# Avaya Call Management System

## Base Load Upgrade

Release 16.3
November 2013

**Notice**

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

**Documentation disclaimer**

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

**Link disclaimer**

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

**Warranty**

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site:

http://www.avaya.com/support

**License**

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://www.avaya.com/support/LicenseInfo ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

**License type(s)**

**Designated System(s) License (DS).** End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified 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 Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

**Named User License (NU).** Customer 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 Product that permits one user to interface with the Product.

**Shrinkwrap License (SR).** With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

**Copyright**

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use 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 Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://www.avaya.com/support/ThirdPartyLicense

**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 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 Web site:

http://www.avaya.com/support

**Trademarks**

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

**Downloading documents**

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

http://www.avaya.com/support

**Avaya support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

# Contents

# Introduction

**Important:**
Customers who have 146 GB disks on their systems, use LAN Backup, and want the new migration capability, must use CUE to upgrade to CMS R16.3.

The Avaya Call Management System(CMS) base load upgrade is installed by Avaya customers who either had problems with an earlier CMS build of release R16.3 or need to upgrade from R16.1 or R16.2 base load to R16.3 load if using a backup procedure other than LAN. This upgrade provides all software fixes from known issues in previous CMS releases.

You must load this upgrade early as Technical Support Organization will troubleshoot the product that has the latest release installed.

This section includes the following topics:



## Purpose of this document

The purpose of this document is to describe the Avaya Call Management System (CMS) base load upgrade process for R16.3xx.x. This Avaya CMS base load upgrade is designed to be installed by Avaya CMS customers who either have had problems with an earlier version of the product or would like access to any new features added in the maintenance release. This upgrade provides all known software fixes from previous versions. The software is acquired by ordering the latest PCN. The PCN provides a list of all fixes and features added in the maintenance release.

**Important:**
Before installing a base load upgrade, verify that the software discs you received when ordering the PCN actually upgrade your current version of software. Verify that you are using the proper base load upgrade document for your release of CMS.

# When and how to use this document

**Important:**
Customers who have 146 GB disks on their systems, use LAN Backup, and want the new migration capability, must use CUE to upgrade to CMS R16.3.

Use this document to upgrade Avaya Call Management System (CMS) from an older CMS Release 16.3 (R16.3) base load to a newer CMS R16.3 load. You can also upgrade CMS Release 16.1 (R16.1) or Release 16.2 (R16.2) base load to the CMS R16.3 load if you have used a backup procedure other than LAN. Unless indicated otherwise, all procedures in the *Avaya CMS Base Load Upgrade* document are required.

Avaya recommends that:

- Before performing the upgrade, read through this entire document so that you are familiar with what tasks you will need to perform. If you decide you would like to have Avaya assist you performing the upgrade, see Contacting Avaya for assistance with your upgrade on page 7.
- Have a pen or pencil during the upgrade so that you can record any required information.
- During the upgrade, mark each step as it is completed.
- You will be required to enter UNIX commands during the upgrade process. You must enter the command from the UNIX prompt in a terminal window. Press the **Enter** key after you have typed in the command. Use the same capitalization and spacing shown in this document.
- If you encounter problems or have questions during the upgrade, contact Avaya technical support.

# Impacts to CMS service

**CAUTION:**
This software upgrade is service affecting.

During the upgrade process you will have to reboot your CMS system and turn off the CMS software. This upgrade can take several hours to complete. During the Solaris patch installation, your system will display an estimate of the amount of time needed to install the Solaris patches. The Solaris patch installation is the part of the base load upgrade that usually requires the longest amount of time to complete.

# Contacting Avaya for assistance with your upgrade

You can make arrangements to have Avaya provide remote assistance for this upgrade. This remote assistance must be scheduled at least two weeks before your upgrade. Charges, which will be quoted, vary for this service. Contact the Technical Support Organization at 1-800-242-2121.

# Possible customization impacts

The software upgrade that you are installing could potentially impact system customization that was performed before this upgrade. For example:

- Custom reports
- LAN printer customization
- Work-force management interfaces
- Operational Analyst

You can schedule an evaluation of your system to determine whether any of your system customizations might be impacted by this upgrade. Schedule this evaluation at least two weeks before your upgrade. Charges, which will be quoted, vary for this service. Contact Avaya CRM at 1-866-282-9266.

# Upgrade kit contents

All the software you need for the upgrade should be included with your upgrade kit.

# Contacting Avaya technical support during the upgrade

If you encounter problems or have questions during the upgrade and are unable to resolve them by following the upgrade instructions, call technical support at 1-800-242-2121. Be ready to provide the number of the Quality Protection Plan you are using.

# Visual Vectors upgrades

If you are upgrading the Visual Vectors software to Visual Vectors 16, which is compatible with CMS R16.3, you must upgrade to the appropriate versions of the following software:

- A CMS load of r16.3xx.x or later.
- Visual Vectors server vvsr16xx.x or later.
- Visual Vectors client software release VV16.

# Preparing for a base load upgrade

This section describes the tasks you must perform before you upgrade your CMS base load. These procedures will help you verify that your CMS system has no existing hardware or software problems before the upgrade. If you do not perform these procedures, your base load upgrade could fail, and your CMS system could be put in a non-functioning state for some time.

This section includes the following topics:



## Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in Introduction on page 5
- The Avaya CMS software disc will include a readme file called **cms.readme**. Avaya recommends you review this file for any changes that might impact the procedures in this document.
- Log in to the system as **root**.

  **Important:**
  You will not be able to log into the system remotely as **root**. If you are logging into the system remotely, log in as a user and then enter: **`su - root`**

# Verifying the current CMS version and load

To verify the version and load of CMS currently on the machine:

1. Log in to the system as **root**.
2. Enter:

   **pkginfo -x cms**

   The system displays the currently installed CMS package, including the load number, for example:

   ```
   cms  Avaya Call Management System (sparc) XXXXX.X
   ```

3. Record the displayed CMS version information for reference later, during the upgrade process.

   CMS version: _____

# Verifying that your previous backups completed successfully

Approximately two days before the CMS base load upgrade, verify that your backups have been completing successfully.

This section includes the following topics:



## Verifying the backup of your CMS system data

To verify that your previous system backup completed successfully, choose one of the following procedures:

- If you backup your data directly to tape, a USB storage device or a network mount point , go to Verifying that your last CMSADM backup completed successfully on page 11.

  You are responsible for backing up your CMS system unless you engage Avaya to perform the backups in conjunction with this base load upgrade.

- If you use the CMS LAN backup feature, go to Verifying that your last LAN backup of the system data completed successfully on page 11

  You are responsible for backing up your CMS system. Avaya is not responsible for performing LAN backups. For more information about the CMS LAN backup feature, see *Avaya Call Management System Release 16 LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

## Verifying that your last CMSADM backup completed successfully

To verify that your last CMSADM backup completed successfully:

1. Enter:

   **`tail /cms/install/logdir/backup.log`**

2. Verify that the previous CMSADM backup completed successfully.

   An example of a successful CMSADM backup message is:

```
===== Begin backup Wed Apr  9 05:37:05 EDT 2009

Converter started Wed Apr  9 05:37:07 EDT 2009
Converter completed successfully Wed Apr  9 05:37:10 EDT 2009

Testing tape on /dev/rmt/0...

Tape test on /dev/rmt/0 is okay...

2873600 blocks

===== Finished backup Wed Apr  9 06:30:35 EDT 2009
```

3. Choose one of the following actions:

   - If your previous backup was successful, go to Verifying the backup of your CMS data on page 12.
   - If your previous backup was *not* successful, contact your Avaya CMS support representative.

## Verifying that your last LAN backup of the system data completed successfully

If you use the CMS LAN backup feature, perform the following procedure:

1. Enter:

   **`cat /cms/install/logdir/backup.log | pg`**

2. Press **Enter** to continue the display. It might be necessary to repeat this step several times.

3. Verify that the previous system backup completed successfully.

   An example of a successful system backup message is:

   ```
   ===== LAN SYSTEM BACKUP SUCCESSFULLY FINISHED Date and time
   ```

4. Choose one of the following actions:
   - If your previous backup was successful, go to Verifying the backup of your CMS data on page 12.
   - If your previous backup was *not* successful, contact your Avaya CMS support representative.

# Verifying the backup of your CMS data

To verify that your previous system backup completed successfully, choose one of the following procedures:

- If you backup your data directly to a tape device, go to Verifying that your previous full or incremental backup completed successfully on page 12.
- If you use the CMS LAN backup feature, go to Verifying that your last LAN backup of CMS data completed successfully on page 13

  For more information about the CMS LAN backup feature, see *Avaya Call Management System Release 16 LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

## Verifying that your previous full or incremental backup completed successfully

To verify that your previous full or incremental backup completed successfully:

1. Verify that you are logged in as **root**.

   **Important:**
   If at anytime during the upgrade process you need to verify that you are logged in as the root user, you can enter the command: **id**

2. Enter:

   **tail /cms/maint/backup/back.log**

3. Verify that the previous full or incremental backup completed successfully.

   An example of a successful full or incremental backup message is:

```
1711  4/15/09  2:14 AM   2  1  INFO
      BACKUP INFO: The backup has completed successfully.
      Please label the volume CMS-030415-01-LSAC-00-F-01-r3milcms
```

4. Choose one of the following actions:
   - If your previous backup was successful go to Verifying that the nightly archiver is functioning on page 13.
   - If your previous backup was *not* successful, contact your Avaya CMS support representative.

## Verifying that your last LAN backup of CMS data completed successfully

To verify that your last LAN backup of CMS data completed successfully:

1. Enter:

   **`cat /cms/install/logdir/backup.log | pg`**

2. Press **Enter** to continue the display. It might be necessary to repeat this step several times.
3. Verify that the previous data backup completed successfully.

   An example of a successful data backup message is:

```
+++++ ON-Bar BACKUP SUCCESSFULLY FINISHED Date and time
```

4. Choose one of the following actions:
   - If your previous backup was successful, go to Verifying that the nightly archiver is functioning on page 13.
   - If your previous backup was *not* successful, contact your Avaya CMS support representative.

# Verifying that the nightly archiver is functioning

To verify that nightly archiver is functioning correctly:

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

2. Enter:

   **su cms cms**

   The system displays the CMS main menu.
3. Press **Enter** to accept the default terminal type.
4. Select Maintenance > Error Log Report.
5. Enter **2600** in the Error codes field.
6. Leave all of the other fields blank.
7. Press **Enter** to select the Run option.
8. Press **Enter**.

   The system displays an archive history report.
9. Verify that the nightly archiver is functioning correctly for all ACDs administered on the system.

   An example of a successful nightly archiver message is:

```
2600  4/15/09   2:15 AM   2   1   INFO
      ARCHIVER status: Daily Archive for (Mon)
      Apr. 14, 2009 Successful
```

10. Select Exit to return to the previous menu.
11. Choose one of the following actions:
    - If the nightly archiver is functioning correctly, go to Checking the status of the disk drives on page 14.
    - If the nightly archiver is *not* functioning correctly, contact your Avaya CMS support representative.

# Checking the status of the disk drives

To check the status of the disk drives:

1. Verify your RAID adapter by entering the following:
   a. To determine that you have the AAC style RAID adapter, enter:

      **grep aac /etc/path_to_inst**

      This command should return the following if you have the AAC style RAID adapter:

      “/pci@0/pci@0/pci@9/scsi@0” 0 “aac”

      Otherwise, it will return the prompt only.

b. To determine that you have the MRSAS style RAID adapter, Enter:

**grep mr_sas /etc/path_to_inst**

This command should return the following if you have the MRSAS style RAID adapter:

```
"/pci@0,0/pci8086,340a@3/pci1000,9263@0" 0 "mr_sas"
```

Otherwise, it will return the prompt only.

2. Verify that you are logged in to the system as **root**.
3. If you have the AAC style RAID adapter, enter:

**/opt/StorMan/arcconf getconfig 1 | egrep "Logical devices" | pg**

This command returns the following output:

```
Logical devices/Failed/Degraded : 1/0/0
```

- If the output shows zero for Failed or Degraded, continue with Checking for memory errors and system panics on page 15.
- If the output shows anything other than zero for Failed and Degraded, your system requires maintenance. Contact your Avaya CMS support representative.

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

**/opt/MegaRAID/CLI/MegaCli –ldinfo –l0 –a0 | grep State**

This command returns the following output:

```
State               : Optimal
```

- If the output shows “Optimal”, continue with Checking for memory errors and system panics on page 15.
- If the output shows anything other than “Optimal”, your system requires maintenance. Contact your Avaya CMS support representative.

# Checking for memory errors and system panics

To check for memory errors and system panics:

1. Enter:

**egrep -i "panic | memory error | afsr" /var/adm/messages* | pg**

**Note:**

It might be necessary to press **Enter** to continue the display.

An example of some memory error messages are:

```
/var/adm/messages:Apr 15 21:27:51 r3upctn SUNW,UltraSPARC-II: [ID 860344 kern.notice]
[AFT0] errID 0x00011903.9c12748f Corrected Memory Error on Board 3 J3600 is Persistent
/var/adm/messages:Apr 16 09:27:52 r3upctn SUNW,UltraSPARC-II: [ID 417990 kern.notice]
[AFT0] Corrected Memory Error on CPU7, errID 0x00014050.8646ccd6
/var/adm/messages:Apr 16 09:27:52 r3upctn     AFSR 0x00000000.00100000<CE> AFAR
0x00000000.09498550
/var/adm/messages:Apr 16 09:27:52 r3upctn    AFSR.PSYND 0x0000(Score 05) AFSR.ETS 0x00
Fault_PC 0x10023bd0
/var/adm/messages:Apr 16 09:27:52 r3upctn SUNW,UltraSPARC-II: [ID 136280 kern.notice]
[AFT0] errID 0x00014050.8646ccd6 Corrected Memory Error on Board 3 J3600 is Persistent
/var/adm/messages:Apr 16 21:27:51 r3upctn SUNW,UltraSPARC-II: [ID 488351 kern.notice]
[AFT0] Corrected Memory Error on CPU6, errID 0x0001679c.f8a4aa5f
/var/adm/messages:Apr 16 21:27:51 r3upctn     AFSR 0x00000000.00100000<CE> AFAR
0x00000000.09498550
/var/adm/messages:Apr 16 21:27:51 r3upctn    AFSR.PSYND 0x0000(Score 05) AFSR.ETS 0x00
Fault_PC 0x10023bd0
/var/adm/messages:Apr 16 21:27:51 r3upctn SUNW,UltraSPARC-II: [ID 599456 kern.notice]
[AFT0] errID 0x0001679c.f8a4aa5f Corrected Memory Error on Board 3 J3600 is Persistent
/var/adm/messages:Apr 17 09:27:51 r3upctn SUNW,UltraSPARC-II: [ID 473191 kern.notice]
[AFT0] Corrected Memory Error on CPU6, errID 0x00018ee9.a6074fb3
```

2. Choose one of the following actions, depending on the message that is displayed:
   - If the system displays no memory error or panic messages, go to Verifying free space in the root file system on page 16.
   - If the system displays any memory error or panic messages, your system requires maintenance. Contact your Avaya CMS support representative.

# Verifying free space in the root file system

To verify that sufficient free space is available in your root file system to accomplish the base load upgrade:

1. Enter:

   **`df -k /`**

   The system displays a message similar to the following:

```
Filesystem             kbytes    used     avail     capacity  Mounted on

/dev/dsk/c1t0d0s0      6201485   1738401  4401070    29%         /
```

2. Check the disk capacity.

3. Choose one of the following actions:
   - If the disk capacity is less than 85%, go to Rebooting your CMS system on page 17.
   - If the disk capacity is 85% or greater, contact your Avaya CMS support representative.

# Rebooting your CMS system

You must reboot your CMS system and verify that the system is functioning properly. Reboot the CMS system before you backup your data.

To reboot your CMS system:

1. Enter the following command from the pound (#) prompt:

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

   The system reboots.
2. Log in to the system as **root**.
3. Choose one of the following actions:
   - If the system does not boot correctly or if any error messages are displayed, contact your Avaya CMS support representative.
   - If the system boots correctly, go to Backing up the CMS system on page 17.

# Backing up the CMS system

Before beginning a CMS base load upgrade, you must backup your CMS system data and CMS data.

This section includes the following topics:



## Backing up your system data

A backup of the system data must be performed approximately one day before the CMS base load upgrade.

To take a back up of your current system files, choose one of the following procedures:

- If you backup your data directly to a tape device, go to Performing a CMSADM backup to tape on page 18.
- If you backup your data to a USB storage device, refer to the section *Performing a CMSADM backup to a USB storage device* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting* document for information on how to perform CMSADM backups to a USB storage device.
- If you backup your data to a network mount point, refer to the section *Performing a CMSADM backup to a network mount point* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting* document for information on how to perform CMSADM backups to a network mount point.
- If you use the CMS LAN backup feature, go to Performing a full system backup with LAN backup on page 19.

  For more information about the CMS LAN backup feature, see *Avaya Call Management System Release 16 LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

## Performing a CMSADM backup to tape

To back up of your current system files, perform the following procedure:

1. Verify that you are using the correct tape for the tape drive for your system. Many of the tape cartridges look alike, and using the wrong tape can damage the tape drive mechanism and tape heads.
2. Log in as **root**.
3. Enter:

   **`cmsadm`**

   The `Avaya Call Management System Administration Menu (CMSADM Menu)` is displayed.
4. Enter the number associated with the `backup` option.

   Depending on the number of tape drives connected to your system, one of the following messages will be displayed by your system.

   - If only one tape drive is available, the system displays the following message:

```
Please insert the first cartridge tape into device name.
Press ENTER when ready or Del to quit:
```

- If more than one tape drive is available for use, the system displays a list of tape devices. Enter a tape drive selection from the displayed list.

  An example of a tape device list is:

```
Select the tape drive:
  1) HP DAT-72 tape drive: /dev/rmt/0
  2) HP DAT-72 tape drive: /dev/rmt/1
Enter choice (1-2):
```

**Note:**
If the system fails to identify the tapes by manufacturer name, tape devices are displayed according to their system device names, such as "`/dev/rmt/0`".

5. Press **Enter**.

   The backup process is initiated.

   When the backup is complete, the system displays the following message:

```
xxxxxxx blocks
Tape Verification
xxxxxxx blocks
WARNING: A CMS Full Maintenance Backup in addition to this cmsadm
backup must be done to have a complete backup of the system.  . .
. .

Please label the backup tape(s) with the date and the current CMS
version (XXXXX.X)
```

6. Write protect the tape and store the tape in a secure location until the next backup is performed.
7. Go to Backing up your CMS data on page 20.

## Performing a full system backup with LAN backup

If you use the CMS LAN backup feature, perform the following procedure:

1. Log in as **root**.
2. Enter:

   **`/cms/LANbkup/bin/backup.tivoli 0`**
3. Verify that the backup has completed successfully by entering:

   **`cat /cms/install/logdir/backup.log`**
4. Go to Backing up your CMS data on page 20.

# Backing up your CMS data

Your CMS data must be backed up approximately one day before the CMS base load upgrade is performed.

To backup your CMS data, choose one of the following procedures:

- If you backup your data directly to a tape device, go to Performing a full data backup with a tape device on page 20.
- If you backup your data to a USB storage device, refer to the section *Performing a CMS Maintenance Back Up of data to a USB storage device* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting* document for information on how to perform CMSADM backups to a USB storage device.
- If you backup your data to a network mount point, refer to the section *Performing a CMS Maintenance Back Up of data to a network mount point* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting* document for information on how to perform CMSADM backups to a network mount point.
- If you use the CMS LAN backup feature, go to Performing a full data backup with LAN backup on page 21.

  For more information about the CMS LAN backup feature, see *Avaya Call Management System Release 16 LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

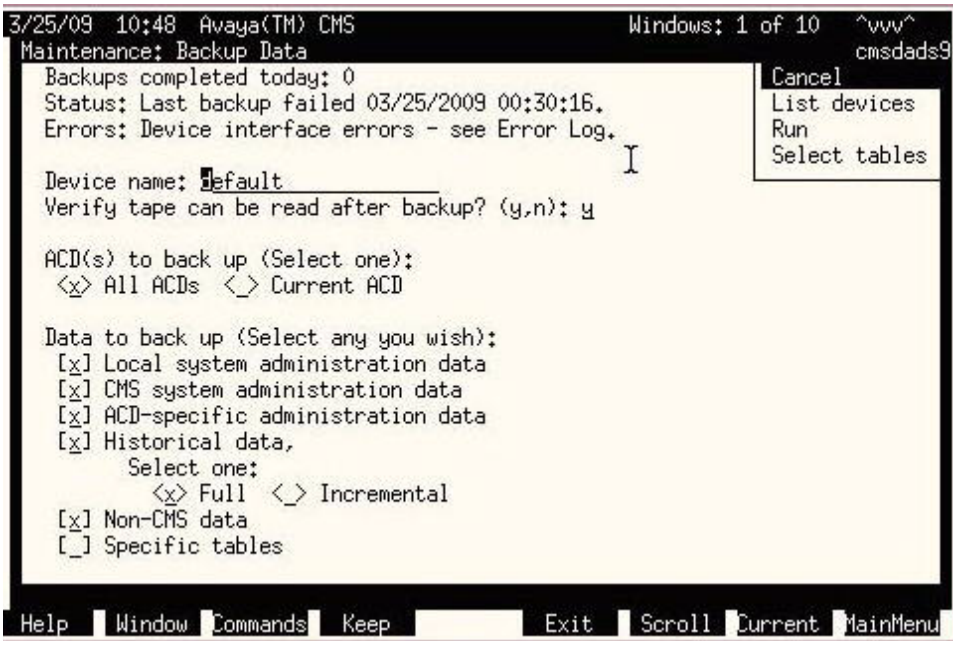
## Performing a full data backup with a tape device

To perform a full backup of CMS data:

1. Verify that you are using the correct tape for the tape drive for your system. Many of the tape cartridges look alike, and using the wrong tape can damage the tape drive mechanism and tape heads.
2. Verify that you are logged in as **cms**.
3. Enter **cms**.

4. From the main menu, select `Maintenance` > `Back Up Data`.

   The system displays the `Back Up Data` window, as shown below. Do not change any of the default selections.




5. Press **Enter** to access the action list in the upper right corner of the window.
6. Select `Run` and press **Enter**.
7. Wait for the backup to complete. If the backup does not complete successfully, contact your Avaya CMS support representative.
8. Write protect the tape and store the tape in a secure location until the next backup is performed.
9. Go to Backing up any new CMS data on page 22.

## Performing a full data backup with LAN backup

If you use the CMS LAN backup feature, perform the following procedure:

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

   **`/cms/LANbkup/bin/onbar_backup.tivoli 0`**
3. Verify that the backup has completed successfully by entering the following commands:

   **`cat /cms/install/logdir/backup.log`**

   **`cat /cms/install/logdir/bar_act.log`**
4. Go to Backing up any new CMS data on page 22.

# Backing up any new CMS data

You must back up any CMS data that has been generated since your last CMS data backup. Choose one of the following options:

- If no new CMS data has been generated since your last CMS data backup, go to Updating the Solaris operating system on page 23.
- If new CMS data has been generated since your last CMS data backup, perform one of the following procedures immediately before the upgrade:
  - Performing a full data backup with a tape device on page 20
  - Performing a full data backup with LAN backup on page 21

For more information about the CMS LAN backup feature, see Avaya Call Management System Release 16 LAN Backup User Guide. This document provides information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

# Updating the Solaris operating system

This section contains procedures for updating your Solaris operating system. You must complete the procedures in this section before upgrading your CMS base load.

This section includes the following topics:



## Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in Introduction on page 5
- Perform all of the required procedures in Preparing for a base load upgrade on page 9
- Verify that you are logged in to the system as `root`.

# Stopping the Avaya Visual Vectors server software

To stop the Avaya Visual Vectors server software:

1. Enter:

   **setupaas**

   The system displays the Avaya Visual Vectors Server System Services Menu, as shown in the following figure.

```
Avaya Visual Vectors Server System Services Menu

Select a command from the list below.

  1) init_vvs     Setup the initial configuration
  2) run_vvs      Turn VVS on or off
  3) auth_display Display simultaneous VVS logins
  4) auth_set     Change simultaneous VVS logins
  5) backup       Backup vector steps and layout files
  6) restore      Restore vector steps and layout files

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

2. Enter the number associated with the run_vvs option.

   The system displays the following message:

```
1) Turn VVS On
2) Turn VVS Off

Enter choice (1-2) or q to quit:
```

3. Enter the number associated with the Turn VVS Off option.

# Stopping CMS WebClient

To stop the CMS WebClient, enter:

**cmsweb stop**

# Stopping AOM

To stop AOM, enter:

**aom stop**

# Stopping Avaya OA data forwarders

If the CMS configuration includes data collection by Avaya OA, turn off all Avaya OA forwarders on the CMS server using the **pa stop all** command. For more information about Avaya OA forwarders, see *Avaya OA Maintenance and Troubleshooting*.

# Installing Solaris patches

To install the Solaris patches:

1. Load the Avaya Call Management System software disc into the disc drive.
2. Enter:

   **cmssvc**

   The system displays the `Avaya Call Management System Services Menu` (`CMSSVC Menu`).

   **CAUTION:**
   CMS must be off in order to install the Solaris patches.
3. Enter the number associated with the `run_cms` option.
4. Enter the number associated with the `Turn off CMS but leave IDS running` option.

   The system returns to the command prompt.
5. Set the IDS environment by entering:

   **. /opt/informix/bin/setenv**
6. Shutdown the Informix database server by running the following command:

   **onmode -yuk**
7. Ignore any error messages.

8. Enter:

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

   The system displays one of the following messages:

   - If the system firmware needs to be updated, the system displays the following message:

```
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)?
```

   - If there are no system 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
beinstalled 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 system displays the approximate amount of time needed to install the Solaris patches.

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

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

**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 you press the power button. 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 the system displays the graphical login screen.

9. If there are no system firmware updates or Solaris patches to install, continue with Step 19.
10. If there are no system firmware updates but there are Solaris patches to install, continue with Step 15.
11. Update the system firmware. Enter **yes**.

**Important:**
If you answer **yes** to updating the system firmware, only the system firmware is updated. Once the system firmware is updated, the user must re-run the `spatches_conf` script to determine if any additional Solaris patches must be installed.

**CAUTION:**
Manually bypassing firmware updates and installing spatches can leave your system unusable. The system is powered down as part of the firmware update. Some Solaris platforms automatically power back on after the firmware updates are applied while other platfomrs do not. Allow 20-30 minutes for the firmware to be updated. If the system does not automatically power on, press the Power button to restart the system.

12. Monitor the system as the firmware is updated. If the system does not power on after 30 minutes, press the power button.
13. After the graphical console returns, log in to the system as `root`.

14. Enter:

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

    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,?]
```

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

    **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**.

    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:**
    Solaris 10 does not display the Solaris patches on the console as they install. The display can become blank for at least the time the Spatches installer reports at the end of Step 10. Once the graphical console returns, the system has completed the Solaris patches installation. Do not halt the system.

16. Monitor the Solaris patch installation process to ensure that the system has not powered off as a result of the installation of a particular Solaris patch. If the system has powered off, press the power button to power the system back on. Refer to the Important message in step 9 for more information.

17. Log in to the system as **root**.

18. 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 following message is displayed:

```
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: Fri Jan 18 13:28:19 MST 2009
```

If the message shown above is displayed, continue with this procedure and the remaining CMS base load upgrade procedures. When the upgrade is complete, notify your Avaya CMS support organization as prompted by the system.

19. Verify IDS is running with the following command:

    Enter **cmssvc**

    The system displays the CMSSVC menu. If the system first displays the following text, then IDS is not running and needs to be started.

    ```
    cmssvc: Warning IDS off-line. IDS can be turned on with the run_ids
    command on the cmssvc menu
    ```

    a. If IDS is running, select **quit** and continue with Step 14.

    b. If IDS is not running, select the option **run_ids**.

    c. Select option **Turn IDS on**.

    The system starts IDS and returns to the command prompt.

20. If the cdrom is not recognized, restart the volfs service with the following command:

    **svcadm disable svc:/system/filesystem/volfs**

    **svcadm enable svc:/system/filesystem/volfs**

21. Go to Installing the Avaya CMS security script on page 30.

# Installing the Avaya CMS security script

To install the Avaya security script:

**Important:**
You will be able to log into the console only as **root** after you run the Avaya CMS security script. If you are logging into the system remotely, you will need to log in as another user and then **su** to root.

1. Verify that you are logged into the system as **root**.
2. Verify the current services running on the system, save the list for comparison against the listing after the security script run.

   **Note:**
   It is necessary to find out which services in the list of differences are used by the customer.

3. To capture the current services and preserve the output to a file, enter:

   **svcs -a > /tmp/current_svcs.txt**

4. Verify the Avaya Call Management System software disc is in the disc drive.
5. Enter:

   **cd /**

6. Enter:

   **/cdrom/cdrom0/security/cms_sec**

   The system configures your security settings. This process will take some time. The system displays the following message when the process is complete:

   ```
   Avaya CMS security configuration completed: date
   ```

   **Note:**
   If the system displays a configuration failed message, contact your Avaya services representative.

7. To capture the new services and preserve the output to a different file, enter:

   **svcs -a > /tmp/new_svcs.txt**

8. Run a diff against the two listings files and search for services that need to be re-enabled.

   **diff /tmp/current_svcs.txt /tmp/new_svcs.txt**

9. View the output from the diff command and re-enable the services that are displayed. To re-enable any customer used services enter:

   **`svcadm enable  <service name>`**

   Service name is the third column in your listing files. You do not typically need the ":default" at the end of the service name.

   Example:

   **`svcadm enable svc:/network/rpc/bind`**

   **Note:**
   The files in **/tmp** directory will not be saved during the reboot process. If you feel you need to keep a copy of the files, move them to another location that is not volatile during a reboot.

10. Reboot the system by entering:

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

    Log into the system as **root**.

# Upgrading the CMS base load

You must complete the procedures in the previous sections before upgrading your CMS base load. Use the procedures in this section to upgrade an older CMS base load to a newer CMS base load.

This section includes the following topics:



## Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in Introduction on page 5
- Perform all of the required procedures in Preparing for a base load upgrade on page 9
- Perform all of the required procedures in Updating the Solaris operating system on page 23
- Verify that you are logged in to the system as `root`.

# Upgrading CMS Supplemental Services

Perform this procedure if the Supplemental Services load on the Avaya Call Management System software disc is newer than the Supplemental Services load on the CMS system.

1. To determine the current Supplemental Services load on the CMS system, enter:

   **pkginfo –x LUahl***

   **Note:**
   Two instances of LUahl may be displayed.

2. Load the software disc Avaya Call Management System for your specific platform architecture (SPARC or x86), into the disc drive.
3. To determine the Supplemental Services load on the Avaya Call Management System software disc, enter:

   **more /cdrom/cdrom0/LUahl/pkginfo | grep VERSION**

4. Perform one of the following:
   - If the Supplemental Services load on the Avaya Call Management System disc is newer than any of the Supplemental Services loads on the CMS system, then you need to upgrade Supplemental Services, continue with Step 5.
   - If the Supplemental Services load on the Avaya Call Management System disc is the same or older than any of the Supplemental Services loads on the CMS system, then you do not need to upgrade Supplemental Services, continue with Removing CMS patches on page 36.
5. Record the version number printed on the software disc, for use later in this procedure.
6. Enter:

   **pkgrm LUim**

   The system displays the following message:

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

7. Enter: **y**

   The system removes the **LUim** package.
8. Enter:

   **/usr/sbin/pkgadd -d /cdrom/cdrom0 LUim**

   The system loads the new **LUim** package.
9. Enter:

   **/opt/LUim/bin/install 2>&1 | tee -a /opt/LUim.log**

**Note:**
If the system displays a series of questions about the SUNWexplo or sneep packages, accept the default answers when provided.

10. Enter:

    **/opt/cc/install/ahl.cssrXXxx.x/bin/setup**

    where ***XX*** is the release number and ***xx.x*** is the specific load.

    The system displays one of the following messages:

    - If no previous version is in place, the system displays a message similar to the following:

```
No previous version is in place.
enable crontab entry...
set up output log configuration...
AHL setup completed successfully.
```

    - If a previous version is in place, the system displays a message similar to the following:

```
Migrating previous version ahl.cssrXXxx.x
.............
.............
.............
AHL setup completed successfully.
```

11. Enter:

    **/opt/cc/install/aot.cssrXXxx.x/bin/setup**

    where ***XX*** is the release number and ***xx.x*** is the specific load.

    The system displays one of the following messages:

    - If no previous version is in place, the system displays a message similar to the following:

```
No previous version is in place.
copy previous log files...
no log files exist for tag "LAN_Admin_Log"
linking new version...
registering server with Orbix daemon
.............
.............
.............
[786: New Connection (cms3,IT_daemon,*,root,pid=645,optimised) ]

AOM setup completed successfully.
```

- If a previous version is in place, the system displays a message similar to the following:

```
Migrating previous version aot.cssrXXxx.x
.............
.............
.............
linking new version...
```

# Removing CMS patches

To remove CMS patches from the system:

1. Enter:

   cmssvc

   - If the system displays the CMSSVC Menu, go to Step 5.
   - If the system displays a warning message that IDS is off-line, continue with Step 2.

   The system then displays the CMSSVC Menu.

2. Enter the number associated with the run_ids option.

   The system displays the following message:

```
Select one of the following
  1) Turn on IDS
  2) Turn off IDS
Enter choice (1-2):
```

3. Enter:1

   The system starts IDS and returns to the command prompt.

4. Enter:

   **cmssvc**

   The system displays the CMSSVC Menu.

5. Enter the number associated with the back_all option.

   The system displays one of the following messages, depending on whether CMS patches are present:

   - If no patches are present, the system displays a "No CMS patches" message.

- If patches are present, the system displays the following message:

```
The following patches are installed on this machine:
   .
   .
   .
Are you sure you wish to remove all these patches? (y|n)
```

**Note:**
Some CMS patches might require additional steps for installation or removal. If additional steps are required, the system will display a message describing the steps you must perform. The patch installation or removal will fail until you perform the required steps. For example, a patch might require both CMS and IDS to be off.

6. Perform one of the following actions:
   - If no patches are present, go to Removing the current CMS load on page 37.
   - If patches are present, enter: **y**

   The system removes the patches. For each patch removed, the system displays messages similar to the following:

```
Removing patch package for cmspx-s:

Patch x has been backed out.
```

   When all patches have been removed, the system returns to the prompt.

# Removing the current CMS load

To remove the current CMS base package:

1. Load the Avaya Call Management System software disc into the disc drive.
2. Enter:

   **pkgrm cms**

   The system checks the package and displays the following message:

```
The following package is currently installed: cms Avaya
Call Management System
(sparc) rxxxxx.x
Do you want to remove this package?
```

3. Enter: **y**

```
Removing installed package instance <cms>
. . .
WARNING: This package contains scripts which will be executed with
super-user permission during the process of removing the package.

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

4. Enter: **y**

   The system displays the following message:

```
Removing installed package instance <cms>
.  .  .
WARNING:
The <LUfaas> package depends on the package currently being
removed.

WARNING:
    The <cmsweb> package depends on the package currently
    being removed.

Dependency checking failed.

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

**Note:**

The <LUfaas> package message will only appear if Visual Vectors is installed on the system. The <cmsweb> package message will only appear if CMS WebClient is installed on the system.

5. Enter: **y**

The system displays the following message:

```
Verifying package dependencies.
Processing package information.
Executing preremove script

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

**WARNING:**
Before continuing, verify you have taken a maintenance backup of the system data. If you fail to verify your data backup and respond incorrectly to the next question in the CMS package removal process, it can lead to extensive loss of data.

**Important:**
Make sure you answer **y** to this prompted question or else you have the danger of losing all your CMS data.

6. Enter: **y**

   The system displays the following message:

```
CMS will be removed from this machine; the data will be preserved.
Are you sure this is correct [y,n,?]
```

7. Enter: **y**

   The system displays the following message:

```
Have you backed up the file systems [y,n,?]
```

8. Enter: **y**

   If CMS has not been turned off, the system displays the following message:

```
CMS must be turned off in order to remove software.

Do you want to turn off CMS now?
```

9. Enter: **y**

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

```
Turning off CMS, please wait.
.................
Removal of <cms> was successful.
```

# Starting AOM

To start AOM, enter:

```
aom start
```

**Note:**
If AOM was started automatically by the system, the system will display a message stating AOM is already on.

# Installing the new CMS base load

To install the new CMS base load:

1. Verify the Avaya Call Management System 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:**

It may be necessary to enter **y** several times to continue the CMS software installation. You can ignore any messages about conflicting files.

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

```
## Upgrading Customer CMS data . . .

Customer CMS data successfully upgraded

Setting UNIX system tunable parameters for CMS.
No changes to tunable parameters were required.
copying zmodem executables to /usr/bin

*** IMPORTANT NOTICE ***
This machine must now be rebooted in order to insure sane
operation. Execute

shutdown -y -i6 -g0

and wait for the Console Login: prompt.

If CMS was installed by choosing cms from the pkgadd menu, type q
and press return to exit.
If cms was installed using pkgadd -d /cdrom/cdrom0 cms, press
return.

       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 message shown above is displayed, notify your Avaya CMS support organization as prompted by the system.

4. Press the **Enter** key.

   The system returns to the command prompt.

5. The system prompts you to reboot the system. Enter:

   **/usr/sbin/shutdown –y –i6 –g0**

   The system reboots.

6. To check the contents and/or attributes of the installed CMS files, run the following command:

   **pkgchk -n cms**

   If the software installation was successful, the system prompt returns to the screen after a few seconds. If you receive any error messages, call the Avaya Technical Services Organization, 1-800-242-2121, or your product distributor.

   **Note:**
   Ignore any messages about sqlhost users and groups.

7. Enter:

   **cat /cms/install/logdir/admin.log |pg**

   The system displays part of the CMS administration log.

8. Verify that there were no errors during the installation.
9. Press **Enter** to continue the display. It might be necessary to repeat this step several times.

# Installing CMS patches

To install the CMS patches:

1. Enter:

   **cmssvc**

   The system displays the `CMSSVC Menu`.

2. Enter the number associated with the `load_all` option.

   Depending on the availability of CMS patches one of the following events occurs:

   - If there are no patches to be installed, the system displays a message to that effect and returns to the system prompt.
   - If there are patches to be installed, the system displays the following message:

```
Are you sure you want to install all these patches? (y|n)
```

   **Note:**
   Some CMS patches might require additional steps for installation or removal. If additional steps are required, the system will display a message describing the steps you must perform. The patch installation or removal will fail until you perform the required steps. For example, a patch might require both CMS and IDS to be off.

3. Choose one of the following actions:

- If there are no patches to be installed, continue with Turning on CMS on page 45.
- If there are patches to be installed, enter: **y**

  The system installs the CMS patches. As the installation proceeds, the system keeps you informed of its progress, as shown in the following message:

```
Generating list of files to be patched...
     .  .  .
Patch installation completed.
```

# Upgrading Avaya CMS Supervisor Web

Perform this procedure to upgrade CMS WebClient.

1. Verify the Avaya Call Management System software disc for your specific platform architecture (SPARC or x86), is loaded in the disc drive.
2. To determine if CMS WebClient is installed on the system, enter:

   **pkginfo -x cmsweb**

   The system displays messages similar to the following if CMS WebClient is installed on the system:

```
# pkginfo -x cmsweb
cmsweb  CMS Web Interface
        (sparc/x86) web16.Xxx.x
```

3. To determine the CMS WebClient version on the Avaya Call Management System software disc, enter:

   **more /cdrom/cdrom0/cmsweb/pkginfo | grep VERSION**

   - If the CMS WebClient version on the Avaya Call Management System disc is newer than the CMS WebClient version on the CMS system, then you need to upgrade CMS WebClient, continue with Step 4.
   - If the CMS WebClient version on the Avaya Call Management System disc is same or older than the CMS WebClient version on the CMS system, then you do not need to upgrade CMS WebClient, continue with Turning on CMS on page 45.
4. To stop the CMS WebClient, enter:

   **cmsweb stop**

5. To remove the current CMS WebClient package, enter:

   **pkgrm cmsweb**

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

6. Enter: **y**

   The system displays the following messages:

```
## Removing installed package instance <cmsweb>
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]
```

**Important:**
Do not start CMS Supervisor Web if the customer does not plan on using CMS Supervisor Web to access CMS reports. Starting CMS Supervisor Web opens ports that the customer may not want opened.

7. Enter: **y**

   The system removes the CMS WebClient package.

8. To install the CMS WebClient package, enter:

   **/usr/sbin/pkgadd -d /cdrom/cdrom0 cmsweb**

   The system displays messages similar to the following:

```
Processing package instance <cmsweb> from </cdrom/cms_<platformtype_XX.xxxx.g>
CMS Web Interface(sparc/x86) webXX.xx.x
Copyright (c) 2011 Avaya Inc.
All Rights Reserved
The selected base directory </opt/cmsweb> must exist before installation is
attempted.
Do you want this directory created now [y,n,?,q]
```

9. Enter: **y**

**Note:**
The prompt to create the `/opt/cmsweb` directory only occurs the first time CMS WebClient is installed on the system.

The system displays messages similar to the following:

```
Using </opt/cmsweb> as the package base directory.
## Processing package information.
## Processing system information.
   1 package pathname is already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.
This package contains scripts which will be executed with super-user
permission during the process of installing this package.
Do you want to continue with the installation of <cmsweb> [y,n,?]
```

10. Enter: **y**

    The system installs the new CMS WebClient package.

11. Continue with Turning on CMS on page 45.

# Turning on CMS

To turn on CMS:

1. Enter:

   **`cmsadm`**

   The system displays the `CMSADM Menu`.

2. Enter the number associated with the `run_cms` option.

   The system displays the following message:

```
Select one of the following
  1) Turn on CMS
  2) Turn off CMS but leave IDS Running
  3) Turn off CMS
Enter choice (1-3):
```

3. Enter: **`1`**

   The system starts CMS and returns to the command prompt.

4. Restart CMS data collection if data collection was turned off at the beginning of the upgrade.

5. Manually run the appropriate Archiver from System Setup if CMS was off during the time your Archiver normally runs.

# Starting CMS WebClient

To start the CMS WebClient, enter:

```
cmsweb start
```

# Starting Avaya OA data forwarders

If the CMS configuration includes data collection by Avaya OA, turn on all Avaya OA forwarders on the CMS server using the **pa start all** command. For more information about Avaya OA forwarders, see *Avaya OA Maintenance and Troubleshooting*.

# Preparing the Avaya Visual Vectors Server software

If you are not using Visual Vectors, go to Completing the base load upgrade process on page 53.

Choose one of the following options:

1. To determine the current Supplemental Services load on the CMS system, enter:

   ```
   pkginfo -x LUfaas
   ```

2. To determine the Supplemental Services load on the Avaya Call Management System software disc, enter:

   ```
   more /cdrom/cdrom0/LUfaas/pkginfo | grep VERSION
   ```

3. Perform one of the following:

- If the Supplemental Services load on the Avaya Call Management System disc is newer than the Visual Vectors Server load on the CMS system, then you need to upgrade Visual Vectors Server, go to Removing the Avaya Visual Vectors Server software on page 47.
- If the Supplemental Services load on the Avaya Call Management System disc is the same or older than the Visual Vectors Server load on the CMS system, then you do not need to upgrade Visual Vectors Server, continue with Turning on Avaya Visual Vectors on page 48.

## Removing the Avaya Visual Vectors Server software

To remove the Avaya Visual Vectors Server software:

1. Verify the Avaya Call Management System software disc is in the disc drive.
2. Enter:

   **pkgrm LUfaas**

   For each package, the system will display at least two messages asking for confirmation to continue the removal.
3. Enter **y** each time you receive messages asking for confirmation to continue the removal.

   When the last package is removed, the system returns to the command prompt.
4. Go to Installing the Avaya Visual Vectors Server software on page 47.

## Installing the Avaya Visual Vectors Server software

To install or upgrade the Avaya Visual Vectors Server software:

1. Enter:

   **aom stop**
2. Verify the Avaya Call Management System software disc is in the disc drive.
3. Enter:

   **pkgadd -d /cdrom/cdrom0 LUfaas**

   The system displays the following message:

```
Processing package instance <LUfaas> from </cdrom/untitled>

Visual Vectors Server Software
(sparc) vvsXX.X

.........
.........
.........

Do you want to continue with the installation of <LUfaas> [y,n,?]
```

**Note:**
You might receive messages about installing conflicting files. Enter **y** to install the files and continue with the installation.

4. Enter: **y**

   The system displays the following message:

```
Installing Visual Vectors Server Software as <LUfaas>

..........
..........
..........

Installation of <LUfaas> was successful.
```

5. Enter:

   **aom start**

6. Go to Turning on Avaya Visual Vectors on page 48.

## Turning on Avaya Visual Vectors

To turn on the Avaya Visual Vectors software:

1. Enter:

   **setupaas**

   The system displays the `Avaya Visual Vectors Server System Services Menu`.

2. Enter the number associated with the `run_vvs` option.
3. Enter the number associated with the `Turn VVS On` option.
4. Enter:

   **eject cdrom**

5. Verify that AOM is on. For more information, see Starting AOM on page 40
6. Go to Authorizing ODBC Connections on page 48.

## Authorizing ODBC Connections

Beginning with R16.2, CMS ODBC connections must be authorized using the `auth_set` command. The customer purchase order will be needed to determine the number of ODBC connections authorized.

1. Use the customer purchase order to determine the number of ODBC connections authorized.

2. Enter:

   **cmssvc**

   The system displays the CMSSVC menu.

3. Enter the number for the auth_set option.

   The system displays the following message:

   ```
   Password:
   ```

4. Enter the appropriate password.

**Note:**
This password is available only to authorized personnel.

5. The current authorization for each CMS feature will be displayed, press Enter to accept the current value.
6. Repeat Step 5 until the ODBC connection feature is displayed, as shown below:

```
Enter the number of authorized ODBC connection (0-10): (default: 0)
```

7. Enter the number of ODBC connections purchased by the customer, from Step 1.

   The system displays the command prompt.

**Note:**
You can verify the authorizations by using the auth_display option of the **cmssvc** command.

8. Go to Installing Access Security Gateway and the CMS Authentication File on page 49.

# Installing Access Security Gateway and the CMS Authentication File

Access Security Gateway (ASG) is an authentication interface used to protect the system logins associated with Avaya CMS. ASG uses a challenge and response protocol to validate the user and reduce unauthorized access.

To install ASG on your CMS server, perform the following steps:

**Note:**
*System* in the following steps refers to the CMS server.

1. Log in as root.

2. Verify that CMS is installed on the system. Enter:

   **pkginfo -x cms**

   If CMS is installed, the system displays the following:

```
cms  Avaya(TM) Call Management System
     (sparc) r16.Xxx.y
```

3. Insert the Avaya Call Management System disc into the disk drive.
4. To install the ASG package, enter:

   **/cdrom/cdrom0/cmssolasg.bin**

   The system displays a list of status messages at the time of installation. It takes less than a minute to install the ASG package.

   - If the system successfully installs the ASG package, the system displays the following message at the end of the installation process:

```
INFO:Install ASG on CMS complete.
Review output on screen above
```

   - If the system does not install the ASG package successfully, the system displays the error on the screen and at the end of the installation, the installer displays a message to review the output on the screen.

5. From your PC, go to the following URL:

   https://rfa.avaya.com/rfa-docs/index.jsp

6. Click on the **Start the AFS Application** button to access the Authentication File System (AFS) application.
7. Select **Avaya CMS** as the product and then select the appropriate release from the drop down list.
8. Navigate to the download page by following the instructions in the intermediate pages and pressing **Next**.
9. Download the CMS Authentication File (AF) file to your PC.

   **Note:**
   You can download the AF file to your PC prior to CMS installation.

10. Transfer the AF file from your PC to the CMS server.

11. Install the AF file. If you transferred the AF file from your PC to the `/tmp` directory of the CMS server, run the following command to install the AF file:

    **`/opt/cmsasg/usr/local/bin/loadauth -af -l /tmp/ AF-7000009669-11.xml`**

    Replace `/tmp` in this example with the actual location of the AF file. Replace the AF file name in this example with the name that corresponds to the AF file that was transferred to the CMS server. Each AF file has a unique name.The **-l** option in the `loadauth` command is a lower case L.

12. Go to Completing the base load upgrade process on page 53.

# Completing the base load upgrade process

You must perform the procedures in this section to complete the CMS base load upgrade process.

This section includes the following procedures:



## Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in Introduction on page 5
- Perform all of the required procedures in Preparing for a base load upgrade on page 9
- Perform all of the required procedures in Updating the Solaris operating system on page 23
- Perform all of the required procedures in Upgrading the CMS base load on page 33

## Returning to the Common Desktop Environment

To return to the Common Desktop Environment (CDE) interface:

1. At the command prompt, enter:

   **exit**

   The system displays the following message:

```
console login:
```

**Important:**
Do not enter anything at the login prompt. After about 10 to 30 seconds, the system will return you to the CDE Login console.

2. Log in as **root**.

   The system displays the Common Desktop Environment, along with one or more open XTERM windows.

# Performing a backup of the system files

After the base load upgrade has completed successfully, perform a backup to create a reliable copy of the computer system files. For instructions on how to backup the system files, see Backing up your system data on page 17.

# Performing a backup of the CMS data

After the base load upgrade has completed successfully, perform a backup to create a reliable copy of the computer CMS data files. For instructions on how to backup the CMS data, see Backing up your CMS data on page 20.