Replacing Field Units for the Avaya S8300D Server with G450 or G430 Branch Gateway
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.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of warranty available to you. If you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Documentation disclaimer

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

Link disclaimer

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

Licenses

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

Avaya grants 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 only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- **Concurrent User License (CU).** End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, partner 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.
- **Database License (DL).** End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- **CPU License (CP).** End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the
Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

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

Copyright

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.

- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or 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 is not 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 through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (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/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company’s Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya’s customer 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

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaita
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference...
caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user’s authority to operate this equipment.

Federal Communications Commission Part 15 Statement:
For a Class A digital device or peripheral:

Note:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Equipment With Direct Inward Dialing (“DID”):
Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC’s rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   • answered by the called station,
   • answered by the attendant,
   • routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   • routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

• A call is unanswered
• A reorder tone is received
• A busy tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:
When programming emergency numbers and (or) making test calls to emergency numbers:

• Remain on the line and briefly explain to the dispatcher the reason for the call.
• Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:
The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer’s employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:
This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:
This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L’indice d’équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d’une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d’indices d’équivalence de la sonnerie de tous les dispositifs n’excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:
Connection of this equipment to the telephone network is shown in the following table:

To consult the dealer or an experienced radio/TV technician for help.

Note:
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
• Reorient or relocate the receiving antenna.
• Increase the separation between the equipment and receiver.
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   • answered by the called station,
   • answered by the attendant,
   • routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   • routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

• A call is unanswered

December 2012

Comments? infodev@avaya.com
Replacing Field Units for the Avaya S8300D Server with G450 or G430 Branch Gateway  December 2012

ManUFACTURER’S PORT IDENTIFIER | FIC CODE | SOC/REN/A.S. CODE | NETWORK JACKS
--- | --- | --- | ---
Off Premises Station | OL13C | 9.0F | RJ2GX, RJ21X, RJ11C
DID Trunk | 02RV2.T | AS.2 | RJ2GX, RJ21X, RJ11C
CO Trunk | 02GS2 | 0.3A | RJ2GX, RJ21X, RJ11C
Tie Trunk | TL31M | 9.0F | RJ2GX
Basic Rate Interface | 02IS5 | 6.0F, 6.0Y | RJ49C
| 04DU9.1K | 6.0F | RJ48C, RJ48M
| 04DU9.1S | 6.0F | RJ48C, RJ48M
120A4 Channel Service Unit | 04DU9.D | 6.0Y | RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier’s Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC’s Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numerique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent matériel est conforme aux specifications techniques applicables d’Industrie Canada.

European Union Declarations of Conformity


Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment
(VCCI). If this equipment is used in a domestic environment, radio
disturbance may occur, in which case, the user may be required to take
corrective actions.

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary
Control Council for Interference from Information Technology
Equipment (VCCI). If this is used near a radio or television receiver in
a domestic environment, it may cause radio interference. Install and
use the equipment according to the instruction manual.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya

Contact Avaya Support

See the Avaya Support Web site: http://support.avaya.com for product
notices and articles, or to report a problem with your Avaya product.
For a list of support telephone numbers and contact addresses, go to
the Avaya Support Web site: http://support.avaya.com, scroll to the
bottom of the page, and select Contact Avaya Support.
### Contents

**Chapter 1: Introduction**
- Purpose........................................................................................................................................... 9
- Intended audience............................................................................................................................ 9
- Related resources............................................................................................................................. 9
  - Documentation............................................................................................................................. 9
  - Avaya Mentor videos................................................................................................................... 10
  - Support....................................................................................................................................... 11
  - Warranty..................................................................................................................................... 11

**Chapter 2: S8300D server or S8300D hard drive**
- Prerequisites for replacing S8300D server or S8300D hard drive.................................................... 13
- Replacing the S8300D server........................................................................................................... 15
- Replacing the S8300D hard drive..................................................................................................... 16
  - S8300D hard drive....................................................................................................................... 18
  - Backing up the data....................................................................................................................... 18
  - Configuring the S8300D server..................................................................................................... 19

**Chapter 3: G450 and G430 branch gateways**
- Prerequisites for replacing the G450 or G430 branch gateway......................................................... 21
- Replacing the G450 or G430 branch gateway................................................................................... 22
- Backing up the branch gateway VAL announcements...................................................................... 26
- Configuring basic branch gateway connectivity................................................................................ 27
- Restoring announcement files......................................................................................................... 28
- Provisioning the new branch gateway............................................................................................... 29
- Setting up a TFTP server................................................................................................................ 29
  - Installing firmware using the TFTP server.................................................................................... 30

**Chapter 4: Media and expansion modules**
- List of media modules...................................................................................................................... 33
- Replacing the Avaya media modules................................................................................................. 34
- Avaya expansion modules................................................................................................................ 35

**Chapter 5: Supported CD/DVD ROM drives**
- Panasonic Digistor.......................................................................................................................... 37
- Sony.................................................................................................................................................. 37
- Addonics.......................................................................................................................................... 38
  - Connecting the CD/DVD ROM drives to the server...................................................................... 38

**Index**............................................................................................................................................. 39
Chapter 1: Introduction

Purpose

This document provides procedures to replace the field units for the Avaya S8300D server with the G450 and G430 branch gateways.

Intended audience

The primary audience for this document is:

- Avaya field technicians
- Avaya partners
- Technical support personnel
- Solution Architects
- Implementation Engineers
- Support Personnel
- Technical support representatives
- Authorized Business Partners

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.
Introduction

<table>
<thead>
<tr>
<th>Document number</th>
<th>Title</th>
<th>Use this document to:</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing</td>
<td></td>
<td>This document provides the process and procedures for upgrading Avaya Aura® Communication Manager.</td>
<td>Avaya field technicians, Avaya partners, Technical support personnel, Solution Architects, Implementation Engineers, Support Personnel, Technical support representatives, Authorized Business Partners</td>
</tr>
<tr>
<td>03-603560</td>
<td>Upgrading to Avaya Aura® Communication Manager Release 6.2</td>
<td>This document provides information on hardware currently supported by Avaya Aura® Communication Manager.</td>
<td>Avaya field technicians, Avaya partners, Technical support personnel, Solution Architects, Implementation Engineers, Support Personnel, Technical support representatives, Authorized Business Partners</td>
</tr>
<tr>
<td>555-245-207</td>
<td>Avaya Aura® Communication Manager Hardware Description and Reference</td>
<td>This document provides information on hardware currently supported by Avaya Aura® Communication Manager.</td>
<td>Avaya field technicians, Avaya partners, Technical support personnel, Solution Architects, Implementation Engineers, Support Personnel, Technical support representatives, Authorized Business Partners</td>
</tr>
</tbody>
</table>

Avaya Mentor videos

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

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

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

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

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under Help & Policies > Policies & Legal > Warranty & Product Lifecycle. See also Help & Policies > Policies & Legal > License Terms.
Introduction
Chapter 2: S8300D server or S8300D hard drive

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. For the product correction notices, go to the Avaya Support website at http://support.avaya.com/.

For information about replacing the S8300A server to S8300D server, see Upgrading Avaya Aura® Communication Manager, 03-603560.

Prerequisites for replacing S8300D server or S8300D hard drive

Procedure

1. Determine the configuration of the existing server.
2. If the existing server runs the CM_onlyEmbed template, determine if:
   a. The server runs Communication Manager Messaging.
   b. Utility Services supports the phone firmware download function.
3. If the existing server runs the CM_SurvRemoteEmbed template, determine if the server runs Session Manager.
4. Determine if Communication Manager has the Unicode Phone Message files installed.
   If Utility Services supports phone firmware download function and the System Platform backup is unavailable, or if the existing server utilizes Services VM with SAL gateway enabled and the System Platform backup is unavailable, go to step 5.
5. Determine whether you can create the backup files for the S8300D server or S8300D hard drive procedure. If you cannot create the files, use the existing customer backup files.
6. 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 alternatives to the preferred backup sets:

- Communication Manager full backup or backup of translation files.
- Utility Services 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.

7. If the existing server is functional, perform the System Platform backup which contains the server configuration for System Platform, Communication Manager, BSM and Utility Services. The System Platform backup does not contain the server configuration for Communication Manager Messaging.

8. If the existing server is functional, perform Communication Manager Messaging backup.

9. Ensure that you have the software versions for the following:

- Avaya Aura® System Platform
- Avaya Aura® Communication Manager
- Communication Manager Messaging
- Services VM
- Utility Services
- Branch Session Manager

10. Download the current license file and authentication file from the PLDS website. The license file must be associated with the serial number of the gateway in which the defective hardware resides.

11. 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.

12. Determine whether software service packs and firmware files are required.

13. If the service pack is required, download the service pack and save it on your laptop.

14. If the hardware is functional, connect your laptop to the services port on the server.
15. On the System Platform home page, select **cdom**.

16. Click **Server Management**.

17. If the system does not display the System Platform home page, perform the following steps to determine whether 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.
   c. If you still face problems while gaining access to the page, then the hardware is not functional.

   **Warning:**
   Turning the server off can cause service outage.

18. Back up the data.

   For more information about backing up the data, see *Backing up the data*.

---

**Related topics:**

[Backing up the data](#) on page 18

---

## Replacing the S8300D server

**Procedure**

1. Shut down the server by using one of the following methods:
   a. On the System Platform home page, click **Server Management > Server Reboot/Shutdown**. Click **Shutdown Server**.
   b. On the server faceplate, press the **Shutdown** 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.

5. Insert the System Platform software media.

6. Completely insert the server in the gateway slot and secure the server faceplate with the thumb screws.

7. Tighten the thumb screws.
8. Turn on the gateway, if you had turned it off earlier.
9. Connect your laptop to the services port on the server.
10. Configure the S8300D server.

   For more information about configuring the S8300D server, see Configuring the S8300D server.

---

Related topics:
Configuring the S8300D server on page 19

---

ReReplacing the S8300D hard drive

About this task
Use the following procedure to replace 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.

Procedure

1. Shut down the server by using one of the following methods:
   b. On the server faceplate, press the Shutdown 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. To remove the S8300D server, perform the following steps:
   a. From the server, remove the two screws that are attached to the hard drive standoffs. See Figure 1: S8300D hard drive.
   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. Before screwing the standoffs into the new hard drive, clean the threads thoroughly with a damp cloth or paper towel.
4. Before completely inserting the server into the appropriate slot of the gateway, connect the USB CD/DVD drive to the server.

5. Insert the System Platform software media.

6. Completely insert the server in the gateway slot and secure the server faceplate with the thumb screws.

7. Tighten the thumb screws.

8. Turn on the gateway, if you had turned it off earlier.

9. Connect your laptop to the services port on the server.

10. Configure the S8300D server.

    For more information about configuring the S8300D server, see Configuring the S8300D server.

Related topics:

S8300D hard drive on page 18
Configuring the S8300D server on page 19
S8300D server or S8300D hard drive

S8300D hard drive

Figure 1: S8300D hard drive

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>S8300D server</td>
</tr>
<tr>
<td>2</td>
<td>Hard drive</td>
</tr>
<tr>
<td>3</td>
<td>Hard drive standoffs</td>
</tr>
<tr>
<td>4</td>
<td>Hard drive mounting screws</td>
</tr>
<tr>
<td>5</td>
<td>Hard drive connector</td>
</tr>
</tbody>
</table>

Backing up the data

Procedure

Configuring the S8300D server

Procedure

1. Install System Platform from the DVD.
   The server reboots after installation.
2. If required, install the System Platform patches and Services VM patches.
3. Use the services laptop or a network connection to gain access to the System Platform home page.
4. Enter the configuration data into the server during template installation.
5. If the server is configured as Main Server, install the CM_onlyEmbed template.
6. If the server is configured as Survivable Remote Server, install the CM_SurvRemoteEmbed template.
7. If required, install the Communication Manager service pack, the BSM service pack and patch, and the Utility Server service pack.
8. If the System Platform backup is available, perform the following steps:
   a. Restore the System Platform data.
   b. If the S8300D server was replaced, you must install an updated license file and authentication file.
   c. If you replaced the disk and are reusing the S8300D server, you do not have to reinstall the license and authentication file.
9. If the System Platform backup is unavailable, perform the following steps:
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 clicking **Shutdown Server** on the Communication Manager Web page or by clicking **Manage** on the System Platform Web page.

10. If required, install the Communication Manager Messaging service pack.

11. If required, restore the Communication Manager Messaging data that includes translations, names, and messages.

12. If required, restore the Communication Manager Messaging announcements.


15. Check for any new alarm and resolve the alarm.

16. Test as appropriate.
   For example, make station and trunk calls.

17. 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.

18. Activate alarm origination.

19. At the server command line, type `almenable -d b -s y` and press Enter.

20. Type `almenable` without any options and press Enter to verify that alarm origination is active.

21. Log off from the system.
Chapter 3: G450 and G430 branch gateways

This chapter describes the procedures to replace an existing G450 or G430 branch gateway with a new G450 or G430 branch gateway. You must replace a G450 or G430 branch gateway in the following cases:

- You cannot log in to the gateway.
- The gateway does not register with its primary controller.
- The gateway reboots repeatedly.
- The VoIP module on the gateway motherboard does not work.

Prerequisites for replacing the G450 or G430 branch gateway

Ensure that an installed S8300D server and any installed media modules are reused in the new branch gateway.

The customer-provided LAN must be available to connect to:

- The primary controller of the branch gateway if the primary controller is remote.
- The TFTP server to back up the branch-gateway configuration files and .dat files and to install new firmware.

Use the Utility server application on System Platform for staging gateway firmware installation. See Installing firmware using the TFTP server.

- The FTP server to back up the branch-gateway VAL announcements.

The Branch Gateway Processor configurations must be valid. The IP addresses on the customer LAN must be available for the following:

- Branch Gateway Processor (BGP)
- VoIP engine on the branch gateway motherboard (voip-v0)
- Primary controller (S8300D, S8510, S8800, HP ProLiant DL360 G7 1U, or Dell™ PowerEdge™ R610 1U)
- Survivable remote servers
- FTP and TFTP server
You can use the Avaya Gateway Installation Wizard for the initial configuration of the new branch gateway as well as the upgrade of firmware. The Gateway Installation Wizard application must be installed on the laptop of the technician.

The technician must be familiar with the procedures to connect and gain access to the G450 or G430 branch gateway and the S8300D server.

---

### Replacing the G450 or G430 branch gateway

**Before you begin**

1. Obtain the IP addresses of the primary controller and the survivable remote servers in the network. The primary controller can be an S8300D, an S8510, an S8800, an HP ProLiant DL360 G7 1U, or a Dell PowerEdge R610 1U server.

2. Obtain the IP addresses and subnet masks of the Branch Gateway Processor (BGP) on the branch gateway that has to be replaced and the default gateway IP address on the LAN of the customer.

3. Obtain the IP address of a computer on the customer LAN that must be set up as a TFTP server.
   
   For instructions on setting up a TFTP server, see *Setting up a TFTP server*.

4. Check the media modules that are installed on the branch gateway. You can use the branch gateway to check the media modules. Alternatively, you can log in to the SAT interface of the primary controller and run the display media-gateway number command.

5. Download the most recent versions of firmware for each device in the branch gateway, including the BGP and the media modules, and save them on your laptop.

   **Note:**
   
   The branch gateway or media module firmware must be compatible with the version of the Avaya Aura® Communication Manager software on the primary controller.

6. Obtain access to the primary controller.

   If the primary controller is the S8300D server in the G450 or G430 branch gateway, use a direct connection from the NIC card of your laptop to the services port on the server. For example, you can configure your laptop with the static IP address 192.11.13.5.

   If the primary controller is at a remote location, gain access to the primary controller over the LAN. The customer should provide a computer connected to the LAN for this purpose. Alternatively, you can contact someone who has access to the primary
controller and ask the contact person to administer a new serial number on the change media-gateway <gateway-number> SAT screen of the primary controller.

**Procedure**

1. Use your laptop to gain access to the branch gateway through a direct serial connection and the primary controller through a direct connection or over the LAN. You will have to alternate between these two connections several times.

2. If the branch gateway is functional, connect your laptop to the console port on the branch gateway with a serial cable.

3. If the primary controller is local, use a crossover cable to connect your laptop to the services port on the server.
   If the primary controller is at a remote location, connect the LAN to the primary controller on the customer computer.

   **Note:**
   If the primary controller is an S8510, an S8800, an HP or a Dell server on a G450 or G430 branch gateway that is not being replaced, do not save translations at this point.

4. If the primary controller is an S8300D server and the branch gateway has to be replaced, save translations by using the SAT interface. Verify that the translations are saved successfully.

5. Back up the branch gateway configuration files to a TFTP server. The TFTP server must be on the customer LAN, and the branch gateway must be connected to the LAN through one of the Ethernet ports, EXT1 or EXT2.

6. To open the SSH interface to the branch gateway, log in with your user name and password. The user name and password are provided by the system administrator.

7. At the CLI prompt, type `copy running-config tftp`.

8. If gateway announcements are present on the branch gateway, back up the branch gateway VAL announcements. See *Backing up the branch gateway VAL announcements*.

9. Ensure that all cables connected to the branch gateway and media modules are adequately marked for later reinstallation in the same location.

10. Turn off the server and the branch gateway.

11. Remove the old branch gateway from the rack and insert the new branch gateway.

12. Transfer the media modules and the server from the old branch gateway to the new branch gateway, maintaining the original slot locations.

13. Reconnect cables in the same location.
14. Configure basic branch gateway connectivity. See Configuring basic branch gateway connectivity.

15. To restore the configuration backup files:
   a. At the MGP prompt, type `copy tftp start-up config`.
   b. To check the status, type `show download status`.
   c. To reset the BGP, type `reset`.

16. To assign IP addresses to VoIP resources, type `set interface voip <number><ip address>` where `<number>` is the slot number of the VoIP media module. The slot v0 designates the VoIP resource resident on the branch gateway motherboard. The MM760 VoIP Media Modules are designated according to the slot. For example, slots v1, v2, v3, and v4 are the slots in which the media module has been installed. `<ip address>` is the IP address of the VoIP resource. For example: `set interface voip v0 132.236.73.3`.

17. To assign the controller list for the branch gateway if the existing branch gateway is not functional, type the following commands to designate the primary, secondary, and survivable remote server controllers for the branch gateway:
   - `clear mgc list`
   - `set mgc list <ip address> [,<ip address> [,<ip address> [,<ip address>]]]`
   where, the first `<ip address>` is the IP address of the primary controller for the branch gateway.

   **Note:**
   To change the mgc list, run `clear mgc list` before you designate the primary, secondary, and survivable remote server controllers.

   The following table describes the possible alternate controllers for an S8300, S8500, S8700, and S8710 primary controller:

<table>
<thead>
<tr>
<th>Primary server</th>
<th>Controller IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>S8300D</td>
<td>First: The IP address of the S8300D primary controller. Next three: One, two, or three IP addresses of the S8300D servers configured as survivable remote servers.</td>
</tr>
<tr>
<td>S8510, S8800, HP ProLiant DL360 G7 1U, or Dell PowerEdge R610 1U</td>
<td>First: The IP address of the C-LAN/PE for the S8510, S8800, HP ProLiant DL360 G7 1U, or Dell PowerEdge R610 1U. Next three: One, two, or three IP addresses of alternate C-LANs or survivable remote servers or both.</td>
</tr>
</tbody>
</table>

18. Set the survivable remote server transition points if the existing branch gateway is not functional. If a network problem occurs:
   a. Type `set mgp reset-times primary-search <search-time>` where `<search-time>` is the time in minutes that the branch gateway searches for a
primary controller before looking for a survivable remote server. You can enter 1 through 60 minutes.

b. Type `set mgp reset-times total-search <search-time>` where `<search-time>` is the time in minutes that the branch gateway searches for both primary controllers or survivable remote servers. You can enter 1 through 60 minutes.

c. Type `set mgp reset-times transition-point <#_of_primary>` where `<#_of_primary>` is the number of primary controllers in the controller list. If the primary controller is an S8510, S8800, HP ProLiant DL360 G7 1U, or Dell™ PowerEdge™ R610 1U server, the range is from 1 through 4. If the primary controller is an S8300D server, `<#_of_primary>` must be 1.

19. Reconnect to the primary server.

20. Restore the announcement files. See Restoring announcement files.

21. Reconnect to the branch gateway.

22. Determine which firmware to install on the branch gateway. Compare software versions running on the branch gateway processors and media modules with the versions that you downloaded from the Avaya Support website. If the versions do not match, installing new firmware for those components is necessary.

23. Install new firmware as appropriate. Use the TFTP server to stage the firmware. See Installing firmware using the TFTP server.

   If you cannot use the TFTP server to stage the firmware, configure a TFTP server on a personal computer connected to the customer LAN. See Setting up a TFTP server.

24. Provision the new branch gateway. See Provisioning the new branch gateway.

25. Save translations on the primary controller.

26. Test as appropriate. For example, make station calls from or to the replaced branch gateway, check for and resolve any new alarms.

Related topics:
- Backing up the branch gateway VAL announcements on page 26
- Configuring basic branch gateway connectivity on page 27
- Restoring announcement files on page 28
- Provisioning the new branch gateway on page 29
- Setting up a TFTP server on page 29
- Installing firmware using the TFTP server on page 30
Backing up the branch gateway VAL announcements

Procedure

1. To determine if VAL announcements are present, log in to the SAT command line interface on the primary server, and type the command `list directory board <xx>v9`, where `<xx>` is the number of the branch gateway.

2. To enable the file system, connect to the primary server and start a SAT session.

3. Type `enable filexfer` and press Enter.

4. On the Enable File Transfer screen, enter your login and password. The login must contain three to six alphanumeric characters, and the password must contain seven to eleven characters and at least one number.

5. In the Reenter Password field, type the password that you created in Step 4.

6. In the Secure field, type `n` for FTP and `y` for SFTP.

7. In the Board address field, type `<nnn>v9`, where `<nnn>` is the administered branch gateway number.

8. Log in to a computer connected to the customer LAN. Use this computer as an FTP client to temporarily store the VAL announcements.

9. Copy the existing announcement files from the branch gateway to the FTP client.

10. Type `ftp <ip-address>` where `<ip-address>` is the IP address of the BGP on the branch gateway.

11. Type the ftp user name.

12. Type the ftp password.

13. Type bin to change to the binary mode.

14. Type `dir` to view the contents of the /annv directory.

15. Type `get filename.wav` where `filename` is the file name of the announcement file that you have to back up.

   The `get` command copies the announcement file to the directory from where you initiated the FTP session on the FTP client.

16. Repeat the `get` command for each announcement file you have to back up.

17. Type `bye` to close the FTP session.
Configuring basic branch gateway connectivity

Procedure

1. Set up a laptop with SSH client software.
2. In the IP address field of the TCP/IP Properties window, type 192.11.13.5.
3. In the Subnet mask field, type 255.255.255.252.
4. Disable DNS service.
5. Disable WINS Resolution.
6. Use an Ethernet cable to connect the laptop to the branch gateway services port.
7. Use SSH to connect to 192.11.13.6.
8. At the prompt, type root as the default user name and rootroot0 as the default password.
9. Configure a new password.
10. At the prompt, type y to configure basic gateway connectivity.

Note:
If you have not saved the configuration changes, you can use the script-config CLI command to run the installation script.

11. If you have not saved any configuration changes, use the script-config CLI command to run the installation script.

The system prompts you to configure the following parameters:

- VLAN number
- IPv4 enabled or disabled
- IPv4 address for the primary management interface
- IPv4 subnet mask for the primary management interface
- IPv4 address for the default gateway (router)
- IPv6 enabled or disabled
- IPv6 unicast global address
- IPv6 prefix length
- IPv6 link local address
- IPv6 PMI (Global or Link Local)
- IPv6 default gateway
G450 and G430 branch gateways

- Eight IP addresses (four IPv4 and four IPv6) to specify the media gateway controllers
- Hostname for the branch gateway

For each parameter, leave the default value or enter a new value. The system displays the settings you configured and the confirmation dialog box.

12. If you confirm the settings, the system saves the settings, and the branch gateway reboots.
   If you do not confirm the settings, the system prompts you to reconfigure the parameters. If you enter y, the system displays the parameters for configuration.

13. To enable remote access to the gateway, connect the Ethernet port to the network.

---

Restoring announcement files

Procedure

1. To enable the file system, connect to the primary server and start a SAT session.
2. Copy the backed-up announcement files from the FTP client to the branch gateway.
3. Type `ftp ip-address` where `ip-address` is the IP address of the BGP.
4. Type the ftp user name.
5. Type the ftp password.
6. Type `bin` to change to the binary mode.
7. Type `dir` to view the contents of the /annc directory.
8. Type `put filename.wav` where `filename` is the name of the announcement file that you have to restore.
9. The `put` command copies the announcement file from the FTP client to the /annc directory on the branch gateway.
10. Use the `put` command to restore each announcement file that you backed up.
11. Type `bye` to close the FTP session.
Provisioning the new branch gateway

Procedure

1. On the primary controller, open a SAT session.
2. Type `change media-gateway mg-number` where `mg-number` is the number assigned to the branch gateway.
3. Type the serial number of the new branch gateway in the **Identifier** field and click **Submit**.
4. To verify that the new branch gateway has registered with Communication Manager, open a SAT session and type `list media-gateway`.
5. The **Registered** column must display `y` for the new branch gateway.

Setting up a TFTP server

**About this task**

The following instructions describe how to configure a Windows-based computer as a TFTP server. A TFTP server is needed for the `copy tftp` commands, which back up the configuration files and install firmware on the branch gateway. The TFTP server can be on any computer that can be networked to a branch gateway.

**Procedure**

1. Create a directory in which you will copy the branch gateway configuration files or load the firmware image files. For example, `C:\tftpboot`.
2. Go to the Avaya Support website at [http://support.avaya.com/](http://support.avaya.com/) and select **Downloads**.
3. Select **4600 Series IP Telephones**.
4. Scroll down the list of **Software Downloads** to recent posting. For example, 4601/... IP Telephone Release 111004 and TFTP Server (November 2012).
5. Search for `iptel_avaya_tftp.exe`.
6. Click the program and download it.
7. Download the `iptel.pdf` file, which provides instructions on installing `iptel_avaya_tftp.exe` on Windows systems.
8. Go to the directory containing the iptel_avaya_tftp.exe file. Double-click the file name and follow the installation wizard instructions to install the file.
   The default installation directory is `C:\Program Files\Walusoft\TFTPSuite`. You can change the default installation directory.

9. Go to the directory where the TFTP software is installed and double-click the program `tftpserver32.exe`.
   The system displays the TFTP Server screen. The upper section of the screen displays the IP address of the computer and port 69.

10. To enable the TFTP server, click **Menu > System > Setup**.
    The system displays the Server option screen.

11. Click the **Outbound** tab and type the path to the location of the tftp directory that you created in the Outbound file path screen.

12. Click the **Inbound** tab and enter the path of the tftp directory that you created in the Inbound file path screen.

13. In the **Options** tab, type 69 in the **Use Port** field.

14. Select **No Incoming**.
    If you want to copy files as a backup prior to performing an upgrade of software, do not select this field.

15. Click **OK**.

   **Note:**
   To use the TFTP server, double-click the program `tftpserver32.exe`. Select **File > Start Serving**. You can turn the program off by selecting **Stop Serving**.

---

**Installing firmware using the TFTP server**

**About this task**

The TFTP server is used to install firmware files on gateways and media modules. For the latest firmware files for gateways and media modules, go to the Avaya Support website at `http://support.avaya.com/`.

To install firmware files, you must use the TFTP server capability of Utility Services. Utility Services is available in all Communication Manager templates other than CM_Duplex.

**Procedure**

1. On the Utility Services Web console, click **Utilities > Utility Admin**.
2. In the left navigation pane of the Utility Admin page, click **Upload Gateway firmware > Display Firmware Directory**.
   The system displays the firmware versions that are available on Utility Services.
3. If the required firmware version is unavailable on Utility Services, download the firmware file from the Web.
4. In the left navigation pane of the Utility Admin page, click **Miscellaneous > Upload Files**.
5. Browse to the downloaded firmware file and select the firmware file.
6. Click **Upload File**.
   The file is uploaded to Utility Services.
7. Check the Display Server Firmware page to ensure that the firmware file is uploaded.
G450 and G430 branch gateways
Chapter 4: Media and expansion modules

List of media modules

The following table lists the necessary information that you require to order and replace the media modules.

Table 1: List of media modules

<table>
<thead>
<tr>
<th>Media modules</th>
<th>Material code</th>
<th>Apparatus code</th>
<th>Material ID (required for maintenance ordering only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1/E1</td>
<td>170900</td>
<td>MM710</td>
<td>700221161R</td>
</tr>
<tr>
<td>DEF DS1 Loopback Jack 700A (used for remotely troubleshooting the T1/E1 media modules)</td>
<td>107988867R</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>DCP</td>
<td>170898</td>
<td>MM712</td>
<td>700221153R</td>
</tr>
<tr>
<td>BRI</td>
<td>170898</td>
<td>MM720</td>
<td>70221138R</td>
</tr>
<tr>
<td>Analog Station/Trunk Module</td>
<td>170899</td>
<td>MM711</td>
<td></td>
</tr>
</tbody>
</table>
A media module needs to be replaced in case of:

- A damaged media module
- A change in the media module type

The modules on the branch gateway are not inserted until the branch gateway registers with Avaya Aura® Communication Manager. Similarly, all media modules and the associated maintenance objects are removed if the branch gateway link stops working. The term board insertion process refers to the process in which the media modules are queried for their type, suffix, and vintage. Use the `list config all` and the `list config media-gateway number` commands to obtain this information. Any media module that does not agree with administration generates a process error and is flagged to the relevant administration screen. The removal of the media modules is detected. Branch gateway circuit packs list the relevant slot location as no board. You can download the T1/E1 modes of operation for the DS1 media modules because the DS1 media module can function as either a T1 or an E1 interface. After replacing the media module, the modules are registered with the branch gateway, where board type, suffix, and vintage are verified. The branch gateway then sends H.248 messages to the controller and creates Communication Manager objects.

**Caution:**

Be careful while aligning and inserting the connector pins.

**Caution:**

Separate the ESD paths to the chassis ground connected to the media modules at the spring-loaded captive screws. Ensure that the captive screws are securely tightened to prevent damage to the equipment.

---

**Replacing the Avaya media modules**

**Procedure**

1. Identify and mark all cables.
2. Remove the cables.
3. Loosen the captive screws and slide out the old media module.
4. Position the media module squarely before the selected slot on the front of the branch gateway chassis and engage both the sides of the module in the interior guides.
5. Slide the module slowly into the chassis. Maintain an even pressure and ensure that the module does not twist or misalign. See the *Inserting media modules* figure.

6. Apply firm pressure to engage the connectors.
   The media module connector has pins of varying lengths. The long pins engage first to provide grounding. The medium length and short pins provide power and signal.

7. Lock the media module into the chassis by tightening the spring-loaded captive screws on the front of the module.

8. Plug in the cables in the correct order.

---

**Avaya expansion modules**

You can optionally extend the G430 by attaching one or two EM200 expansion modules to the branch gateway. Since the cables attaching the EM200 expansion modules to the branch gateway are short, you must install the branch gateway and the expansion modules directly above or below each other. For more information on the EM200 expansion module, see *Installation and Upgrades for the Avaya Branch Gateway G430*, 03-603233.
Media and expansion modules
Chapter 5: Supported CD/DVD ROM drives

This chapter describes the supported CD/DVD ROM drives that technicians must use to install software on the Avaya S8300D server. The CD/DVD drives supported on the S8300D server are:

- Panasonic Digistor
- Sony
- Addonics

Panasonic Digistor

You can purchase Avaya-approved Panasonic Digistor models 73082 or 73322 (Comcode: 700406267).

Instead of AC power, the Panasonic Digistor drives use lithium-ion battery for additional power. USB 2.0 readers draw more power than the standard USB ports from the S8300D server. The Digistor drive contains an internal lithium-ion battery that makes up the current difference between what the USB port can provide and what the CD/DVD ROM drive requires.

Ensure that the internal lithium-ion battery is fully charged for the drive to operate properly. When the lithium-ion battery is depleted and the drive attempts to operate, the red LED on the case turns on and the screen displays the failed to mount cdrom message. The red LED is not bright so careful observation is required. The lithium-ion battery can be charged by plugging the CD/DVD ROM drive in a USB port for approximately 30 minutes. The lithium-ion battery charges faster if the ON/OFF switch is OFF. To preserve the battery, keep the ON/OFF switch in the OFF position until you are ready to use the Digistor drive.

Note:
The functionality of the internal lithium-ion battery charging the drive is only applicable with the original CD/DVD ROM drive.

Sony

The DRX-S70U-W model of SONY CD/DVD rewritable drive is unavailable through Avaya. The drive requires 5.2 V DC and comes with an AC power adapter.
Addonics

The AEPDVRWII824 model of Addonics CD/DVD reader is unavailable through Avaya. You must place the CD/DVD ROM drive on a surface within 5 degrees of level. The Addonics CD/DVD reader requires AC power to operate. You must set the power switch to EXT for the CD/DVD reader to operate.

Connecting the CD/DVD ROM drives to the server

Procedure

1. On an Addonics drive, plug one end of the power cord into the drive and the other end into an electrical outlet.
2. Set the power switch to EXT (Addonics) or to ON (Panasonic).
3. Connect the USB cable to the USB port on the server faceplate and the other end of the USB cable to the CD/DVD drive.
4. Place the media into the external CD/DVD drive.
Index

A
Addonics .........................................................38
Avaya expansion modules ..............................35
Avaya Mentor videos ......................................10

B
Backing up the branch gateway VAL announcements 26
Backing up the data ...........................................18

C
Configuring basic branch gateway connectivity ....27
Configuring the S8300D server ..........................19
Connecting the CD/DVD ROM drives to the server ...38

G
G430 Branch Gateway .......................................21
G450 Branch Gateway .......................................21

I
Installing firmware using the TFTP server ..........30
Intended audience ............................................9

L
legal notice .....................................................2

M
Media modules ................................................33

P
Panasonic Digistor ..........................................37
Prerequisites for replacing S8300D server or S8300D hard drive .............................................13
Prerequisites for replacing the G430 branch gateway 21
Prerequisites for replacing the G450 branch gateway 21
Provisioning the new branch gateway ..................29
Purpose ................................................................9

R
related documentation .......................................10
related resources .............................................10
   Avaya Mentor videos .....................................10
Replacing the Avaya media modules ..................34
Replacing the G430 branch gateway ....................22
Replacing the G450 branch gateway ....................22
Replacing the S8300D hard drive .........................16
Replacing the S8300D server .............................15
Restoring announcement files ............................28

S
S8300D hard drive ...........................................18
S8300D server or S8300D hard drive .................13
Setting up a TFTP server ..................................29
Sony ....................................................................37
   support .........................................................11
      contact .....................................................11
Supported CD/DVD ROM drives .......................37

V
videos ................................................................10
   Avaya Mentor ...............................................10

W
Warranty .........................................................11