Job Aid: Replacing the S8300D server or the S8300D server hard drive

This job aid describes the procedures to replace an installed S8300D server or the S8300D hard drive. For replacing the S8300A, S8300B and S8300C servers, see *Upgrading Avaya Aura® Communication Manager*, 03-603560.

The procedures in this job aid are applicable only to the replacement of the S8300D server running on either the CM_SurvRemote or CM_onlyEmbed template.

The term S8300 hardware refers to the S8300D server and its 250 GB hard disk drive. The material ID of the S8300D server is 700447675.

The Product Correction Notices are available at http://support.avaya.com/.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Before you begin

1. Determine the configuration of the existing server.

   If the existing server runs the CM_onlyEmbed template, determine if:

   - The server runs Communication Manager Messaging.

- Utility Server supports the phone firmware download function.

If the existing server runs the CM_SurvRemoteEmbed template, determine if it also runs Branch Session Manager.

Determine if Communication Manager has the Unicode (Phone Message) files installed.

If Utility Server supports phone firmware download function and the System Platform backup is unavailable, go to Step 2.

If the existing server utilizes Services VM with SAL gateway enabled and the System Platform backup is unavailable, go to Step 2.

2. Determine the backup files you will use in the S8300D server or S8300D hard drive procedure.

   Check if backup files can be created. If they cannot be created, use the existing customer backup files.

   Ensure that you have the customer backup server IP address and the account required to access the files.

   The following are the preferred backup sets:

   - System Platform.
   - Communication Manager Messaging translations, names, and messages. This backup is applicable only to the CM_onlyEmbed template.
   - Communication Manager Messaging announcements. This backup is applicable only to the CM_onlyEmbed template.

   The following are the first alternatives to the preferred backup sets:

   - Communication Manager full backup or backup of translation files.
   - Utility Server backup.
   - Communication Manager Messaging translations, names, and messages. This backup is applicable only to the CM_onlyEmbed template.
   - Communication Manager Messaging announcements. This backup is applicable only to the CM_onlyEmbed template.
3. If the existing server is functional, perform the System Platform backup which contains the server configuration for System Platform, Communication Manager, BSM and Utility Server. The System Platform backup does not contain the server configuration for Communication Manager Messaging.
4. If the existing server is functional, perform Communication Manager Messaging backup.
5. Ensure that you have the software versions for the following:
   - Avaya Aura® System Platform
   - Avaya Aura® Communication Manager
   - Communication Manager Messaging

- Services VM
- Utility Server
- BSM

6. Download the current license file and authentication file from the PLDS Web site. The license file must be associated with the serial number of the gateway in which the defective hardware resides. Save the license and authentication files on the laptop that you will use at the customer site. For the replacement of the hard drive, use the license file that has been generated by the system.
7. Determine whether software service packs and firmware files are required. If the service pack is required, download the service pack and save it on your laptop.

At the customer site

1. If the hardware is functional, connect your laptop to the services port on the server. Then, on the **System Platform** home page, select **cdom** and click **Server Management**.

   If the system does not display the **System Platform** home page, perform the following steps to determine if the hardware is functional:

   a. Connect the customer laptop with a crossover cable to the services port on the server, and go to the **System Platform** home page.

   b. If you do not get the **System Platform** home page, unplug and replug the power cord, and try navigating to the page again. If you still face problems while gaining access to the page, then the hardware is not functional. See Replacing the S8300D server on page 4.

   WARNING:
   Turning the server off can cause service outage.

2. Back up data:

   a. On the **System Platform** home page, click **Server Management** > **Backup/Restore** > **Backup**.

   b. On the **Backup** screen, click the **Backup** tab.

   c. Click **Backup Now**.

   d. Select SFTP as the backup method and enter the following customer information:

      - User Name
      - Password
      - Host Name
      - Directory

e. Click **Backup Now**.

Note:
You must take a complete backup of the system, including Communication Manager Messaging, if installed.

Replacing the S8300D server

1. Shut down the server using either the Web interface or the **Shutdown** button on the server faceplate.
   - On the **System Platform** home page, click **Server Management** > **Server Reboot/ Shutdown**. Click **Shutdown Server**.
   - Alternatively, press the **Shutdown** button on the server faceplate. Hold the button until the green **OK to Remove** LED starts blinking.
2. When the **OK to Remove** LED is steady, loosen the two thumb screws on the server.
3. Remove the S8300D server.
4. Connect the USB CD/DVD drive to the server. Insert the System Platform software media.
5. Completely insert the server in the gateway slot and secure the server faceplate with the thumb screws. Tighten the thumb screws.
6. Turn on the gateway if you had turned it off earlier.
7. Connect your laptop to the services port on the server.
8. Install System Platform from the DVD.

   The server reboots after installation.
9. If required, install the System Platform patches and the Services VM patches.
10. Use the services laptop or a network connection to gain access to the **System Platform** home page.
11. Enter the configuration data into the server during template installation.
12. If the server is configured as Main Server, install the CM_onlyEmbed template.

    If the server is configured as Survivable Remote Server, install the CM_SurvRemoteEmbed template.
13. If required, install the Communication Manager service pack, the BSM service pack and patch, and the Utility Server service pack.
14. If the System Platform backup is available:
    a. Restore the System Platform data.
    b. If the S8300D server was replaced, you must install an updated license file and authentication file. If you replaced the disk and are reusing the S8300D server, you do not need to reinstall the license and authentication file.

15. If the System Platform backup is unavailable and you have a Communication Manager backup:
    a. Configure Communication Manager as you would configure a new installation.
    b. Restore the Communication Manager data.
    c. Reboot the Communication Manager virtual machine by using the Communication Manager Web page and clicking **Shutdown Server** or the System Platform Webconsole Web page and clicking **Manage**.
16. If required, install the Communication Manager Messaging service pack.
17. If required, restore the Communication Manager Messaging data that includes translations, names, and messages.
18. If required, restore the Communication Manager Messaging announcements.
19. Start Communication Manager Messaging.
20. If required, install Communication Manager Unicode (phone messages) file.
21. Check for any new alarm and resolve the alarm.
22. Test as appropriate. For example, make station and trunk calls.
23. Save the translations files. If the server on which you replaced the hardware is configured as a survivable remote server, save the translations files on the primary controller and not on the survivable remote server.
24. Activate alarm origination.
    a. At the server command line, type **`almenable -d b -s y`** and press **Enter**.
    b. Type **`almenable`** without any options and press **Enter** to verify that alarm origination is active.
25. Log off from the system.

Replacing the S8300D hard drive

CAUTION:
Ensure that you wear a properly grounded ESD wrist strap while handling the server hard drive. Place all components on a grounded, static-free surface while working on them. Hold the hard drive by the edges. Do not touch the bottom of the hard drive.

1. Shut down the server using either the Web interface or the Shutdown button on the server faceplate.
   - On the **System Platform** home page, click **Server Management** > **Server Reboot/ Shutdown**. Click **Shutdown Server**.

- Alternatively, press the **Shutdown** button on the server faceplate. Hold the button until the green **OK to Remove** LED starts blinking.

2. When the **OK to Remove** LED is steady, loosen the two thumb screws on the server.
3. Remove the S8300D server.

Note:
If standoffs are not included with the new hard drive, remove the standoffs from the old hard drive and reuse them. Before screwing the standoffs into the new hard drive, clean the threads thouroughly with a damp cloth or paper towel.

a. From the server, remove the two screws that are attached to the hard drive standoffs. See S8300D hard drive replacement.

Figure 1: S8300D hard drive replacement

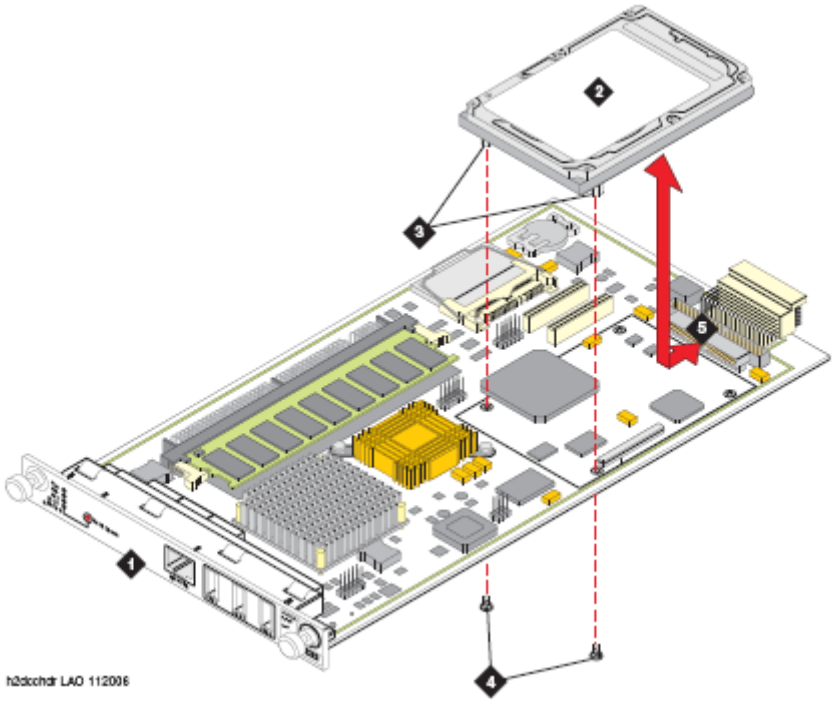

Figure notes:

1. S8300D server
2. Hard drive
3. Hard drive standoffs
4. Hard drive mounting screws (2)
5. Hard drive connector

b. Detach the hard drive by pulling it out of the connector.

c. Locate the standoffs for the new hard drive. If standoffs are not included in the new hard drive, remove the standoffs from the old drive and reuse them.

d. Screw the standoffs into the new hard drive.

e. Connect the hard drive to the hard drive connector.

f. Align the hard drive standoffs with the mounting holes on the server.

g. Hold the server by its side, with the hard drive aligned with the mounting holes, and attach the server to the hard drive standoffs.

h. Insert the server into the appropriate slot of the gateway. For example, use slot V1 of the G450 or G430. Do not completely insert the server in the slot.

4. Before completely inserting the server into the appropriate slot of the gateway, connect the USB CD/DVD drive to the server. Insert the System Platform software media.
5. Completely insert the server in the gateway slot and secure the server faceplate with the thumb screws. Tighten the thumb screws.
6. Turn on the gateway if you had turned it off earlier.
7. Connect your laptop to the services port on the server.
8. Install System Platform from the DVD.

   The server reboots after installation.
9. If required, install the System Platform patches and Services VM patches.
10. Use the services laptop or a network connection to gain access to the **System Platform** home page.
11. Enter the configuration data into the server during template installation.
12. If the server is configured as Main Server, install the CM_onlyEmbed template.

    If the server is configured as Survivable Remote Server, install the CM_SurvRemoteEmbed template.
13. If required, install the Communication Manager service pack, the BSM service pack and patch, and the Utility Server service pack.
14. If the System Platform backup is available:
    a. Restore the System Platform data.
    b. If the S8300D server was replaced, you must install an updated license file and authentication file. If you replaced the disk and are reusing the S8300D server, you do not have to reinstall the license and authentication file.
15. If the System Platform backup is unavailable:
    a. Configure Communication Manager as you would configure a new installation.
    b. Restore the Communication Manager data.
    c. Reboot the Communication Manager virtual machine by using the Communication Manager Web page and clicking **Shutdown Server** or the System Platform Webconsole Web page and clicking **Manage**.
16. If required, install the Communication Manager Messaging service pack.
17. If required, restore the Communication Manager Messaging data that includes translations, names, and messages.
18. If required, restore the Communication Manager Messaging announcements.
19. Start Communication Manager Messaging.
20. If required, install Communication Manager Unicode (phone messages) file.

21. Check for any new alarm and resolve the alarm.
22. Test as appropriate. For example, make station and trunk calls.
23. Save the translations files. If the server on which you replaced the hardware is configured as a survivable remote server, save the translations files on the primary controller and not on the survivable remote server.
24. Activate alarm origination.
    a. At the server command line, type **`almenable -d b -s y`** and press **Enter**.
    b. Type **`almenable`** without any options and press **Enter** to verify that alarm origination is active.
25. Log off from the system.

Job Aid: Replacing the S8300D server or the S8300D server hard drive