Avaya Call Management System
Customer requirements for backup and recovery processes
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 may 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 and does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of 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 following Web site:  
http://www.avaya.com/support

Preventing toll fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf). Be aware that there may 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 +1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:  
http://www.avaya.com/support

Providing telecommunications security
Telecommunications security (of voice, data, and video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) interfaces.

- Use (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labor costs, and legal costs).

Your responsibility for your company's telecommunications security
The final responsibility for securing both this system and its networked equipment rests with you, an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources, including, but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Trademarks
Avaya is a trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Avaya support
Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:  
http://www.avaya.com/support
Contents

Avaya CMS backups and recovery ........................................... 3
Customer case studies ......................................................... 4
General recommendations ..................................................... 5
  Why you should routinely back up your CMS ............................. 5
  Your responsibilities ......................................................... 6
  Periodically restarting your CMS server .................................. 6
  Optimize your backup and restore times ................................ 6
Avaya CMS LAN backups ....................................................... 9
Avaya CMS tape backups ....................................................... 10
  About CMS tape backups ................................................... 10
  Tape devices and their associated components .......................... 11
  CMS tape backup recovery kit .............................................. 12
  Recommendations for your tape backup process ........................ 12
  Commands for checking your backup tapes .............................. 13
    Reporting the status of a backup tape .................................. 13
    Verifying the Maintenance backup ...................................... 14
    Verifying contents of the CMSADM backup ............................ 15
  Verifying completion of the previous CMSADM backup ................. 16
  Verifying completion of the previous Maintenance backup ............ 17
  Performing a Maintenance backup manually ............................. 18
  Performing a CMSADM backup .............................................. 19
  Restoring data from a Full Maintenance backup ......................... 20
  Restoring data from a Incremental Maintenance backup ............... 21
  CMSADM restore ............................................................ 22
2 Customer requirements for backup and recovery processes
If your Avaya Call Management System (CMS) crashes with a fatal disk error, your Avaya CMS support representative will ask you if you have the appropriate materials available to quickly get your CMS operational and recover as much data as possible. The usual answer the Avaya CMS support representative receives is, "No."

Your Avaya CMS support representative is aware that in many cases your whole operation is at stake. There is nothing more frustrating than knowing that if the backups were done, and if the software was available, your CMS could have been fixed and operational in hours instead of days.

This document provides information about how you can maintain quality backups, be prepared for an unexpected recovery, and provides an overview of the backup and recovery procedures for CMS.

This document is not release specific, and is not intended to replace the CMS documentation that was created for your version of CMS. To get a full description of the backup and restore process, you must read the appropriate sections in the CMS administration, and CMS installation, maintenance, and troubleshooting documentation provided for your CMS release.

⚠️ Important:
Avaya recommends that all of your CMS administration staff read the appropriate CMS administration, and CMS installation, maintenance, and troubleshooting documents.

This section includes the following topics:
- Customer case studies on page 4
- General recommendations on page 5
- Avaya CMS LAN backups on page 9
- Avaya CMS tape backups on page 10
Customer case studies

This section contains some examples of some CMS customers who have found themselves unable to recover from a disk crash in a timely manner.

Customer A

Customer A was running CMS Full Maintenance backups every night. A combination of several events made their recovery from a hard disk crash difficult. It took two days to recover enough data to be operational, and nearly two weeks to recover all their data.

The events that caused the recovery to take so long were:

- Customer A re-used the same two tapes on alternate days for over a year. This exceeded the tape media usage by considerable margin. The over usage of tape media can cause data corruption and loss of data. The data was not retrievable by standard methods.
- Customer A did not have the software needed to recover from catastrophic failure on site. It took a considerable amount time to obtain the correct software.
- Customer A did not have a vital password needed to activate some critical software. A considerable amount of time was spent on retrieving password data.

Customer B

Customer B also had a system disk crash and needed to recover quickly. Their hardware was quickly replaced and the system became operational, but recovering the software took a considerable amount of time. The lingering effects of trying to take shortcuts with backups were finally resolved a month later.

The events that caused the recovery to take so long were:

- Customer B did not have a current CMSADM backup.
- Customer B did not have the CMSADM backup that was shipped with the CMS.
- Customer B scheduled a Full Maintenance backup to occur on a regular basis through a time table, but the same tape was repeatedly used for over four months. A database table in CMS became corrupt, and was subsequently backed-up on tape. Once the corrupt table was written to tape the backup became corrupt and became unusable.
- Customer B’s copy of necessary operating system and application software packages were not available to restore the CMS.

Summary

Performing routine backups of your CMS is extremely important and cost effective. The CMS software and hardware platforms provide the necessary resources to generate quality backups of your CMS.
If you backup your CMS on a routine schedule, then you will have the necessary resources to minimize down time from a hard disk crash. The backups are critical and without them the restore process is not possible. The restore process allows you to maintain a stable CMS and preserve your data.

It is your responsibility to:

- Store all original factory shipped software, passwords, and documentation in a secure, but accessible location
- Store your original factory CMSADM backup tape in a secure, but accessible location
- Perform routine CMS backups
- Follow Avaya’s recommendations for your backup process

---

### Why you should routinely back up your CMS

Maintaining quality backups is economical and minimizes costs for your contact center operation. Your contact center will have additional costs if your CMS must be restored, and your backups are not available or are of poor quality. You might experience these costs as system down time, data loss, or unnecessary financial expense. If you maintain good quality backups, then your CMS could be operational within hours instead of days with minimal data loss.

The backup operation is simple, easy, and protects your CMS data. The restore operation will validate your efforts if you maintain quality stable backups. Maintaining quality backups is required if you want a stable CMS. Data is crucial to the successful operation of your call center. Therefore, backups are critical for maintaining your data.
Your responsibilities

It is recommended that your CMS administration staff be responsible for:

- Storing all original factory shipped software, passwords, and documentation in a secure, but accessible location
- Storing your original factory CMSADM backup tape in a secure, but accessible location

⚠️ Important:
Do not overwrite your original factory CMSADM backup tape
- Performing routine CMS backups

Periodically restarting your CMS server

Avaya recommends that you restart your CMS server once every three months for preventative maintenance reasons. Rebooting your CMS server should not take longer than 10 minutes and should be performed when the CMS server load is low.

Although restarting your CMS server is not a requirement, periodically restarting your CMS server is a recommended procedure targeted at minimizing the risk of a system failure and reducing events requiring data restoration. Restarting your CMS server lessens the possibility of your system being adversely impacted by anomalies such as memory leaks, packet loss, un-released file locks, data inconsistency, data corruption, and storage space fragmentation. These types of problems are known to occur on any computer system.

Avaya offers a High Availability (HA) solution if data loss from a server restart is a concern. The Avaya CMS HA solution provides an uninterrupted data stream between the communication server and two HA CMS servers. If you use the HA solution, restart each CMS server at a different time to prevent data loss.

Avaya support personnel who are performing system maintenance work may require you to restart your CMS. If Avaya support personnel require you to restart your CMS, they will work with you to determine the best time to perform the restart. Avaya support personnel will make every attempt to determine the root cause of any problem that might require a restart.

Optimize your backup and restore times

Avaya recommends that you take steps to optimize your CMS backup and restore times. This section describes several factors that will impact the amount of time it takes to backup or restore your data and presents options to reduce backup and restore times.
Factors that impact backup and restore times

The amount of time it takes to back up or restore data depends on the:

- **Amount of data** - An increase in the amount of data will cause an increase in the amount of time it takes to back up or restore the data. Some factors that will increase the amount of data being stored are:
  - Number of items being measured - CMS R3V9 and later have increased capacities. More data is generated if you measure 100,000 agent skill pairs instead of 10,000.
  - Number of days information is stored - The greater the data storage time, the greater the amount of data that will have to be backed up or restored. When CMS reaches a predetermined threshold for data storage, the oldest record is deleted so that the newest record can be stored. Twice the amount of data is stored if you set your data storage for 62 days instead of 31 days.
  - Interval size - Shorter intervals generate more data. A 15 minute interval will generate significantly more data than a 60 minute interval.

- **System load** - Processes that require a large amount of system resources will slow down the CMS. Backing up data requires a large amount of system resources. Additional processes that require a large amount of system resources are:
  - Running reports - Running a single large report or multiple smaller reports will use a large amount of system resources.
  - Archiving data - Archiving a large amount of data will use a large amount of system resources.

- **Necessity for manually changing backup tapes** - If the amount of data exceeds the capacity of a single backup tape, someone must monitor the system and manually load additional tapes. A data backup or restore will not finish unless someone is able to load tapes into the tape device as needed.

Reducing tape backup and restore times

If you do not take steps to optimize your CMS backup and restore times, you will begin to experience performance issues. Your CMS performance will drop if the backup continues to run when contact center activity increases. With the increased CMS capacities that are now available, CMS backups and restores could take much longer to complete than they have in the past. To reduce the amount of time it takes to backup or restore data, you can:

- Select the maximum interval time that will meet your data collection needs.
- Select the minimum data storage times that will meet your data collection needs for all the historical database tables.
- Run reports when CMS is not actively backing up or restoring data.
- Schedule routine backups to occur at a time that is different from data archiving.
- Schedule routine backups to occur when CMS activity is low.
Avaya CMS backups and recovery

- Reduce the amount of data being stored so only one backup tape is needed to store the data.
- Upgrade your CMS to a more powerful hardware platform or add additional memory and CPUs.

Alternate methods for backing up and restoring data

If you need a higher capacity process for backing up and restoring your data, you might want to use the Avaya CMS LAN Backup feature. For more information, see Avaya CMS LAN backups on page 9.
Avaya CMS LAN backups

The CMS LAN backup feature provides an alternative to the traditional method of backing up and restoring data. In the past, the only way to backup and restore data was to use a tape device located with the CMS. LAN backup allows you to back up Avaya CMS data and system information over a local area network (LAN) to a storage manager.

The storage manager is a third party software package that controls where, how, and when the data is stored. The only storage manager that is supported by Avaya is Tivoli Storage Manager. Using any other type of storage manager software is considered permissive use, and not supported by Avaya.

The *Avaya Call Management System LAN Backup User Guide* provides information about using the Avaya CMS LAN backup feature, guidelines for backups, hardware requirements, software requirements, and support guidelines. The LAN backup feature is only available with CMS versions R3V11 or later.

⚠️ **Important:**

If you use the Avaya CMS LAN backup feature, use the information in the appropriate *Avaya Call Management System LAN Backup User Guide* for backing up or restoring your CMS.
Avaya CMS backups and recovery

Avaya CMS tape backups

Your CMS is shipped with functioning hardware and software components to allow you to backup and restore the system. CMS has software that enables you to backup and restore CMS software and data.

This section includes the following topics:

- About CMS tape backups on page 10
- Tape devices and their associated components on page 11
- CMS tape backup recovery kit on page 12
- Recommendations for your tape backup process on page 12
- Commands for checking your backup tapes on page 13
- Verifying completion of the previous CMSADM backup on page 16
- Verifying completion of the previous Maintenance backup on page 17
- Performing a Maintenance backup manually on page 18
- Performing a CMSADM backup on page 19
- Restoring data from a Full Maintenance backup on page 20
- Restoring data from an Incremental Maintenance backup on page 21
- CMSADM restore on page 22

About CMS tape backups

There are two types of tape backups available through CMS:

- CMSADM
- Maintenance

CMSADM backup

The CMSADM backup saves all of the system data on the computer onto a tape. The CMSADM backup includes the following data:

- Solaris system files and programs
- CMS programs
- Non-CMS customer data placed on the computer

The CMSADM backup will not save CMS database tables. For complete data recovery, both the CMSADM and Maintenance backups are required.
**Maintenance backup**

Maintenance backups are used to archive and restore CMS database tables. If you do not have a backup, historical data is lost and cannot be recovered in the event of system or disk failure.

---

**Tape devices and their associated components**

CMS is configured with specific tape devices according to the CMS hardware platform. Avaya provides a few blank tape cartridges with every new CMS.

⚠️ **CAUTION:**

Backup tapes can wear out. Be sure to refresh your supply of backup tapes occasionally to avoid problems.

You must obtain additional blank tapes and cleaning cartridges from a source other than Avaya. Some sources for backup tapes are local office supply stores, or mail-order computer supply stores. Use the information in the following table to assist with ordering replacement tapes.

⚠️ **WARNING:**

Always verify that you are using the correct tape for the tape drive on your system. Many of the tape cartridges look alike, and using the wrong tape can damage the tape drive mechanism and tape heads.

The following table lists information about the tape devices, tape components, and hardware platforms that are supported by Avaya at this time:

<table>
<thead>
<tr>
<th>Tape drive</th>
<th>Tape description</th>
<th>Generic name</th>
<th>Platforms¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAT 72</td>
<td>36/72GB, 4mm, 170m</td>
<td>4mm DDS-5</td>
<td>Sun Blade 150</td>
</tr>
<tr>
<td></td>
<td>DDS cleaning cartridge</td>
<td>4mm cleaning cartridge</td>
<td>Sun Fire V880</td>
</tr>
<tr>
<td></td>
<td>DDS cleaning cartridge</td>
<td></td>
<td>Sun Fire V890</td>
</tr>
<tr>
<td>DDS-4</td>
<td>DDS4, 20/40GB, 4mm, 150m</td>
<td>4mm DDS-150</td>
<td>Sun Blade 100</td>
</tr>
<tr>
<td></td>
<td>DDS cleaning cartridge</td>
<td>4mm cleaning cartridge</td>
<td>Sun Blade 150</td>
</tr>
<tr>
<td></td>
<td>DDS cleaning cartridge</td>
<td></td>
<td>Sun Fire V880</td>
</tr>
<tr>
<td></td>
<td>DDS cleaning cartridge</td>
<td></td>
<td>Ultra 5</td>
</tr>
<tr>
<td>Mammoth</td>
<td>20/40GB, 8mm, 170m</td>
<td>170m AME Mammoth</td>
<td>Enterprise 3500</td>
</tr>
<tr>
<td></td>
<td>8mm cleaning cartridge</td>
<td>Mammoth cleaning cartridge</td>
<td></td>
</tr>
</tbody>
</table>

¹. For more information about supported CMS platforms and tape devices, contact your Avaya sales or support representative. Different platforms and tape devices might be supported depending on your CMS load.
CMS tape backup recovery kit

The tape backup recovery kit is composed of the backup media that the Avaya Technical Services Organization will need to restore service to your system if major problems occur. This kit should be stored in a secure, but accessible location in order to minimize the time your system is out of service.

The recovery kit should contain the most recent:

- CMSADM backup tape
- Full Maintenance backup tape and any Incremental Maintenance backup tapes since the latest full backup
- CMS CD-ROM
- CMS Supplemental Services CD-ROM
- Solaris CD-ROMs
- Informix CD-ROMs
- All the software packages and passwords that were shipped with the CMS.

Recommendations for your tape backup process

Avaya recommends that you:

- Back up your CMS on a monthly basis, and rotate through 3 to 4 backup tapes.
- Back up your CMS ACD data on a daily basis, and rotate through 7 to 8 backup tapes.
- Store the backup tapes in a location where they will be secure, but easily retrievable.
- Correctly label backup tapes so the contents are easily identified.
- Replace worn out backup tapes.
- Run backups when CMS activity is low.
  
  Running system backups is not service affecting with CMS releases later than R3V8, but the backups will impact the performance of the CMS.
- Monitor CMS tape devices and software to verify that the backup process is working properly.
- Check the backup tapes to verify data integrity.
- Do not leave a "good backup tape" in the tape device overnight. Tape rotation is essential for maintaining the quality of your backup tapes.
- Clean your tape device with the appropriate tape-cleaning cartridge once a month.
  
  The backup process will fail if the tape device is not clean.
● When major changes are applied to the CMS, back up your system after the change is made. Reserve copies of these backup tapes.

Some examples of major changes would be:
- The Avaya CMS is provisioned
- The Avaya CMS software is upgraded
- The IP address or network configuration is changed

---

**Commands for checking your backup tapes**

CMS has several commands that you can use to check the current status of a backup tape, verify the integrity of a backup tape, and verify completion of a backup.

This section includes the following topics:

- Reporting the status of a backup tape on page 13
- Verifying the Maintenance backup on page 14
- Verifying contents of the CMSADM backup on page 15

**Reporting the status of a backup tape**

You can use the `mt` command to see the current status of a tape in the tape device.

**Example 1:**

● Enter at the UNIX command prompt (#):

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

where 0 is the device number.

The system displays a message similar to the following example:

```
/dev/rmt/0: no tape loaded or drive offline
```

This message indicates that no tape is loaded into device /dev/rmt/0.
Example 2:

- Enter at the UNIX command prompt (#):

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

where 0 is the device number.

The system displays a message similar to the following example:

```
Tandberg 8 Gig QIC tape drive:
sense key(0x0)= No Additional Sense residual= 0 retries= 0
file no= 0 block no= 0
```

This message indicates that there is a tape is in the tape device.

**Verifying the Maintenance backup**

You can use the `br_check` command to verify the CMS Maintenance backup tape.

**Example:**

1. Enter at the UNIX command prompt (#):

```
/cms/bin/br_check
```

The system displays the following message:

```
Enter device type ['q' for qtape, 'f' for floppy]:
```

2. Enter: `q`

The system displays the following message:

```
Enter device path:
```

3. Enter the tape device path.

For example, `/dev/rmt/0`

The system displays a message similar to the following example:

```
Opening the volume...  
Label: CMS-010713-01-LSAC-00-F-01  
CMS Database Version: r3v8ai.b.0  
Machine name: r3gpbxx  
ACD(s) backed up on the volume:  
ACD Switch EAS Vectoring  
1 R8 n y  
Enter 'l' to list the tables or 'v' to also verify the volume:
```
4. Enter: v

The system displays a message similar to the following example:

<table>
<thead>
<tr>
<th>File</th>
<th>Type</th>
<th>Size</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>htrunk</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/13/2001</td>
</tr>
<tr>
<td>hvdn (V)</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/13/2001</td>
</tr>
<tr>
<td>hvector (V)</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/13/2001</td>
</tr>
<tr>
<td>m_secs</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>magent</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>mcwc</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>msplit</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>mtkgrp</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>mtrunk</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>mvdn (V)</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>mvvector (V)</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>06/30/2001</td>
</tr>
<tr>
<td>w_secs</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wagent</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wcwc</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wsplit</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wtkgrp</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wtrunk</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wvdn (V)</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
<tr>
<td>wvector (V)</td>
<td>Full</td>
<td>1</td>
<td>12/31/1899</td>
<td>07/07/2001</td>
</tr>
</tbody>
</table>

End of Backup.
Terminating...

Verifying contents of the CMSADM backup

You can use the cpio command to list the contents of a CMSADM backup tape. This list contains hundreds of files.
Avaya CMS backups and recovery

Example:

- Enter at the UNIX command prompt (#):
  
  ```
  cpio -icvt -C 10240 -I /dev/rmt/0
  ```

  where 0 is the device number.

  The system displays a message similar to the following example:

| drwxr-xr-x 3 root other 0 Mar 14 17:58 2001, cms/cc |
| drwxr-xr-x 3 root other 0 Mar 14 17:58 2001, cms/cc/c |
| .......................................................... |
| .......................................................... |
| .......................................................... |
| .......................................................... |
| drwxr-xr-x 6 root root 0 Mar 14 16:11 2001, cms/cow |
| drwxr-xr-x 2 root root 0 Mar 14 16:13 2001, cms/cow/1 |
| .......................................................... |
| .......................................................... |
| .......................................................... |

Verifying completion of the previous CMSADM backup

To verify that your last CMSADM backup completed successfully:

1. Enter at the UNIX command prompt (#):

   ```
   tail -f /cms/install/logdir/backup.log
   ```

2. Verify that the previous CMSADM backup completed successfully.

   Depending on your CMS version, you should see one of the following successful backup messages:

   - Some versions of CMS will only display a successful backup message.

   ```
   ====== Begin backup Wed Apr  9 05:37:05 EDT 2003
   Converter started Wed Apr  9 05:37:07 EDT 2003
   Converter completed successfully Wed Apr  9 05:37:10 EDT 2003
   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 2003
   ```
Some versions of CMS will display a message to verify a list of failed backup files in addition to a successful backup message. The failed backup files are usually temporary files that do not need to be backed up.

Verifying completion of the previous Maintenance backup

To verify that your previous Full or Incremental backup completed successfully:

1. Log 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.
5. Enter 1711 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 a backup history report.
9. Verify that the previous full or incremental backup completed successfully.

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

```
1711 4/15/03 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
```

10. Select the Exit option to return to the previous menu.

---

**Performing a Maintenance backup manually**

If you start a Maintenance backup manually then you must complete or cancel the backup manually before another Maintenance backup can run. This could cause your regularly scheduled backup to fail.

⚠️ **Tip:**

You can also perform Maintenance backups through the CMS Supervisor interface. For more information, see the appropriate Administration document for your CMS release.

To perform a Maintenance backup:

1. Verify that a write enabled tape is in the tape device.
2. From one of the windows at a console, log into the system by using a CMS administrator’s login ID (for example `su - cms`). Enter the correct password if prompted.
3. Enter at the UNIX command prompt (#):

   ```
cms
   ```

   A series of prompts about system status may appear before the system displays the CMS main menu.
4. Enter the correct terminal type.
5. From the CMS main menu, select Maintenance > Back Up Data.

   The system displays the Back Up Data window.
6. Select one of the following options under Historical data:

   - Full - includes data for all the time periods in the historical database. *You must do a Full backup before the first Incremental backup*. It is recommended that you periodically (for example, once a week) do a Full backup of your system if you will use Incremental backups.
   - Incremental - includes the new CMS data recorded since the last backup (incremental or full) was completed. Only the historical data can be stored incrementally; administration data is stored in full.
Avaya CMS tape backups

Tip:

If all of your Maintenance backup data fits on one tape, then Incremental backups are not necessary.

7. Press **Enter** to access the action list in the upper right corner of the window.

8. Select **Run** and press **Enter**.

   Wait for the backup to complete. If your backup requires more than one tape, you will receive a message telling you to mount another volume to complete the backup.

9. Press **Enter** when the backup completes to manually finish the backup.

10. Write protect, label, and store the tapes in a secure location.

Performing a CMSADM backup

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

1. Verify that a write enabled tape is in the tape device.

   **Important:**
   Running system backups is not service affecting with CMS releases later than R3V8, but once a CMSADM backup is started, new logins are blocked through:
   - The ASCII interface
   - Avaya CMS Supervisor
   - Avaya Visual Vectors

2. Log into the Solaris operating system as **root** and open a terminal window

3. Enter at the UNIX command prompt (#):

   ```
cmsadm
   ```

   The **Avaya Call Management System Administration Menu (CMSADM Menu)** is displayed.

4. Enter the number associated with the **backup** option.

   **Note:**
   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) Exabyte EXB-8900 8mm Helical Scan tape drive: /dev/rmt/0
   2) Exabyte EXB-8500 8mm Helical Scan tape drive: /dev/rmt/1
   Enter choice (1-2):
   ```
5. Press **Enter**.

   The backup process is initiated.

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

   ```
   xxxxxxxx blocks
   Tape Verification
   xxxxxxxx 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, label, and store the tape in a secure location.

---

**Restoring data from a Full Maintenance backup**

To restore data from a Full Maintenance backup:

1. Load the most recent Full Maintenance backup tape into the tape drive.

2. From one of the windows at a console, log into the system by using a CMS administrator’s login ID (for example `su - cms`). Enter the correct password if prompted.

3. Enter:

   ```
   cms
   ```

   A series of prompts about system status may appear before the system displays the CMS main menu.

4. Enter the correct terminal type.

5. Verify that the Avaya CMS software is in the single-user state, and data collection is off.

6. Select the **Maintenance** option.

7. Select the **Restore Data** option.

8. Enter the values shown in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td><code>default</code></td>
</tr>
<tr>
<td>Restore from last backup?</td>
<td><code>n</code></td>
</tr>
<tr>
<td>Restore historical data from</td>
<td>(leave blank)</td>
</tr>
</tbody>
</table>
9. Press **Enter** to access the action list in the upper right corner of the window.

10. Select **Run** and press **Enter**.

    The system begins restoring the data.

11. Remove the backup tape from device when the restore is complete.

12. Exit from the CMS menu and log off system.

13. Log onto CMS server as **root**.

14. Reboot the system.

15. Verify that the Avaya CMS software is in the multi-user state, and data collection is on after the reboot is complete.

### Restoring data from a Incremental Maintenance backup

To restore data from a Incremental Maintenance backup:

**CAUTION:**

You must perform a Full CMS Maintenance restore before you begin this procedure.

1. Insert the most recent Incremental Maintenance backup tape into the tape drive.

2. From one of the windows at a console, log into the system by using a CMS administrator's login ID (for example `su - cms`). Enter the correct password if prompted.

3. Enter:

    `cms`

    A series of prompts about system status may appear before the system displays the CMS main menu.

4. Verify that the Avaya CMS software is in the single-user state, and data collection is off.

5. Enter the correct terminal type.
7. In the Restore Data window, select the following options:

<table>
<thead>
<tr>
<th>Item</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name</td>
<td>default</td>
</tr>
<tr>
<td>Restore from last backup?</td>
<td>n</td>
</tr>
<tr>
<td>Restore historical data from</td>
<td>(leave blank)</td>
</tr>
<tr>
<td>ACDs to restore</td>
<td>All ACDs</td>
</tr>
<tr>
<td>Data to restore</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Local System Administration data</td>
</tr>
<tr>
<td></td>
<td>● CMS System Administration data</td>
</tr>
<tr>
<td></td>
<td>● ACD-specific administration data</td>
</tr>
<tr>
<td></td>
<td>● ACD-specific administration data</td>
</tr>
<tr>
<td></td>
<td>● Historical data</td>
</tr>
<tr>
<td></td>
<td>● Non-CMS data</td>
</tr>
</tbody>
</table>

1. Only select Non-CMS data if you have custom CMS database tables.

8. Press Enter, select Run, and press Enter again.
9. Remove the backup tape from device when the restore is complete.
10. Exit from the CMS menu and log off system.
11. Log onto CMS server as root and reboot system.
12. Verify that the Avaya CMS software is in the multi-user state, and data collection is on.

---

**CMSADM restore**

There are several reasons why a CMS might require a CMSADM restore:

- A CMSADM restore of Solaris and CMS is required if the boot disk fails mechanically, or the data on the disk becomes corrupt.
- A CMSADM restore of CMS is required if a non-boot disk fails mechanically, or the data on the disk becomes corrupt.

**Important:**

For detailed instructions of the procedures to follow for a CMSADM restore, see the appropriate [Avaya Call Management System Software, Installation, Maintenance, and Troubleshooting](#) document for your CMS release.