
Enter:

```
cd /adminsaver/cmsadmin.saved
cp -p setup.out setup.out.save
```

- b. Edit the `setup.out` file. Enter:

```
vi setup.out
```

- c. Change the backup device type option from 2 to 1.

```
Select the type of backup device you are using
1) Tape
2) Other
Enter choice (1-2):
1
```

- d. Change the backup device path to `/dev/null`.

```
Enter the default backup device path:
/dev/null
```

- e. Save and quit the `vi` editor. Enter:

```
:wq!
```



**Important:**

You need to restore the CMS setup file to its original state before the `cvue_cleanup` script is executed.

4. Continue with [Activating customer options](#) on page 103.

---

## Activating customer options

The amount of time to activate customer options depends on the number of customer options, the number and size of the disk drives, the number of ACDs, and other parameters.



**Important:**

If your backup device uses a mount point for backups, verify that the mount point is accessible.

To activate the customer's software options:

1. Enter:

```
cd /cdrom/cdrom0
```

2. Perform one of the following actions:

- If you are running the command locally at the console, enter:

```
./cvue_activate
```

- You must read the following admonishment before running the command in this step:

**CAUTION:**

If the system drops the remote connection after starting this command with **nohup**, reconnect to the system, but *do not* rerun this command. Use **tail -f /nohup.out** to view the progress of the command. When finished viewing the **nohup.out** file, press **Del** to break out of the command.

Optionally, if you are running the command remotely on a dial-up line, enter:

```
nohup ./cvue_activate | tee /nohup.out
```

**For On Site Personnel:** If the upgrade is being supported by remote personnel (for example, CMS Provisioning), use the following command from the local console during the copy and activate process to view the upgrade log file and track the progress of the upgrade:

```
tail -f /var/log/cvuelog
```

When finished viewing the **/var/log/cvuelog** file, press **Del** to break out of the command.

3. One of the following conditions occur:

- If the copy was not successful, the system displays the following message. You must run copy again (see [Copying customer data](#) on page 96):

```
cvue_copy not successful, run the cvue_copy again
```

- If the copy completed successfully, the system starts activating the customer's options. The system displays messages such as the following example:

```
CUE VERSION: <cue_version>

..
S00Sethostname Start Time -> <time stamp>

S00Sethostname End Time -> <time stamp>

.
.
```

4. The system continues activating the customer's options. The system displays messages similar to the following examples to show that serial printers are readministered. Network printers must be readministered after the upgrade:

```
.
.
S12AdministerPrinters Start Time -> <time stamp>
S12AdministerPrinters End Time -> <time stamp>
.
.
S21checkdevices Start Time -> <time stamp>
S21checkdevices End Time -> <time stamp>
.
.
```


**Important:**

If the extract process used a USB storage device or a network server mount point and the S21checkdevices fails, it is probably because the default backup path in the /cms/db/cms.install file is a tape drive or the path does not exist. Make a note of the default backup device currently defined in the /cms/db/cms.install file. Make a copy of the /cms/db/cms.install file and modify the original /cms/db/cms.install file, making the default backup device path the mount point being used for the extract device. Save the file and exit the editor. Rerun the ./cvue\_activate script.

5. The system continues activating the customer's options. The system displays messages similar to the following examples:

```
.
.
S59init_db Start Time -> <time stamp>
S59init_db End Time -> <time stamp>
.
.
```

6. The system continues activating the customer's options. The system displays messages similar to the following examples:

```
.
.
S70converter End Time -> <time stamp>

S80cmssetup Start Time -> <time stamp>
CMS setup started <time stamp>
Schema updated started <time stamp> .
.
.
```

If you are looking at the `/var/log/cvue1og` file during CMS setup (the `S80cmssetup` script), you can see failure messages about the SQL database. You can ignore these messages. CMS setup takes several minutes to complete.

7. The system continues activating the customer's options. The system displays messages similar to the following examples:

```
.
.
Customer CMS data successfully initialized <time stamp>
.....
Computing space requirements and dbspace availability.
Setup completed successfully.
S80cmssetup End Time -> <time stamp>
.
.
```

8. The system continues activating the customer's options. The system displays messages similar to the following:

```
.
.
S81cmsfeatpkg Start Time -> <time stamp>
.
.
.
.
```

9. If the system did not encounter any errors during the `cvue_activate` process, the system displays the following message:

```
The CUE Activate process is complete.
```

- If the `cvue_activate` process completed without errors, continue with [Removing temporary ACD 1](#) on page 109.

- If the `cvue_activate` process encountered errors with one or more of the activate scripts or the activate process does not complete, refer to [Recovering from failed installation scripts](#) on page 107.

---

## Recovering from failed installation scripts

If the system displays an error message, such as the following example, a failure occurred in one of the installation scripts.

```
ERROR[1]: FUNCTION S00Sethostname() FAILED at <time stamp>
script /adminsave/init.d/S00Sethostname failed
```

You can recover and continue with the upgrade by skipping the failed installation script during this part of the upgrade. However, any script skipped during this part of the upgrade must be installed later using the standard software installation procedures found in the CMS software installation document.

The following sections list all the possible software installation scripts and explains what to do if one of the scripts fails during the upgrade. When identifying the installation scripts, note that each script is numbered with a prefix (for example, S04) before the script name.

This section includes the following topics:

- [Scripts that can be skipped and installed later](#) on page 107
- [Failures that require escalation to support](#) on page 108
- [Failures that occur when adding features](#) on page 109

---

## Scripts that can be skipped and installed later

The installation scripts listed in the following table can be skipped during this part of the upgrade. All these scripts install optional software or drivers needed by the customer. However, any script that is skipped during this part of the upgrade must be installed later using the standard software installation procedures found in the CMS software installation document.

| Script name | Description          |
|-------------|----------------------|
| cmsfeatpkg  | CMS Feature Packages |

To recover from these failed scripts:

1. Enter: `cd /adminsave/init.d`
2. Enter: `mv scriptname /adminsave/` where *scriptname* is the name of the script.

3. Enter: `cd /cdrom/cdrom0`
4. Run the `./cvue_activate` command again.
5. Install the software package that you skipped before you migrate the customer's data.

**Note:**

After each script is executed, a copy of the script is automatically moved to the directory `/adminsave/init.d.completed`.

---

## Failures that require escalation to support

For the scripts listed in the following table, do not attempt to continue with the upgrade. Escalate the problem through the normal channels.

| Script name        | Description                    |
|--------------------|--------------------------------|
| Sethostname        | Sets the host name             |
| install_cmsweb     | CMS WebClient                  |
| sqlhosts           | SQL hosts file setup           |
| AdministerPrinters | Administers serial printers    |
| modifyfile         | Restores CMS setup information |
| checkdevices       | Checks for devices             |
| MigrateAlarmData   | Migrate Alarm Data             |
| init_db            | Database initialization        |
| storage            | Data storage allocation        |
| converter          | Preserves CMS setup data       |
| cmssetup           | CMS setup command              |

---

## Failures that occur when adding features

If ECH is installed on a system and pseudo-ACDs are also administered on the system, the restore process and the CUE process fail during the installation of the CMS feature packages (script `S81cmsfeatpkg`).

If the restore process or the CUE process fails when installing CMS feature packages:

1. See `/var/log/cvuelog` for error messages.
2. Verify whether the script `/adminsave/init.d/S81cmsfeatpkg` exists.
3. If the script exists, open the file `/adminsave/cmsadmin.saved/fp.install` and search for any ACD entry that references an `unnamed_acd`.
4. If the entry exists, make a copy of the original `fp.install` file.
5. Edit the `/adminsave/cmsadmin.saved/fp.install` file and delete or comment out the `unnamed_acd` value that is displayed on the line following the `unnamed_acd` line. In the following example, the value to be commented out is 20000.

```
Number of call segments to buffer for ACD unnamed_acd9:
#20000
```

6. Save the modified file.

**Note:**

If you installed Forecasting also, you must remove Forecasting. Use the `cmsadm` command before proceeding.

7. Re-execute command `./cvue_activate` from the `/cdrom/cdrom0` directory.

---

## Removing temporary ACD 1

Perform this procedure to remove any temporary ACDs created during the extract process of the upgrade.

- If you did not create a temporary ACD 1 during the extract process, continue with [Restoring the cms.install file](#) on page 110.
- If you created a temporary ACD 1 during the extract process, continue with this procedure.

To remove temporary ACD 1:

1. Enter:

```
cmsadm
```

The system displays the **CMS Administration** menu.

2. Enter the number that corresponds to the `acd_remove` option.
3. Enter ACD 1.  
The system displays a warning message.
4. Enter: `y`
5. Continue with [Restoring the cms.install file](#) on page 110.

---

## Restoring the cms.install file

- If the `/adminsave/cmsadmin.saved/setup.out` file was not modified to change the default backup device information, continue with [Turning on CMS](#) on page 111.
  - If the extract process used a USB storage device or network server mount point and the `setup.out` file was modified, then you must check the `/cms/install/cms_install/cms.install` file to ensure that the default backup device path is correct. Continue with Step [1](#).
1. Run the `cmsadm` command to create the `/cms/install/cms_install/cms.install` file, enter:

```
cmsadm
```

The system displays the **Avaya Call Management System Administration** menu.

2. Enter the number associated with the backup option.  
The system displays a list of backup options.
3. Press the `Del` key to exit the backup.
4. To change the default backup device in the `/cms/install/cms_install/cms.install` file, enter:  

```
cd /cms/install/cms_install
```
5. Edit the `cms.install` file. Enter:

```
vi cms.install
```

**Note:**

Review the `/adminsave/cmsadmin.saved/setup.out.save` file for the original default backup device information.

6. Change the backup device type option back to the value in the `/adminsave/cmsadmin.saved/setup.out.save` file:

```
Select the type of backup device you are using
1) Tape
2) Other
Enter choice (1-2):
2
```

7. Change the backup device path back to the value in the `/adminsave/cmsadmin.saved/setup.out.save` file:

```
Enter the default backup device path:
/CUE_extract_dir/hostname
```

8. Save and quit the `vi` editor. Enter:  
`:wq!`
9. Continue with [Turning on CMS](#) on page 111.

---

## Turning on CMS

To turn on CMS:

1. Enter:  
`cmsadm`  
 The system displays the **CMS Administration** menu.
2. Enter the number that corresponds with the `run_cms` option.
3. Enter 1 to turn on CMS.
4. Choose the operation from the following choices based on whether you are using CMS Supervisor Web client or not:
  - If you are not using CMS Supervisor Web client, continue with [Verifying that CMS is operating](#) on page 114.
  - If you are using CMS Supervisor Web client, continue with [Starting CMS WebClient](#) on page 112.

## Starting CMS WebClient

To start the CMS WebClient, enter:

```
cmsweb start
```

---

## Certificate Management

A security certificate is needed to encrypt communication between browsers and CMS Supervisor Web server. Upon first installation of the cmsweb package, the installation process automatically generates a self-signed certificate based on the host name and domain name of the host server. You can view the URL/Common Name used in this certificate by the following command:

```
/opt/cmsweb/bin/showcrt.sh
```

Example:

```
URL/Common Name: cms163.avaya.com
```

The URL/Common Name should be used to access the CMS Supervisor Web GUI from the browser. If the URL does not appear correct due to the network and host setup, use the following command to change it:

```
/opt/cmsweb/bin/chgcrt.sh
```

The above command prompts for the new URL. The default value for this command is your host name and domain name, provided the domain name is configured on your host. Press **Enter** to accept the default or type in your preferred URL.

If the CMS Supervisor Web certificate changes, then you must restart CMS Supervisor Web to accept the changes. To restart cmsweb, enter:

```
cmsweb stop
```

```
cmsweb start
```

---

## Signing in

The output of the `/opt/cmsweb/bin/showcrt.sh` command contains the CMS Server address and domain needed to sign in to CMS Supervisor Web. For example, if your server is cms163.avaya.com, go to the following URL using any web browser.

<https://cms163.avaya.com:8443/CMSWeb/>

**Note:**

The 's' in https is important as all data in CMS Supervisor Web is secured using https.

In the User ID and Password fields, enter the same information you currently use for CMS Supervisor or Terminal Emulator.

---

## Configuring Access Security Gateway

Use this procedure if the customer wants to use Avaya Access Security Gateway (ASG).

ASG is installed as part of the CUE process but must be configured using the customer specific Authentication File system (AFS) file.

1. Verify that you are logged in to the system as **root**.
2. Copy the AFS authentication file from the destination path. Enter:

```
cp -p <destination_path>/<AFS_filename> /tmp/AFS_file.xml
```

where `destination_path` and `AFS_filename` are the names noted in Step 2 of the section *Preserving the CMS authentication file*. Depending on the destination path, you may require a secure copy. For example, you may have to use `scp` instead of `cp`.

3. Verify that the AFS authentication file was copied from the destination directory to `/tmp/AFS_file.xml`.
4. Verify that the file properties of `/tmp/AFS_file.xml` are correct.

To install the AFS authentication file, enter:

```
/opt/cmsasg/usr/local/bin/loadauth -af -l /tmp/AFS_file.xml
```

**Note:**

Ignore any X11 warning messages.

The system displays the following messages while loading the AFS authentication file:

```
Loading file /tmp/AFS_file.xml
copying the AFS file
```

5. Continue with [Verifying that CMS is operating](#) on page 114.

## Verifying that CMS is operating

To verify that CMS is fully functional:

1. Enter:

```
su - cms
```

The system displays the \$ prompt.

2. Enter:

```
cms
```

Ignore any messages about backups.

3. The system displays the CMS main window. Verify that the status of the switch links before the upgrade match the status of the switch links after the upgrade. That is, if a switch link was operating before the upgrade, the switch link must be operating after the upgrade. If a switch link that must be operating is not, make sure that data collection is turned on.
4. Continue with [Verifying unmeasured trunks](#) on page 114.

---

## Verifying unmeasured trunks

1. View Data Storage Allocation.
2. Verify that the value for unmeasured trunks is 50% of the value entered for trunks. This verification will prevent future problems in trunk administration.

**Note:**

If the unmeasured trunks value must be modified:

- CMS Must be in single user mode
- Data collection must be off for all ACDs
- Data Storage Allocation must be modified for each ACD

3. Continue with [Updating storage interval data](#) on page 115.

---

## Updating storage interval data

During a CUE upgrade, the procedure does not preserve all storage interval data. The majority of the storage interval data is preserved in the `storage.def` file. However, the information for the data summarizing time, switch time zone offset, and master clock ACD are not part of the `storage.def` file.

To update the storage interval data that you noted in [Recording storage interval data](#) on page 19:

1. Select **System Setup > CMS State**.
2. Update the **Master ACD for clock synchronization** option.
3. Save the update.
4. For each ACD, Select **System Setup > Storage Intervals**.
5. Update the **Data summarizing time** and the **Switch time zone offset** options.
6. Save the update.
7. Repeat Steps 4 through 6 for each ACD.
8. Log out of CMS.
9. Continue with [Checking manual merge discrepancies](#) on page 115.

---

## Checking manual merge discrepancies

The `cvue_extract` command compares customer system files to the new Solaris operating system files installed on the CUE master disk. The new Solaris operating system files to be compared are located on the CUE upgrade software disc. The files on the CUE upgrade software disc are compared to files located on the customer's current system. Any files that show a difference between the CUE upgrade software disc and the current customer system are written to a manual merge directory.

Only files which are in the `okdiff` directory are copied to tape. CUE writes these files to tape during the `cvue_extract` process and the files are copied to the directory `/manual_merge` on the CUE master disk during the `cvue_copy` process. These files are identified in `/var/log/cvuelog` file as "manual merge" discrepancies.



**Important:**

The customer must look at the manual merge discrepancies outlined in the `/var/log/cvuelog` to determine if they are Solaris changes or customer customization changes. Solaris changes must not be modified. Customization changes might need to be modified. The files that are identified can be important to the new system. The customer can find that these files need to be copied to a location that will eventually fix a problem. These files can contain networking information, customizations, or security settings that are critical to the customer.

To check for discrepancies between the earlier system and the new system:

1. Enter:  

```
cat /var/log/cvuelog | grep "merged manually" | pg
```
2. Check the displayed messages and correct any problems that you find.
3. Continue with [Updating unmeasured trunks](#) on page 116.

---

## Updating unmeasured trunks

Measured and unmeasured trunks have separate system and ACD limits in CMS R14 or later. In previous CMS releases, measured and unmeasured trunks made up trunk limits. When CMS setup is run, unmeasured trunks will always default to half of the value entered for trunks. CUE has run setup using the previous system setup, so this value might need to be updated.

To update unmeasured trunks:

1. Verify that you are in single-user mode, and data collection is off for all ACDs.
2. Perform the following steps for *each* ACD:
  - a. Access Data Storage Allocation.
  - b. Modify the unmeasured trunks to be half of the trunks you entered.
3. Continue with [Updating the switch setup](#) on page 116.

---

## Updating the switch setup

In many cases, the switch is upgraded to a new release when the CMS is upgraded. Verify switch setup for any ACDs where the switch model was changed.

If the switch model has changed, you must perform the following procedures:

- Check the switch links on the CMS main window and verify that the switch links are up.

- If the links are not active, use the `swsetup` option of the `cmsvc` command to check the administration of each ACD on the CMS. CMS must be turned off to administer the ACDs. For more information about converting links, see *Avaya CMS Switch Connections, Administration and Troubleshooting*. Remember to turn CMS on after setting up the ACDs.
- Readminister the CMS version on the switch using the Feature Parameters form.

Continue with [Removing the upgrade files](#) on page 117.

---

## Removing the upgrade files

You must remove the files that you used for the upgrade.

To remove the upgrade files:

1. Enter:

```
cd /cdrom/cdrom0
```

**Note:**

If the system does not display **File Manager** window, enter the following commands to start the volume manager:

```
svcadm disable volfs
```

```
svcadm enable volfs
```

2. Perform one of the following actions:

- If running the command locally at the console, enter:

```
./cvue_cleanup
```

- You must read the following admonishment before running the command in this step:



**CAUTION:**

If the dial-up modem line is dropped after starting this command with `nohup`, reconnect to the system but *do not* rerun this command. Use `tail -f /nohup.out` to view the progress of the command. When finished viewing the `nohup.out` file, press **Del** to break out of the command.

Optionally, if running the command remotely on a dial-up line, enter:

```
nohup ./cvue_cleanup | tee /nohup.out
```

The system displays the following message:

```
Beginning cvue_cleanup process...please wait.
```

3. Note that if the number of files to remove is large, this procedure can take several minutes to complete. When the files are removed, the system displays the following message:

```
The cvue_cleanup process is complete...<time stamp>
#
```

4. Enter:  
`cd /`
5. Enter:  
`eject cdrom`
6. Remove the Avaya CUE upgrade software disc from the disc drive and keep the disc in a safe place.
7. Continue with [Authorizing ODBC Connections](#) on page 118

---

## Authorizing ODBC Connections

Perform this procedure if the number of authorized ODBC connections has not been configured.

1. Determine if the number of authorized ODBC connections has been configured. Enter:  
`cmssvc`  
The system displays the CMSSVC menu.
2. Enter the number associated with the `auth_display` option.
  - If the number of authorized ODBC connections is non-zero, continue with [Migrating customer data](#) on page 119.
  - If the number of authorized ODBC connections is zero, continue with this procedure.The ODBC connections must be authorized using the `auth_set` command. You require the customer purchase order to determine the number of authorized ODBC connections.
3. Use the customer purchase order to determine the number of ODBC connections authorized.
4. Enter the number for the `auth_set` option.  
The system displays the following message:  
`Password:`
5. Enter the appropriate password.

**Note:**

This password is available only to authorized personnel.

6. The system displays the current authorization for each CMS feature, press **Enter** to accept the current value.
7. Repeat Step 5 until the system displays the ODBC connection feature, as shown below:

Enter the number of authorized ODBC connection (0-10): (default: 0)

8. Enter the number of ODBC connections purchased by the customer, from Step 3.  
The system displays the command prompt.

**Note:**

You can verify the authorizations by using the `auth_display` option of the `cmssvc` command.

9. Continue with [Migrating customer data](#) on page 119.

---

## Migrating customer data

You must migrate the following customer data from the maintenance backup tapes:

- [Migrating system administration data](#) on page 119
- [Migrating agent and call center administration data](#) on page 121

---

## Migrating system administration data



**CAUTION:**

Perform this procedure only once! Attempting to migrate system administration data more than once causes *catastrophic errors* from which you are unable to recover. Failure to heed this warning can *irretrievably destroy data*.

To migrate the system administration data:

1. If CMS is not turned on, perform the following procedure:
  - a. Enter:  
  
`cmsadm`  
  
The system displays the **CMS Administration** menu.
  - b. Enter the number for the `run_cms` option.
  - c. Enter 1 to turn on CMS.

2. Log on to CMS.

The system displays the CMS main window.

3. From the CMS main menu, select **System Setup > CMS State** to put CMS into single-user mode.
4. Turn off data collection for all ACDs.
5. Insert the most recent full maintenance backup tape or mount the extract device.
6. From the CMS Main Menu, select **System Setup > R3 Migrate Data**.

The **R3 Migrate Data** window is displayed.

7. In the **R3 Migrate Data** window, select the options and enter the values from the following table:

| Field          | Value to enter or option to select |
|----------------|------------------------------------|
| Device name    | Extract device name                |
| Data Type      | System Administration data         |
| Specify ACD(s) | All ACDs                           |

8. Press **Enter** to access the action list in the top right corner.

9. Select **Run** and press **Enter**.

The progress of the migration is displayed in the *Status* field. When the migration ends, the system indicates the success or failure of the migration in this field.

10. Press **F3** and select the UNIX option to display the UNIX prompt.

**Note:**

After the migration is complete, you will receive a message if migration of any custom reports fail. Information about the failed reports are written to the **r3mig.log** file. Acknowledge the message and contact Avaya Professional Services to have the custom report migrated to the new system.

11. Enter:

```
pg /cms/migrate/r3mig.log
```

The system displays the customer migration log.

12. Verify the contents of the customer migration log and take any necessary corrective action. For help with interpreting the log, contact technical support or your customer representative.
13. Repeat steps 6-12 using the incremental backup media, if one was created.
14. To exit the UNIX window, enter:

```
exit
```

## Migrating agent and call center administration data

To migrate agent and call center administration data:

1. Verify that the most recent full maintenance backup is accessible by the extract device.
2. From the CMS Main Menu, select **System Setup > R3 Migrate Data**.

The system displays the **R3 Migrate Data** window.

3. In the **R3 Migrate Data** window, select the options and enter the values from the following table:

| Field          | Value to enter or option to select |
|----------------|------------------------------------|
| Device name    | Extract device name                |
| Data Type      | Agent/Call Center Admin data       |
| Specify ACD(s) | All ACDs                           |

4. Press **Enter** to access the action list in the top right corner.
5. Select **Run** and press **Enter**.

The system displays the progress of migration in the `Status` field. When the migration ends, the system indicates the success or failure of the migration in this field.

6. Turn on data collection for all ACDs.
7. Press **F3** and select the UNIX option to display the UNIX prompt.
8. Enter:

```
pg /cms/migrate/r3mig.log
```

The system displays the customer migration log.

9. Verify the contents of the customer migration log and take any necessary corrective action. For help with interpreting the log, contact technical support or your customer representative.
10. Repeat steps 1-9 using the incremental backup media, if one was created.
11. To exit the UNIX window, enter:  
`exit`
12. Select **System Setup > CMS State** to put CMS into multiuser mode.
13. Continue with [Verifying that the CONSOLE parameter is set properly](#) on page 122.

---

## Verifying that the CONSOLE parameter is set properly

After you have migrated the customer data and you are about to complete the upgrade, you must verify that the CONSOLE parameter in the `/etc/default/login` file is set properly.

To check the CONSOLE parameter:

1. Enter:

```
vi /etc/default/login
```

2. Search for the following lines:

```
.
.
If CONSOLE is set, root can only login on that device.
Comment this line out to allow remote login by root.

CONSOLE=/dev/console
.
.
```

3. If there is a leading pound sign (#) on the `CONSOLE=/dev/console` line, delete the pound sign.
4. Press **ESC**.
5. Enter:  

```
:wq!
```

This command writes and closes the file.
6. Continue with [Replacing the customer's tapes](#) on page 123.

---

## Verifying auto-boot is set to true

You must verify that `auto-boot?` is set to true before handing over the system to the customer.

**Note:**

If the system is an x4270 platform, continue with [Replacing the customer's tapes](#) on page 123.

1. Enter

```
eeeprom auto-boot?=true
```

This command sets `auto-boot?` to true.

---

## Replacing the customer's tapes

After you migrate the customer's data, remove the tapes from the tape drives and replace any tapes that the customer originally had in the tape drives. These tapes that the customer had in the tape drives can be used for scheduled backups and must be replaced before leaving the customer site.

Continue with [Turning the upgraded system over to the customer](#) on page 123.

---

## Turning the upgraded system over to the customer

After the data migration is complete, inform the customer that they must complete the post-upgrade procedures documented in *Avaya Call Management System Upgrade Express (CUE) Customer Requirements*.

---

## Configuring alarming options

Configure alarming options using the Alarm Origination Manager (AOM) tool. This tool should only be used by provisioning personnel. This tool is available in the `/cms/aom/bin` directory, and can be run using either the interactive mode or the command line mode. To run the AOM tool in interactive mode, run the following commands:

```
cd /cms/aom/bin
./aom_tool
```

To get command line usage help for the AOM tool, run the following commands:

```
cd /cms/aom/bin
./aom_tool ?
```

