Upgrading the Solid State Drive on S8300C/S8300D servers with CM 5.2.1 and co-resident SES
Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be 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.

End User agrees to indemnify and hold harmless Avaya, its agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

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

Warranty
Avaya provides a limited warranty on 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 to Avaya customers and other parties through the Avaya Support Website: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

Licenses
The software license terms available on the Avaya Website, http://support.avaya.com/licensetools/ are applicable to anyone who downloads, uses and/or installs Avaya software, purchased from Avaya Inc., any Avaya affiliate, or an authorized Avaya reseller (as applicable) under a commercial agreement with Avaya or an authorized Avaya reseller. Unless otherwise agreed to by Avaya in writing, Avaya does not extend this license if the software was obtained from anyone other than Avaya, an Avaya affiliate or an authorized Avaya reseller, and Avaya reserves the right to take legal action against you and anyone else using or selling the software without a license. By installing, downloading or using the software, or authorizing others to do so, you, on behalf of yourself and the entity for whom you are installing, downloading or using the software (hereinafter referred to interchangeably as “you” and “end user”), agree to these terms and conditions and create a binding contract between you and Avaya Inc. Or the applicable Avaya affiliate (“Avaya”).

Avaya grants 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 originally sold by Avaya and ultimately utilized by End User.

License types
- 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 Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU): End User 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 (for example, webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SL): Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (See Third-party Components for more information).

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

Third Party Components
Certain software programs or portions thereof included in the 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 regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Website: http://support.avaya.com/Copyright.

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

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to securityalerts@avaya.com.

Trademarks
Avaya® and Avaya Aura™ are trademarks of Avaya Inc. The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party. Use of any Marks without the express written permission of Avaya or the applicable third party. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading documents
For the most current versions of documentation, see the Avaya Support Website: http://www.avaya.com/support.

Contact 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 Website: http://www.avaya.com/support.
## Contents

**Job Aid: Solid State Drive (SSD) replacement in S8300C/S8300D servers** 7

- **Introduction** ................................................................. 7
- **Prerequisites** ............................................................... 8
  - **Hardware** ................................................................. 8
  - **Software** ................................................................. 8
  - **Configuration values** .................................................. 8
  - **URLs** ....................................................................... 9
- **Reference documentation** ............................................... 10
- **Determining hardware condition** ..................................... 10
- **Back up system data** ..................................................... 11
- **Upgrading the Solid State Drive** .................................... 12
  - **Shutting down the S8300 server** ................................... 12
  - **Removing the solid state drive** ................................... 13
  - **Installing the solid state drive** ................................... 14
  - **Reseating the server in the Media Gateway** ..................... 15

**Job Aid: Reinstalling the S8300 system software** .................. 17

- **Setting TELNET parameters** .......................................... 18
- **Installing Communication Manager 5.2.1 software** ............. 18
  - **Verifying the software version** ................................... 19
  - **Setting the time, date, and time zone** ........................... 20
- **Copying files to the server** ........................................... 20
- **Downloading optional language files** ................................ 21
- **Installing service pack updates** ..................................... 21
- **Kernel Replacement** .................................................... 22
  - **About kernel replacement** ........................................ 22
- **Kernel replacement using System Management Interface** ...... 23
  - **Logging in to System Management Interface (SMI) from your laptop** ................................................... 23
  - **Downloading the kernel file** ...................................... 23
  - **Copying files to the server** ...................................... 24
  - **Installing the kernel update** ..................................... 24
  - **Testing the system using the System Management Interface** ................................................................. 26
- **Manage Updates** .......................................................... 26
  - **Manage updates field descriptions** .............................. 27
- **Configuring network parameters** .................................... 28
- **Enabling SES** ............................................................. 29
- **Installing the CM Messaging Remote Field Update (RFU)** ...... 29
- **Verifying connectivity to the backup files** ....................... 30
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restoring Data from a Network Device</td>
<td>30</td>
</tr>
<tr>
<td>Restoring Data from Compact Flash card</td>
<td>31</td>
</tr>
<tr>
<td>Checking for superuser login</td>
<td>32</td>
</tr>
<tr>
<td>Installing the Communication Manager license and authentication files</td>
<td>33</td>
</tr>
<tr>
<td>Installing the SES license</td>
<td>34</td>
</tr>
<tr>
<td>Rebooting the server</td>
<td>36</td>
</tr>
<tr>
<td>Checking server integrity</td>
<td>36</td>
</tr>
<tr>
<td>Final replacement tasks</td>
<td>37</td>
</tr>
</tbody>
</table>

Index                                                                 | 39   |
Job Aid: Solid State Drive (SSD) replacement in S8300C/S8300D servers

Introduction

This Job Aid describes the procedures to replace the Solid State Drive (SSD) in S8300C or S8300D servers for Communication Manager (CM) 5.2.1

Note:
This procedure is only applicable for Communication Manager 5.2.1.
Prerequisites

Hardware

- Replacement 8GB SSD kit
- Antistatic wrist strap
- Antistatic mat

Software

Download the following software to the laptop that you will use at the customer site:

- Communication Manager license file and authentication (password)
- SES license file
- Security updates
- Software service pack:
  - Downloading Communication Manager service packs
  - Downloading (option software) service packs
- Firmware upgrades:
  - Media gateway
  - Media module(s)
  - IP telephone firmware

Configuration values

Server

- Server host name
- Subnet mask
- IP addresses for server, default gateway, and Communication Manager Messaging (if installed)
- IP addresses associated with any optional software components
Backup

- Device
- Location
- User name
- FTP host name
- Directory
- Password

System Attributes

a. CM web pages 'Installation' Configure Server
   - Run through the Wizard and capture all screens, when you get to "Update System" press "Cancel"
   - You will need to input the CMM IP address in the Configuration Wizard after the Restore.

b. CM SAT interface
   - Run the command "Display System -Parameter Customer-Option"
   - Copy the SID and MID down. These will be useful in retrieving a new license if necessary.

c. CM Linux Shell
   - Run the commands: "productid", "almcall", "almenable", and "almsnmpconf"
   - The above commands should be checked after restoration to ensure proper alarming is configured.
   - "almsnmpconf" will only be configured if using SAL, SSG or SIG
   - "get-mac-address" is used for SES license

URLs

The Avaya Support URL is http://support.avaya.com/downloads.
- The RFA URL is http://rfa.avaya.com/.
Reference documentation

- Installing and Upgrading Avaya S8300 Server guide (555-234-100)
- "Administering Communication Manager for SIP Enablement Services" in Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server guide (03-602508).

Determining hardware condition

To determine whether the S8300C or S8300D is functional:

1. Connect your laptop to the Services port on the S8300C or S8300D.

2. Visit https://192.11.13.6 and access the Communication Manager System Management Interface main page (formerly called, Integrated Management Standard Management Solutions; pre-5.2 release). If you can connect to this page, the hardware is functional. Continue with **Backing up system data** on page 11.

3. If you do not know whether the S8300C or S8300D hardware is functional or you cannot connect to the **Server (Maintenance)** Web page:
   a. Access the server’s command line interface using an SSH client, like PuTTY, with an IP address of 192.11.13.6.
   b. Type `df` at the command line.
      The system displays a list of file systems.
   c. Look for "/dev/sda" and "/dev/hda" entries:
      - `/dev/sda` means that files on the hard drive are accessible.
      - `/dev/hda` means that files on the on-board CompactFlash are accessible.
   d. If you can see both "/dev/sda" and "/dev/hda" entries, the hard drive and onboard CompactFlash are functional. Continue with **Backing up system data** on page 11.
   e. If you cannot see the "/dev/sda" or "/dev/hda" entries, power-cycle S8300C or S8300D (press the Shutdown button on the S8300C or S8300D faceplate and hold the button until the green "OK to Remove" LED starts blinking, wait for the LED to go steady on, then reset the S8300 server to initialize it again) and then repeat Steps a-c above. If you still cannot see the "/dev/sda" or "/dev/hda" entries, the hardware is not functional, and you must use the customer’s backups (translations, SES database, operating system, security, and messaging data and announcements) when you get to **Restoring Data from a Network Device** on page 30.

   Skip to **Shutting down the S8300 server** on page 12.
4. You can also use the `hardware_info` command to determine the hardware health. This command also shows the size and model of the solid state drive.

---

**Backing up system data**

To back up the data on the S8300C or S8300D Server:

**Note:**

These instructions apply if your laptop is connected to the network and you are using System Management Interface.

1. At a browser on your laptop log in to the Maintenance Web Pages (192.11.13.6).
2. At the Maintenance Web page select **Data Backup / Restore > Backup Now**.
   
   The system displays the **Backup Now** screen.
3. In the **Data Sets** section select (check) all of the following data sets:
   - Server and System Files
   - Security Files
   - SES Files
   - If the S8300C or S8300D Server is not an LSP, select **ACP Translations** and click **Save ACP translations before backup**.
   - If Communication Manager Messaging is installed on the S8300C or S8300D Server, select **Communication Manager Messaging, Names, Translations** and **Messages**.
4. Select the Backup Method:
   - Local PC Card.

**Note:**

Use Network Device only if you are backing up Communication Manager Messaging.

- Network Device: enter the customer-supplied information for:
  - Choose from FTP, SCP, or SFTP
  - User Name
  - Password
  - Host Name
  - Directory

5. Click **Start Backup**.

   Wait for the message indicating that the backup was successful.
6. If Communication Manager Messaging is installed on the S8300C, back up AUDIX announcements:
   ● Return to the Backup Now screen and uncheck all but Audix Announcements.
   ● Select the Backup Method (see Step 4 above).
   ● Click Start Backup.

Upgrading the Solid State Drive

Upgrade the Solid State Drive (SSD) using the following procedure:
   ● Shutting down the S8300 server, on page 12
     - Shutting down the server through Web interface on page 12
     - Shutting down the server manually on page 13
   ● Removing the solid state drive on page 13
   ● Installing the solid state drive on page 14
   ● Reseating the server in the Media Gateway on page 15

Shutting down the S8300 server.

You can power down the Avaya S8300 Server using either of the procedures:
   ● Shutting down the server through Web interface on page 12
   ● Shutting down the server manually on page 13

Shutting down the server through Web interface

At the Web interface main menu for the Avaya S8300C/S8300D server:
1. Select Shutdown Server with these options:
   ● Check (select) Immediate Shutdown.
   ● Uncheck (deselect) Restart server after shutdown.
2. Click Shutdown and wait until the server has shut down.
   The green, OK to Remove LED (Note 2 in Figure 1: Avaya S8300 front faceplate on page 13) flashes to indicate that shutdown is in progress.
3. When the green, **OK to Remove LED** is on steady, unscrew the circuit pack, (Note 1 in Figure 1: Avaya S8300 front faceplate on page 13), slide it out of its slot, and set it on the antistatic mat.

4. Proceed with Removing the solid state drive on page 13.

**Shutting down the server manually**

If you cannot access the server’s Maintenance Web Interface, you can shut down the Avaya S8300C/S8300D server manually:

**Figure 1: Avaya S8300 front faceplate**

![Figure 1: Avaya S8300 front faceplate](image)

Figure Notes:

1. Screws
2. Circuit pack failure LED
3. Shutdown button (hold for more than 2 seconds)
4. Services port
5. USB port

1. Hold the Shutdown button (Note 3 in Figure 1: Avaya S8300 front faceplate on page 13) for more than two (2) seconds.

   The green OK to Remove LED (Note 2 in Figure 1) flashes to indicate that shutdown is in progress.

2. When the green OK to Remove LED is on steady, unscrew the circuit pack (Note 1 in Figure 1), slide it out of its slot, and set it on the antistatic mat.

**Removing the solid state drive**

The solid state drive is a 4GB card with Avaya Communication Manager and associated files that resides on the Avaya S8300C/S8300D server. After you replace the failed Solid State Drive on the Avaya S8300C/S8300D server, you must remaster it using the customer’s CD.
1. Lift the retainer clip as shown Note 2 of Figure 2: Removing the solid state drive from the S8300C/S8300D server on page 14.

![Figure 2: Removing the solid state drive from the S8300C/S8300D server](image)

2. Remove the solid state drive from the solid state drive connector.

3. Set the solid state drive on the antistatic mat. You will return it to Avaya later.

---

### Installing the solid state drive

To replace the solid state drive:

1. Carefully remove the replacement solid state drive from its protective antistatic packaging and place it on the antistatic mat.

2. Place the solid state drive into the solid state drive connector (Note 1 in Figure 2: Removing the solid state drive from the S8300C/S8300D server on page 14) pushing gently so that the drive seats securely in the connector.

3. Secure the retainer clip (Note 2 in Figure 2: Removing the solid state drive from the S8300C/S8300D server on page 14).
Reseating the server in the Media Gateway

To replace the Avaya S8300/S8300D server in its carrier:

1. Place the customer’s unity CD in the USB CD/DVD reader connected to the USB port on the front faceplate of the Avaya S800C/S8300D Server (Note 5 in Figure 1: Avaya S8300 front faceplate on page 13).

2. Insert the Avaya S8300 Server into the Media Gateway carrier slot, slide it all the way into the carrier, and screw the circuit pack in place (Note 1 in Figure 1: Avaya S8300 front faceplate on page 13).

3. Wait until the server boots up and the red circuit pack failure LED (Note 2 in Figure 1: Avaya S8300 front faceplate on page 13) is off.
Job Aid: Reinstalling the S8300 system software

This Job Aid describes the procedures to reinstall an S8300C or S8300D system software.

1. Setting TELNET parameters on page 18
2. Installing Communication Manager 5.2.1 software on page 18
   ● Verifying the software version on page 19
   ● Setting the time, date, and time zone on page 20
3. Copying files to the server on page 20
4. Downloading optional language files on page 21
5. Installing service pack updates on page 21
6. Kernel Replacement on page 22
7. Kernel replacement using System Management Interface on page 23
8. Manage Updates on page 26
9. Configuring network parameters on page 28
10. Enabling SES on page 29
11. Installing the CM Messaging Remote Field Update (RFU) on page 29
12. Verifying connectivity to the backup files on page 30
13. Restoring Data from a Network Device on page 30
14. Restoring Data from Compact Flash card on page 31
15. Checking for superuser login on page 32
16. Installing the Communication Manager license and authentication files on page 33
17. Installing the SES license on page 34
18. Rebooting the server on page 36
19. Checking server integrity on page 36
Setting TELNET parameters

The Microsoft TELNET application might be set to send a carriage return (CR) and line feed (LF) each time you press Enter. The installation program interprets this as two key presses. You must change this before you TELNET to the server.

**Note:**
This procedure is performed entirely at your laptop, not on the server.

1. Click on Start > Run to open the Run dialog box.
2. Type telnet and press Enter to open a Microsoft TELNET session.
3. Type unset crlf and press Enter.
4. Type display and press Enter to confirm that either Sending only CR or Line feed mode--causes the return key to send CR displays.
5. Type quit or close the TELNET window by clicking on the X icon in the upper-right corner.

This resets your Microsoft TELNET defaults and does not need to be done each time you use TELNET.

Installing Communication Manager 5.2.1 software

To install the software (Communication Manager and optionally, Communication Manager Messaging on the server):

1. At your laptop click on Start > Run to open the Run dialog box.
2. Type telnet 192.11.13.6 and press Enter.
3. The installation script looks for the software CD in the DVD/CD drive connected to the USB port. If the DVD/CD drive was not attached to a USB port when the server booted up, you will not see any activity on the screen. In this case perform the following:
   a. Press the Shut Down button on the server.
   b. When the OK-to-remove light comes on, connect the DVD/CD-ROM drive to a USB port.
   c. Unseat and reseat the S8300C in its slot.

   **Tip:**
   To navigate the installation screens, use the arrow keys to move to an option, then press the space bar to select the option. Press Enter to submit the screen.
4. Select Install and press Enter.

The Select Release Version screen displays.
5. Select the appropriate release version then select OK and press Enter.

The **Run AUDIX Installation** screen displays.

**Note:**

Communication Manager Messaging is optionally installed on the server when you install Communication Manager. If the customer was not using Communication Manager Messaging before the equipment replacement, do not install it.

6. Select Yes if you want to install Communication Manager Messaging concurrently with Communication Manager; select **No** if you do not.

The following processes are initiated:

- The server’s hard drive and internal solid state drive are partitioned and reformatted.
- The Linux operating system is installed.
- Once the drive is properly configured, Communication Manager software is installed and the progress reported.
- If elected, Install Communication Manager Messaging using the following steps.
  - Use the arrow key to move the cursor to "CM <embedded messaging>".
  - Press the space bar to move the asterisk to "CM <embedded messaging>".
  - Highlight the "OK" tab.
  - Press Enter.

The process takes about 30 minutes. When the server is ready to reboot, the CD drive door opens and a reminder to check the Avaya Support Site ([support.avaya.com/downloads](http://support.avaya.com/downloads)) for the latest software and firmware updates displays.

The reboot takes 1-3 minutes without Communication Manager Messaging and 3-6 minutes if it is present.

7. At your laptop click **Start > Run** to open the **Run** dialog box.

8. Type **ping -t 192.11.13.6** and press **Enter**.

9. Wait for the reply from the server to ensure connectivity to it.

---

**Verifying the software version**

To verify the software version that you just installed:

1. At a browser on your laptop log in to the Maintenance Web Pages (192.11.13.6).
2. Select **Server > Software Version**.
   
   The Software Version page displays.
3. Verify that the server is running Release 5.0 software. The beginning of the Report as: string should show R015x.00.
4. Verify that the DVD/CD-ROM drive opened at the end of the software installation.
5. Disconnect the DVD/CD-ROM drive from the server’s USB port.

Setting the time, date, and time zone

To set the time, date, and time zone on the server:

1. At the Maintenance Web page select Server > Server Date/Time.
   The system displays the Server Date/Time screen.
2. Set the server time within five (5) minutes of the Network Timer Server (NTS) time, date and time zone so that synchronization can occur.

   Note: If you change the time zone, reboot the server.

Copying files to the server

While reformatting the hard drive a new directory, /var/home/ftp/pub, is created. You must copy these files to the pub directory on the server’s hard drive:

- Communication Manager software service pack
- License file (if required)
- Avaya authentication file (if required)
- Security updates
- Messaging application service packs, RFUs, announcement files, or language sets
- SIP Enablement Services Service Pack (if using SES)
- Add Communication Manager Messaging RPMs

To copy files to the server:

   The system displays the Download Files screen.
2. Select File(s) to download from the machine I’m using to connect to the server.
3. Click Browse to open the Choose File window to navigate to the files you want to download.
4. Select the file(s) to download.

**Note:**
If you need to download an IP telephone firmware file, download this file last with the "Install this file on the local server" checked. The files are copied to the ...
tftpboot directory, the IP telephone Web page is reinstated, and the firmware restored at the next reboot.

**Note:**
To manually FTP files from your laptop to /var/home/ftp/pub, you must change the directory to pub (type cd pub) after starting FTP and logging in.

5. Click **Download** to copy the files to the server.

The transfer is complete when the message, "Files have been successfully downloaded to the server" displays.

---

**Downloading optional language files**

If the optional language files are needed, copy the files from the language CD to /var/home/ftp/pub.

1. Insert the language CD in your laptop's CD-ROM drive.

2. On the Maintenance Web page select **Miscellaneous > Download Files**.

3. Select **File(s) to download from the machine I’m using to connect to the server**.

4. Browse to the laptop CD and select each language file that you want to copy to the server.

5. Click **Download**.

The transfer is complete when you see the message, "Files have been successfully downloaded to the server."

6. If you need to copy more than four (4) optional language files, repeat this procedure.

Copies of the optional language files are now in the /var/home/ftp/pub directory and are automatically installed during the next reboot.

---

**Installing service pack updates**

If there is a service pack available for the server:

1. On the Maintenance Web page select **Server Upgrades > Manage Updates**.

The system displays the **Manage Updates** screen.
2. If an update file that you want to activate, shows **packed** in the **Status** column, select that file (radio button) and click **Unpack**.

3. Wait until the system displays the message, "...**unpacked successfully,**" and click **Continue**.

   The system displays the **Manage Updates** screen.

4. If the update that you want to activate shows **unpacked** in the **Status** column, select the file (radio button) and click **Activate**.

   The status of the activation process displays on the screen. If a reboot is required, the system automatically reboots.

5. Click on **Yes**.

   Wait until the system displays the Continue button.

6. Click **Continue**.

---

**Kernel Replacement**

**About kernel replacement**

You can replace the Linux kernel using the existing update mechanism in Communication Manager servers including servers that support RAM disk. For procedures on replacing the kernel, see Kernel replacement using Communication Manager System Management Interface.

Avaya Aura™ SIP Enablement Services (SES) Release 5.2.1 and Avaya Software Update Manager (SUM) also support kernel updates. For more information on replacing the kernel using SUM, see **Avaya Integrated Management Release 5.2 Software Update Manager**.

A kernel update is independent of the following:

- Service pack, security service pack, or SIP Enablement Services updates.
- Whether the system is running on the kernel that came with the release or a kernel from a prior update.

**Note:**

Any upgrade to a new load is blocked if a kernel update is in a pending state.
Kernel replacement using System Management Interface

Logging in to System Management Interface (SMI) from your laptop

1. Connect the laptop to the services port (eth1) using a crossover cable.
2. Open Internet Explorer (5.5 or later) on the laptop computer.
3. In the Address (or Location) field of your browser, type 192.11.13.6 and press Enter.
   If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate. The system displays the Welcome screen.
4. Click Continue.
   The system displays the Logon screen.
5. Log in as craft.
   The system displays the main menu for SMI.
7. On the Administration menu, click Server (Maintenance).
   The system displays the main menu in the left panel and a usage-agreement notice in the right window.

Downloading the kernel file

Download the latest kernel.tar file from the Web site http://support.avaya.com. The kernel file may look like the following: KERNEL-1.2.34-56.AB04XYZ.tar.gz.

Note:
A Product Correction Notice (PCN) is issued whenever a new kernel update is available. To view the PCN, visit http://support.avaya.com.
Copying files to the server

1. On the SMI, select **Miscellaneous > Download Files**.
   The system displays the Download Files page.
2. Select **File(s) to download from the machine I’m using to connect to the server**.
3. Click **Browse** to open the Choose File window to navigate to the files you want to download.
4. Select the files to download.
5. Click **Download** to copy the files to the server.
6. The kernel file is downloaded into the `/var/home/ftp/pub` directory.

   **Note:**
   To manually FTP files from your laptop to `/var/home/ftp/pub`, you must change the directory to pub (type `cd pub`) after starting FTP and logging in.

   The transfer is complete when the system displays the message, "Files have been successfully downloaded to the server".

Installing the kernel update

**Important:**
   Back up the server data before you upgrade the kernel.

1. On the SMI, select **Server Upgrades > Manage Updates**.
   The system displays the Manage Updates page. For more information, see Manage updates field descriptions on page 27.
2. If the status of the kernel update file that you want to activate shows packed in the Status column, select the file (radio button) and click **Unpack**.
   The system displays the status of the unpacking process.
3. After the system displays the message, "...unpacked successfully", Click **Continue**.
   The system displays the Manage Updates page.
4. If the update that you want to activate shows unpacked in the Status column, select the file (radio button) and click **Activate**.

The system displays the following message on the Manage Updates page.

**WARNING:** Activation of update KERNEL-1.2.34-56.AB04XYZ will cause a server reboot. Do you want to continue?

5. Click **Yes**.

The system displays the status of the activation process and will indicate the update was successfully activated. Do not click Continue until the automatic reboot has completed. The server reboot takes approximately 3 to 8 minutes. After the server reboots, the new kernel runs.

**Tip:**

When you are waiting for the system to reboot, type `ping -t 192.11.13.6` from a command prompt window on your services laptop computer to start a continuous ping command. If you start getting a reply, the reboot is complete.

6. Verify that your system is running properly. For more information, see Testing the system using the System Management Interface on page 26.

7. Click **Server > Process Status**.

The system displays the default settings for the output of the Process Status report.

8. Click **View**.

The system displays the process status results.

9. Verify that all processes are active before you return to the Manage Updates page, and click **Continue**.

**WARNING:**

You must verify that the server reboot is complete before clicking continue. An automatic server reboot occurs about 1 minute after successful activation of a kernel service pack. You should wait for at least 5 minutes for the server reboot to complete, and for all Communication Manager processes to restart.

10. If the kernel service pack you want to activate shows Pending_Commit in the Status column, click **File**.

11. Click **Commit**.

When using Linux commands to activate the kernel service pack, before you commit the service pack, use the `statapp` command after the reboot to verify that all applications are active.

Perform the steps to commit the kernel service pack for deactivating the kernel service pack. The server reboots after the deactivation. Verify that all processes and applications are active before proceeding.

12. If the update that you want to activate shows Pending_Commit in the Status column, select the file (radio button) and click **Commit**.
Testing the system using the System Management Interface

1. On the SMI, click **Administration > Server (Maintenance)**.
2. Under **Server** click **Status Summary**. Verify that the **Server Hardware** and the **Processes** fields say **okay**.
3. Under **Diagnostics** select **Ping**.
4. Under **Endpoints to Ping**, select **All IPSI's, UPS's**.
5. Click **Execute Ping**.
   
   If the ping is successful, the Execute Ping results page displays a brief summary that shows the number of packets sent and received. The summary also shows the minimum, average, and maximum of the round-trip times.
6. From a computer on the customer LAN, use Internet Explorer to connect to the server.
7. Log in as **craft**.
   
   This action verifies that connectivity exists and the customer can log in to perform administration or other tasks.

   **Note:**
   
   If you do not commit the update within ten minutes of the server reboot, a minor platform alarm is generated. Also, if a reboot occurs before the update is committed, the server will come back up running the original kernel rather than the kernel from the update.

Manage Updates

Use this page to manage the updates. The types of updates are service pack, security service pack, kernel, and SIP Enablement Services updates. This page displays:

- The current release that is running on the server
- Mode of the server
- Updates available for the server and their corresponding status
## Manage updates field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update ID</td>
<td>The unique update identifier. For example, the Update ID may look like the following for a kernel update: <code>KERNEL-2.6.18-53.AB04XYZ</code>.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the current update.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Activated</strong>: The update is functioning correctly.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Packed</strong>: A new update is available.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Unpacked</strong>: A new update is successfully unpacked.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Pending_Commit</strong>: The kernel update is activated but the activation is not committed.</td>
</tr>
<tr>
<td></td>
<td>● <strong>Pending_Deactivate</strong>: The kernel update is deactivated but the deactivation is not committed.</td>
</tr>
<tr>
<td>Type</td>
<td>Either hot or cold, where cold means the update is service affecting, hot means the update is not service affecting. This page prompts the user to continue if the update is of type cold.</td>
</tr>
<tr>
<td>Unpack</td>
<td>Unpacks the update file. The update file is read from the update repository (<code>/var/home/ftp/pub</code>).</td>
</tr>
<tr>
<td>View</td>
<td>Displays the information about the update file.</td>
</tr>
<tr>
<td>Activate</td>
<td>Activates the update file.</td>
</tr>
<tr>
<td>Deactivate</td>
<td>Deactivates the update file.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes all the files associated with an update that is not active. If the update is in an unpacked state and exists in the update repository, the update will show as packed after the unpacked version is removed.</td>
</tr>
<tr>
<td>Commit</td>
<td>Completes the current kernel update process. The system displays the state of the current kernel update.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>The Commit button is unavailable if the kernel update is not in the pending state.</td>
</tr>
</tbody>
</table>
Configuring network parameters

If you have backed up the server data to a USB CompactFlash card / reader, omit this section and continue with Enabling SES on page 29. Otherwise, complete this section.

**Note:**

You must have the host name, subnet mask, and IP addresses of the server and default gateway to complete this procedure.

To configure the network parameters on the server:

1. On the Maintenance Web page select **Server Configuration > Configure Server**.

   The system launches **Configure Server** wizard.

2. Click **Continue** until you get to the "Specify how you want to use this wizard" screen.

3. Select **Configure individual services** and click **Continue**.

4. Click **Set Identities**, from the "Configure Individual IP Services" list.

   The system displays the **Set Identities** screen.

5. Fill in the host name with the name of the server.

6. Click **Continue**.

   The system displays the **Configure Interfaces** screen.

7. Fill in the correct server and gateway IP addresses, the subnet mask, and, if Communication Manager Messaging is installed, its IP address (but not if this server is an LSP).

   If these fields are already filled in, overwrite them with the correct information. Leave the **Integrated Message** field blank.

   **Note:**

   CMM IP Address needs to be manually entered after a restoration.

8. Click **Change** to update the system files.

   **Note:**

   If an Action Cancelled message appears before the Success message, refresh the screen and click **Change** again.

9. The system displays "**Successfully configured ethernet interfaces**" message when the configuration change is complete.

10. Click **Close Window**.
Enabling SES

If the S8300C is a main server (primary controller) and was running SES before the equipment replacement, you must re-enable SES:

1. On the Maintenance Web page select Miscellaneous > SES Software.
   
   The system displays SES Software page.
   
   **Note:**
   
   The text, "SES is disabled" should appear just above the Enable SES button.

2. Click Enable SES.

3. Wait approximately 30 seconds and click the refresh button on your browser.
   
   The SES Software page should show, "SES is enabled."

4. To verify that SES is enabled go to the Integrated Management Standard Management Solutions main page.

5. Verify that the SES Administration option is now available.
   
   **Note:**
   
   If an SES Service Pack is available, refer Installing service pack updates on page 21 to install it.

---

Installing the CM Messaging Remote Field Update (RFU)

1. On the Administration menu, click Messaging.
   
   The system displays the Messaging Administration screen.

2. On the left navigation pane, under Software Management, select Software Install.
   
   The system displays the backup reminder screen.

3. Click Continue without current system backup.
   
   The system displays the Packages will be installed from screen. The CM Messaging RFUs are listed and are preselected for installation.

4. Click Install selected packages.
   
   The system displays the list of packages to be installed.
5. Click the Proceed with installation button.

The screen displays status of the installation. When the installation is complete, the message, All packages successfully installed appears at the bottom of the screen.

6. Close the browser window.

⚠️ Important:
Do not start the messaging software at this time.

---

**Verifying connectivity to the backup files**

To verify that the Ethernet port is working, ping the FTP server where the backup files are stored.

2. Enter the IP address of the device on which the backup files are stored.
3. Click Execute Ping.

If the ping is successful, continue with Restoring Data from a Network Device on page 30. Otherwise, check the IP address and connectivity to the server.

---

**Restoring Data from a Network Device**

To restore backup data:

   
   The system displays the View/Restore Data screen.
2. Select Network Device (radio button).
3. In the Method drop-down box, select FTP.
4. Fill in these fields:
   - User Name
   - Password
   - Host Name (enter the host IP address)
   - Directory
5. Click View.

The system displays the View/Restore Data Results screen.
6. If you need to restore the OS data set (server and system files), restore the OS data set first. If not, restore the security data set now.

7. Select both "Force..." options then click Restore.

8. To monitor the restore progress at the Server (Maintenance) Web page select Data Backup/Restore > Restore History.
   The system displays the Restore History screen.

9. Select the backup file that you want to monitor and click Check Status.
   The system displays the Restore History Results screen.

10. Click Refresh periodically until the message indicates that the restore was successful. This takes approximately five (5) minutes.

11. Repeat Steps 1-10 above to restore:
   a. Security data set (if not performed in Step 6 above)
   b. Communication Manager translations (main server/primary controller only, not a LSP) data
   c. Messaging application data in the "audix-tr-name-msg" file (primary controller only, not a LSP)
   d. Messaging application announcements in the "audix-ann" file (primary controller only, not a LSP)
   e. SES database

12. Reboot the server after you complete the restore procedure.

---

Restoring Data from Compact Flash card

To restore backup data from Compact Flash (CF) card:

1. On the Maintenance Web page select View/Restore Data > Local PC card.

2. Click View.
   The system displays the View/Restore Data Results screen.

3. If you need to restore the OS data set (server and system files), restore the OS data set first. If not, restore the security data set now.

4. Select both "Force..." options then click Restore.

5. To monitor the restore progress at the Server (Maintenance) Web page select Data Backup/Restore > Restore History.
   The system displays the Restore History screen.
6. Select the backup file that you want to monitor and click **Check Status**.
   The system displays the **Restore History Results** screen.

7. Click **Refresh** periodically until the message indicates that the restore was successful. This takes approximately five (5) minutes.

8. Repeat Steps 1-10 above to restore:
   a. Security data set (if not performed in Step 6 above)
   b. Communication Manager translations (main server/primary controller only, not a LSP) data
   c. Messaging application data in the "audix-tr-name-msg" file (primary controller only, not a LSP)
   d. Messaging application announcements in the "audix-ann" file (primary controller only, not a LSP)
   e. SES database

9. Reboot the server after you complete the restore procedure.

---

**Checking for superuser login**

**Note:**

If you restored Communication Manager translations (xln file) earlier, omit this section and continue with [Installing the Communication Manager license and authentication files](#) on page 33.

When you are replacing a server or hard drive, the Communication Manager Maintenance Web Pages might time out if too much time elapses without activity. In this case, you might not be able to log in again with the craft login. This problem can occur after you install the new server and restore translation and security files, but before you install the new authentication file. Restoring translation and security files does not restore the *init* and *inads* service accounts, nor is "sroot" available until the authentication file is installed. However, you can log in with the customer’s super-user login, if it exists.

To ensure that a super-user login exists in Communication Manager:

1. SSH to and log in as **craft** to the server command line interface.
2. At the Linux command line interface type **cat /etc/passwd |grep 555** and press **Enter**.

---

32 Upgrading the Solid State Drive on S8300C/S8300D servers with CM 5.2.1 and co-resident SES
Installing the Communication Manager license and authentication files

A list of super-user logins displays (example only):

init:x:778:555::/var/home/defty:/bin/bash
inads:x:779:555::/var/home/defty:/bin/bash
craft:x:780:555::/var/home/defty:/bin/bash
dadmin:x:1101:555::/var/home/defty:/bin/bash
erik:x:1002:555::/var/home/defty:/bin/bash

Look for any logins other than the init, inads, and craft logins.

Installing the Communication Manager license and authentication files

Note:
If you restored the operating system (.os file) and security (.security) files earlier, omit this section and continue with Installing the SES license on page 34.

⚠️ CAUTION:
If the Communication Manager/SES software version matches the translation’s version, use the following procedure to install the Communication Manager license and authentication file. If they do not match, install the license and authentication files manually.

⚠️ CAUTION:
A super-user login, admin, or other customer super-user login must exist before you install an authentication file. See Checking for superuser login on page 32.

To install the Communication Manager license and authentication files:

   The License File page displays.
2. Select Install the license file I previously downloaded (radio button) and click Submit.
   The system displays a message telling you that the license was installed successfully.
   The Authentication File page displays.
4. Select Install the Authentication file I previously downloaded (radio button) and click Install.
   The system displays a message telling you that the authentication file was installed successfully.
5. Verify the license and authentication file installation by issuing the statuslicense -v command from the server command line:
Job Aid: Reinstalling the S8300 system software

- The License Mode should be Normal.
- The report should list a License Serial Number.

---

Installing the SES license

Install the SES license from the WebLM server that is located on an edge or a combined home/edge server:

1. At the Integrated Management Standard Management Solutions main page select Launch SES Administration Interface.
   The Integrated Management SIP Server Management Top page displays in a new window.

2. Select Server Configuration > License.
   The system displays List Licenses page.

3. Click Access WebLM.
   The WebLM application screen displays in a new window.

4. If this is the first time the application has run, you must log in with "admin" as the default login and "weblmadmin" as the default password, then change both the default login and password to the customer's preferences for this account.

   **Note:**
   If the WebLM server is on a different subnet than the server, you must change the URL in your browser to include the server's DNS name. When you mouse-over the WebLM link on the List Licenses page, the URL includes an IP address, for example, "https://12.34.56.78/WebLM/index.jsp/". Change the URL to "https://server-name/WebLM/index.jsp/" where server-name is the DNS name of the server on which you want to install the SES license.

5. Select License Administration.
   The authentication screen displays.

6. Login as admin and enter the password.
   After this initial login, the system prompts you to change the password.

7. Change the password.
   WebLM logs you out.

8. Log in again as admin with the newly-created password.
   The server displays Web License Manager (WebLM) screen.

9. Select Install License.
   The system displays Install License page.
10. Click **Browse** to navigate to the SES license that you want to install.

11. Click **Install**.

   If the license is valid, the system indicates that it was installed successfully; otherwise the process fails with a brief description.

   **Note:**
   
   The license update for the home seats can take up to 15 minutes. Wait approximately 15 minutes before continuing with verifying the license installation (Step 12).

12. To verify the license installation go to the Integrated Management SIP Server Management Top page and select **Server Configuration > License**.

   The List Licenses page displays.

13. Ensure that the following three (3) licenses are listed in the **Name** column:

   - - Edge Proxy
   - - Basic Proxy
   - - Home Seats

14. Click **Show** by the Edge Proxy listing.

   The system displays **License Information** page.

15. Ensure that the page displays the following information:

   Proxy Name sipserver
   Requested 1
   Acquired 1

16. Click **Show** by the Basic Proxy listing.

   The system displays **License Information** page.

17. Ensure that the page displays the following information:

   Proxy Name sipserver
   Requested 1
   Acquired 1

18. Click **Show** by the Home Seats listing.

   The system displays **License Information** page.
19. Ensure that the page displays the following information:

Proxy Name sipserver
Requested XXX
Acquired XXX
where XXX is the actual number of seats in the license.

---

Rebooting the server

To commit the foregoing administration and provisioning:

   The system displays Shutdown This Server page.
2. Select Delayed Shutdown and check the Restart server after shutdown box.
3. Click Shutdown.

---

Checking server integrity

After the server comes up verify the following:

1. Ping the IP address of the server and ensure connectivity.
   The system displays Status Summary Page.
3. Ensure the following:
   ● Mode is Active.
   ● Server Hardware is okay.
   ● Processes is okay.
   The system displays Process Status page.
5. Select Summary from the Content section.
6. Select Display once from the Frequency section.
7. Click View.
   The system displays View Process Status Results page.
8. Ensure that all processes are **UP**.

---

**Final replacement tasks**

Perform the following tasks to complete the server or hard drive replacement:

1. On the Maintenance Web page select **Server > Status Summary** and check the overall health of the system.

2. Run the port check tool:
   a. At the server command line type `portcheck` and press **Enter**.
   b. Select **Server Interface (ethX) test (#4)**, and press **Enter**.
   c. Ensure that the interfaces listed in the **Link** column are **up**.

3. Resolve any alarms (**Alarms > Current Alarms**).

4. Save translations (**Data Backup/Restore > Backup Now**).

5. Set backup schedules (**Data Backup/Restore > Schedule Backup**).

6. At the server command line type `productid -p product_id`, where `product_id` is the product ID you received from the customer or the ART tool.

7. Re-enable alarm origination:
   a. At the server command line type `almenable -d b -s y` and press **Enter**, where:
      - **-d b** sets the dial-out option to both numbers
      - **-s y** enables sending SNMP traps.
   b. Type `almenable` without any options and press **Enter** to verify that alarm origination is enabled.

8. Logoff the system.
# Index

<table>
<thead>
<tr>
<th>Letter</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Antistatic mat</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Antistatic wrist strap</td>
<td>8</td>
</tr>
<tr>
<td>C</td>
<td>Communication Manager 5.2.1</td>
<td>7</td>
</tr>
<tr>
<td>F</td>
<td>Firmware upgrades</td>
<td>8</td>
</tr>
<tr>
<td>I</td>
<td>IP telephone firmware</td>
<td>8</td>
</tr>
<tr>
<td>M</td>
<td>Media gateway</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Media module</td>
<td>8</td>
</tr>
<tr>
<td>S</td>
<td>SES.</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Solid State Drive</td>
<td>7</td>
</tr>
</tbody>
</table>