Installation and Upgrade for the Avaya G250 Media Gateway

03-300434
Issue 1.1
June 2005

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

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

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

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

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. 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 to/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.

Standards Compliance

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.

Product Safety Standards

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

Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) – Part 3-3: Limits – Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

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 when the equipment is operated 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.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder 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.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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 G250 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

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. 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.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

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	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G250, G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) 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. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

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. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

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://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

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://www.avaya.com/support.

Japan

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.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

About this book

Overview

Installation of the Avaya G250 Media Gateway describes how to:

- Physically install the Avaya G250 Media Gateway
- Establish remote connectivity to the G250 via a modem
- Perform a basic initial configuration of the G250
- Upgrade G250 hardware and firmware
- Upgrade software for an Avaya S8300B Media Server installed in a G250

Audience

This book is for the following audiences:

- Trained field installation personnel
- Technical support personnel
- Network engineers and technicians
- Authorized business partners

Downloading this book and updates from the Web

You can download the latest version of *Installation and Upgrades for the Avaya G250 Media Gateway* from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You can also download these updates from the Avaya Web site.

Downloading this book

To download the latest version of this book:

1. Access the Avaya web site at http://www.avaya.com/support.
2. On the left side of the page, click **Product Documentation**.

   The system displays the Welcome to Product Documentation page.
3. On the right side of the page, type TBA and click **Search**.

   The system displays the Product Documentation Search Results page.
4. Scroll down to find the latest issue number, and click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:
   - **PDF Format** to download the book in regular PDF format.
   - **ZIP Format** to download the book as a zipped PDF file.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

CAUTION:

A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

WARNING:

A warning statement calls attention to a situation that can result in harm to hardware or equipment. A warning can also indicate the presence of a hazard that could cause personal injury if the hazard is not avoided by following the instructions provided.

DANGER:

A danger statement indicates the presence of a hazard that can result in severe personal injury or death if the hazard is not avoided by following the instructions provided.

ELECTROSTATIC ALERT:

An ESD warning calls attention to situations that can result in ESD damage to electronic components.

SECURITY ALERT:

A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

Related resources

For more information on the Avaya G250 Media Gateway and related features, see the following books:

Title	Number
Overview of the Avaya G250 Media Gateway	
Quick Start for Hardware Installation for the Avaya G250 Media Gateway	
Administration of the Avaya Branch Media Gateways	
Avaya Branch Media Gateway CLI Reference	
Avaya Branch Media Gateway Glossary	
Maintenance of the Avaya Branch Media Gateways	

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya Technical Consulting Support System at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer.

Trademarks

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.

  Product Documentation Group

  Room B3-H13

  1300 W. 120th Ave.

  Westminster, CO 80234 USA
- E-mail, send your comments to:

  document@avaya.com
- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, *Installation and Upgrades for the Avaya G250 Media Gateway, TBA*.

Chapter 1: Introduction

This guide explains how to install and upgrade the Avaya G250 Media Gateway and contains the following chapters:

- Chapter 2: Before you install. Describes how to prepare for an installation of the G250.
- Chapter 3: Installing the Avaya G250 Media Gateway. Describes how to install the G250 chassis and media modules, install ground conductors and connect power to the G250.
- Chapter 4: Connecting devices. Describes how to connect data and voice devices to the G250.
- Chapter 5: Connecting and enabling a modem for remote access. Describes how to connect a modem to the G250 to enable remote access.
- Chapter 6: Configuring the G250. Describes how to configure the G250.
- Chapter 7: After installation. Describes how to test an installation of the G250.
- Chapter 8: Upgrading media modules and devices. Describes how to add media modules and devices to a G250 that is already installed.
- Chapter 9: Upgrading the Avaya Communication Manager software. Describes how to upgrade the Avaya Communication Manager software that runs on the S8300B media server.
- Chapter 10: Upgrading the G250 firmware. Describes how to upgrade the G250 firmware.
- Chapter 11: Upgrading IP phone configuration and firmware files. Describes how to upgrade software and firmware on IP phones.
- Chapter 12: Troubleshooting. Provides basic troubleshooting information.
- Appendix A: Front panel description. Describes the G250 chassis front panel.
- Appendix B: Technical specifications. Provides the technical specifications of the G250.
- Appendix C: Running the Avaya Installation Wizard (Avaya IW). Describes the Avaya Installation Wizard, which configures a G250 with an S8300B.
- Appendix D: Running the Gateway Installation Wizard (GIW). Describes the Gateway Installation Wizard which configures a G250 without an S8300B.

Chapter 2: Before you install

Read this chapter carefully before you begin the installation. If you are installing the G250 at a customer site, read this chapter before going to the customer site.

This chapter includes:

Before going to the site

Before going to the site, work through the following sections to prepare required information and equipment.

Read the planning documentation

Before you begin the installation, read the planning documentation.

The planning documentation provides you with information about:

- What media modules you will be installing. Take note of whether or not you are installing an S8300B Media Server module. The installation process is different depending on whether or not you are installing an S8300B.
- Which voice devices and data devices need to be connected to the G250.
- Whom to contact on site about delivery, system questions, or network concerns.
- Whom to contact at your home office in case of questions.
- Whether you need a special pass or an escort.
- How to gain entrance to the installation location if it is locked.
- Where to install equipment.
- Where to find a telephone near the installation location.

Prepare required equipment

You need the following equipment to assist you in the installation:

- One loop start analog trunk for connecting a modem
- A separate telephone line, if needed, for verbal communication during remote configuration

You may also need some of the following equipment for mounting the G250:

- A crosspoint screwdriver if rack mounting or wall mounting the G250
- If you will mount the G250 on a flat wall: screws to fasten the G250 to the wall
- If you will mount the G250 on a non-flat wall:
  - A 365 x 465 mm plywood board (US: 3/4 inch plywood), 20 mm (0.79 in) thick
  - Wood screws to fasten the G250 to plywood
  - Screws to fasten the plywood board to the wall

If you are installing an S8300B media server in the G250, you also need:

- One USB modem. The recommended USB modem is Multitech MultiModemUSB MT5634ZBA-USB-V92.
- One USB CD-ROM drive.
- A laptop computer with internet browser.

If you are not installing an S8300B media server in the G250, you also need:

- A PC on the local network with a CD-ROM drive.
- A laptop computer running Windows XP or Windows 2000 with a serial port recognized by the operating system on the laptop. If the port is recognized, it is listed by the Device Manager.
- A modem to connect to the G250 to enable dial-in configuration. The recommended modem is the serial Multitech MultiModemZBA MT5634ZBA-V-V92.

Obtain the G250 serial number

You will need the serial number for the G250 to create the customer's license file. To get this number, look for the serial number sticker on the back of the G250 chassis. If the unit is delivered directly to the customer and you will not have phone or LAN line access from the customer site to access the rfa.avaya.com web site, this task will require a preliminary trip to the customer site.

Obtain RFA access

Obtain a personal Single Sign-On (SSO) for Remote Feature Activation (RFA) website authentication login before going to the site for installation. You must complete the authentication process before you can be assigned an SSO authentication login.

As a first-time user:

- Business Partners should point their browsers to the Business Partner portal option sales_market, services-voice, training tools and procedures to select RFA (or go directly to: http://rfa.avaya.com).
- Associates should point their browsers to the Avaya Associate portal (or go directly to http://rfa.avaya.com).
- Contractors should point their browsers to Avaya.com (or go directly to http://rfa.avaya.com).

From that point, log into SSO and complete the process to obtain your personal login.

Check license file and Communication Manager versions for a Local Survivable Processor (LSP)

If you are installing an S8300B as a Local Survivable Processor (LSP), the license file for the S8300B must have a feature set that is equal to or greater than that of the media server that acts as primary controller (an S8300B or S8700). This is necessary so that if control passes to the LSP, it can allow the same level of call processing as that of the primary controller.

Additionally, the LSP must have a version of Communication Manager that is identical to that of the primary controller.

The license file requirements of the LSP should be identified in your planning documentation.

Check license file for VPN

If you are installing VPN, obtain a VPN license file from RFA.

Download License and Authentication Files to Your Laptop

To download the customer's license and authentication files to your laptop:

1. Use Windows File Explorer or another file management program to create a directory on your laptop for storing license and authentication files (for example, C:\licenses).
2. Access the Internet from your laptop and go to rfa.avaya.com.
3. Use the System ID or the SAP ID of the customer to locate the license and authentication files for the customer.
4. Check that the license and authentication files are complete.
5. If the files are not complete, complete them. You might need to add the serial number of the customer's G250. See Obtain the G250 serial number on page 20. If any other information is missing, contact your project manager.
6. Use the download or e-mail capabilities of the RFA web site to download the license and authentication files to your laptop.

Run the Automatic Registration Tool (ART) for the RAS IP address

Note:

ART is available only to Avaya associates. Business Partners call 800-295-0099.

The ART tool is a software tool that generates a remote access (RAS) IP address and password, for accessing a product attached to a customer's modem. This IP address is required for configuring remote access to a modem on the S8300B or G250. If you need to configure remote access to both the G250 and the S8300B, follow this procedure twice, once for the G250 and once for the S8300B.

Note:

You must generate a license and authentication file before you use the ART tool. In addition, the ART process is available *only* to Avaya personnel. You need an ART user name and password, which you can set up at the ART web site. Non-Avaya personnel must contact their service support or customer care center for INADS addresses, if required.

To obtain the RAS IP address and password:

1. Access the ART web site on your laptop at http://spiexp1.eng.avaya.com:8000/cgi-bin/ARTexp/ARTgltop.cgi.
2. From the User menu, select **Administer an S8x00, G250, CCS, CVLAN, or ASG Guard II**. The Enter Network Password dialog box appears.

3. Enter your ART user name and password.
4. Click **OK**. The **Start of Installation script & IP Addr Admin** screen appears.
5. In the FL Number field, enter the customer's FL number.
6. In the Session Type field, select **Installation Script Administration**.
7. In the Product Type field, select **G250 MEDIA GATEWAY** if you want to configure remote access for the G250, or **S8300B MEDIA SERVER** if you want to configure remote access for the S8300B.
8. In the INADS field, enter the number of the telephone line to which you will connect the modem.
9. Click **Start Installation script & IP Addr Admin**. ART validates your input and the Customer Validation screen appears.
10. Read the customer information displayed, to check that it is correct.
11. In the Customer Type field, select **Other**.
12. Click **Continue Installation Script Administration**. A product list appears.
13. Click the number of the product for which you are configuring remote access. The G250 MEDIA GATEWAY Installation Script Administration Data screen appears.
14. In the Product Name field, enter the product name.
15. In the INADS Number field, make sure the correct customer provided dial-in number for the G250 Media Gateway appears.
16. Click **Continue Installation Script Administration**. ART generates the RAS IP address and password (CHAP secret key) and generates an installation script for the product. Keep the RAS IP address and password to configure your modem later.
17. Click **Download Installation Script File** to download the installation script to your laptop, or **Email Installation Script File** to have the script emailed to you.

    A script file is created and downloaded or emailed to you.

You can use the installation script to automatically set up an IP address and other alarming parameters.

If the G250 will be configured using Gateway Installation Wizard (GIW) or Avaya Installation Wizard (Avaya IW), and you have an Electronic Planning Worksheet (EPW), enter the ART information contained in the installation script into the EPW (see Obtain the Electronic Preinstallation Worksheet (EPW) on page 24). When you run GIW, you will have the opportunity to import the EPW. The ART information will be imported along with all the other information in the EPW. Alternatively, if the G250 will be configured using the CLI, keep the installation script to run as a CLI command at the configuration stage.

Download recent firmware

Download any recently updated firmware for the G250 and media modules to your laptop. Visit the Avaya support web site to check the latest firmware image file versions against the factory installed versions in the hardware you are installing. Download any firmware image file upgrades you need from the Avaya Support Web site.

Obtain the Electronic Preinstallation Worksheet (EPW)

For greatest efficiency, obtain the Electronic Preinstallation Worksheet (EPW), which is filled in by the customer and Avaya project manager. This worksheet is an Excel spreadsheet from which Avaya configuration wizards automatically pull data to configure and install the S8300B Media Server and the G250 Media Gateway.

Site requirements

Inspect the site before you begin the installation. Verify that the site requirements have been met for adequate environmental conditions, power and grounding availability, safety, and security conditions. If you find discrepancies between the specifications necessary for proper installation of equipment and the conditions on site, contact your project manager before proceeding with the installation.

The G250 may be installed in a 19" rack, mounted on a wall, or placed on a sturdy table. Installation instructions are provided in Chapter 3: Installing the Avaya G250 Media Gateway. The surrounding temperature should be in the range 32° to 104°F (0° to 40°C). The humidity should not be higher than 95%.

Environmental Verification

Verify that temperatures and clearances are within the recommended technical parameters. Consult the table of Technical Specifications in Appendix B: Technical specifications.

WARNING:
Verify that temperature and clearance ranges are within tolerable limits. The thermal sensors may shut down equipment if it is subjected to conditions beyond the recommended limits. Equipment can be damaged if these restrictions are not respected.

Power Verification

Check that an adequate number of power outlets are available. Verify that the G250 Media Gateway and the other equipment in the rack do not present a possible overcurrent or overload to the customer's branch circuit and/or power distribution strip. Power requirements are listed in Appendix B: Technical specifications.

WARNING:
Do not overload the power circuit.

Grounding Verification

The G250 may be installed either by a trained technician or by the customer. Refer to the requirements below for each type of installer:

- Trained Technician: The G250 must be connected to a socket-outlet with a protective earthing connection. The protective earthing in the socket-outlet must be verifired whether the trained technician or a licensed electrician.
- Customer: Ensure that the installation site has access to approved grounds (refer to Approved grounds on page 39). This can be verified by the customer, a trained technician or a licensed electrician. For customer-installed equipment, the G250 must be installed with a Supplementary Ground Conductor. See Connect the safety ground on page 40 for instructions to connect the Supplementary Ground Connector.

Ensure that the installation site has access to approved grounds and that either a trained technician or a licensed electrician will be verifying all grounds and installing the Supplementary Ground Conductor (consult Step 3: Attach ground conductors on page 38).

WARNING:
Installation in a Restricted Access Location and secure access are required in Finland and Norway and Sweden. The G250 must be connected to a reliable earth. Additionally, the Supplementary Ground Connector must be installed. Because of unreliable earthing concerns in Finland, Norway, and Sweden, the G250 Media Gateway must be installed in a Restricted Access Location (RAL). An RAL is defined as an access that can be gained only by trained service personnel or customers who have been instructed about the reasons for the restricted access and any safety precautions that must be taken. In these cases, access to the G250 Media Gateway is gained by the use of a tool (such as a lock and key) or other means of security.

If you have any questions about the safety conditions, contact your project manager. When you have verified that the site is ready for a safe installation, proceed with the installation.

Unpacking

The G250 chassis and accessories are shipped in a box. The package should contain the following items:

- One empty Avaya G250 Media Gateway chassis, with blanking plates over empty module slots.
- One accessories box, containing:
  - One power cord. If the power cord provided does not have the correct plug configuration needed in a particular country, see the power cord specifications in Appendix B: Technical specifications.
  - One flat RJ-45 to RJ-45 cable.
  - One RJ-45 to DB-9 cable adapter.
  - One RJ-45 to DB-25 cable adapter.
  - Two standard mounting brackets.
  - One mounting bracket with cable guides.
  - One Supplementary Ground Conductor.
  - Nine 5/16" flat head screws.
  - Four rubber feet.
- Documentation CD.
- Auto-run CD.
- Release Notes.

Media modules for connecting voice and data devices and outside lines are packaged and shipped in separate boxes. The Avaya Partner Contact Closure adjunct box, if ordered, is also packaged separately.

Before you begin the installation:

1. Unpack the G250 and accessories.
2. Unpack each media module.

   ELECTROSTATIC ALERT:
   Wear an anti-static wrist ground strap whenever handling components of an Avaya G250 Media Gateway. Connect the strap to an approved ground, such as an unpainted metal surface.
3. Check the contents of the packaging against the customer order.
4. Cross-check the customer order with the planning documentation you have been given. Media modules, telephones and other equipment are listed on your planning and shipping documentation. Placement for the media modules and other equipment are also indicated.

5. Verify that all necessary elements have been received and are in good condition. If there are missing or damaged elements, contact your project manager. The planning documentation will list contact information for key personnel.

If you have any questions about the equipment order, or if the equipment has been damaged, contact your project manager.

Chapter 3: Installing the Avaya G250 Media Gateway

This chapter describes the physical installation of the G250. Perform the following steps in the order in which they are listed:

- Step 1: Mount the G250 chassis on page 29
- Step 2: Install the media modules on page 34
- Step 3: Attach ground conductors on page 38
- Step 4: Connect power to the G250 on page 41

When you have installed the chassis and media modules, and connected the power, you can move on to Chapter 4: Connecting devices, and connect external devices to the G250.

Step 1: Mount the G250 chassis

Mount the G250 in one of the following ways:

- In a rack
- On a wall
- On a table

ELECTROSTATIC ALERT:

When handling any components of an S8300B Media Server or G250 Media Gateway, wear an anti-static wrist ground strap. Connect the strap to an approved ground, such as an unpainted metal surface.

Note:

Avaya has developed special hardware platforms for customers with harsh environmental conditions. These platforms have been tested to meet stringent physical and environmental requirements (i.e., shock, vibration, EMI, etc.) imposed by the United States Navy for use on their ships. The platforms make use of specialized racks and reinforcements. If you wish to obtain information about the design and implementation of such a ruggedized solution, contact the Avaya Navy Shipboard Services organization.

Mounting the G250 in a rack

The G250 mounts in a standard 19-inch rack.

If the G250 is to be mounted in a rack, you can fasten the G250 to the rack either at the front of the G250 or at the middle. In either case, mounting brackets must be attached to the G250.

There are two types of mounting brackets provided with the G250:

- Without cable guides. Two mounting brackets without cable guides are provided.
- With cable guides. One mounting bracket with cable guides is provided. This bracket provides guides for electrical cables.

Mounting brackets without cable guides can be attached in either of the following positions:

- To each side of the front of the G250 for fastening the unit to the rack at the front
- To the middle of each side panel of the G250 for fastening the chassis to the rack at the middle

Figure 1: Attaching a mounting bracket to the front of the G250

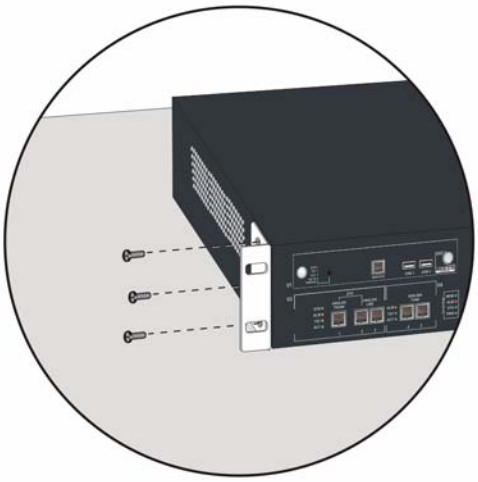
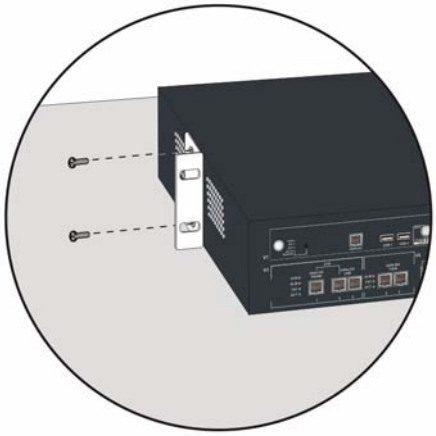
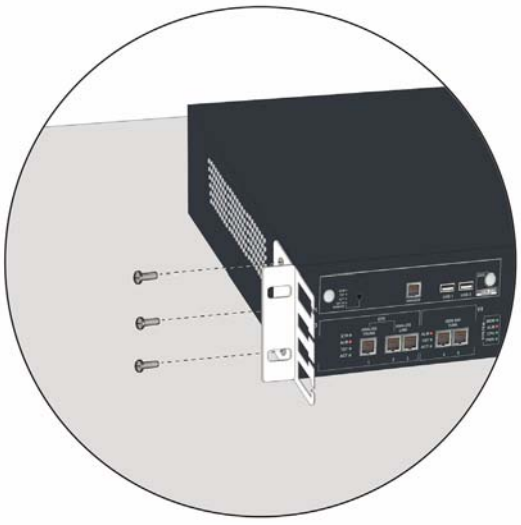


Figure 2: Attaching a mounting bracket to the middle of the G250



The mounting bracket with cable guides is useful for cable management. You can attach the mounting bracket with cable guides to the front of the G250 at one side, as shown in the following figure. If you are fastening the chassis to the rack at the front, use the mounting bracket with cable guides as one of the two front brackets. If you are fastening the chassis to the rack at the middle, use the mounting bracket with cable guides at the front of the chassis, in addition to the two regular mounting brackets on the sides of the chassis. In this case, the mounting bracket with cable guides serves for cable management only - you do not fasten it to the rack.

Figure 3: Attaching a mounting bracket with cable guides



To attach each mounting bracket to the G250:

1. Position a bracket over the desired mounting position.
2. Affix the bracket to the chassis with three of the nine 6-32 x 3/8 screws provided.
3. Tighten with a screwdriver.

The G250 is held in place by mounting screws through the two mounting ears. To avoid balancing problems and cabling complications, the racks should be filled from the bottom; that is, mount units in the lower positions first.

Before mounting the G250, check for the following:

- Ensure that the rack is bolted to the floor and is earthquake-protected, if required. If the rack is not securely fixed in place, do not proceed with the installation.
- If the G250 is being mounted in a rack with other equipment already installed, the G250 must be positioned to avoid imbalance.
- The G250 is shipped with 3 sets of four mounting screws. Choose the set of screws that match the screw holes in the rack being used.
- The G250 weighs pounds (kg) empty and between and pounds (between and kg) when equipped with media modules. Two people may be needed to mount the G250 Media Gateway in the rack.

To mount the G250 in the rack:

1. Position the G250 in the rack. Ensure that there is adequate ventilation.
2. Verify that the screw holes are aligned with the rack hole positions.
3. Insert two mounting screws on each side.
4. Tighten the mounting screws. Avoid overtightening.
5. Verify that ventilation vents are not obstructed.

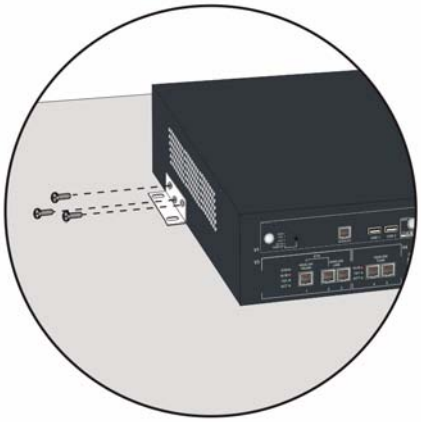
At this point, you have mounted the G250 chassis in the rack and are ready to insert media modules as required in the planning documentation.

Mounting the G250 on a wall

To mount the G250 on a wall, use the two mounting brackets without cable guides. If the wall is flat, you can screw the G250 directly to the wall. If the wall is not flat, screw a plywood board (415 x 465 mm, 20 mm thick) to the wall with wood screws, and fasten the G250 to the board.

To attach brackets to the G250 for wall mounting:

1. Attach a bracket to each side of the G250, as shown in the figure below.



Placing the G250 on a table

If you will be installing the G250 as a tabletop unit, you need to affix the provided rubber feet to the underside of the G250.

To affix the feet:

1. Remove the four feet from their packaging.
2. Turn the G250 upside down.
3. Position each foot into one of the mounting sites, near each corner of the chassis.
4. Press the plastic rivet into the foot with a stylus until it is firmly seated on the chassis.

Step 2: Install the media modules

When the G250 chassis is installed, you can insert the media modules. Each module is shipped with two thumb screws for securing the position of the module in the G250 chassis.

Before inserting media modules into the G250 chassis, make sure:

- Not to install an unsupported media module. See Supported Modules.
- To allocate a permissible slot to each media module. See Allocating slots on page 34.

To install an S8300B media module, see Inserting the S8300B Media Server module on page 35.

To install each of the other media modules, see Inserting media modules on page 37.

WARNING:
The Avaya G250 Media Gateway must not be operated with any open slots. Failure to cover empty slots with the supplied blank plates can cause overheating due to inadequate air distribution.

Supported Modules

The G250 does not support all Media Modules. Before you insert other Media Modules, review the following list for combination limitations.

The Avaya G250 Media Gateway supports the following modules only:

- S8300B Media Gateway in slot V1
- MM340 in slot V2
- MM342 in slot V2

Allocating slots

You insert media modules into the slots marked V1 and V2 on the G250 front panel, shown in Figure 4 below.

Tip:
The slot positions and names are the same on the G250 and the G250-BRI.

Figure 4: The G250 front panel ports and slots

Table 1 describes which media modules can be inserted into which slots:

Table 1: Permitted slots for media modules

Media module	Permitted slot	Description
MM340	V2	Provides one E1/T1 WAN port for connecting to a WAN endpoint device.
MM342	V2	Provides one USP WAN port for connecting to a WAN endpoint device.
S8300B	V1	Media Server

Inserting the S8300B Media Server module

ELECTROSTATIC ALERT:

Hold media modules only by the edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear an anti-static wrist-strap and use an anti-static bag.

CAUTION:

The connector pins can be bent or damaged if the module is handled roughly, or if misaligned and then forced into position.

CAUTION:

Separate ESD paths to the chassis ground connect to the media modules at the spring-loaded captive screws. Use a screwdriver to ensure the captive screws are securely tightened to prevent damage to the equipment.

You can only insert the S8300B in slot V1 on the left side of the G250 Media Gateway.

To insert the S8300B Media Server module

1. Remove the plate above slot V1, labelled "Remove before removing or inserting S8300 module."
2. Remove the blank plate from slot V1.
3. Position the media module before the V1 bay opening and engage both sides of the module in the interior guides.
4. Slide the S8300B module slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengaged from the guides.

Figure 5: Inserting the S8300B media server module.

5. Apply firm pressure to engage the connectors.

   The connector has different length pins. The long pins will engage first to provide grounding. Medium length and short pins will provide power and signal.

6. Lock the S8300B Media Server module into the chassis by tightening the spring-loaded captive screws on the front of the module.
7. Replace the plate labelled "Remove before removing or inserting S8300 module" above slot V1, and tighten the screws on the front of the plate.

DANGER:
To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Inserting media modules

After you have inserted the S8300B Media Server module, if applicable, insert the rest of the media modules. Make sure to insert each module in a permissible slot. For information about which slots to allocate to which modules, see Allocating slots on page 34.

CAUTION:

Hold media modules only by the edges to avoid damage from static electricity. Do not touch the top or bottom of the circuit board. If possible, wear a wrist-strap and use an anti-static bag.

CAUTION:

The connector pins can be bent or damaged if the module is handled roughly, or if misaligned and then forced into position.

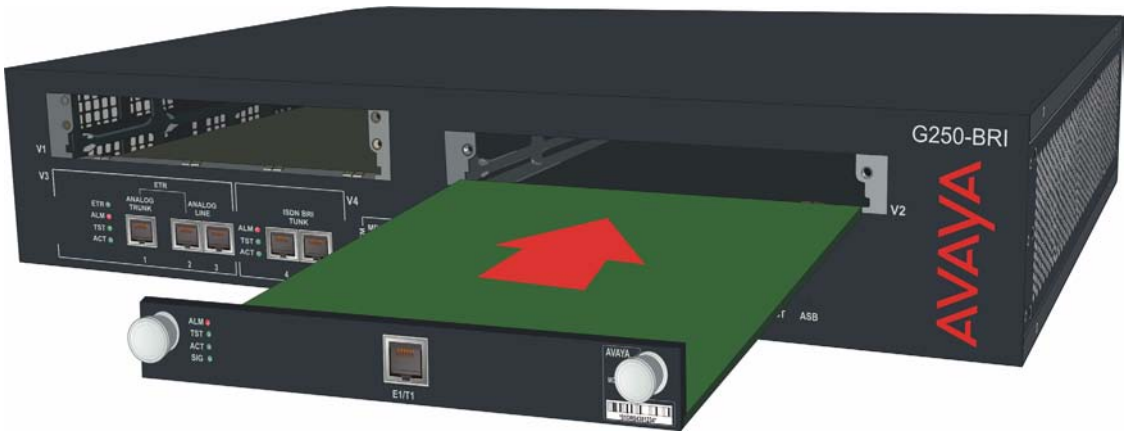
CAUTION:

Separate ESD paths to the chassis ground connect to the media modules at the spring-loaded captive screws. Use a screw driver to ensure the captive screws are securely tightened to prevent damage to the equipment.

To insert a media module:

1. Remove the blank plate from the empty bay.
2. Position the media module before the selected bay on the front of the G250 chassis and engage both sides of the module in the interior guides.
3. Slide the module slowly into the chassis, maintaining an even pressure to assure that the module does not become twisted or disengaged from the guides.

Figure 6: Inserting a media module



4. Apply firm pressure to engage the connectors.

   The media module connector has different length pins. The long pins will engage first to provide grounding. Medium length and short pins will provide power and signal.

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

   DANGER:
   To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

Step 3: Attach ground conductors

To assure safe installation and operation, carefully read all requirements, recommendations, and instructions. Pay special attention to all CAUTION, WARNING, and DANGER statements.

WARNING:
System grounding must comply with the general rules for grounding provided in Article 250 of the National Electrical Code (NEC), National Fire Protection Agency (NFPA) 70, or the applicable electrical code in the country of installation.

General grounding requirements

For customer-installed equipment, the field-installed green/yellow conductor referred to as the Supplementary Ground Connector (SGC) must be connected to the G250 and attached to an approvedl ground. If a power cord accompanies the G250, use that cord whenever possible.

The customer must select a location for the G250 Media Gateway installation that is no more than 16 feet (5 m) from an approved ground. If this location requirement is not met, the customer must contact a licensed electrician to install a Supplementary Ground Conductor per Article 250 of the National Electrical Code (NEC).

WARNING:
If the installation location is greater than 16 feet (5 m) from an approved ground, do not install the Avaya G250 Media Gateway until a licensed electrician is present to install a Supplementary Ground Conductor.

A 16-foot (5 m) Supplementary Ground Conductor is provided with the equipment, and is constructed of 14 AWG (1.5 mm^2) wire, with an insulated ring terminal crimped to one end that is suitable for the #8 (M4) stud/screw on the rear of the G250 chassis.

The customer will need to provide a means of connecting this Supplementary Ground Conductor to an approved ground according to Article 250 of the National Electrical Code (NEC).

DANGER:
For custumer-installed euipment, failure to install the Supplementary Ground Connector will void the Product Safety certifications (UL and the CE Mark) on the product, as well as allow a hazard to be present that could result in death or severe personal injury.

Approved grounds

An approved ground is the closest acceptable medium for grounding the building entrance protector, entrance cable shield, or a single-point ground of electronic telephony equipment. If more than one type of approved ground is available on the premises, the grounds must be bonded together as required in Section 250-81 of the NEC for the US or per the local electrical code regulations in the country of installation.

- Grounded Building Steel. The metal frame of the building where it is effectively grounded by one of the following grounds: acceptable metallic water pipe, concrete encased ground, or a ground ring.
- Acceptable Water Pipe. A metal underground water pipe, at least 1/2-in. (1.3 cm) in diameter, in direct contact with the earth for at least 10 ft. (3m). The pipe must be electrically continuous (or made electrically continuous by bonding around insulated joints, plastic pipe, or plastic water meters) to the point where the protector ground wire connects. A metallic underground water pipe must be supplemented by the metal frame of the building, a concrete-encased ground, or a ground ring. If these grounds are not available, the water pipe ground can be supplemented by one of the following types of grounds:
  - Other local metal underground systems or structures, such as tanks and piping systems.
  - Rod and pipe electrodes. A 5/8-in. (1.6 cm) solid rod or 3/4-in. (2 cm) conduit or pipe electrode driven to a minimum depth of 8 ft. (2.4 m).
  - Plate electrodes. Must have a minimum of 2 sq. ft. (0.185 sq. m) of metallic surface exposed to the exterior soil.
- Concrete Encased Ground. An electrode encased by at least 2 in. (5.1 cm) of concrete and located within and near the bottom of a concrete foundation or footing in direct contact with the earth. The electrode must be at least 20 ft. (6.1 m) of one or more steel reinforcing bars or rods, 1/2-in. (1.3 cm) in diameter, or at least 20 ft. (6.1 m) of bare solid copper, 4 AWG (26 mm^2) wire.
- Ground Ring. A buried ground that encircles a building or structure at a depth of at least 2.5 ft (0.76 m) below the earth's surface. The ground ring must be at least 20 ft. (6.1 m) of 2 AWG (35 mm^2), bare copper wire.

- Approved Floor Grounds. Floor grounds are those grounds on each floor of a high-rise building that are suitable for connection to the ground terminal in the riser closet and to the cabinet single-point ground terminal. Approved floor grounds may include the following:
  - Building steel.
  - The grounding conductor for the secondary side of the power transformer feeding the floor.
  - Metallic water pipes.
  - Power-feed metallic conduit supplying panel boards on the floor.
  - A grounding point specifically provided in the building for that purpose.

  WARNING:
  If the approved ground or approved floor ground can only be accessed inside a dedicated power equipment room, then connections to this ground must be made by a licensed electrician.

Connect the safety ground

Proper grounding of the G250 Media Gateway installation safeguards the system, users, and service personnel by providing protection from lightning, power surges, AC mains faults, power crosses on central office trunks, and electrostatic discharge (ESD).

Local electrical installation codes must be followed when installing the G250.

WARNING:
An improper ground can cause electrical shock as well as equipment failures and service outages.

For customer-installed equipment

To attach the ground wires:

1. Remove the ground screw on the rear of the chassis adjacent to the ground symbol.
2. Place the ring terminal of the 14 AWG (1.5 mm^2) Supplementary Ground Conductor on the screw.
3. Replace the ground screw on the chassis and securely tighten the screw such that it cannot be loosened without the use of a tool.
4. Attach the Supplementary Ground Conductor to an approved ground.
5. Connect the AC power cable to the inlet receptacle on the rear of the chassis.

You have now mounted the fully equipped G250 Media Gateway and connected to electrical ground conductors. You are now ready to connect power.

Step 4: Connect power to the G250

After you have mounted the G250, installed the media modules, and attached the necessary grounding conductor, you can connect power to the G250.

To connect power to the G250:

1. Connect the power cable to the power connector on the G250 back panel.
2. Plug the power cable into a mains socket. The G250 is now powered. The PWR LED on the front panel lights. The CPU LED lights up if the firmware is running.

WARNING:

Never unplug the power cord from the G250 without unplugging *all* telephone cables from line and trunk ports for Avaya G250 Media Gateways installed by service personnel without the Supplementary Ground Connector.

Chapter 4: Connecting devices

This chapter describes how to connect external endpoint devices to the G250, and install the coupled bonding conductor.

Devices can be connected to the ports on the front panels of the installed media modules and to the fixed front panel ports. Before you connect endpoint devices, the G250 should be mounted and all media modules should be inserted.

This chapter describes various possible ways of connecting different devices. See your planning documentation for any topology requirements to connect specific devices to specific ports. As you connect devices, keep a record of the slots and ports into which specific devices are connected. You will need this information when configuring the G250.

Perform the following steps in order:

- Step 1: Connecting data and voice devices
- Step 2: Connect to the Wide Area Network (WAN) on page 47
- Step 3: Install the Coupled Bonding Conductor on page 49
- Step 4: Install the Avaya Partner Contact Closure Adjunct on page 50

The steps are described in the sections below.

WARNING:
To reduce the risk of fire, use only 26 AWG or larger telecommunication line cords when installing telephones or adjuncts.

WARNING:
Attention: Pour réduire les risques d'incendie, utiliser uniquement des conductors de télécommmunications 26 AWG ou de section supérieure.

Step 1: Connecting data and voice devices

The following sections describe how to connect various data and voice devices to the G250:

- Connecting a switch or a network data port on page 44
- Connecting a computer on page 44
- Connecting a server on page 44
- Connecting an IP telephone on page 45
- Connecting an analog telephone on page 45

- Connecting an E1/T1 WAN link on page 48
- Connecting an ISDN BRI trunk on page 46

Connecting a switch or a network data port

The G250 can provide network switching and also supports the connection of switches. Therefore, depending on the number of devices on your network, you may need to connect any of the following devices:

- One or more LAN switches
- The network data ports in the office

You can connect either a LAN switch or a network data port, via a network cable, to the ETH LAN PoE (Power over Ethernet) ports on the G250 front panel

Connecting a computer

You can connect a computer to any of the following:

- a switch connected to the G250
- the data port of an IP telephone connected to a PoE port on the G250
- one of the following ports on the front panel of the Avaya G250 Media Gateway chassis:
  - the ETH LAN PoE ports
  - the ETH WAN port

To connect the computer to the ETH LAN port, use a straight network cable with an RJ-45 connector, or a crossover cable with an RJ-45 connector. To connect the computer to the ETH WAN port, use a straight network cable with an RJ-45 connector.

Connecting a server

You can connect a server to any of the following:

- a switch connected to the Avaya G250 Media Gateway
- one of the following ports on the front panel of the Avaya G250 Media Gateway chassis:
  - the ETH LAN PoE ports
  - the ETH WAN port

To connect the server to the ETH LAN PoE ports, use a straight network cable with an RJ-45 connector, or a crossover cable with an RJ-45 connector. To connect the server to the ETH WAN port, use a straight network cable with an RJ-45 connector.

Connecting an IP telephone

This section describes how to connect an IP telephone to the G250.

To connect an IP telephone:

1. Wire a telephone port to a LAN port on the G250. If the IP telephone will be powered through the G250, make sure you use a ETH LAN PoE port on the G250. In this case, you do not need to plug the IP telephone into a power supply.
2. Plug the telephone into the telephone port.
3. If the IP telephone will be powered independently, plug the IP telephone into a power supply and check that the IP telephone is powered up.
4. If the IP telephone will be powered through the G250, you must use a telephone that supports PoE, and the telephone will power up if and when PoE is configured on the port to which the telephone is connected. For information about configuring PoE, see Chapter 10, *Configuring PoE*, in *Administration of the Avaya G250 Media Gateway*, 555-245-501.

   Note:

   First generation IP phones do not support PoE.

Alternatively, you can connect the telephone to an external Avaya Ethernet switch, including a P330, P333T-PWR, C360, or C360-PWR. This switch must be connected to an ETH LAN port on the Avaya G250 Media Gateway.

If the telephone is not an Avaya IP telephone, you can connect it to any port on the network switch. Note the port number on the Avaya G250 Media Gateway to which you connect the telephone.

Connecting an analog telephone

This section explains how to connect an analog telephone.

To connect an analog telephone:

1. Wire a telephone port to one of the two fixed LINE ports on the G250 front panel
2. Plug the analog telephone into the telephone port.

Note:

The leftmost LINE analog telephone port on the G250 front panel forms a mechanical analog relay with the TRUNK port next to it. See Figure 4. This relay can be configured to provide emergency transferred telephone service in the case of a power outage or disconnection from an external media server. Therefore, the analog telephone connected to this LINE jack is usually installed for this emergency purpose. Regular analog telephones on the network are usually connected to other analog ports.

Connecting an analog trunk

To connect an analog trunk:

1. Connect the trunk to one of the ports labelled TRUNK on the G250.

Note:

For an analog DID trunk, you can *not* use a TRUNK port on theG250. Instead, you must connect the trunk to one of the ports marked LINE.

Note:

The TRUNK analog telephone port on the G250 front panel forms a mechanical analog relay with the LINE port next to it. See Figure 4. This relay can be configured to provide emergency transferred telephone service in the case of a power outage or disconnection from an external media server. During an emergency situation, all incoming calls on the trunk are directed to the telephone plugged into the LINE jack. Conversely, the telephone plugged into the LINE jack can use the trunk during an emergency situation to make outgoing calls.

Connecting an ISDN BRI trunk

To connect an ISDN BRI trunk:

1. Connect the trunk to any ISDN port on the G250-BRI front panel.

Note:

In the US, you need to connect a separately purchased NT1 device to each ISDN port you use to connect an ISDN BRI trunk.

Step 2: Connect to the Wide Area Network (WAN)

Since the G250 contains an internal router, you can connect the G250 directly to a WAN endpoint device. You can also connect a WAN endpoint device to the G250 via an external router.

Connecting a WAN to the G250

There are some differences in how to connect the WAN, depending on the type of WAN link you are connecting. This section provides separate instructions for connecting various types of WAN links, as follows:

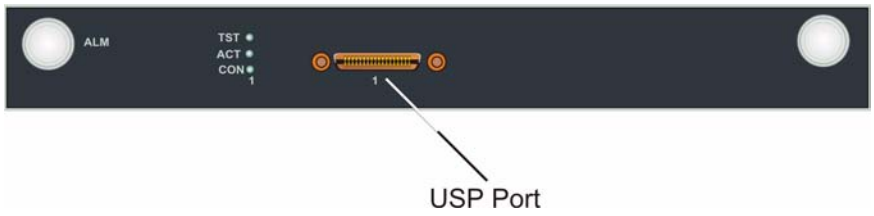
- Connecting a USP WAN link
- Connecting an E1/T1 WAN link
- Connecting an Ethernet WAN link

Connecting a USP WAN link

You must connect the USP WAN link to a device connected to the Avaya MM342 media module. To connect the WAN link, plug the WAN line into the USP port on the MM342 media module. This port is marked USP. To connect the WAN line to the port, use one of the following cable types, depending on the service provider's equipment:

- Avaya Serial Cable DTE V.35
- Avaya Serial Cable DTE X.21

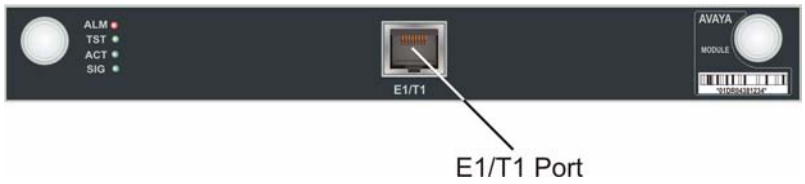
Figure 7: The MM342 media module



Connecting an E1/T1 WAN link

You must connect the E1 or T1 WAN line to the Avaya MM340 media module. To connect the WAN line, plug the WAN line into the E1/T1 port on the MM340 media module. This port is marked E1/T1. Use an unshielded twisted pair cable, straight or crossover, depending on the WAN equipment.

Figure 8: The MM340 media module



Connecting an Ethernet WAN link

You must connect the Ethernet WAN line (DSL, firewall, etc.) to the Ethernet WAN port on the front panel of the Avaya G250 Media Gateway chassis. This port is marked ETH WAN. See Figure 4. Use a CAT5 Ethernet cable to connect the WAN line to the port.

Connecting an external router to the G250

You can connect a router to any of the following ports on the G250:

- The ETH WAN port on the G250 front panel
- An ETH PoE LAN port on the G250 front panel

Step 3: Install the Coupled Bonding Conductor

The Coupled Bonding Conductor (CBC) provides mutual inductance coupling between the CBC and the telephone cables that are exposed to lightning. The conductor can be a 10 AWG (4 mm^2) wire tie wrapped to the exposed cables, a metal cable shield around the exposed cables, or six spare pairs from the exposed cable. In a high-rise building, connect the CBC to an approved building ground on each floor.

Before you begin, be sure the telephone lines are cross-connected to the appropriate media module(s).

To install the CBC:

1. Connect one end of the conductor to a telephone cable building entrance protector ground that is connected to an approved ground.
2. Route the rest of the conductor next to the exposed telephone cables being protected until they reach the cross-connect nearest to the telephone system.
3. Terminate the other end to the single-point ground block provided for the telephone system.

Note:

Position the non-exposed telephone cables at least 12 in. (30.5 cm) away from exposed telephone cables whenever possible.

Step 4: Install the Avaya Partner Contact Closure Adjunct

The Contact Closure feature is a controllable relay providing dry contacts for various applications. To implement the contact closure feature, you connect an Avaya Partner Contact Closure Adjunct box to the CC port on the G250 chassis. The adjunct box provides two contact closures that can be operated in either a "normally closed" or "normally open" state. The contact closures can control auxiliary devices such as devices that automatically lock or unlock doors or voice recording units. The CC port can be configured so that the connected devices can be controlled by an end device, such as a telephone. For example, a user can unlock a door by keying a sequence into a telephone keypad.

To install the contact closure:

1. Follow the installation instructions in the *Avaya Partner Contact Closure Adjunct Installation Instructions* leaflet to install the Contact Closure and connect the auxiliary devices that will be activated and deactivated by the Contact Closure relays.
2. Note which device is connected to each relay. You will need this information for configuration.
3. Connect the Avaya Partner Contact Closure adjunct box to the CC port on the G250 front panel. Use a 24-gauge minimum telephone wire, no longer than 200 ft, with a standard four-wire RJ-11 connector.

Chapter 5: Connecting and enabling a modem for remote access

This chapter describes how to connect and enable a modem on the G250. You can connect a modem to the G250 to enable configuration from a remote location. If an S8300B is installed in the G250, leave a modem connected permanently to enable reporting of alarms to remote locations.

Select one of the following sections, depending on your hardware configuration:

- Connecting and enabling a modem (G250 without S8300B) on page 51
- Connecting and enabling a modem (G250 with S8300B) on page 58

Note:

If you choose to configure the G250 by running an installation wizard, you can enable a modem with the wizard as part of the configuration. Instructions for connecting the modem are included in Appendix C: Running the Avaya Installation Wizard (Avaya IW) on page 119 and in Appendix D: Running the Gateway Installation Wizard (GIW) on page 169. You do not need to read this chapter.

Connecting and enabling a modem (G250 without S8300B)

Connect a serial modem to the CON port on the G250 front panel. For instructions on enabling and connecting the modem, see the relevant section:

- Enabling and connecting a serial modem

When you have enabled and connected the modem, test the modem connection. See Test the modem connection on page 57.

Enabling and connecting a serial modem

To enable and connect a serial modem:

1. Prepare a PC with a CD-ROM drive and a TFTP server on the network. This may be needed for installing software and firmware upgrades.

   Note:

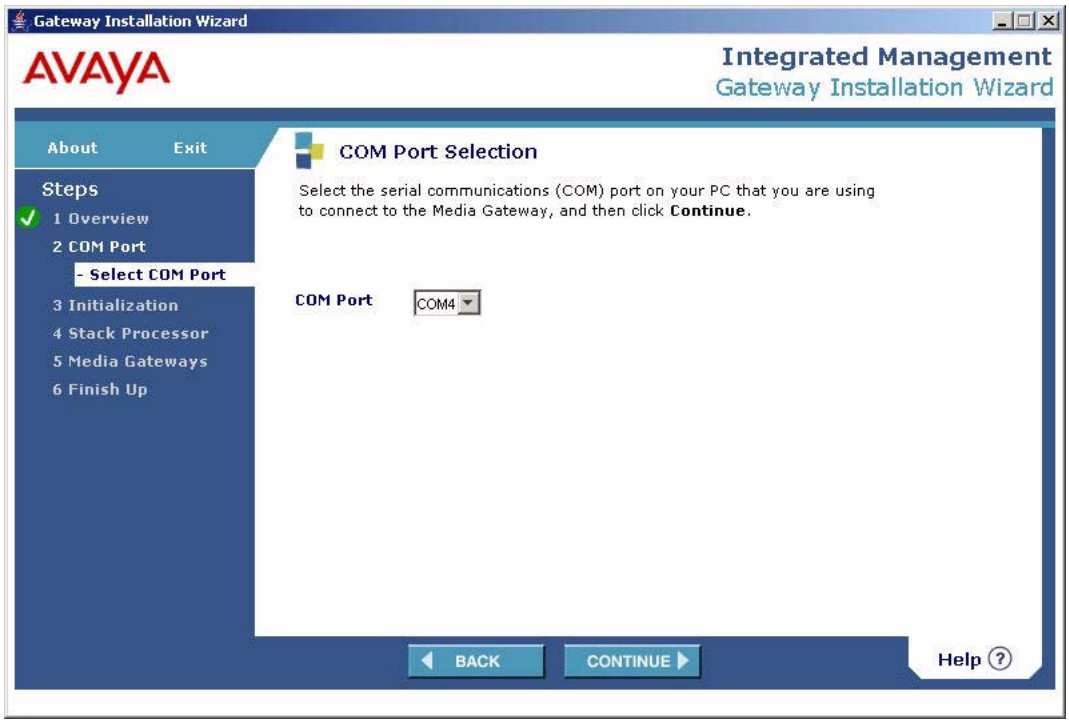
   When uploading firmware from the S8300B using TFTP, you may need to enable TFTP service in the Set LAN Security parameters of your web server.

   Note:

   Firmware upgrades for the G250 and media modules can either be installed from CD or downloaded from the Web.

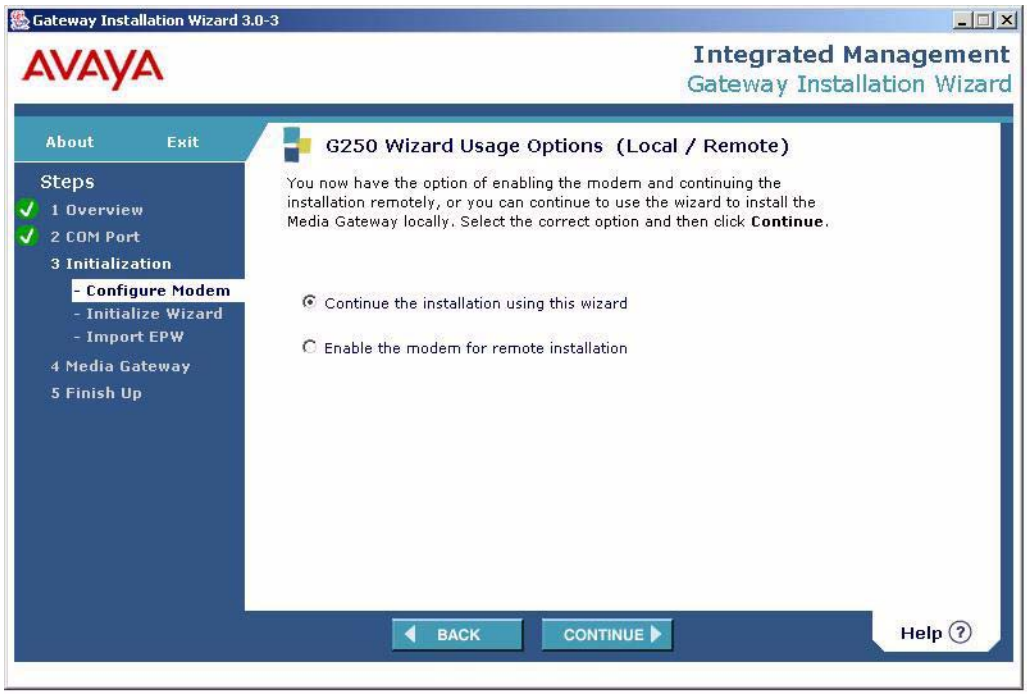
2. Download Gateway Installation Wizard (GIW) from the Avaya website (support.avaya.com/avaygiw) to the laptop computer. The laptop should be running Windows 2000 or Windows XP to support GIW.
3. Plug one end of the provided flat RJ-45 to RJ-45 cable into the provided DB-9 adapter.
4. Plug the RJ-45 connector at the other end of the cable into the CON port of the G250.
5. Plug the DB-9 end of the flat cable into the COM port of the laptop computer.
6. From your laptop computer, double-click the GIW icon to run GIW. The Overview screen appears.
7. Click **Continue**. The COM Port Selection screen appears.

Figure 9: COM Port Selection screen



8. Select the COM port on the laptop that you are using to connect to the G250.
9. Click **Continue**. The G250 Wizard Usage Options screen appears.

Figure 10: G250 Wizard Usage Options screen

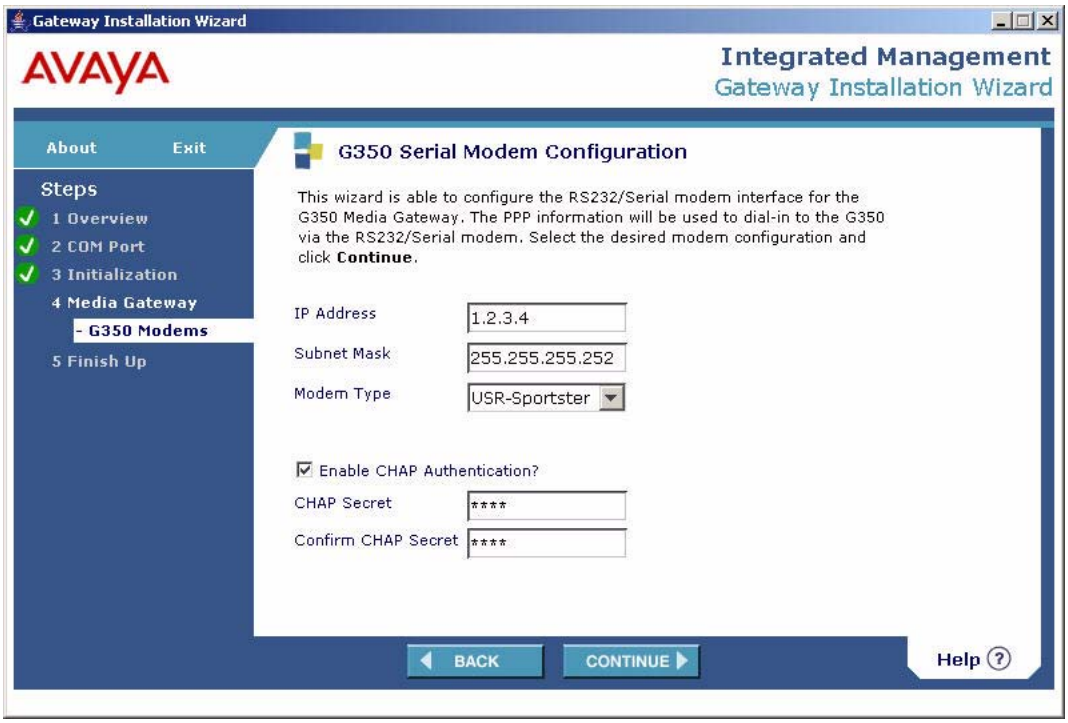


10. Select **Enable the modem for remote installation**.
11. Click **Continue**. The G250 Modem Type Selection screen appears.

Figure 11: G250 Modem Type Selection screen

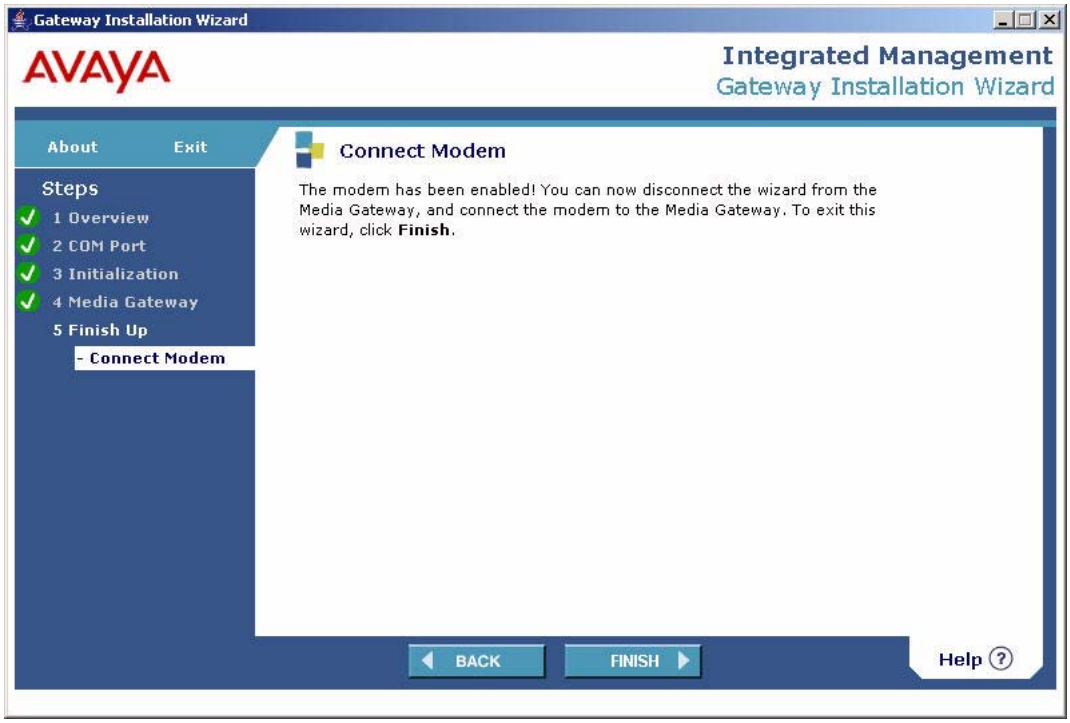
12. Select **Serial Modem**.
13. Click **Continue**. The G250 Serial Modem Configuration screen appears.

Figure 12: G250 Serial Modem Configuration screen



14. In the IP Address field, enter the RAS IP address of the modem obtained using the ART tool. See Run the Automatic Registration Tool (ART) for the RAS IP address on page 22.
15. Fill in the remaining modem information fields.
16. Check **Enable CHAP Authentication**.
17. In the CHAP Secret field, enter the CHAP secret key obtained using the ART tool. See Run the Automatic Registration Tool (ART) for the RAS IP address on page 22.
18. In the Confirm CHAP Secret field, reenter the CHAP secret key.
19. Click **Continue**. The Connect Modem screen appears.

Figure 13: Connect Modem screen



20. Click **Finish**.
21. Connect the serial modem to a working telephone line.
22. Connect the provided DB-25 adapter to the modem.
23. Disconnect the flat cable from the COM port of the laptop computer.
24. Connect the flat cable to the DB-25 connector on the modem.

Test the modem connection

Dial into the modem to verify that you can authenticate to the modem.

The G250 is now prepared for remote configuration via the modem.

Connecting and enabling a modem (G250 with S8300B)

To connect and enable a modem:

1. Access the Maintenance web pages.
2. Change the modem settings on the Configure Server Maintenance web pages.
3. Connect and enable the USB modem.
4. Test the modem connection.
5. If you require a USB CD-ROM drive to download software upgrades, connect the USB CD-ROM drive to the remaining available USB port on the S8300B module.

The G250 is now prepared for remote configuration using Avaya Installation Wizard (Avaya IW) via the USB modem.

Access the Maintenance web pages

Most of the preparations you are making require you to access the Maintenance web pages part of Avaya Integrated Management from your laptop. Use this procedure to access the Maintenance web pages and leave the Maintenance web pages open until you have completed all the preparations.

To access the Maintenance web pages:

1. Connect the laptop you prepared to the Services port on the S8300B. Use a standard Ethernet crossover cable.
2. Configure the network settings on the laptop, according to the following tables:

Table 2: TCP/IP settings

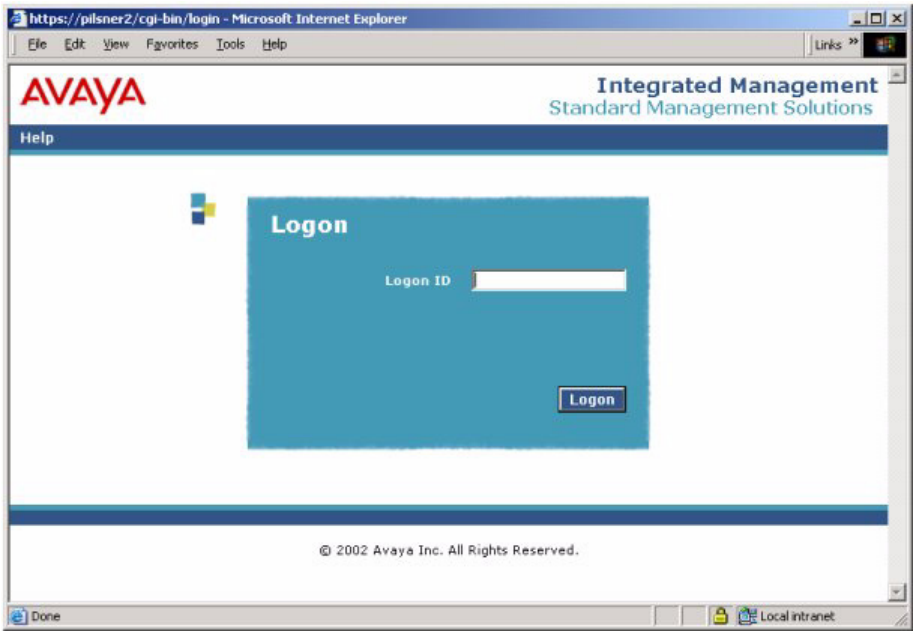
Setting	Value
IP Address	192.11.13.5
Subnet Mask	255.255.255.252
DNS	disable
WINS Servers	do not use (clear out any values)

Table 3: Internet Browser Settings

Setting	Value
Proxy Server	disable

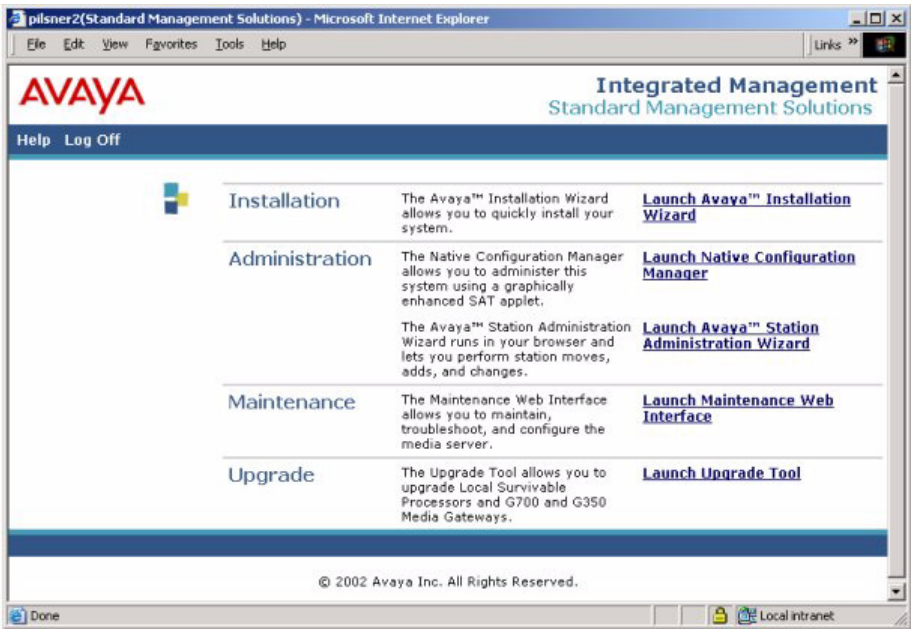
3. Open Internet Explorer, and browse to 192.11.13.6. The welcome screen for Avaya Integrated Management appears.
4. Click **Continue**. The Logon screen for Avaya Integrated Management appears.

Figure 14: Integrated Management Logon screen



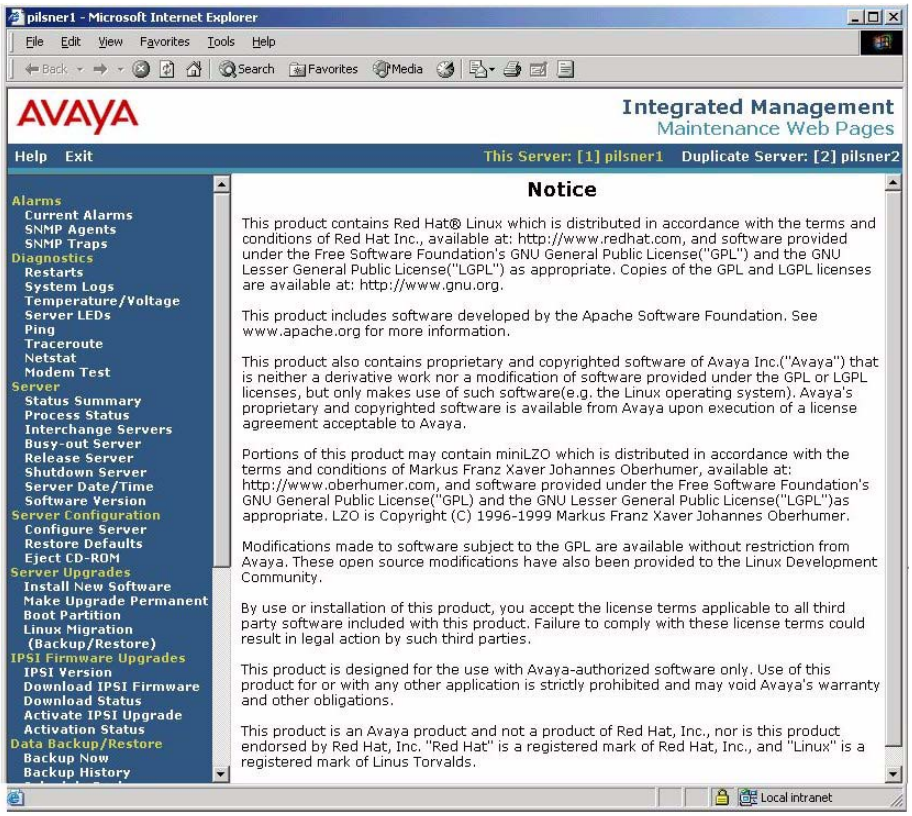
5. Enter your S8300B initial entry username in the Logon ID box.
6. Click **Logon**. The password field appears.
7. Enter your password in the password field, and click **Logon**. The main menu for Avaya Integrated Management appears.

Figure 15: Integrated Management Main Menu



8. From the Integrated Management main menu, select Launch Maintenance Web Interface. The Maintenance Web Pages Notice page appears, with a navigation menu at the left.

Figure 16: Maintenance Web Pages Notice page



9. Leave the Maintenance Web Pages open to perform the tasks described in the coming sections.

Change the modem settings on the Configure Server Maintenance web pages

If you have an Avaya Maintenance contract, change the modem settings on the Configure Server Maintenance Web Pages.

To change the modem settings:

1. Select **Configure Server** from the left-hand menu on the Maintenance web page. The Back Up Data page appears.
2. Follow the on-screen instructions to back up the current data.
3. Click **Continue**.
4. Select **Configure individual services**.

5. Click **Continue**.
6. From the left navigation menu, click **Set Modem Interface**. The Set Modem Interface page appears.
7. Enter the RAS IP address you obtained using the ART tool. See Run the Automatic Registration Tool (ART) for the RAS IP address on page 22.
8. Click **Change modem settings**.
9. Click **Continue**.
10. Click **Close Window**.

Connect and enable the USB modem

If your installation includes an S8300B Media Server module, you need to connect the USB modem to the S8300B. After the G250 is configured, you can leave the modem permanently connected to enable the S8300B to report alarms to remote locations.

To connect and enable the modem:

1. Connect the USB modem to a working telephone line.
2. Connect the modem to one of the USB ports on the S8300B module.
3. From the navigation menu of the Maintenance Web Pages, select **Security > Modem**. The Modem screen appears.

Figure 17: Modem web page

4. Select **Enable modem for unlimited incoming calls**.
5. Click **Submit**.

The modem is now connected and enabled.

Test the modem connection

To ensure that the modem is enabled correctly:

1. Setup a dialup connection on a remote PC with the following settings:
   - Automatically detect settings.
   - No Username, Password, or Domain.
   - Security > Show Terminal Window.
2. Dial in to the modem from the remote PC.
3. When prompted, provide the rasaccess login and password in the Terminal Window.
4. Close the Terminal Window to complete the connection.

Refer to *Job Aid: Creating Additional Remote Access Logins*, 03-300451 on the Avaya Support site for additional information about creating and testing remote logins.

Chapter 6: Configuring the G250

The G250 requires software configuration. The G250 can be configured using:

- The Avaya Installation Wizard (Avaya IW). Avaya IW is a wizard that prompts you for all configurations required to complete the installation of the G250. Avaya IW is used only to configure a G250 with an S8300B. Refer to Appendix C: Running the Avaya Installation Wizard (Avaya IW) on page 119.
- The Gateway Installation Wizard (GIW). The GIW is a wizard that prompts you for all configurations required to complete the installation of the G250. You can run GIW to configure a G250 without an S8300B. Refer to Appendix D: Running the Gateway Installation Wizard (GIW) on page 169.
- The Avaya G250 Command Line Interface. The CLI is a comprehensive tool for configuring the gateway and includes all supported configuration tasks. For information about configuration using the CLI, see *Administration of the Avaya G250 Media Gateway*, 555-245-501. For detailed information on CLI commands, refer to the *Avaya G250 Media Gateway CLI Reference Guide*, 555-245-201.

The G250 can be configured at the customer site via a laptop connected to the CON port of the G250 or from a remote location via a modem. For information about connecting and enabling a modem, refer to Chapter 5: Connecting and enabling a modem for remote access on page 51.

Chapter 7: After installation

After initial configuration, perform the following steps:

- Step 1: Test the installation on page 67
- Step 2: Remove the installation equipment on page 70

Step 1: Test the installation

When the installation is complete, simple tests must be performed to test telephone and data connectivity.

Test data connectivity by pinging the IP address of each device to test the device's connectivity within the network and outside the network.

Test local data connectivity on-site by checking that you can send an email between two PCs that are connected to the G250.

Test telephone connectivity as follows:

- Test each telephone.
- Test each trunk.
- Perform a Local Survivable Processor (LSP) failover test if you have an S8300B installed as an LSP.

Testing telephones

To test a telephone:

1. Make outgoing calls from the telephone. Make sure you hear a dial tone when you pick up the receiver. Make sure you can make both an internal (within the local network) and an external (outside the local network) call.
2. Make a call to the telephone from both within the network and outside of the network.

Testing trunks

Use the facility test call feature to verify that each trunk is functioning properly. For information about how to use the facility test call feature, see *Maintenance for the Avaya G250 and the G350 Media Gateway*, 03-300438.

LSP failover testing

If you have an S8300B media server module installed in the G250 and configured as an LSP, you need to perform a test to make sure that the LSP takes over control of the G250 if the G250 becomes disconnected from the primart media server.

Note:

If SLS mode is enabled and the primary controller and LSP both fail, then the G250 enters SLS mode.

To perform the LSP failover test:

1. Verify that valid translations are file synchronized to the LSP by logging into Avaya Communication Manager from the LSP and listing either stations or trunks (refer to *Administrator's Guide for Avaya Communication Manager*, 555-233-506). Verify that the list of stations or trunks is valid. If the files are not synchronized, verify that you have correctly configured the required IP address(es) for the primary controller (media server). If you are using Avaya IW to configure the G250, the following are key actions that must be done in the wizard to ensure correct IP address configuration:

   a. In the Usage options screen, select the one of the following usage options that corresponds to the correct primary controller type:

      - **Install an LSP that is associated with an S8700 Primary Controller**.
      - **Install an LSP that is associated with an S8500 Primary Controller**.
      - **Install an LSP that is associated with an S8300B Primary Controller**.

      If you selected the correct usage option, the Primary Controller IP Address screen appears later in the wizard, and calls for the required primary controller IP addresses for your primary controller type. The following IP addresses need to be configured for each primary controller type:

Primary media gateway controller	Number of IP addresses to be configured	IP addresses to configure
S8300B	1	The IP address of the primary S8300B
S8500	2	The IP address of the S8500's Control-LAN card (CLAN) and the IP address of the S8500
S8700	3	The IP address of the S8500's CLAN, the IP address of the Server A LAN, and the IP address of the Server B LAN

b. In the Primary Controller IP address screen, enter all the required IP addresses for the primary controller type.

   There may be a delay after running Avaya IW until the LSP is registered with the primary MGC and the translations are file synchronized.

2. If valid translations are not file synchronized to the LSP, do the following:

   a. From a SAT session run from the primary controller, verify that the LSP node-name and IP address are correctly entered.

   b. Use the **`save translation lsp`** command to start the file synchronization process.

      There may be a delay while the files are synchronized, especially during high network traffic.

   c. Log in again to Avaya Communication Manager from the LSP and list either stations or trunks.

   d. Verify that the list of stations or trunks is valid.

3. Ensure that the green LED on the faceplate of the S8300 LSP is on.

4. Disconnect the G250 from the primary controller, ensuring that all telephones are still connected to the G250.

5. Verify that calls can be made between local telephones and to outside telephones.

Step 2: Remove the installation equipment

Remove all equipment that you used to assist you in the installation process. This may include:

- The CD-ROM drive
- The software upgrade CDs
- The laptop computer
- The modem (for installations without an S8300B module only)

Note:

If you have an S8300B media server module installed in the G250, leave the modem connected to enable reporting of alarms to remote locations.

The installation is now complete.

Chapter 8: Upgrading media modules and devices

This chapter describes how to add new media modules and endpoint devices to a G250 that is already installed. When adding new devices to the G250, consult your project manager for topology requirements for specific ports to be connected to specific devices.

See one of the following sections:

Adding a media module

Before adding a new media module to the G250, see one of the following sections:

- Adding S8300B modules on page 72. Describes important information when adding a new voice module to the G250.
- Adding WAN and LAN modules on page 72. Describes important information when adding a WAN or LAN module to the G250.

To install a new module, follow the instructions in Step 2: Install the media modules on page 34. Consult with your project manager to find out if the network topology necessitates installing media modules in specific slots.

Adding S8300B modules

You can hot-swap S8300B modules. This means you can add a voice module to the Avaya G250 Media Gateway while the system is running, without any disruption to your network. Configuration of the G250 is not necessary when you add an S8300B module. Configuration is only necessary when you add telephones, fax machines, and trunks to the new module. See Adding a telephone on page 74 and Adding a trunk on page 75.

Adding WAN and LAN modules

You can hot-insert WAN and LAN modules. This means you can add a WAN or LAN module to the Avaya G250 Media Gateway while the system is running, but the G250 resets when you add the module. However, hot insertion is not recommended in most cases. Because hot insertion resets the G250, any translation and other data that is in the running configuration but has not been saved to the startup configuration will be lost.

There is no configuration necessary when you add a WAN or LAN module. Configuration is only necessary when you add telephones, WAN lines, and LAN devices to the new module. See Adding a LAN device on page 73, Adding a telephone on page 74, Adding a WAN line on page 76.

Adding a LAN device

Adding a LAN device requires you to do the following tasks:

- Connect the LAN device
- Configure the LAN device on the G250
- Test the LAN device

Connect the LAN device

To add a new LAN device, see one of the following sections:

- Connecting a switch or a network data port on page 44
- Connecting a computer on page 44
- Connecting a server on page 44

Configure the LAN device on the G250

Before software configuration for the new LAN device takes place, gather the following information:

- the name and location of the owner of or person responsible for the LAN device
- the slot and port number on the Avaya G250 Media Gateway to which the LAN device connects. If the LAN device is connected to an IP telephone, note the extension of the telephone to which the LAN device connects, and the slot and port number on the G250 to which the telephone connects.

Configuration may be performed on site by connecting a laptop computer connected to the CON port of the G250, or remotely via a modem connected to the G250 or S8300B. For information about preparing a modem, see Chapter 5: Connecting and enabling a modem for remote access on page 51. For information about configuration, see Chapter 6: Configuring the G250 on page 65.

Test the LAN device

After installation and configuration of the LAN device is complete, ping the IP address of the device to test the device's connectivity within the network and outside the network.

Adding a telephone

Adding a telephone requires you to do the following:

- Connect the telephone
- Configure the telephone on the G250
- Test the telephone

Connect the telephone

To connect a new telephone, see one of the following sections:

- Connecting an IP telephone on page 45
- Connecting an analog telephone on page 45

Configure the telephone on the G250

When you add a new telephone, note the following information for software configuration:

- name and location of the owner of the telephone
- model number of the telephone
- extension of the telephone
- slot and port number on the Avaya G250 Media Gateway to which the telephone connects

Configuration may be performed on site by connecting a laptop computer connected to the CON port of the G250, or remotely via a modem connected to the G250 or S8300B. For information about preparing a modem, see Chapter 5: Connecting and enabling a modem for remote access on page 51. For information about configuration, see Chapter 6: Configuring the G250 on page 65.

Test the telephone

After installation and configuration of the telephone is complete, test the telephone. To test the telephone, perform the following two steps:

1. Make outgoing calls from the telephone. Make sure you hear a dial tone when you pick up the receiver. Make sure you can make both an internal (within the local network) and an external (outside of the local network) call.
2. Make a call to the telephone from both within the network and outside of the network.

Adding a trunk

Adding a trunk requires you to do the following:

- Order the trunk
- Connect the trunk
- Configure the trunk on the G250
- Test the trunk

Order the trunk

When you order the trunk:

- Make sure to install the trunk near the physical location of the Avaya G250 Media Gateway.
- Make sure that the telephone service provider installs the trunk and verifies that the trunk is working properly before you contact the technician that is performing or supervising the configuration.
- Note the telephone number of the trunk.

Special considerations when ordering an analog trunk

When you order an analog trunk, there are several recommendations depending on your system's particular needs:

- For optimal functioning of the Emergency Transfer Relay feature, it is recommended to use a loop-start trunk.
- Request conditioned lines to ensure satisfactory voice quality and trunking interactions.

Connect the trunk

To connect a new trunk, see one of the following sections:

- Connecting an analog trunk on page 46

Configure the trunk on the G250

When you add a new trunk, note the following information for software configuration:

- slot and port number on the Avaya G250 Media Gateway to which the trunk connects
- telephone number of the trunk

Configuration may be performed on site by connecting a laptop computer connected to the CON port of the G250, or remotely via a modem connected to the G250 or S8300B. For information about preparing a modem, see Chapter 5: Connecting and enabling a modem for remote access on page 51. For information about configuration, see Chapter 6: Configuring the G250 on page 65.

Test the trunk

After installation and configuration of the trunk is complete, test the trunk. To test the trunk:

1. Make outgoing calls from the trunk. Ask the technician that is performing or supervising the configuration for instructions how to access the trunk. Make sure you can make both an internal (within the local network) and an external (outside of the local network) call.
2. Make a call into the G250 trunk.

Adding a WAN line

Adding a telephone requires you to do the following:

- Order the WAN line
- Connect the WAN line
- Configure the WAN line on the G250
- Test the WAN link

Order the WAN line

If you need to order the WAN line, make sure that the service provider installs the line near the physical location of the G250 and verifies that the line is working before you configure the WAN on the G250.

Connect the WAN line

To connect a WAN line, see Step 2: Connect to the Wide Area Network (WAN) on page 47.

Configure the WAN line on the G250

When you add a new WAN line, note the following information for software configuration:

- slot and port number on the Avaya G250 Media Gateway to which the WAN line connects

Configuration may be performed on site by connecting a laptop computer to the CON port of the G250, or remotely via a modem connected to the G250 or S8300B. For information about preparing a modem, see Chapter 5: Connecting and enabling a modem for remote access on page 51. For information about configuration, see Chapter 6: Configuring the G250 on page 65.

Test the WAN link

After installation of the WAN line is complete, test the link by verifying that the SIG LED for the port to which the link connects is lit. It is also recommended that you ping the IP address of a device using the WAN line and perform a trace route test in order to test connectivity with the network and outside the network.

Adding an Avaya Partner Contact Closure Adjunct

To install an Avaya Partner Contact Closure Adjunct, follow the instructions in Step 4: Install the Avaya Partner Contact Closure Adjunct on page 50.

Chapter 9: Upgrading the Avaya Communication Manager software

If your Avaya G250 Media Gateway includes an Avaya S8300B Media Server, it might be necessary to upgrade the Avaya Communication Manager software. Upgrading the software can be performed in one of the following several ways:

- Remote configuration via Telnet - upgrade the software remotely via Telnet. In this scenario, a modem is required at the local site. See Chapter 5: Connecting and enabling a modem for remote access on page 51.
- Remote configuration via network - upgrade the software remotely via a network connection.
- Local configuration with S8300B Media Gateway - upgrade the software at the site, using a laptop computer and a CD-ROM drive connected to the S8300B Media Gateway.

Note:

You must have an S8300B in order to upgrade to Communication Manager 3.0 or later. If you have an S8300, you must replace it with an S8300B board before beginning the upgrade.

Upgrading the software using a CD-ROM drive

The upgrade software is usually installed from a CD-ROM drive connected to the S8300B. If the upgrade is performed locally, you might need to provide a laptop and a USB CD-ROM drive. If the upgrade is performed from a remote location, you must connect a USB CD-ROM drive (Material code 700289580) to the S8300B and insert the upgrade CD-ROM in the CD-ROM drive. You also might need to connect a modem. This depends on the method used to perform the upgrade.

For a software upgrade on an Avaya G250 Media Gateway with an S8300B Media Server, use a USB modem. It is recommended to use a Multitech MultiModem USB, MT5634ZBA-USB-V92. To prepare for the upgrade, perform the following steps:

1. Connect the modem to a working telephone line. Note the telephone number of the line to which you connect the modem, so that you can provide the number to the technician that is performing or supervising the configuration.
2. Connect the USB modem to either of the two USB ports in the Avaya S8300B Media Server.

Note:

You may be required to enable the modem and port. For instructions on enabling the modem, see Chapter 5: Connecting and enabling a modem for remote access on page 51.

3. Connect a USB CD-ROM drive to the free USB port on the Avaya S8300B Media Server. Then, insert the CD-ROM provided by Avaya into the CD-ROM drive.

Upgrading the software without a CD-ROM drive

You can upgrade the Avaya Communication Manager software without a CD-ROM drive by downloading the upgrade software or installing it from a laptop computer. If the upgrade is performed from a remote location, you might need to connect a modem. This depends on the method used to perform the upgrade.

Performing the upgrade

You can upgrade the S8300B software using Avaya IW or the Upgrade Tool. To upgrade S8300B software using Avaya IW, see Appendix C: Running the Avaya Installation Wizard (Avaya IW) on page 119. For information about upgrading S8300B software using the upgrade tool, see Chapter 10: Upgrading the G250 firmware on page 81.

Chapter 10: Upgrading the G250 firmware

You can upgrade software on the Avaya G250 Media Gateway. Software used to control the Avaya G250 Media Gateway itself and firmware for the media modules installed on the G250 is called firmware.

Note:

The G250 firmware also includes the firmware for the MM340 and MM342 media modules.

You can upgrade the firmware on the Avaya G250 Media Gateway and media modules using various different tools, each suitable for specific types of installation. See one of the following sections:

- Upgrading G250 firmware using Avaya Software Update Manager. Describes how to upgrade firmware on a single or multiple G250 within your network from one management station. This ensures that all G250 gateways in your network are running the same firmware.
- Upgrading G250 firmware using Gateway Installation Wizard (GIW). Describes how to use GIW to upgrade firmware on a G250 that does not contain an S8300B. This upgrade must be done locally.
- Upgrading G250 firmware and Avaya Communication Manager software using Avaya Installation Wizard (IW). Describes how to upgrade firmware and software on a G250 that contains an S8300B, using Avaya IW. The upgrade configuration may be performed locally or remotely, but the software must be loaded locally.
- Upgrading G250 firmware using the CLI. Describes how to use the CLI to upgrade G250 firmware locally or remotely.

Upgrading G250 firmware using Avaya Software Update Manager

You can use Avaya Software Update Manager to view your network inventory and the firmware vintages of devices on your network. Avaya Software Update Manager can also check the software versions currently in use against the latest versions available from Avaya and recommend updates when a newer version is available. Based on this information, you can download new firmware to multiple network devices simultaneously from a single management station, ensuring all devices are updated.

You can use Avaya Software Update Manager to take a new release from Avaya's Web site and store it on your hard disk for subsequent downloading to the appropriate devices.

Avaya Software Update Manager is a server application hosted on the Avaya Network Management server. The server stores all the software retrieved from the Web and can download the software to appropriate devices. You may also copy files containing embedded software to the server. You can reach the server locally or via remote access, so you can update the software on your devices from anywhere in the world.

Avaya Software Update Manager is part of the Integrated Management Enterprise Package which is an entitlement for all Avaya Communication Manager non-introductory offers.

For information about using Avaya Software Update Manager, see the *Avaya Software Update Manager 3.6 User Guide, 14-300168.*

Upgrading G250 firmware using Gateway Installation Wizard (GIW)

Perform the following steps to use GIW to upgrade firmware on a local G250:

1. Prepare installation worksheets. See Preparing installation worksheets on page 86
2. Download GIW from the Avaya website (support.avaya.com/avayagiw) to the laptop computer. The laptop should be running Windows 2000 or Windows XP to support GIW.
3. Set up a TFTP server on the G250 network. See Setting up a TFTP server on page 87. The GIW runs the CLI commands on the G250 so the G250 can obtain the files from the TFTP server.
4. Download the G250 firmware files to the TFTP server. See Downloading G250 firmware files to a local TFTP server on page 88.
5. Run GIW to perform the upgrade. For instructions on performing the upgrade, see Run the Gateway Installation Wizard (GIW) on page 169.

Upgrading G250 firmware and Avaya Communication Manager software using Avaya Installation Wizard (IW)

For a G250 with an S8300B installed, you can use Avaya IW to upgrade G250 firmware and Avaya CM software. You can run Avaya IW from a remote location if the software is loaded locally. You can point your browser to the ip address of the S8300B if you are in the customer network or via the modem ppp connection.

Perform the following steps:

1. Prepare installation worksheets. See Preparing installation worksheets on page 86.
2. Place the upgrade software and firmware files on a laptop. These files are on the Avaya Communication Manager CD-ROM. To upgrade the S8300B Media Server software and G250 firmware, insert the Communication Manager CD-ROM into a CD-ROM drive connected to a laptop. Alternatively, you can upload the individual files to the hard drive of the laptop. For more details, see *Job Aid: Avaya Installation Wizard*, 555-245-754.
3. Upgrade the S8300B Media Server using the Avaya Installation Wizard (For more details, see *Job Aid: Avaya Installation Wizard*, 555-245-754). This procedure also copies the G250 firmware as an RMP (Red Hat Package Manager) file from the Communication Manager CD-ROM into the */tftproot* directory on the S8300B.

   Note:

   The CD-ROM may not contain the latest firmware. Therefore, you should check the Avaya Support Web site for the latest firmware versions and match these against the versions in the directory. If the CD-ROM does not contain the latest versions, you should download the latest versions from the Support Web site to the laptop.
4. Connect the laptop to the services port of the S8300B media server.
5. Access Avaya IW. See Accessing Avaya IW on page 119.
6. Run Avaya IW to perform the required upgrades:
   - See Gateway configuration on page 139 for instructions for upgrading Avaya CM software.
   - See Firmware configuration on page 143 for instructions for upgrading G250 firmware.

Upgrading G250 firmware using the CLI

You can upgrade firmware using the CLI. You can perform the upgrade remotely via a modem connection, but the upgrade files must first be downloaded to an FTP or TFTP server on the LAN connected to the G250.

To upgrade G250 firmware using the CLI:

1. Prepare installation worksheets. See Preparing installation worksheets on page 86.
2. Set up an FTP or TFTP server on the LAN connected to the G250. For information about setting up a TFTP server, see Setting up a TFTP server on page 87.

   Note:

   If you use an FTP server, the G250 prompts you for a username and password when you enter a command to transfer a file. Also, when opening an FTP connection to the S8300B, all anonymous FTP file transfers are restricted to the /var/home/ftp/pub directory. Permission for anonymous FTP users to create files in other directories is denied.
3. Download the firmware files to the FTP or TFTP server. See Downloading G250 firmware files to a local TFTP server on page 88 or Installing firmware from the TFTP server on the S8300B Media Server on page 89.
4. Connect to the G250 via modem or via the CON port on the front panel. For information about connecting and enabling a modem for remote access, see Chapter 5: Connecting and enabling a modem for remote access on page 51.
5. Run CLI commands. See CLI Commands for upgrading G250 firmware on page 84.

CLI Commands for upgrading G250 firmware

You can use one of the following commands to upload an upgrade file to the G250. For each of these commands, include the full path of the file and the IP address of the FTP or TFTP host as parameters. When you enter the command, the CLI prompts you for a username and password.

- Use the **`copy ftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an FTP server.
- Use the **`copy ftp SW_imageA`** command to upgrade the G250 firmware into Bank A from an FTP server.
- Use the **`copy ftp SW_imageB`** command to upgrade the G250 firmware into Bank B from an FTP server.
- Use the **`copy tftp module`** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from a TFTP server.

- Use the **copy tftp SW_imageA** command to upgrade the G250 firmware into Bank A from a TFTP server.
- Use the **copy tftp SW_imageB** command to upgrade the G250 firmware into Bank B from a TFTP server.
- Use the **copy ftp module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from an FTP server.
- Use the **copy ftp SW_imageA** command to upgrade the G250 firmware into Bank A from an FTP server.
- Use the **copy ftp SW_imageB** command to upgrade the G250 firmware into Bank B from an FTP server.
- Use the **copy tftp module** command, followed by the module number of the module you want to upgrade, to upgrade the firmware on a media module from a TFTP server.
- Use the **copy tftp SW_imageA** command to upgrade the G250 firmware into Bank A from a TFTP server.
- Use the **copy tftp SW_imageB** command to upgrade the G250 firmware into Bank B from a TFTP server.

When using FTP or TFTP commands, you must use the specific path to the file on the FTP or TFTP server according to the home directory of the service (FTP or TFTP) that you are using. For example, to upgrade the firmware of an MM340 media module in slot 2 from a TFTP server with the IP address 192.1.1.10, where the home directory is c:\home\ftp\ and the upgrade file is located in the directory c:\home\ftp\version, use the following command:

```
copy tftp module \version\mm340v51.fdl 192.1.1.10 2
```

Note:

When uploading firmware from the S8300B, use only the file name, without the directory path, in the command line. Otherwise, the procedure will fail. For instance, in the example above, you must use the following command:

```
copy tftp module mm340v51.fdl 192.1.1.10 2
```

Note:

When uploading firmware from the S8300B using TFTP, you may need to enable TFTP service in the Set LAN Security parameters of your web server.

The following example uploads a firmware version with the path and file name C:\G250.net from an FTP server with the IP address 149.49.134.153 to Bank A of the G250:

```
copy ftp SW_imageA C:\G250.net 149.49.134.153
```

Preparing installation worksheets

Before you perform the upgrade, enter the names of the target software and firmware versions that you need to install in the software and firmware upgrade worksheet. See Software and firmware upgrade files for upgrade on page 86.

If you will need to set up a TFTP server, you also need to plan the TFTP server IP address, login and password. Enter these values in the TFTP Server Values worksheet. See TFTP server values on page 86.

Software and firmware upgrade files for upgrade

Enter software and firmware upgrade file names in the following table:

Table 4: Software and firmware upgrade file names

Items for Upgrading	New file name for target
Files for LSP and primary controller (not used with Gateway Installation Wizard or for individual files)	
G250 Processor	
MMANALOG (Integrated Analog)	

TFTP server values

Enter the TFTP server information in the following table:

Table 5: Global Settings for TFTP Server

TFTP Server IP Address	TFTP Server Directory

Setting up a TFTP server

To load individual firmware files on an Avaya G250 Media Gateway, you must place the files on a PC connected to the customer's LAN or on an S8300B Media Server in the customer's network. Later, you will log onto the G250 and use its TFTP capability to download the new firmware. If you can use an S8300B Media Server to stage the firmware, see Installing firmware from the TFTP server on the S8300B Media Server on page 89. If not, a TFTP server must be set up on the LAN.

Note:

A Linux or Unix TFTP server should be used only if a Linux or Unix TFTP server already exists on the local network. In this case, download the appropriate files to your laptop and give it to the customer for proper placement and execution.

To set up a TFTP on the LAN:

1. On the hard drive of the local PC, create a directory into which you will load the G250 firmware. It is recommended that you call the directory C:\tftp.
2. Connect to the LAN using a browser on the local PC and access http://www.avaya.com/support on the Internet.
3. Search for Software Downloads or FTP Server Application
4. Double-click one of the links listed with *TFTP Server*. The TFTP Server is on the Communication Manager CD-ROM For example:
   4630 IP Telephone R 1.73 and TFTP Server.
5. Scroll to the bottom of the page to find the TFTP Server Application file, *iptel_avaya_tftp.exe*.
6. Double-click the file and download it to the local PC that will serve as the TFTP server. Record the directory location of the file.

   Note:

   You may also wish to download and view or print the file *iptel.pdf*, which provides instructions on installing *iptel_avaya_tftp.exe* for Windows servers.
7. After downloading the *iptel_avaya_tftp.exe* file to the PC, double-click the file and follow instructions to install it. By default, the installation program creates the directory *C:\Program Files\Walusoft\TFTPSuite* containing the application files.
8. When the file has been installed, go to the directory where the software was installed and double-click the file *tftpserver32.exe* to open the program. The TFTP Server window appears and displays the IP address of the PC in the upper border, plus port 69.

9. Enable the TFTP server as follows:
   - From the **System** menu, select **Setup**. The server option window appears.
   - Select the **Outbound** tab, and enter the directory location of the TFTP server for the outbound file path.
   - Select the **Options** tab, and enter **69** in the **Use Port** field (default).
   - Select **No Incoming** (default). However, if you wish to copy files as a backup prior to performing a software upgrade, leave this field unselected.
   - Select the **Inbound** tab, and enter the directory path of the TFTP server for the inbound file path.
   - Click **OK**.

Downloading G250 firmware files to a local TFTP server

This section describes how to download the individual firmware files from the Avaya website to a TFTP server on the local network with the G250.

If you are upgrading

Note:

If you are performing the upgrade using the G250's Command Line Interface (CLI) or the Upgrade Tool, you can place the upgrade files on an FTP server. However, the GIW requires that the files be placed on a TFTP server.

To download firmware files from the Avaya Web site to a TFTP directory:

1. Access the www.avaya.com/support Web site.
2. Navigate to the G250 Media Gateway Downloads section:

   A list of firmware files appears.
3. Locate the file names that match the files listed in your installation worksheet. See Table 6: Sample Software and Firmware Filenames on page 89 for sample firmware file names.
4. Double-click the file name of the file you want to download. A File Download window appears.
5. Select **Save this file to disk**.
6. Save the file to directory on the TFTP server on the local LAN that was created for this purpose. See Setting up a TFTP server on page 87.

Note:

Use WinZip or another zip file tool to unzip the file, if necessary, *before* you copy the file to the TFTP server.

Table 6: Sample Software and Firmware Filenames

Component	Filename Example
G250 Processors	
G250 Processor	G250_sw_21_11_0.bin
G250 Device Manager	G250_emweb_1_0_7.bin
MMANALOG Media Module (Integrated Analog)	mmanalogv3.fdl

Installing firmware from the TFTP server on the S8300B Media Server

Note:

You only have to do this if you have not upgraded the 8300B first or if you did upgrade it first and found that the gateway files on the communication manager CD were out of date. Otherwise when you upgrade the 8300B, the files appear in the /tftpboot directory automatically.

Instead of using a separately configured TFTP server on the LAN, you can use the TFTP server capability of an S8300B Media Server to stage the firmware for upgrading the G250. To do this, you must copy the individual firmware files to the */var/home/ftp/pub directory* on the S8300B Media Server using the Download Files Web page on the S8300B Media Server. You must then copy the files to the */tftpboot* directory of the S8300B Media Server.

After copying the files to the */tftpboot* directory, you can use the GIW or the Upgrade Tool to install the files to the G250 or its media modules by specifying the S8300B Media Server's IP address as the TFTP server containing the new firmware files.

To copy firmware files to the */tftpboot* directory of an S8300B Media Server:

1. Use Telnet, Avaya Site Administration, or another tool to access the S8300B Media Server command line.
2. Log in as *craft*.
3. At the Linux prompt, type **`cd /var/home/ftp/pub`** and press **<Enter>**. The Linux prompt reappears. The current directory has changed to */var/home/ftp/pub*.

4. At the Linux prompt, type **mv** <***firmware_filename***> **/tftpboot**, and press **<Enter>** to move the firmware file to the */tftpboot* directory. To move multiple firmware files (most firmware files have an .fdl suffix), use the command **mv *.dfl /tftpboot**. The Linux prompt reappears. The firmware file has been moved to the */tftpboot* directory. If you copy the firmware using the cp command, remove the files from the */var/home/ftp/pub* directory after you have copied them.
5. Repeat step 4, if necessary, for each firmware file you want to install.
6. At the Linux prompt, type **cd /tftpboot**. The Linux prompt reappears. The current directory has changed to */tftpboot*.
7. At the Linux prompt, type **ls**, and press **<Enter>**. A list of files in the directory appears.
8. Check the directory to make sure the firmware files you want to install are listed.

Chapter 11: Upgrading IP phone configuration and firmware files

This chapter describes how to upgrade the firmware and configuration files for IP phones using the G250 TFTP server and includes the following sections:

- Overview. An overview of upgrading the configuration and firmware files for IP phones
- Administering the Upgrade. Step-by-step instructions for upgrading IP phones
- TFTP IP telephone upgrade example. A complete example of performing upgrades for three types of IP phones
- Upgrading Considerations. Additional information for performing an upgrade

Note:

If you have an S8300B installed in the G250, you can upgrade IP phones using the CM web pages.

Overview

Configuration files and firmware files for IP phones can now be downloaded using Trivial File Transfer Protocol (TFTP). TFTP can be used to download configuration, update instructions, and firmware files to IP phones. The TFTP server stores the image files and configuration (upgrade and settings) files of the IP phones. You can use both Avaya Installation Wizard and GIW to upload IP phone files to the TFTP Server located on the G250 Media Gateway.

The TFTP server supports requests to read files from a special directory ("/phonedir/") for phone images and scripts.

Note:

The IP address of the TFTP server is the PMI.

The TFTP Server feature supports the following IP telephones:

- 4601
- 4602
- 4602SW
- 4606
- 4610SW
- 4612/24

- 4620
- 4620SW
- 4690
- SIP phone: 4602 SIP

The TFTP Server feature does not support the following IP telephones:

- 4630
- 4630SW

Administering the Upgrade

When using supported IP phones with the G350, the IP phones require the downloading of the settings file and the upgrade scripts. These files are stored in the script banks in NVRAM and are preserved in the event of a reset or power failure. There are two script banks.

In addition, each phone can have a booter and a phone application. There are four banks that can store up to two phone images (booter and phone application files) at any given time. Since the image files are stored in RAM, a reset or power failure *erases* these files. The image files are used only for upgrading the IP phone, so there is no need to store them permanently. However, the scripts are used by the IP phones when they are reset, and are therefore stored in NVRAM. You can upgrade up to two types of phones and then release the banks for use with another IP phone type.

There are cases where the image files are the same for different IP phone types. In these cases, you can download the image files once for the IP phones that use the same image. The scripts are global to all the supported IP phone images.

You can download and then upload setting script files in order to update their content. It is not recommended to change the upgrade script.

There are four image banks, supporting two complete IP phone images in RAM, provided the combined file sizes do not exceed the RAM allocation for TFTP server. The maximum size for a booter application or phone application file is 4.5 MB.

By default, the RAM allocation for TFTP server is 18 MB. You cannot increase the RAM allocation for TFTP server. You can, however, increase the allocation to the Sniffer cache application, by up to 10 MB, at the expense of TFTP allocation. The maximum RAM for both applications is 20 MB. There is usually no necessity to increase the RAM allocation for the Sniffer cache application, but, since configuring memory allocation is supported, it is advisable to check memory size before performing an upgrade.

CAUTION:

To activate a change in RAM allocation to the TFTP server, reset is required. Upon reset, any phone image files stored in RAM are erased.

Note:

Previous releases of TFTP server required the configuration of the DHCP server option 43/176 with the named value pair TFTPDIR=/phonedir/ in order to allow the IP phone to access the files in this directory. This configuration is still supported but is no longer required.

To upgrade IP telephones:

1. Check the available memory size for the image files using the **`show application-memory`** command. If the memory size needs to be changed, proceed to step 2, otherwise proceed to step 5.
2. Set the memory size for the image files using the **`ip tftp-server file-system size`** command.
3. Copy the running configuration to the start-up configuration using the **`copy running-config startup-config`** command.
4. Reset the G250 using the **`reset`** command.
5. Disable the TFTP server while copying new files to the device using the **`[no] ip tftp-server`** command.
6. Copy the script files for the IP phone family using one of the following commands:
   - **`copy scp phone-script`**.
   - **`copy ftp phone-script`**.
   - **`copy tftp phone-script`**.

   Note:

   The G250 uses the SSH protocol to support the use of SCP for secure file transfer. When using SCP, the G250 is the SCP client, and an SCP server must be configured on the management station. For more information about establishing an SCP session, see *Administration of the Avaya G250 Media Gateway*, 555-245-501.
7. Copy the boot image files for up to two IP phone types, using either the **`copy ftp phone-image`** command or the **`copy tftp phone-image`** command for each IP phone type.

   Note:

   The use of the **`copy scp phone-script`** command is limited to copying files of 1 MB or less. Therefore, an SCP server can be used for copying the script files, which do not exceed 128 KB, but cannot be used for copying image files.
8. Copy the phone image files for up to two IP phone types using either the **`copy ftp phone-image`** command or the **`copy tftp phone-image`** command for each IP phone type.

9. Enable the TFTP server to allow loading of the new files to the IP phones using the **ip tftp-server** command.
10. Reset the phones and wait for the installation to be completed.

Note:

Once the upgrade procedure is complete, you can delete the files using the **erase phone-image** command.

TFTP IP telephone upgrade example

In the following example, 4602SW and 4602D phones, which use the same image files, are upgraded first. Later, 4620 phones are upgraded. The script files are not copied for the second upgrade, since they are already stored in NVRAM.

To upgrade the 4602SW and 4602D phones:

1. Check the available memory size for the image files using the **show application-memory** command. If the memory size is smaller than the combined sizes of the image files for the phones, proceed to step 2, otherwise proceed to step 5.
2. Set the memory size for the image files using the **ip tftp-server file-system size** command.

```
G250-001(super)# ip tftp-server file-system-size 18128
To change ip tftp-server file system size, copy the running configuration
to the start-up configuration file, and reset the device
G250-001(super)
```

3. Copy the running configuration to the start-up configuration using the **copy running-config startup-config** command.

```
G250-001(super)# copy running-config startup-config
Beginning copy operation ..................... Done!
```

4. Reset the G250 using the **reset** command.

```
G250-001(super)# reset
This command will reset the device
*** Reset the device *** - do you want to continue (Y/N)? y

Resetting the device...
```

5. Disable the TFTP server while copying new files to the device using the **[no] ip tftp-server** command.

```
G250-001(super)# no ip tftp-server
Done!
```

6. Copy the script files for the 46xx IP phone family using the **copy scp phone-script** command:

```
G250-001(super)# copy scp phone-scriptA 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y

Username: root
Password:
Beginning download operation ...

This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-script-file status'
command
G250-001(super)#
G250-001(super)# copy scp phone-scriptB 46xxupgrade.txt 192.168.49.10
Confirmation - do you want to continue (Y/N)? y

Username: root
Password:
Beginning download operation ...

This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-script-file status'
command
G250-001(super)#
```

7. Copy the boot image files for the 4602 IP phone type BOOYAPP4602D using the **copy ftp phone-image** command.

```
G250-001(super)# copy ftp phone-imageA pub\4602dbte1_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
G250-001(super)# copy ftp phone-imageB pub\4602sbte1_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

8. Copy the phone image files for the 4602 IP phone type DEF4602D using the **copy ftp phone-image** command.

```
G250-001(super)# copy ftp phone-imageC pub\4602dape_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
G250-001(super)# copy ftp phone-imageD pub\4602sape_8.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

9. Enable the TFTP server to allow loading of the new files to the IP phone using the **ip tftp-server** command.

```
G250-001(super)# ip tftp-server
Done!
```

10. Reset the phones and wait for the installation to be completed.

To upgrade 4620 IP phones later, when the script files are already stored in NVRAM:

1. Disable the TFTP server while copying new files to the device, using the **[no] ip tftp-server** command.

```
G250-001(super)# no ip tftp-server
Done!
```

2. Copy the boot image files for the 4620 IP phone using the **copy ftp phone-image** command.

```
G250-001(super)# copy ftp phone-imageA pub\bbla20_1817.bin 192.168.49.10


Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

3. Copy the phone image files for the 4620 IP phone using the **copy ftp phone-image** command.

```
G250-001(super)# copy ftp phone-imageB pub\def20r1_8_1.bin 192.168.49.10

Username: root
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download phone-image-file status'
command
```

4. Enable the TFTP server to allow the IP phones to load the new files using the **ip tftp server** command.

```
G250-001(super)# ip tftp server
Done!
```

Note:

Once the upgrade procedure is complete, you can delete the files using the **erase phone-image** command.

Failure scenarios and repair actions

Problem	Possible cause	Action
"Free Application Memory is xxx MB. Use **show application-memory** for more details"	You tried to configure more memory than is available in the main bank.	Reduce the application memory allocation.
"Application Memory reached its limits. Sniffer and TFTP server application memory sizes restore to defaults"	You configured the total memory allocations for applications and Sniffer to more than 20 Mb in the startup configuration and performed a reset.	None. The memory allocations are set to the default values.
Cannot download file to Gateway.		Refer to the specific error message you receive.
"Not enough memory in RAM"	The remote file is larger than the available RAM.	Free more space in the RAM using the **erase phone-script** or **erase phone-image** command.
"Not enough memory in NVRAM"	The remote file is larger than the available NVRAM.	Free space in the NVRAM using the **erase phone-script** command.
"File already Exists in other Bank"	You tried to download the same file to more than one bank.	None. You cannot load the same file to more than one bank.
"TFTP - General failure"	File name or path incorrect	Check the file name and path.
"Can't start upload operation. Wrong operation parameters or other operation already in progress, please try again"	You are trying to upload a file from an empty bank.	Upload from a different bank. Download a file to the bank.

Upgrading Considerations

The following are some considerations that affect the user when upgrading IP phone configuration and upgrade files:

- Configuration files, such as upgrade script and setting files, are copied to the phone configuration banks in NVRAM, while phone images are stored in RAM.

  Note:

  Image files are cleared if you reset the gateway.

- Phone image banks are stored in the same TFTP directory. Therefore, you can not copy the same filename to more then one bank. Copying a file to a bank containing a file with the same filename causes the old file to be overwritten by the new one.
- File names for IP phone image files and script files are limited to 32 characters.

Chapter 12: Troubleshooting

This chapter provides basic troubleshooting information.

One telephone stops working

If one telephone in the network stops working, but the other telephones and data devices continue to work normally, the problem is probably with the telephone itself. There could also be a problem with the telephone's connection to the Avaya G250 Media Gateway. Take the following steps to identify the problem:

1. Replace the telephone. If the new telephone works, the problem is with the telephone itself. If the new telephone does not work, go on to the next step.
2. Connect the telephone to a different power supply. If the telephone works, the problem is with the original power supply. If the telephone still does not work, go on to the next step.
3. Connect the telephone to a different network port. If the telephone works, the problem is with the original network port. If the telephone still does not work, go on to the next step.
4. Check the module on the Avaya G250 Media Gateway to which the telephone is connected. Check whether the physical connection is loose, and tighten the connection if necessary. If the telephone still does not work, go on to the next step.
5. If the telephone is connected to a PoE port and does not have its own power supply, plug in a power supply and see if the telephone works. If it works, the problem is with the PoE configuration or power allocation. Use the **`show powerinline`** CLI command to display the relevant information. PoE may have been disabled on the port to which the telephone is connected, of the telephone may not be receiving power due to the priority level configured on the port, or due to the overall PoE power budget being exceeded. For information about PoE configuration, see *Administration of the Avaya G250 and the G350 Gateways*, 03-300436.
6. Check the LEDs on the module to which the telephone connects. Make sure the LED for the port to which the telephone is connected is lit. If it is not lit, the problem may be with the port or the module. If the ALM LED is lit, this is also an indication that there is a problem with the port or the module. Note the port and module and contact your project manager. For information on the various modules and their LEDs, see Appendix A: Front panel description on page 105.

Several telephones stop working

If some telephones in the network stop working, but others continue to work, the problem could be with a trunk or with one of the modules in the G250. If the telephones that don't work are IP telephones connected to the PoE ports, the problem could be that PoE is disabled on certain ports, or that too many or a bad selection of PoE ports are being used, or that the power supply to the PoE ports is not working. Take the following steps to identify the problem:

1. Determine whether all the telephones that are affected connect to the same switch or port. If they do, the problem is probably with that switch or port. If they do not, go on to the next step.
2. Determine whether all the telephones that are affected connected to the same module. If they do, check the LEDs on that module. If the ALM LED is lit, there may be a problem with the module. Contact your project manager. If not, go on to the next step. For information on the various modules and their LEDs, see Appendix A: Front panel description on page 105.
3. If the affected telephones are IP telephones connected to the G250, check the following:
   - The PoE configuration and status of the IP telephones. Use the **`show powerinline`** CLI command to display the relevant information. The affected telephones may not be receiving power due to the PoE power status or priority level configured on the port, or due to the overall PoE power budget being exceeded. For information about PoE configuration, see *Administration of the Avaya G250 Media Gateway*, TBA.
   - The power supply of the G250.
4. Check the ALM LED on the Avaya G250 Media Gateway chassis. If it is lit, there may be a system-wide problem. Contact your project manager. For information on the chassis, see Appendix A: Front panel description on page 105.

No power on the G250

If there is no power at all on the Avaya G250 Media Gateway, take the following steps to identify the problem:

1. Check the AC power source with a voltmeter.
2. Connect the Avaya G250 Media Gateway to a different AC power source. If the G250 has power, the problem is with the original power source. If the G250 still does not work, go on to the next step.
3. Check the ALM LED on the Avaya G250 Media Gateway chassis. If it is lit, there may be a system wide problem. Contact your project manager. See Appendix A: Front panel description on page 105.

A trunk stops working

If a trunk stops working, take the following steps to identify the problem:

1. Check the connection between the trunk and the Avaya G250 Media Gateway. If the physical connection is loose, tighten the connection. If the trunk still does not work, go on to the next step.
2. Check the ALM LED on the module to which the trunk connects. If it is lit, see *Maintenance Alarms for Communication Manager 2.1, Media Gateways and Servers*, 03-300190 for testing procedures.

A WAN line stops working

If a WAN line stops working, take the following steps to identify the problem:

1. Check the connection between the WAN line and the Avaya G250 Media Gateway. If the physical connection is loose, tighten the connection. If the line still does not work, go on to the next step.
2. Check the ALM LED on the module to which the WAN line connects. If the ALM LED is lit, the problem may be the configuration of the module or a lack of T1 signal. You can try the following:
   - For E1/T1 interfaces, use the **`show controllers`** command to view the status of the interface's controller. Make sure the controller is up, and that all error counters do not increase.
   - For all serial interfaces (E1/T1 and USB), use the **`show interfaces Serial`** command to verify that the interface and line protocol are both up.
   - For USB interfaces only, use the **`show interfaces Serial`** command to verify that all line signals are up.
   - Swap the module with another one.

     CAUTION:

     Hot insertion of a WAN module resets the G250. Therefore, any translation and other data that is in the running configuration but has not been saved to the startup configuration will be lost.

   - Check the CON LED on the module. The CON LED indicates if you have a signal. If the CON LED is lit, check with your provider that you a receiving a signal.

   For information on the various modules and their LEDs, see Appendix A: Front panel description on page 105.
3. Check the ALM LED on the Avaya G250 Media Gateway chassis. If it is lit, there may be a system-wide problem.

Appendix A: Front panel description

This appendix describes the front panels of the Avaya G250 Media Gateway chassis and media modules. You can use the front panel of the Avaya G250 Media Gateway to:

- Connect devices
- Add media modules
- View LEDs
- Reset the device
- Reset and recover from the alternate bank

The first section in this appendix describes the front panel of the Avaya G250 Media Gateway chassis, without any media modules. The subsequent sections describe the front panels of the modules that you can insert in the Avaya G250 Media Gateway.

The front panel of the Avaya G250 Media Gateway chassis

The following figures show the G250 chassis:

Figure 18: G250 chassis

Figure 19: G250-BRI chassis

The following front panel features are described:

- Media module slots on page 106
- System LEDs on page 107
- Analog telephone ports and LEDs on page 108
- Contact closure port (CCA) on page 108
- Router port (ETH WAN) on page 109
- Switched PoE ports (ETH PoE LAN) on page 109
- Console port (CON) on page 109
- USB port on page 109
- Reset (RST) and Alternate Software Bank (ASB) buttons on page 109

Media module slots

The G250 has the following media module slots:

- One standard media module slot for the S8300B (V1)
- One standard media module slot for the MM340 or MM342 (V2)

For information about the different media modules that can be housed in the media module slots, see Allocating slots on page 34.

System LEDs

The system LEDs show the status of the Avaya G250 Media Gateway. The following table shows the meaning of the system LEDs when they are lit:

Table 7: System LEDs

LED	Name	Color	Meaning
MDM	Modem Detected	Green	A modem is connected to the CONSOLE or USB port
ALM	Alarm	Red	An alarm is present in the system
CPU	CPU	Green	OFF - A test is in progress ON - Normal operation
PWR	Power	Green	OFF - No power BLINKING - Problem with power ON - Normal operation

Analog telephone ports and LEDs

The analog telephone ports are standard RJ-11 telephone network ports.

- TRUNK is a trunk port.
- The two LINE ports (ports 2 and 3) are analog telephone ports.

The analog telephone port LEDs show the status of the analog telephone ports.

The following table shows the meaning of the analog telephone LEDs when they are lit:

Table 8: Analog telephone port LEDs

LED	Name	Color	Meaning
ETR	Emergency Transfer	Green	The Emergency Transfer Relay (ETR) feature has been activated. This feature provides an emergency link between the telephone connected to the first LINE port (port 2) and the trunk connected to the TRUNK port if power is disconnected from the G250 or if the G250 becomes unregistered from its Media Gateway Controller (MGC).
ALM	Alarm	Red	An alarm is present on the board
TST	Test	Green	A test is in progress
ACT	Activity	Yellow	A call is in progress

Contact closure port (CCA)

The contact closure port (CCA) is wired as an RJ-14 port, but uses an RJ-45 network jack. This port is used to support the G250's Contact Closure feature. The Contact Closure feature is a controllable relay providing dry contacts for various applications. To implement the Contact Closure feature, connect an Avaya Partner System Contact Closure Adjunct™ box to the CCA port. The adjunct box provides two contact closures that can be operated in either a normally closed or normally open state. The contact closures can control devices such as devices that automatically lock or unlock doors or voice recording units. The CCA port can be configured so that the connected devices can be controlled by an end device, such as a telephone. For example, a user can unlock a door by keying a sequence into a telephone keypad. For more information on Contact Closure, see Step 4: Install the Avaya Partner Contact Closure Adjunct on page 50.

Router port (ETH WAN)

ETH WAN is a standard RJ-45 network port. Use ETH WAN to connect a data device to the internal router through a 10/100 mbps Ethernet port. The G250 serves as a router for the WAN.

Switched PoE ports (ETH PoE LAN)

There are eight 10/100BASE-T Power over Ethernet ports for connecting powered end devices or LAN equipment.

Console port (CON)

CON is a standard RJ-11 network port. Use the CONSOLE port to connect a console device or modem to the G250.

USB port

The USB port is not supported in this release of the G250.

Reset (RST) and Alternate Software Bank (ASB) buttons

RST is the reset button. ASB is the Alternate Software Bank button.

The Avaya G250 Media Gateway has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains a version of the G250 firmware. These may be different versions. The purpose of this feature is to provide software redundancy. If one of the versions becomes corrupted, you can reset the G250 using the other version. This is particularly important when uploading new versions.

By default, when you turn on or reset the G250, the G250 loads firmware from Bank B. This default setting can be changed by the system administrator.

You can use the ASB button on the front panel to load firmware from the bank other than the default bank during startup:

1. Press and hold the reset button.
2. Press and hold the ASB button.
3. Release the reset button.
4. Release the ASB button.

For example, if the G250 is configured to load firmware from Bank B, use the steps listed above to reset the G250 to load the firmware from Bank A instead.

The front panel of the Avaya S8300B Media Server

The S8300B Media Server is a Pentium-based processor that runs on a Linux operating system. The S8300B runs Avaya Communication Manager (ACM) to provide call control services to the G250 and other Avaya gateway devices.

The front panel of the S8300B includes:

- 10/100BaseT Fast Ethernet port (SERVICES)
- Two USB ports for modem connections or the USB CD-ROM drive (USB 1 and USB 2)

Figure 20: The S8300B Media Server

Ports

The S8300B's 10/100BaseT Fast Ethernet port is labeled SERVICES, and is located in the center of the front panel. The S8300B's two USB ports are labeled USB 1 and USB 2. They are located towards the right of the front panel.

Port LEDs

The following table shows the meaning of the S8300B's LEDs when they are lit:

LED	Name	Color	Meaning
ALM	Alarm	Red	An alarm is present
TST	Test	Green	A test is in progress When the S8300B is used as an LSP, the green LED remains lit when Avaya Communication Manager is running.
ACT	Activity	Yellow	This LED is lit whenever a G250, a G700, an IP telephone, or an IP console is registered with the S8300B. It is off when none of these IP endpoints are registered with the S8300B.

In addition, the front panel of the S8300B has a LED labeled OK TO REMOVE, which is connected to a button labeled SHUT DOWN. This LED indicates that the S8300B has been shut down, and can be removed from the G250 chassis. Do not attempt to remove the S8300B without instructions from a specially trained technician.

The front panel of the Avaya MM340 media module

The MM340 media module provides one WAN access port for the connection of an E1 or T1 WAN line. The following figure shows the MM340 media module front panel.

Figure 21: The MM340 media module front panel

Ports

The MM340's E1/T1 WAN access port is marked E1/T1. This port is located in the center of the front panel.

LEDs

The following table shows the meaning of the MM340's LEDs when they are lit:

LED	Name	Color	Meaning
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	A port is being initialized or a loopback is present
ACT	Activity	Yellow	At least one PPP/Frame Relay session is active
SIG	Signal	Green	The physical connection is up

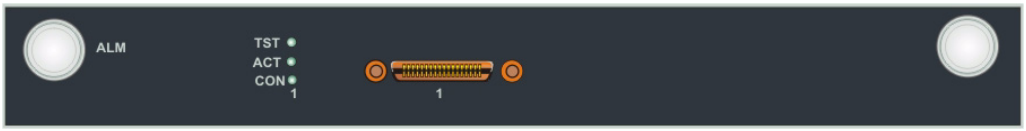
The front panel of the Avaya MM342 media module

The MM342 media module provides one USP WAN access port and supports the following WAN interface types:

- V.35/ RS449
- X.21

The following figure shows the MM342 media module front panel.

Figure 22: The MM342 media module front panel



Ports

The MM342 contains one WAN SCSI access port.

LEDs

The following table shows the meaning of the MM342's LEDs when they are lit:

LED	Name	Color	Meaning
ALM	Alarm	Red	The module type is not the type configured in the MSG for the slot
TST	Test	Green	A port is being initialized or a loopback is present
ACT	Activity	Yellow	At least one PPP/Frame Relay session is active
CON	Connection	Green	The physical connection is up

Appendix B: Technical specifications

This appendix provides technical specifications for the G250 and for compatible power cords.

G250 Media Gateway specifications

The table of technical specifications provides detailed information on the physical dimensions and tolerances of the G250 Media Gateway.

Table 9: G250 Media Gateway specifications

Description	Value
Height	2U (3.5 in., 88.9 mm)
Width	17.3 in. (440 mm)
Depth	13.375 in. (340 mm)
Weight of fully configured chassis	22 lb. (10 kg)
Ambient working temperature	32° to 104°F (0^{O} to 40^{O}C)
Operation altitude	up to 6,560 ft. (2,000) m
Minimum clearance for ventilation	2.5 in. (6.4 cm)
Humidity	5% to 95%, non-condensing

Power Cord Specifications

Following are specifications for power cords suitable for use with the G250:

For North America: The cordset must be UL Listed/CSA Certified, 18 AWG, 3-conductor (3rd wire ground), type SJT. One end is to be terminated to an IEC 60320, sheet C13 type connector rated 10A, 250V. The other end is to be terminated to either a NEMA 5-15P attachment plug for nominal 125V applications or a NEMA 6-15P attachment plug for nominal 250V applications.

For Outside North America: The cord must be VDE Certified or Harmonized (HAR), rated 250V, 3-conductor (3rd wire ground), or 0.75 mm^2 minimum conductor size. The cord is to be terminated at one end to a VDE Certified/CE Marked IEC 60320, sheet C13 type connector rated 10A, 250V and the other end to a 3-conductor grounding type attachment plug rated at a minimum of 10A, 250V and a configuration specific for the region/country in which it will be used. The attachment plug must bear the safety agency certifications mark(s) for the region/country of installation.

G250-BRI Pinouts

Table 10shows the G250-BRI printouts.

Table 10: G250-BRI pinouts

G250 RJ-45 pin	DTE View	DCE View	RJ-45 pin
1	No connection	No connection	1
2	No connection	No connection	2
3	Tx	Rx	3
4	Rx	Tx	4
5	Rx	Tx	5
6	Tx	Rx	6
7	No connection	No connection	7
8	No connection	No connection	8

Appendix C: Running the Avaya Installation Wizard (Avaya IW)

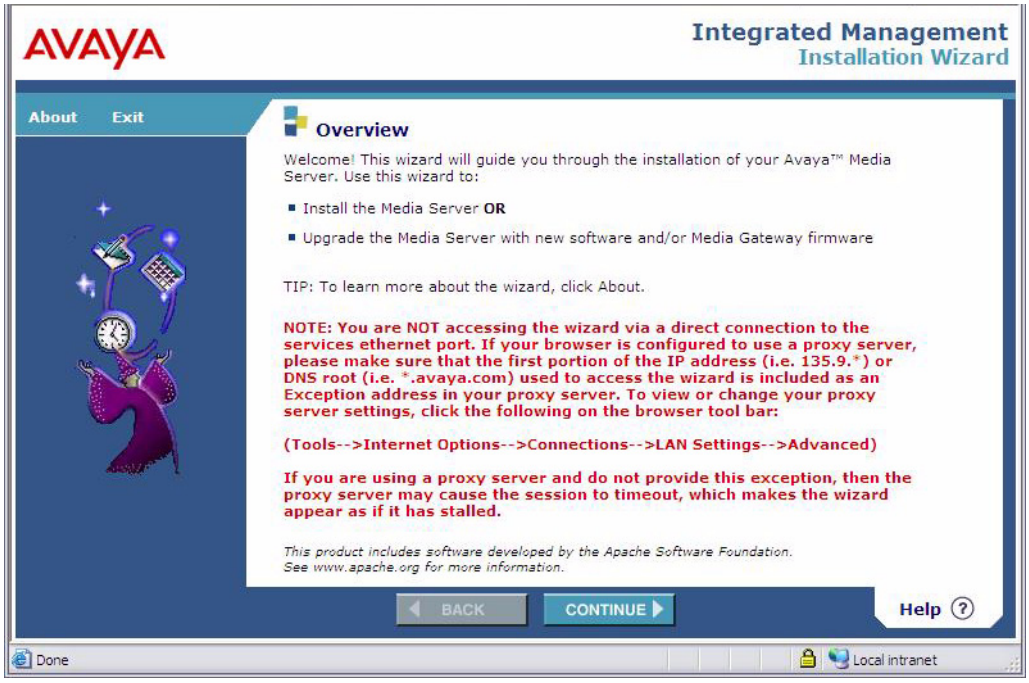
This appendix explains how to run Avaya Installation Wizard (Avaya IW). The Avaya IW is a web-based installation wizard that is used with the Avaya G250 Media Gateway to perform initial configuration tasks and to upgrade software and firmware. The Avaya IW is designed for use with systems that contain an S8300B Media Server, operating in either ICC or LSP mode. You can use Avaya IW to configure the Avaya G250 Media Gateway or to upgrade an installed S8300B with new Avaya Communication Manager (ACM) software and/or G250 firmware. If you have an EPW (see Obtain the Electronic Preinstallation Worksheet (EPW) on page 24), you will be able to upload configuration parameters from the EPW to AIW as part of your AIW session.

Accessing Avaya IW

To access the Avaya IW:

1. Connect a laptop computer to the Services port of the S8300B, using a crossover cable.
2. Make sure the laptop is configured as follows:
   - IP Address: 192.11.13.5
   - NetMask: 255.255.255.252
   - Disable DNS
   - Clear the primary WINS and secondary WINS IP Addresses
   - Disable the Proxy Server in the Internet Explorer
3. Launch Internet Explorer on the laptop and type the following URL to access the S8300B Media Server Home Page: http://192.11.13.6
4. Enter the appropriate login name and password.

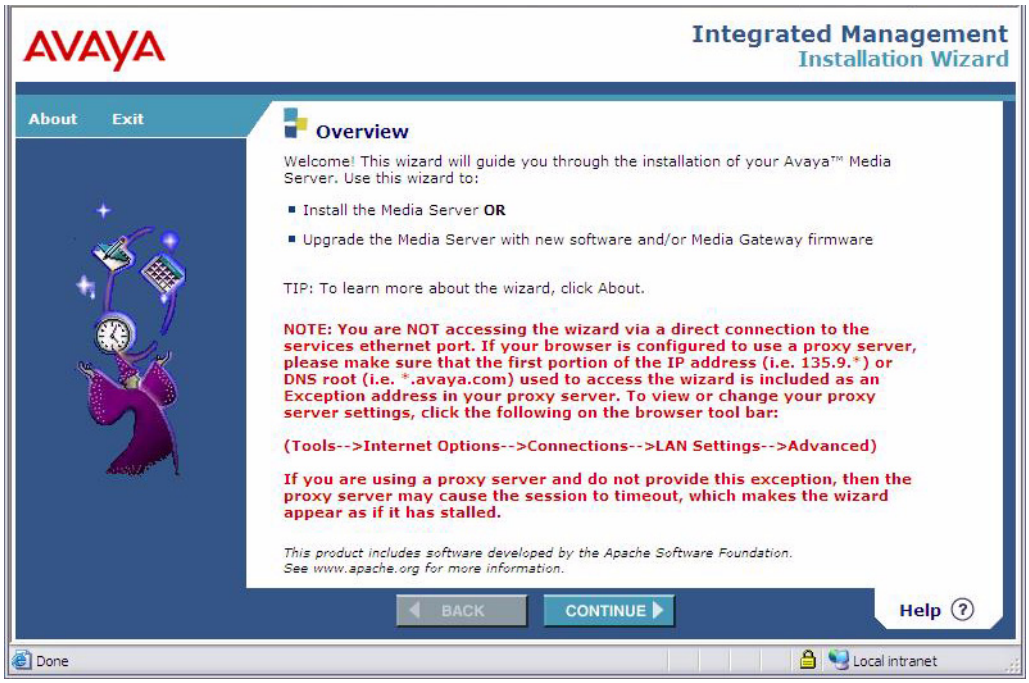
5. Select the Launch Installation Wizard link from the home page. The Overview screen appears:



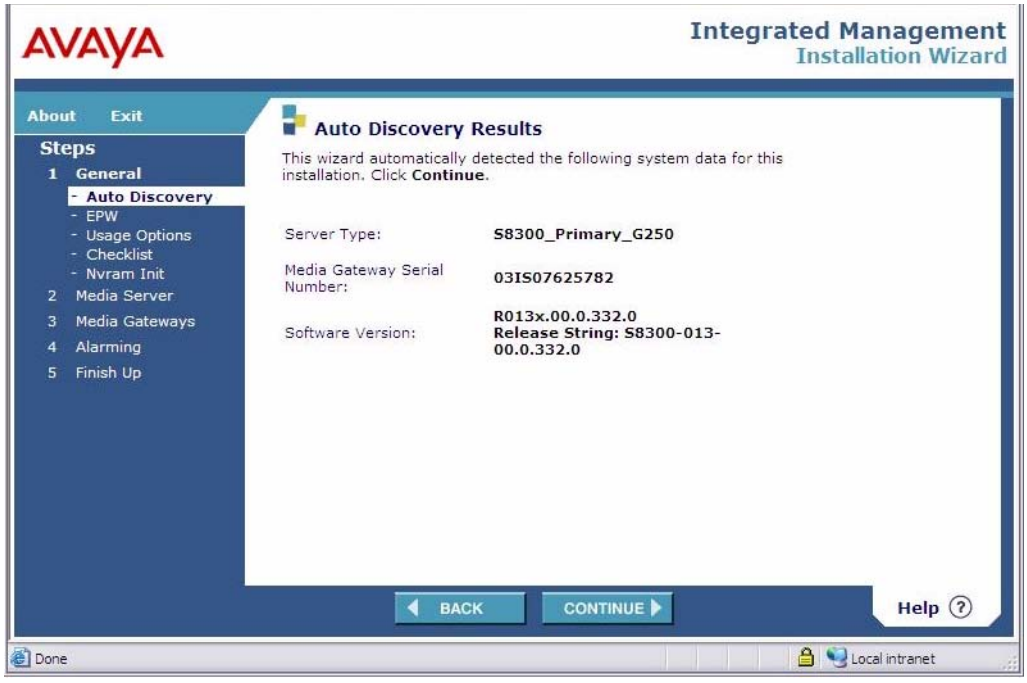
Preliminary screens

View the preliminary screens:

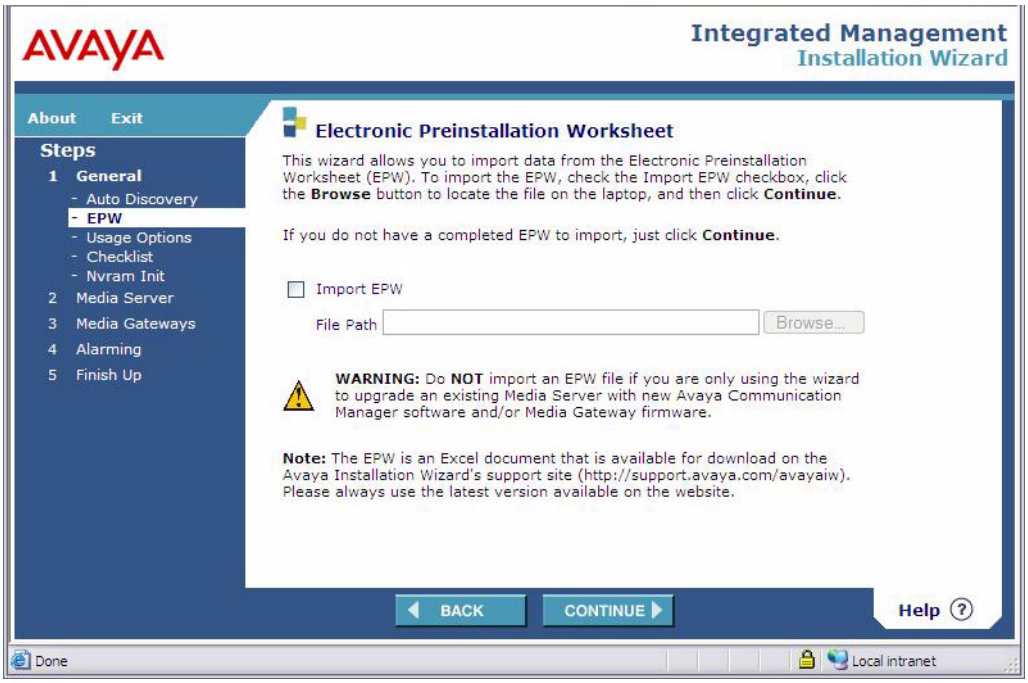
1. When you access the Avaya IW, the first screen that appears is the Overview screen:



2. Click **Continue**. The Avaya IW performs system auto-discovery and displays the results on the following screen:



3. Click **Continue**. The Import Electronic PreInstallation Worksheet screen appears. This screen allows you to import system data from the Electronic PreInstallation Worksheet (EPW). If you import and EPW, some of the fields on the subsequent screens will be filled automatically. For information about obtaining the EPW, see Obtain the Electronic Preinstallation Worksheet (EPW) on page 24.

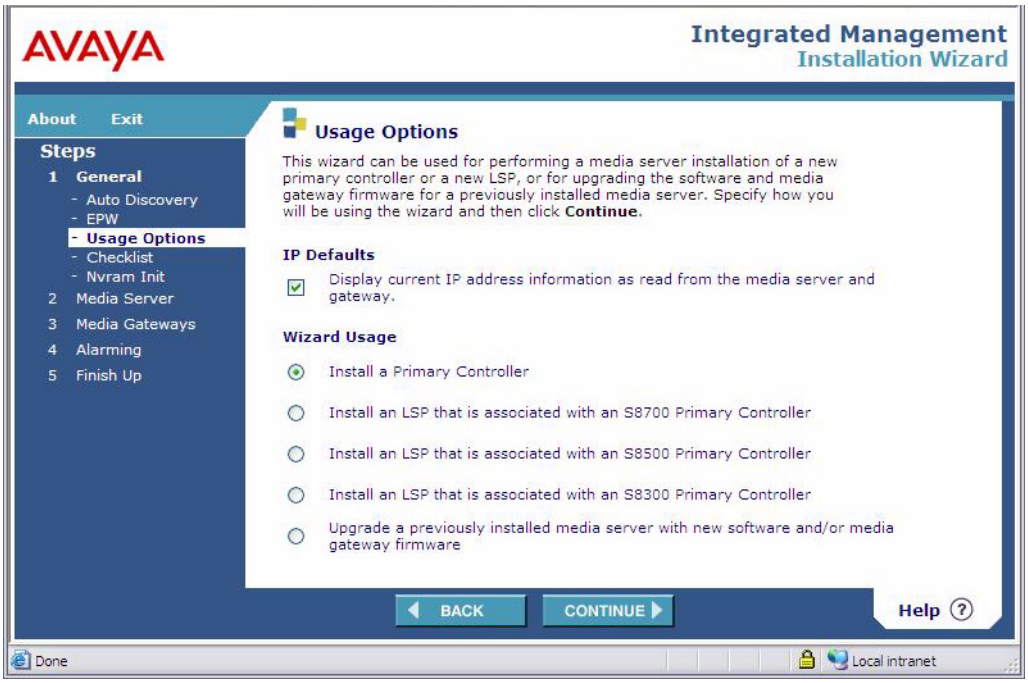


MGC configuration and upgrade

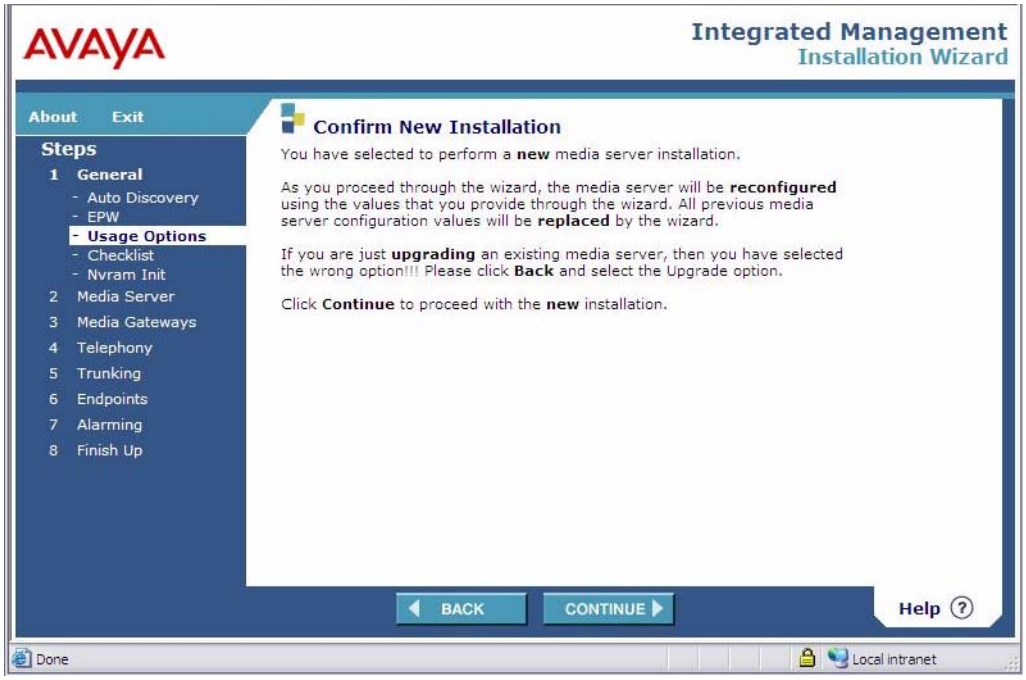
Follow these steps for an MGC configuration and upgrade:

1. Click **Continue**. The Usage Options screen appears. Specify which of the following configuration processes you would like to initiate:
   - **Install a Primary Controller**. Select this option to configure the installed S8300B media server as the primary Media Gateway Controller (MGC). The primary MGC is the MGC that the G250 searches for first to provide call processing services to the G250.
   - **Install an LSP that is associated with an S8700 Primary Controller**. Select this option to configure the installed S8300B media server as a backup MGC (LSP) and to configure an external Avaya S8700 Media Server as the primary MGC. In this case, the installed S8300B will provide backup call processing services to the G250 in case of connection failure to the primary MGC.

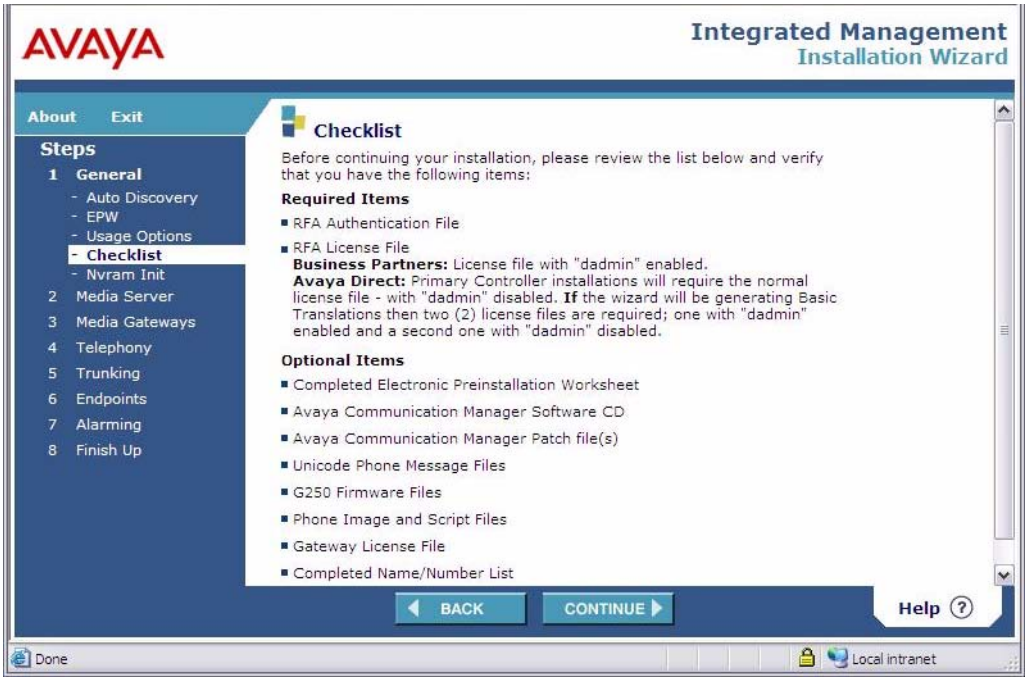
- **Install an LSP that is associated with an S8500 Primary Controller**. Select this option to configure the installed S8300B media server as a Local Surviving Processor (LSP) and to configure an external Avaya S8500 Media Server as the primary MGC. In this case, the installed S8300B will provide backup call processing services to the G250 in case of connection failure to the primary MGC.
- **Install an LSP that is associated with an S8300B Primary Controller**. Select this option to configure the installed S8300B media server as a Local Surviving Processor (LSP) and to configure an Avaya S8300B Media Server installed on an external media gateway as the primary MGC. In this case, the installed S8300B will provide backup call processing services to the G250 in case of connection failure to the primary MGC.
- **Upgrade a previously installed Media Server with new software and/or Media Gateway firmware**. Select this option to upgrade an installed Media Server with new Avaya Communication Manager software and/or Media Gateway firmware.



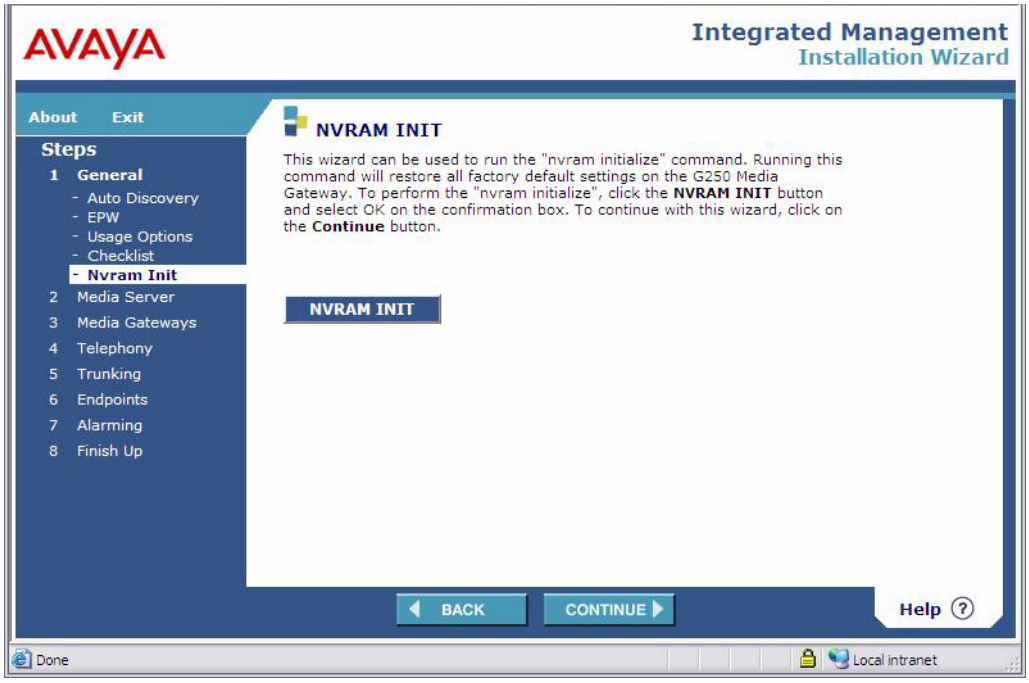
2. Click **Continue**. If you are configuring a new MGC, the Confirm New Installation screen appears, as shown below. If you are upgrading an existing MGC, the Avaya Communication Manager Software screen appears. See Upgrading an existing MGC on page 130.



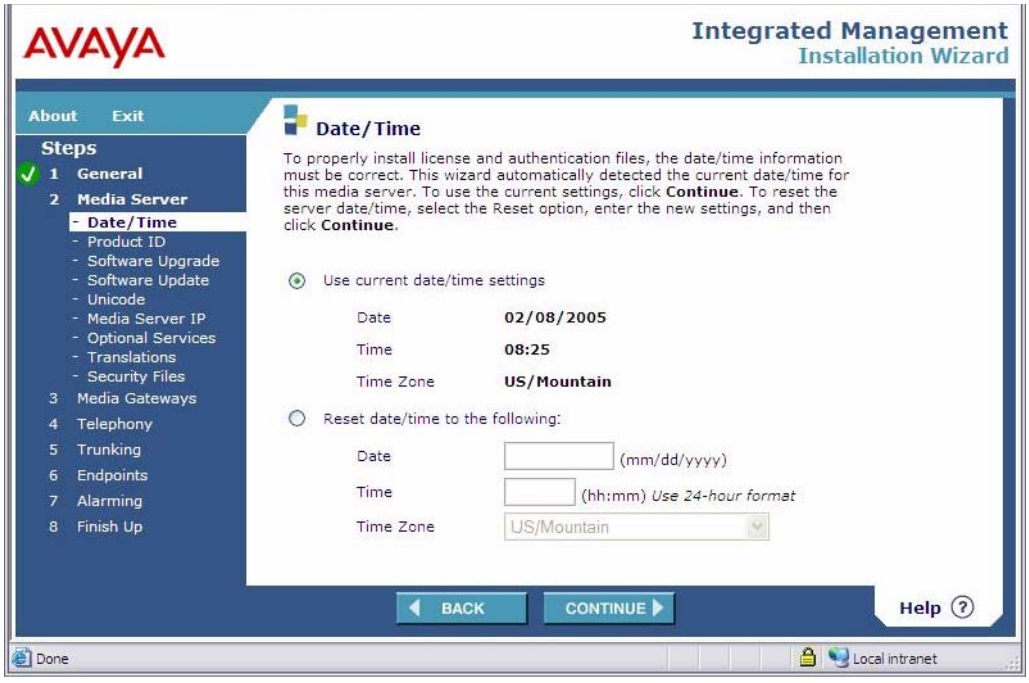
3. Click **Continue**. The Checklist screen appears. The Checklist screen displays a list of required and optional items you need to configure the G250. For details, see Chapter 2: Before you install on page 19.



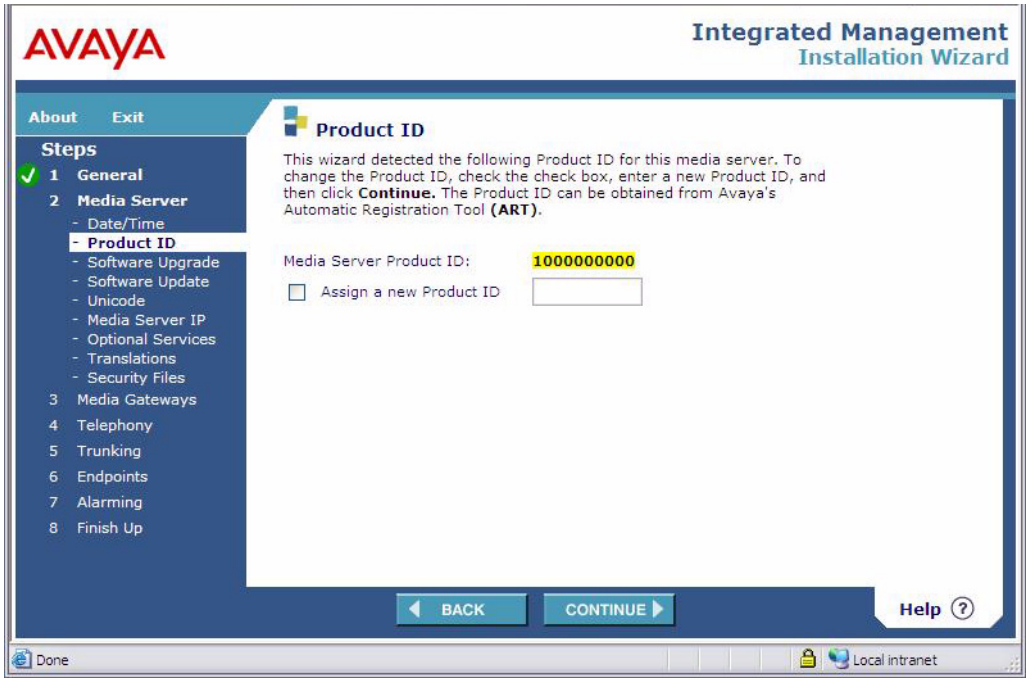
4. Click **Continue**. The NVRAM INIT screen appears. This screen allows you to restore all factory default settings.



5. Click **Continue**. The Date/Time screen appears. This screen allows you to reset the G250's date and time.



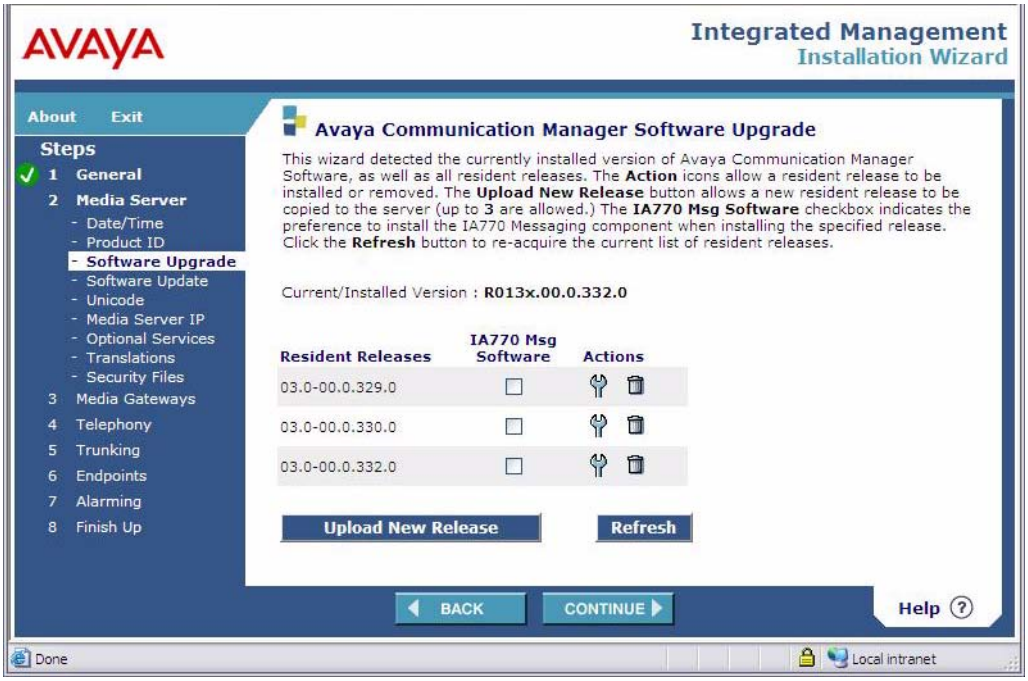
6. Click **Continue**. The Product ID screen appears. If you are configuring a new G250, enter the product ID in the ID field and select **Assign the new product ID**.



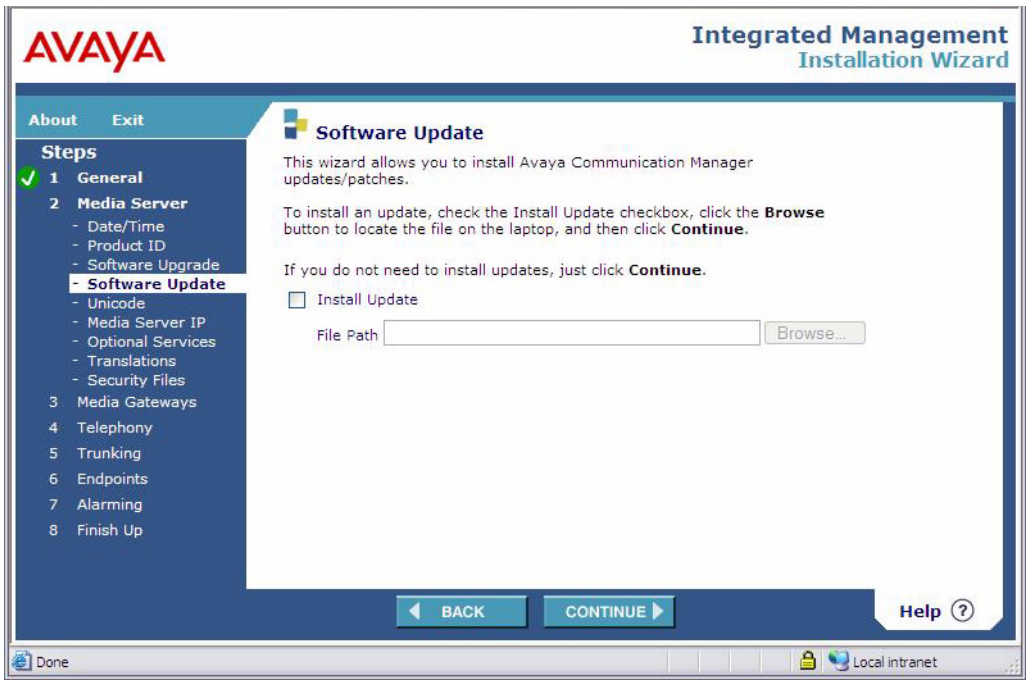
Upgrading an existing MGC

Follow these steps to upgrade an existing MGC:

1. Click **Continue**. The Avaya Communication Manager Software Upgrade screen appears. This screen allows you to upgrade the Communication Manager software on the S8300B installed in the G250.

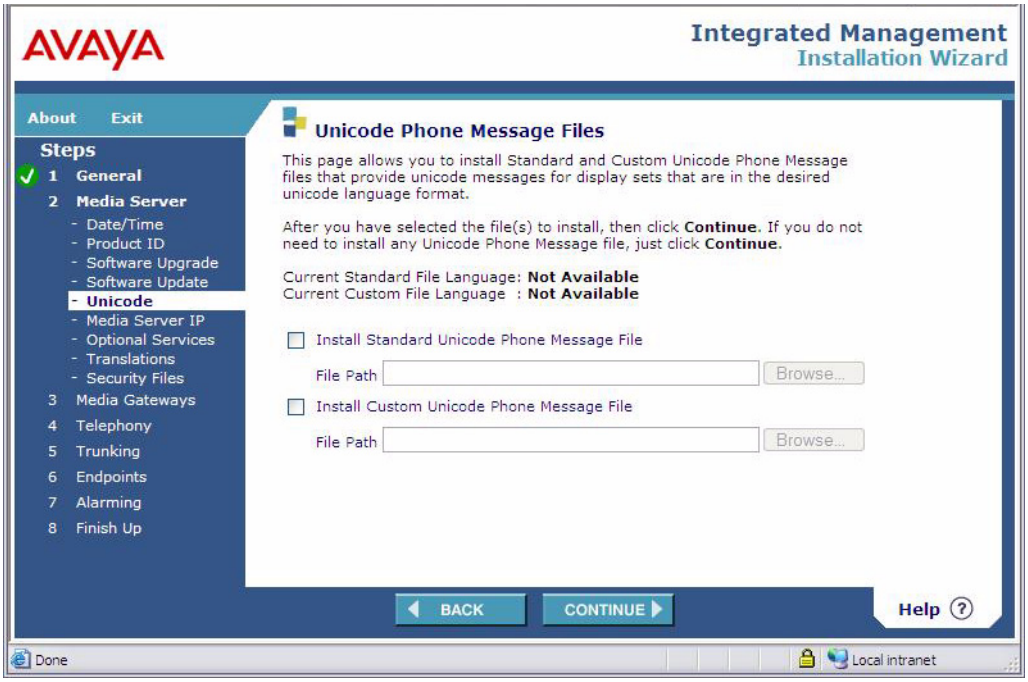


2. If you want to use the currently installed version of Avaya Communication Manager software, move on to step 6. If you want to upload aa new release of Avaya Communication Manager, click **Upload New Release**. The Software Update screen appears. This screen allows you to install Avaya Communication Manager updates.

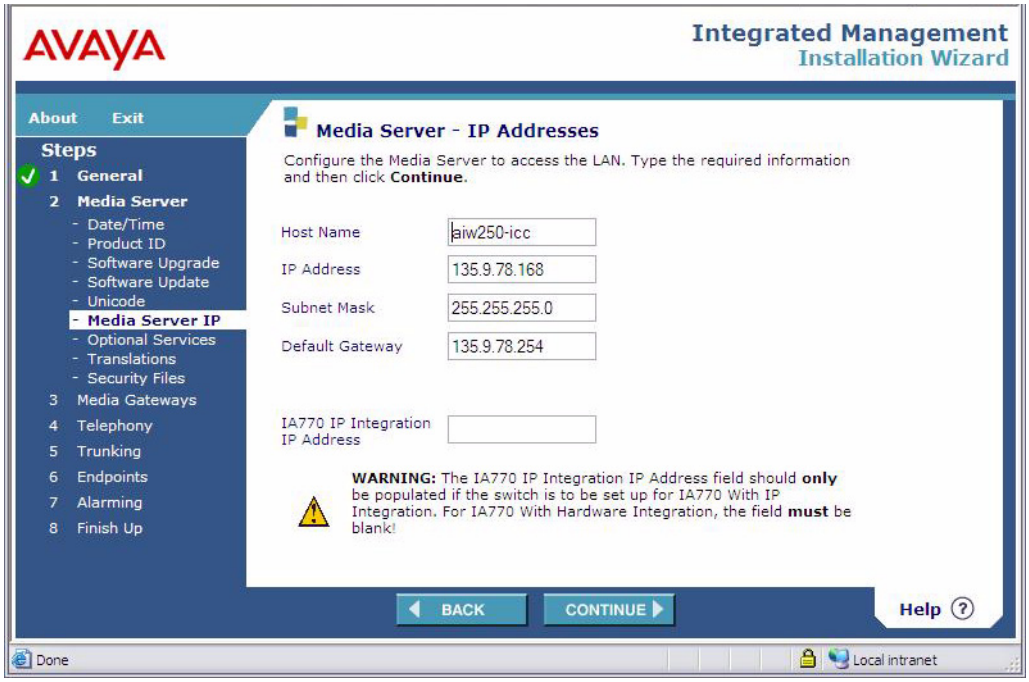


3. Check the Install Update box.
4. Enter the file path for the Avaya Communication Manager release you want to upload in the **File Path** field.
5. Click **Continue**.

6. Click **Continue**. The Install Unicode Phone Message Files screen appears. This screen allows you to install files that provide unicode messages for display sets that are in the desired unicode language format.



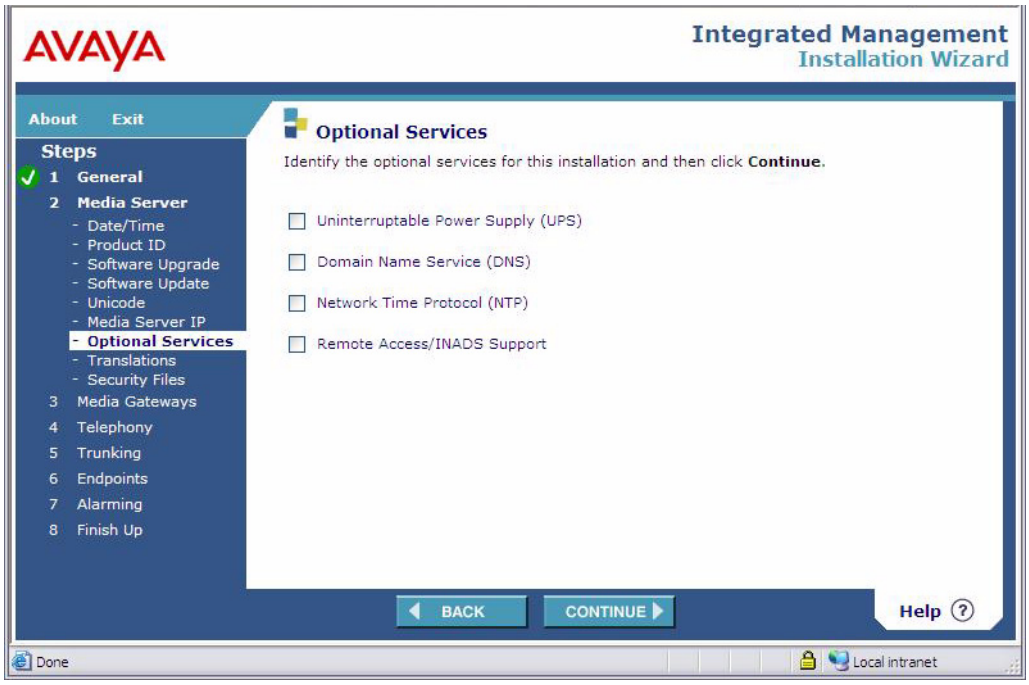
7. Click **Continue**. The Media Server - IP Addresses screen appears. If your S8300B media server is already configured, the Avaya IW should detect and display its address information in this screen. If not, you must enter the required information.



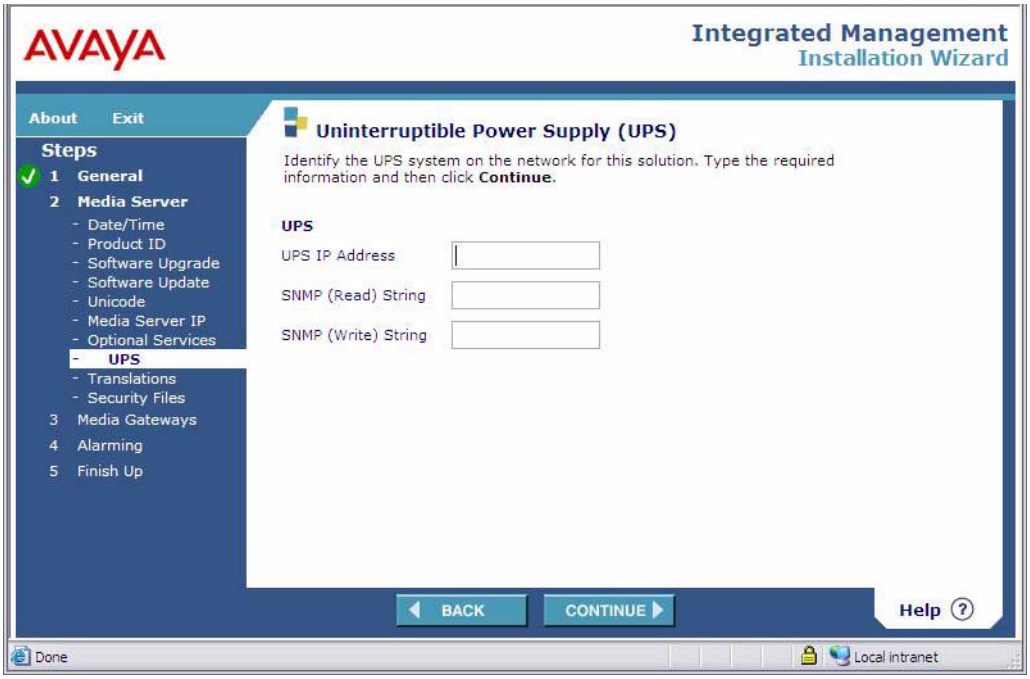
Configuring the primary controller IP addresses

To configure the primary controller IP addresses follow these steps:

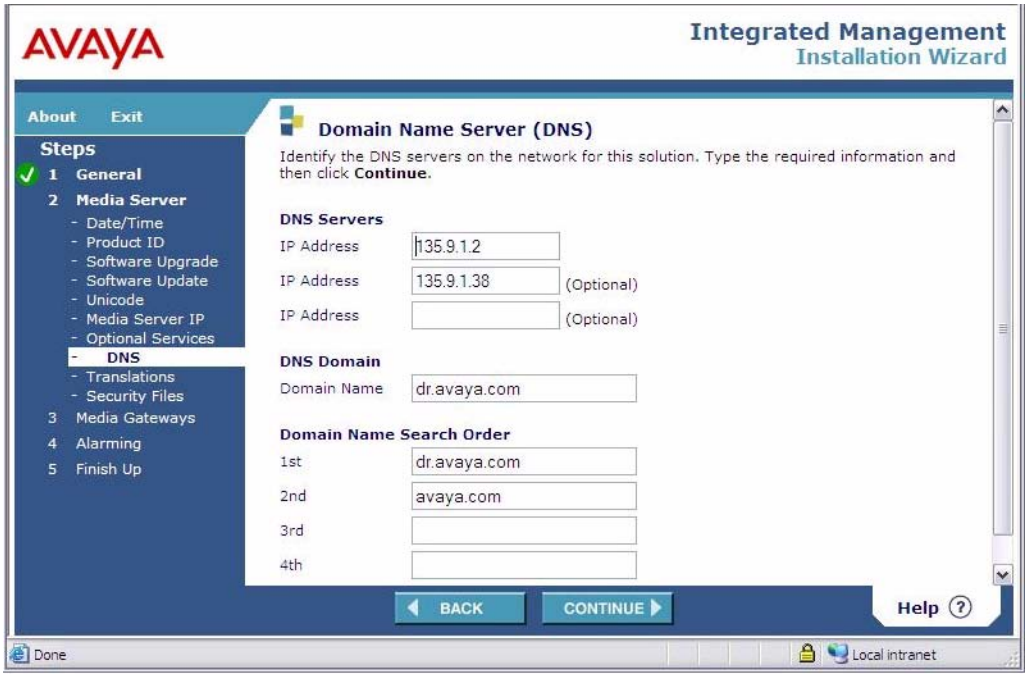
1. Click **Continue**. If you selected one of the wizard usage options for configuring an LSP in the Usage Options screen, the Primary Controller IP Address screen appears. The IP address fields differ depending on the type of primary controller. Enter the required IP address(es) for the primary controller.
2. Click **Continue**. The Optional Services screen appears. Select the services you want.



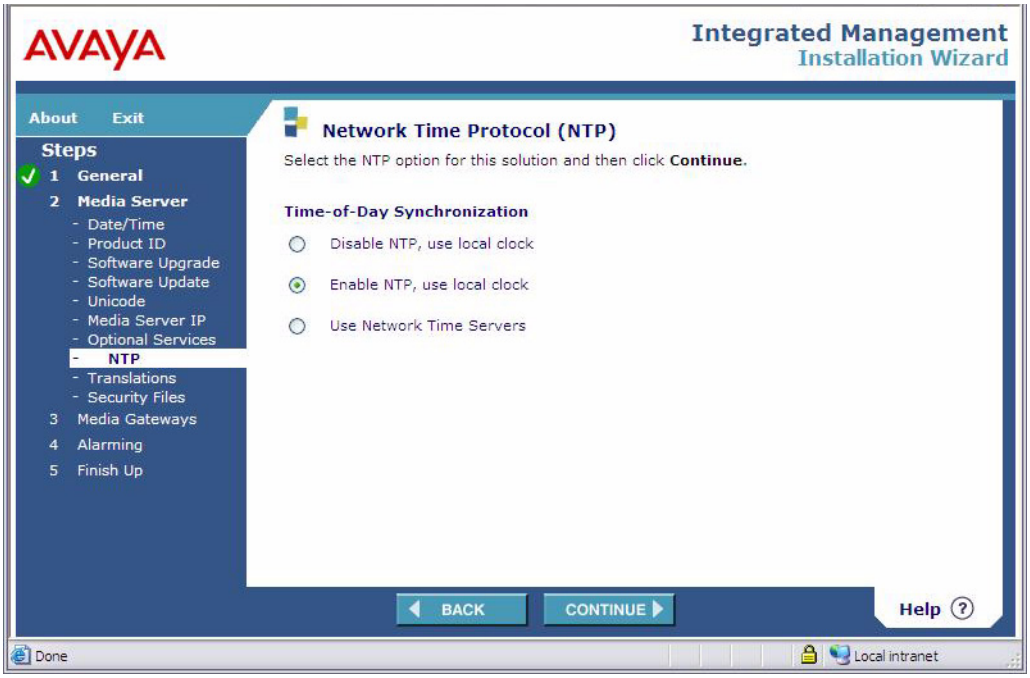
3. Click **Continue**. If you selected Uninterruptible Power Supply (UPS) in the Optional Services screen, the Uninterruptible Power Supply (UPS) screen appears. Enter the required information.



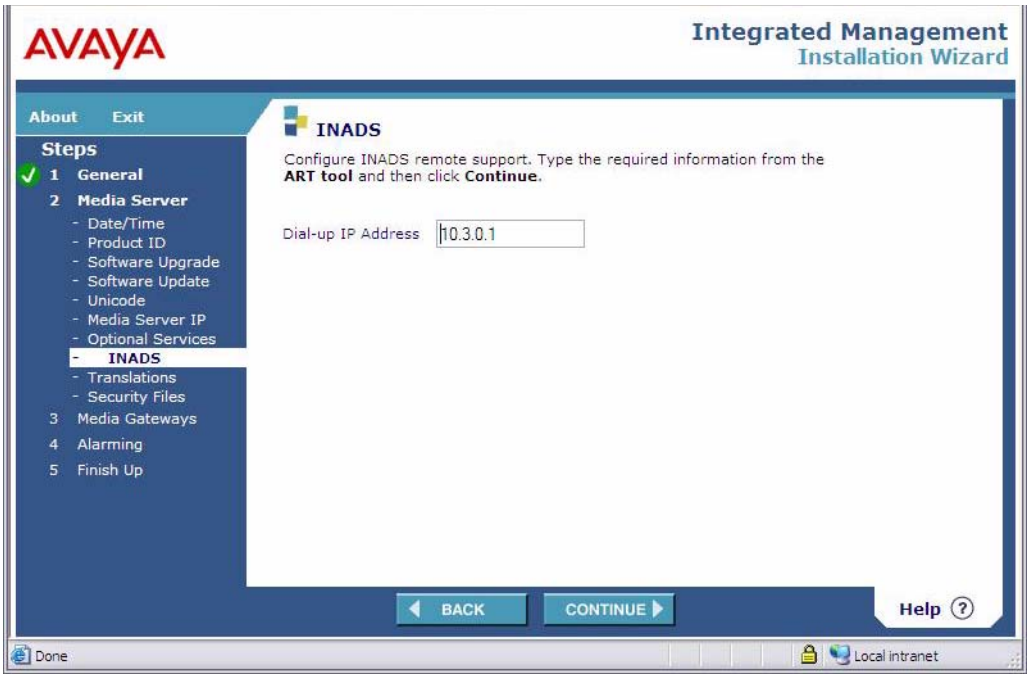
4. Click **Continue**. If you selected Domain Name Service (DNS) in the Optional Services screen, the Domain Name Service (DNS) screen appears. Enter the required information.



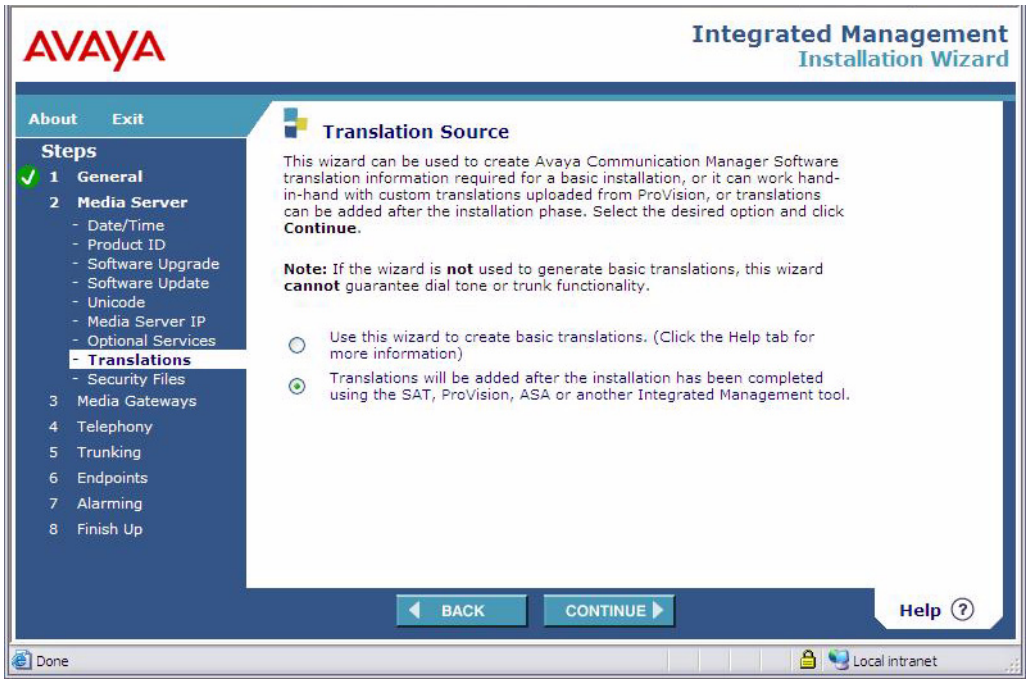
5. Click **Continue**. If you selected Network Time Protocol (NTP) in the Optional Services screen, the Network Time Protocol (NTP) screen appears. Select an NTP option.



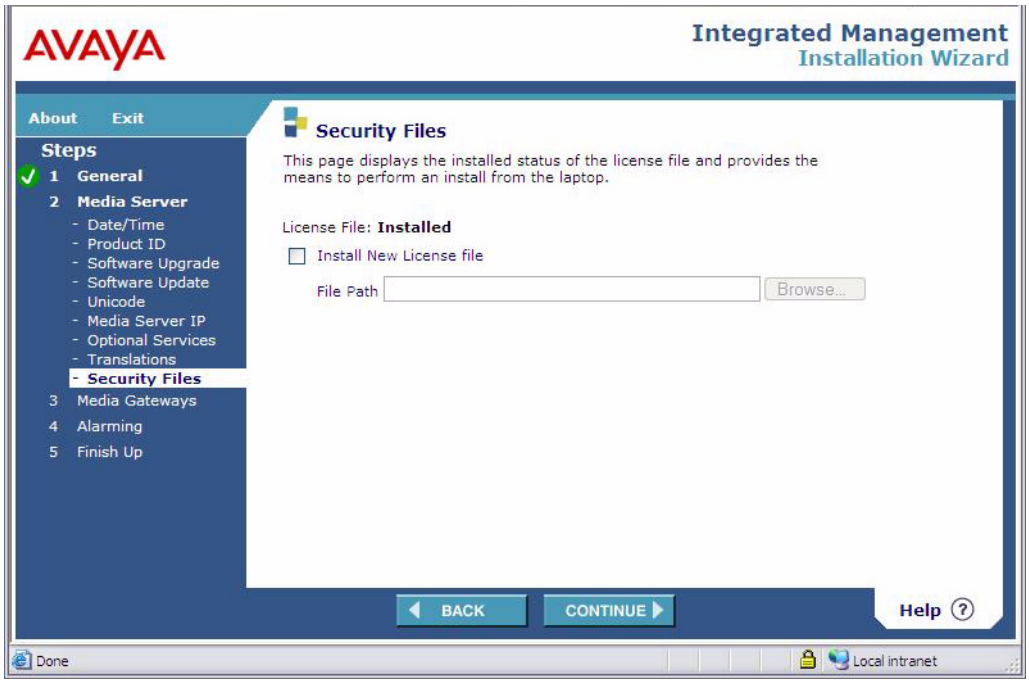
6. Click **Continue**. If you selected Remote Access/INADS Support in the Optional Services screen, the INADS screen appears. Enter a dialup IP address for Installation and Administration System (INADS) remote support. For instructions on how to obtain the INADS IP address, see *Run the Automatic Registration Tool (ART) for the RAS IP address* on page 22.



7. Click **Continue**. The Translation Source screen appears. This screen allows you to generate Avaya Communication Manager translation information. This feature provides basic translations for administration of extension ranges, trunk types, routes, class of service, feature access codes, trunk access codes, station button assignment, and several other parameters.



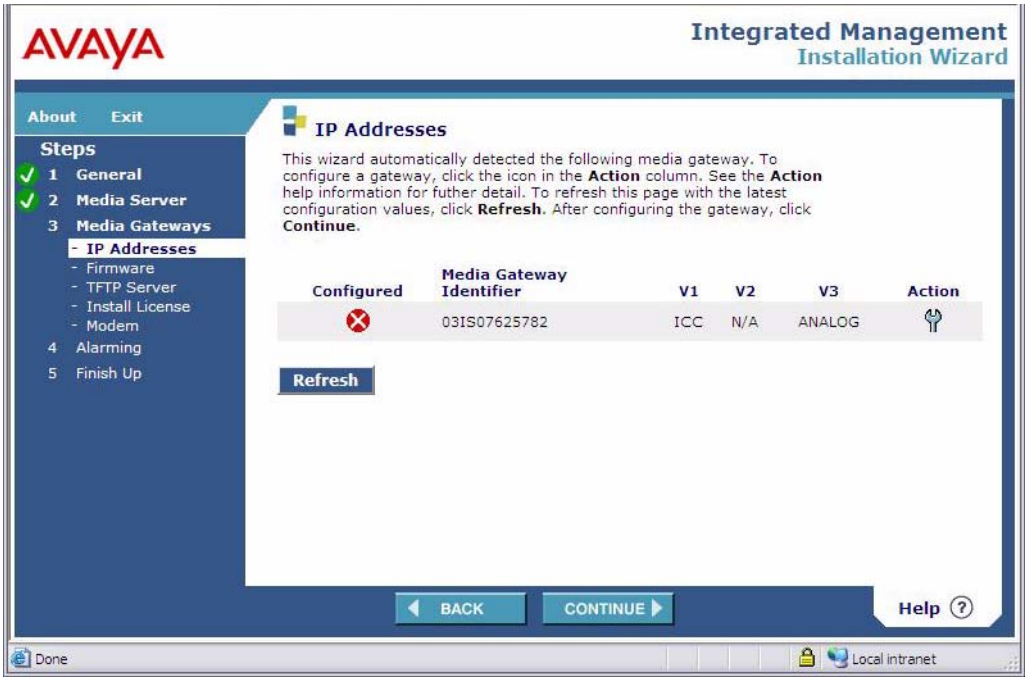
8. Click **Continue**. The Security Files screen appears. This screen displays the status of your license and authentication files, and allows you to install these files from a laptop. For information on these files, see Download License and Authentication Files to Your Laptop on page 22.



Gateway configuration

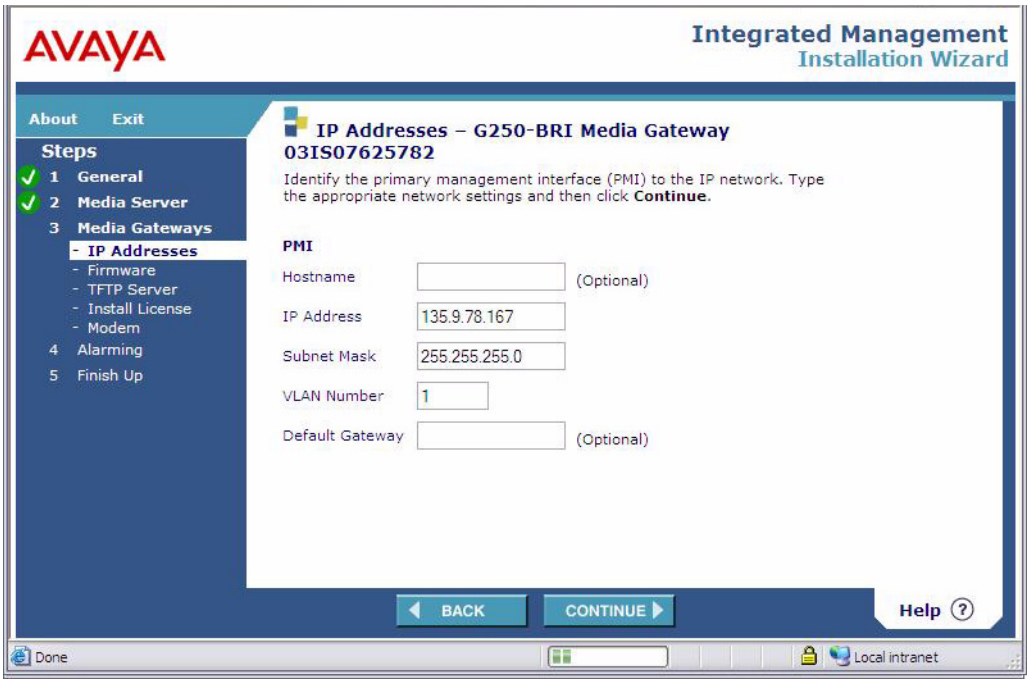
For Gateway configuration:

1. Click **Continue**. The IP Addresses screen appears. This screen displays the G250's ID, as well as the type of media module residing in each slot of the G250's chassis. To continue, click the icon corresponding to the G250 in the **Action** column.

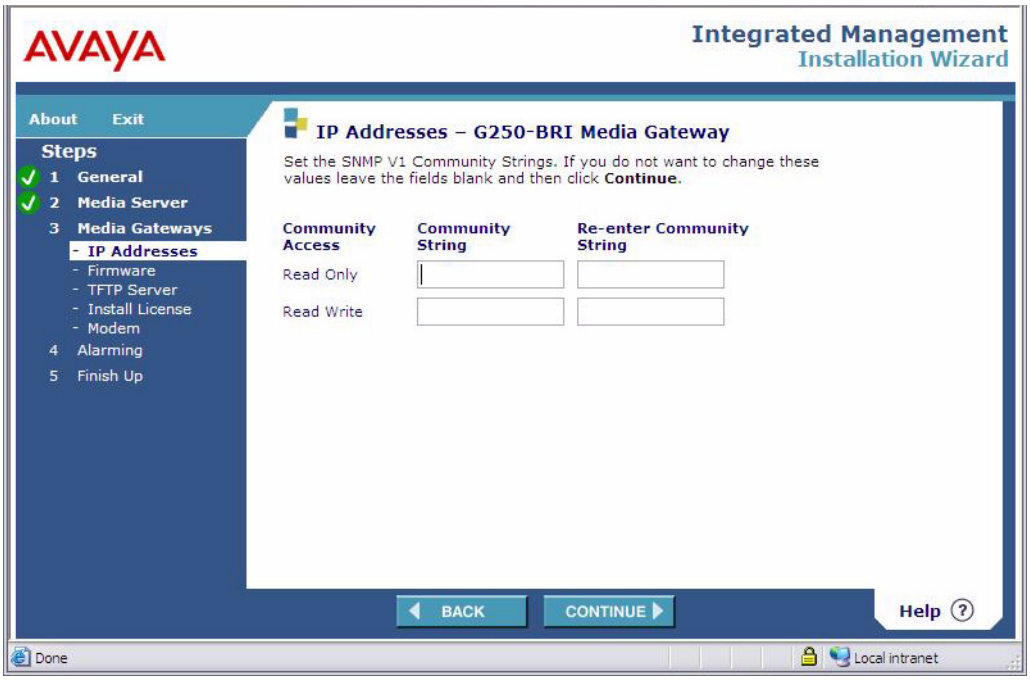


2. Click **Continue**. The PMI configuration screen appears. The IP address and subnet mask of the PMI should appear in this screen. Change this IP address and subnet mask in accordance with your system specifications. The Primary Management Interface (PMI) address is the interface used for the following management functions:
   - Registration of the G250 to an MGC
   - Sending SNMP traps
   - Opening telnet sessions from the G250
   - Sending messages from the G250 using FTP and TFTP protocol

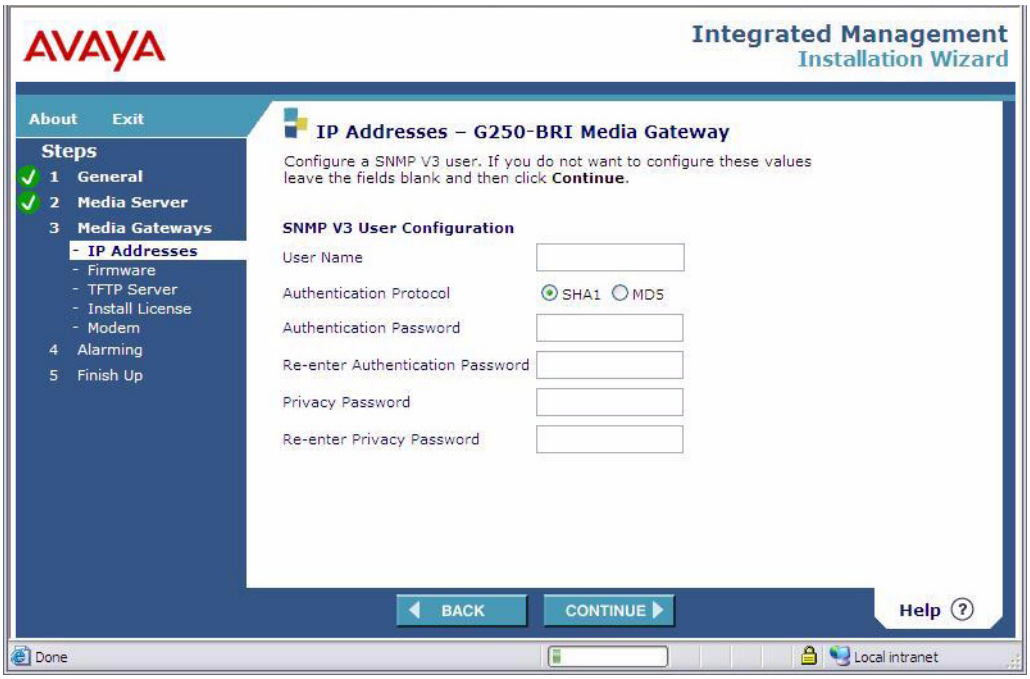
   You can assign any IP interface that the MGC recognizes to be the PMI.



3. Click **Continue**. The SNMP Community Strings screen appears. In the Read Only Community String field, specify a name for the SNMP read community access name to assign to the G250. In the Read Write Community String field, specify a name for the SNMP write community access name to assign to the G250. Re-enter the strings in the Re-enter Community String fields for confirmation. For information about SNMP, see *Administration of the Avaya G250 and the G350 Gateways,* 03-300436.



4. Click **Continue**. The SNMP V3 screen appears.

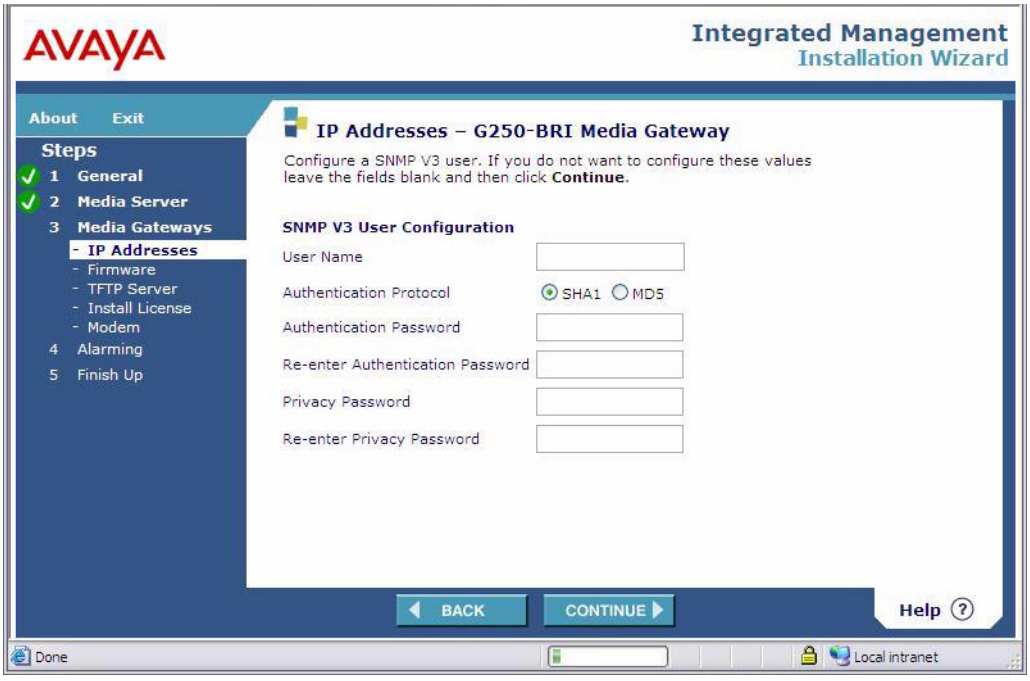


5. Complete all fields if you want to configure and SNMPv3 user. Otherwise leave all fields blank.

6. Click **Continue**. The Media Gateway Controller Information screen appears. Configure the list of Media Gateway Controllers (MGCs) that will provide call processing services for the G250. You must specify a primary MGC in the first IP address box. You can specify up to three backup MGCs in the optional IP address boxes, in priority order. The G250 searches for the primary MGC first. If it cannot connect to the primary MGC, it searches for a backup MGC. An MGC may be the Avaya S8300B Media Server installed in the G250 or an external Avaya S8500 Media Server or Avaya S8700 Media Server, or an Avaya S8300B Media Server installed in an external media gateway. Specify your primary MGC in accordance with the usage option you chose (see MGC configuration and upgrade on page 123). If you do not configure the S8300B installed in the G250 as the primary MGC, configure the S8300B as a backup MGC.

   Note:

   To register an S8500 or S8700 media server as the MGC, use the IP address of the media server's Control-LAN card (CLAN) rather than the IP address of the media server itself.



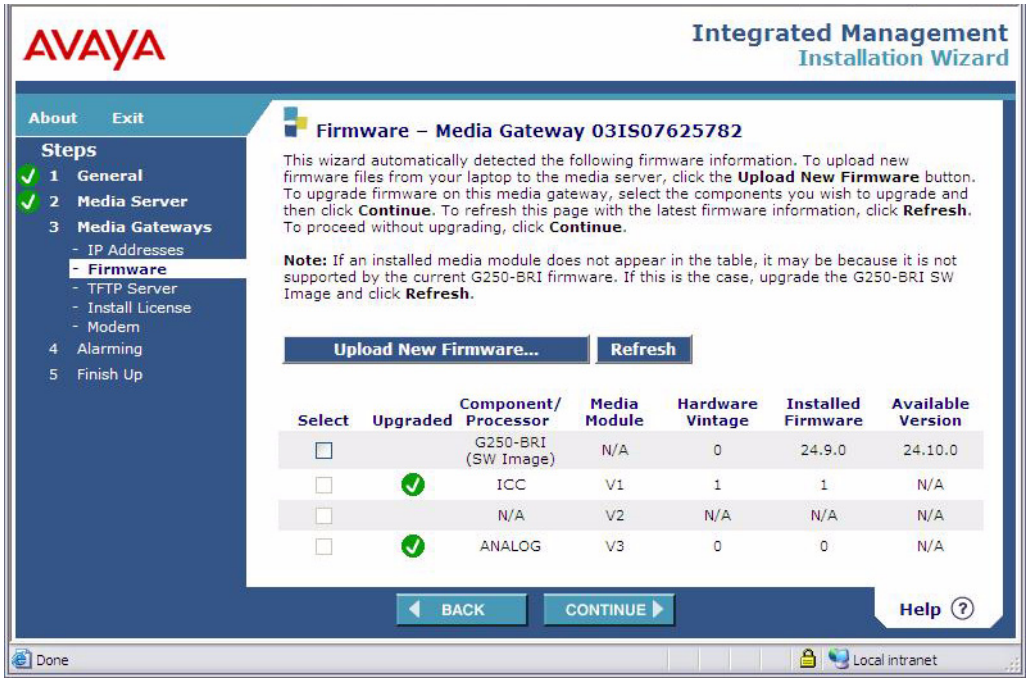
Firmware configuration

For firmware configuration:

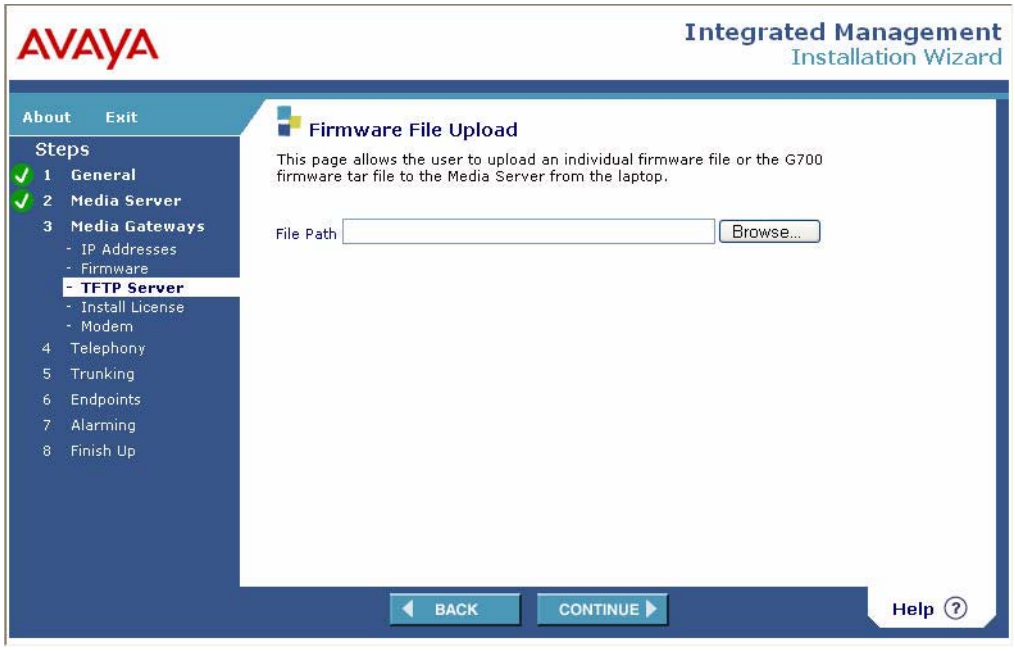
1. To upgrade the G250 firmware, click **Continue** on the Media Gateway Controller Information screen.

   The Firmware screen appears. This screen displays the currently installed firmware versions on the G250 and its media modules, as well as the most recent available versions.

   - To upgrade firmware, select the modules you want to upgrade and click **Continue**.
   - To upload a new firmware version from a laptop, click **Upload New Firmware**. The Firmware File Upload screen appears.
   - To proceed without upgrading any firmware, clear all the boxes in the **Select** column and click **Continue**.



2. The Firmware File Upload screen allows you to upload a new firmware file from a laptop. Enter the file path of the file you want to upload, or use the **Browse** button to locate the file.



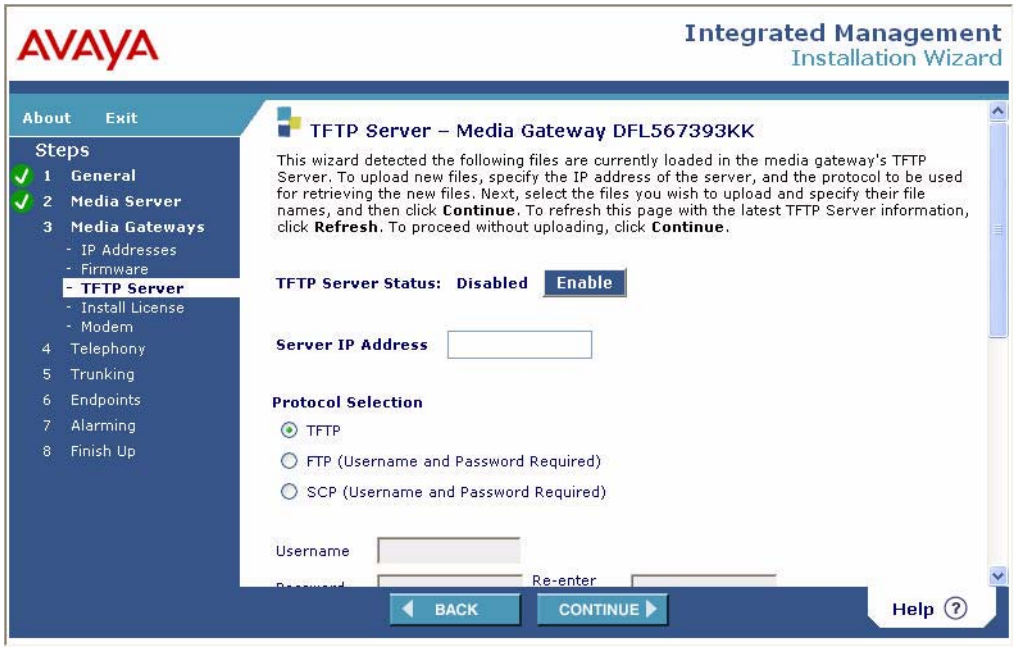
3. Then, click **Continue** to upload the file.
4. The Firmware screen re-appears.

TFTP server configuration

For TFTP server configuration:

1. To configure the G250 server, clear all the boxes in the **Select** column and click **Continue** on the Firmware page.

   The TFTP Server screen appears.



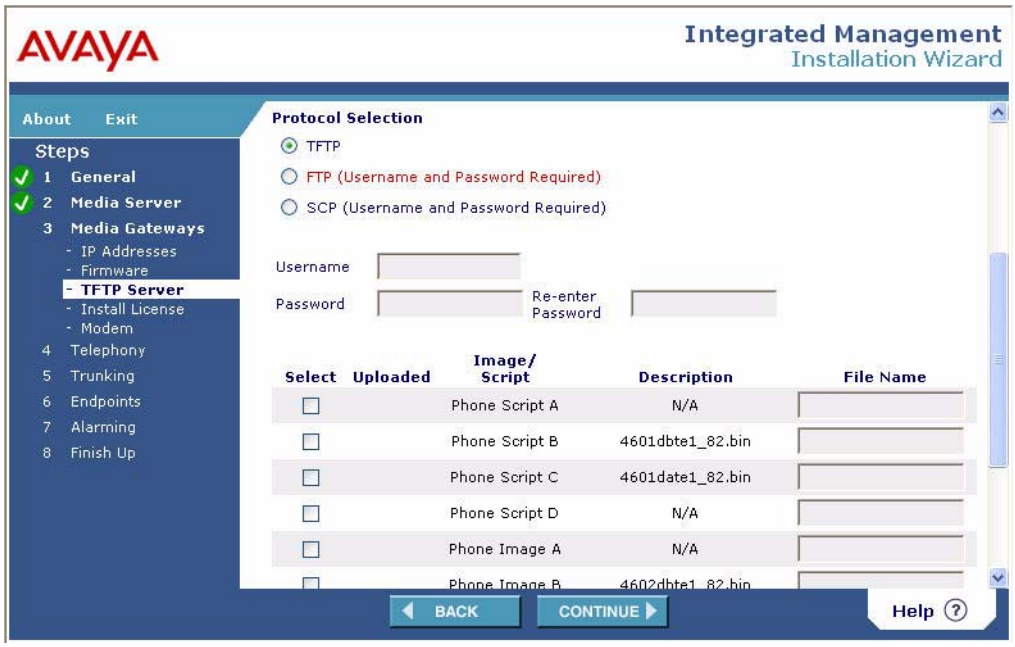
2. If you want to upload configuration and firmware files for IP phones to the G350 TFTP Server, do the following:

   a. In the Server IP Address field, enter the IP address of the machine hosting the files that are to be uploaded.

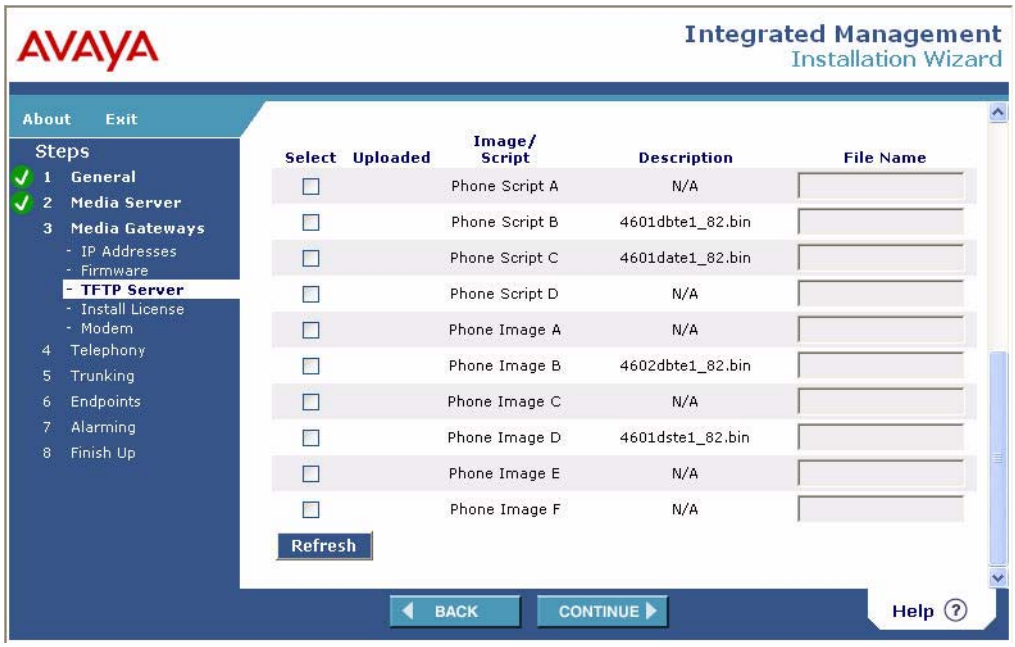
   b. Select the file transfer protocol (TFTP, FTP, or SCP) you want to use to upload the files from the host machine. TFTP is selected by default.

   c. The use of the SCP protocol is limited to copying files of 1 MB or less. Therefore, an SCP server can be used for copying the script files, which do not exceed 128 KB, but cannot be used for copying image files.

d. If you selected FTP or SCP, enter the username and password in the Username and Password fields, and re-enter the password for confirmation in the Re-enter Password field.



3. In the Select column, check any files you wish to upload. If you selected SCP as your upload protocol, the checkboxes for the phone images are disabled. If a green circled checkmark is displayed in the Uploaded column, the file has already been uploaded.



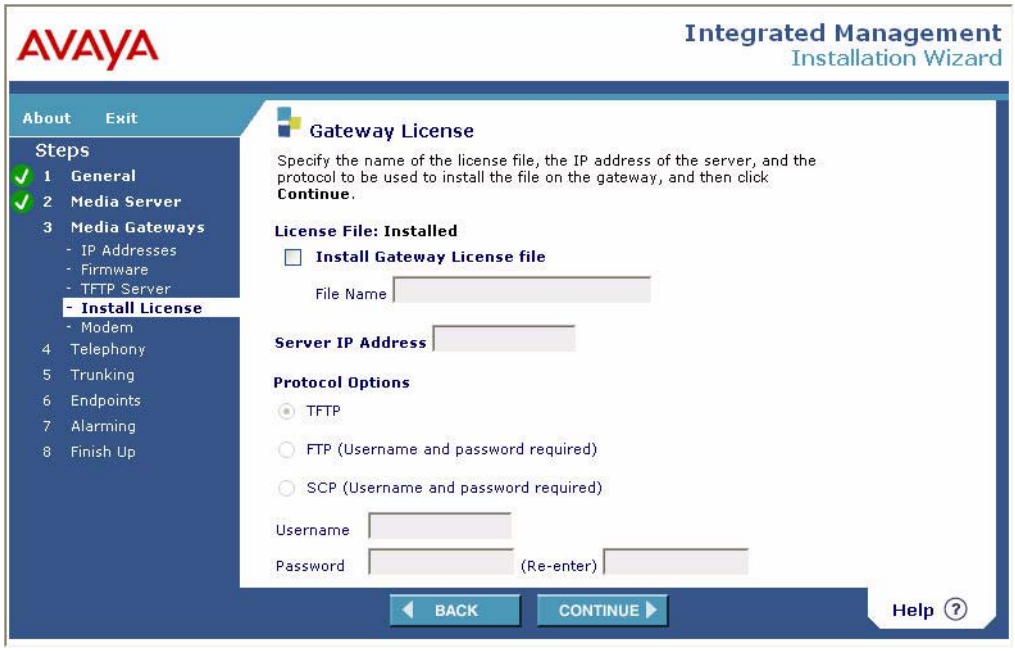
4. Cick **Continue**. The files are uploaded and the Gateway License screen appears.

Gateway license configuration

For gateway license configuration:

1. To configure the G250 license, click **Continue on** the TFTP Server screen.

   The Gateway License screen appears.

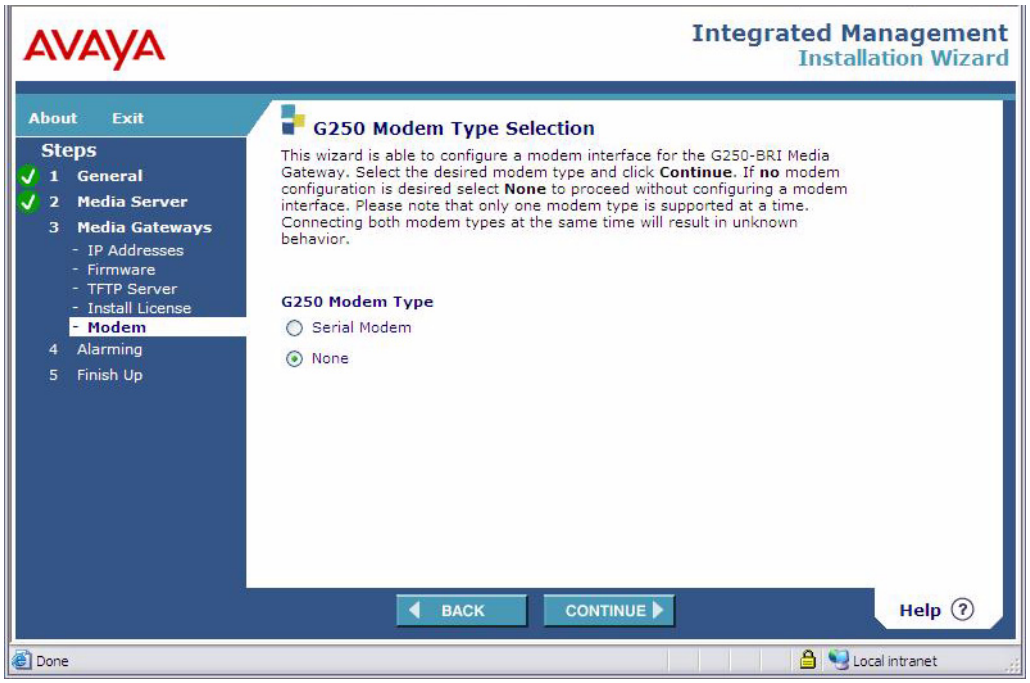


Modem configuration

For modem configuration:

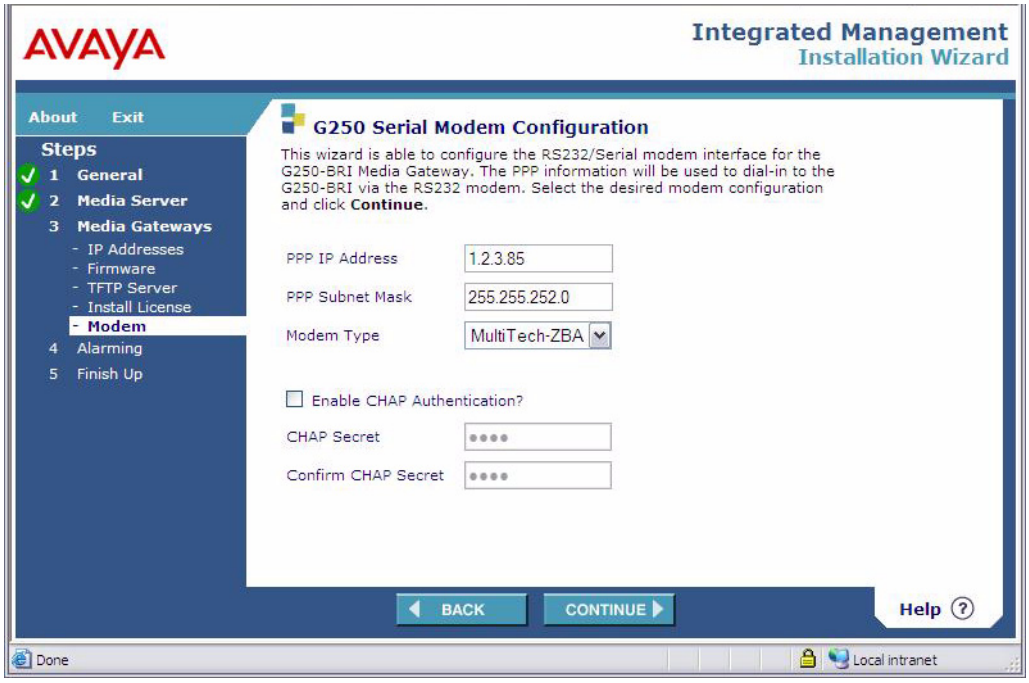
1. To configure the G250 modem, click **Continue** on the Gateway License screen.

   The G250 Modem Type Selection screen appears. Select the modem type you want to use. For more information on using a modem with the G250, see Chapter 5: Connecting and enabling a modem for remote access on page 51.



2. Click **Continue**. If you selected **Serial Modem**, the G250 Serial Modem Configuration screen appears. If you selected **None**, the Country screen appears. See Telephony configuration on page 149.

3. If you selected **Serial Modem**, enter the required information in the G250 Serial Modem Configuration screen, then click **Continue**.

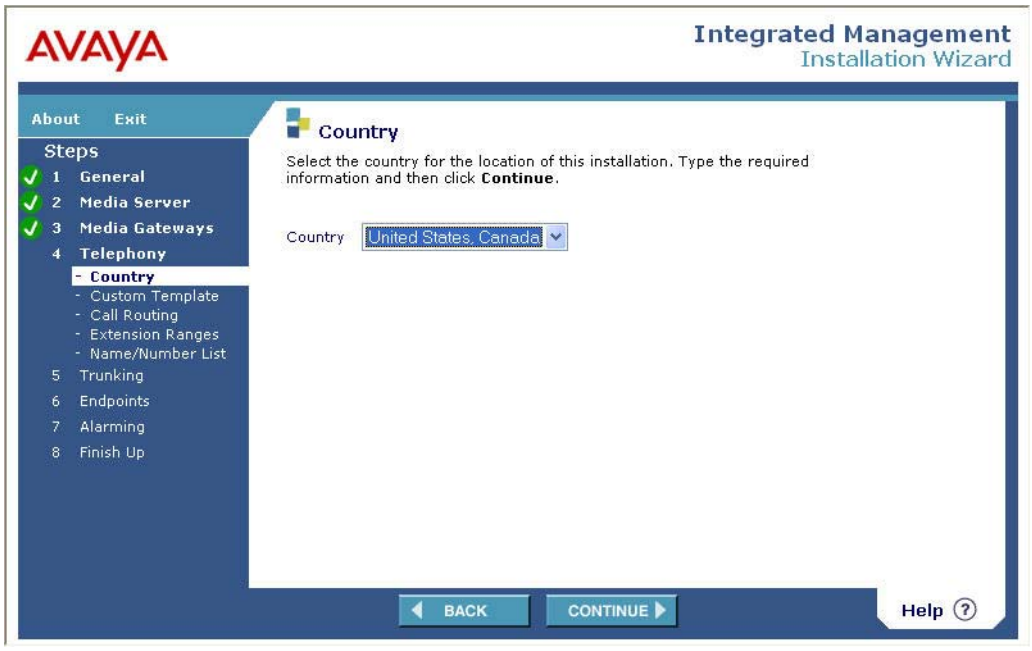


Telephony configuration

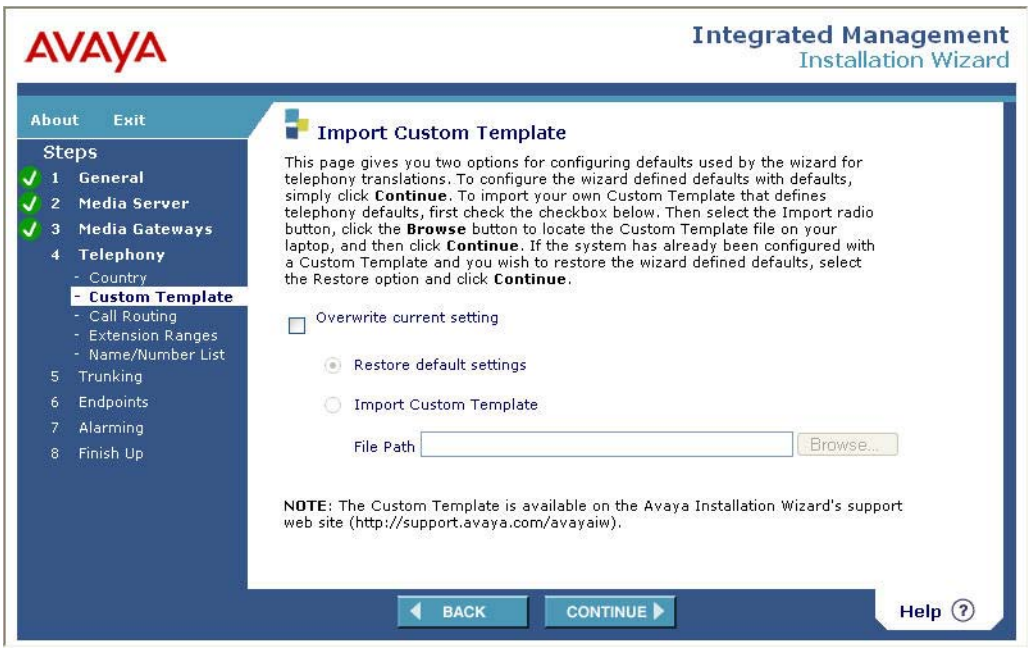
For telephony configuration:

1. To configure the G250's telephony parameters, click **Continue** from the applicable modem configuration screen.

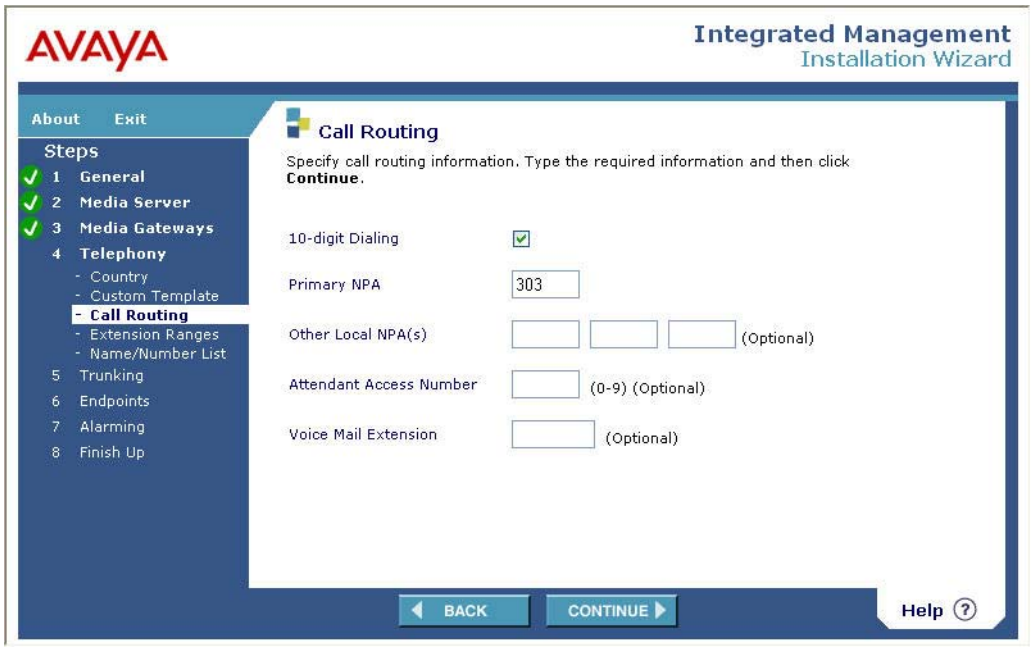
   The Country screen appears. Select the country in which the installation is taking place.



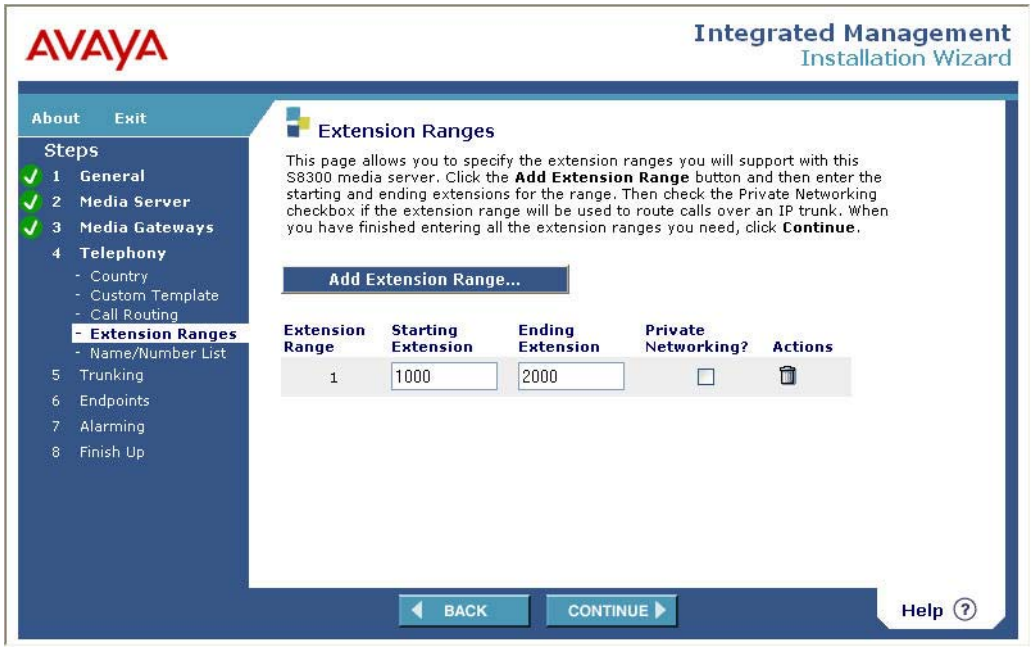
2. Click **Continue**. The Import Custom Template screen appears. This screen allows you to configure telephony translation defaults for the Avaya IW.



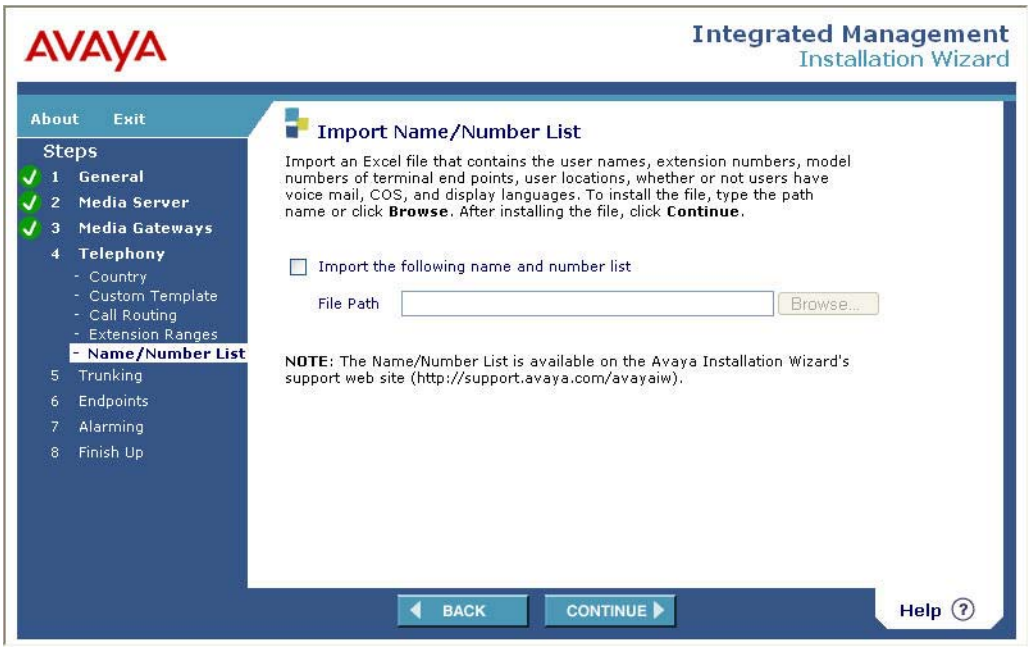
3. Click **Continue**. The Call Routing screen appears. Enter the required call routing information.



4. Click **Continue**. The Extension Ranges screen appears. To add a range, click **Add Extension Range** and enter the starting and ending extensions for the range. If you want this range to be used to route calls over an IP trunk, select **Private Networking**. To add additional extension ranges, repeat these steps. When you are finished, click **Continue**.



5. Click **Continue**. The Import Name/Number List screen appears. This screen allows you to import an Excel file that contains user names, extension numbers, and other information. To import this file:
   a. Select **Import the following name and number list**.
   b. Enter the file path of the file you want to import, or use the **Browse** button to locate the file.
   c. Click **Continue**.

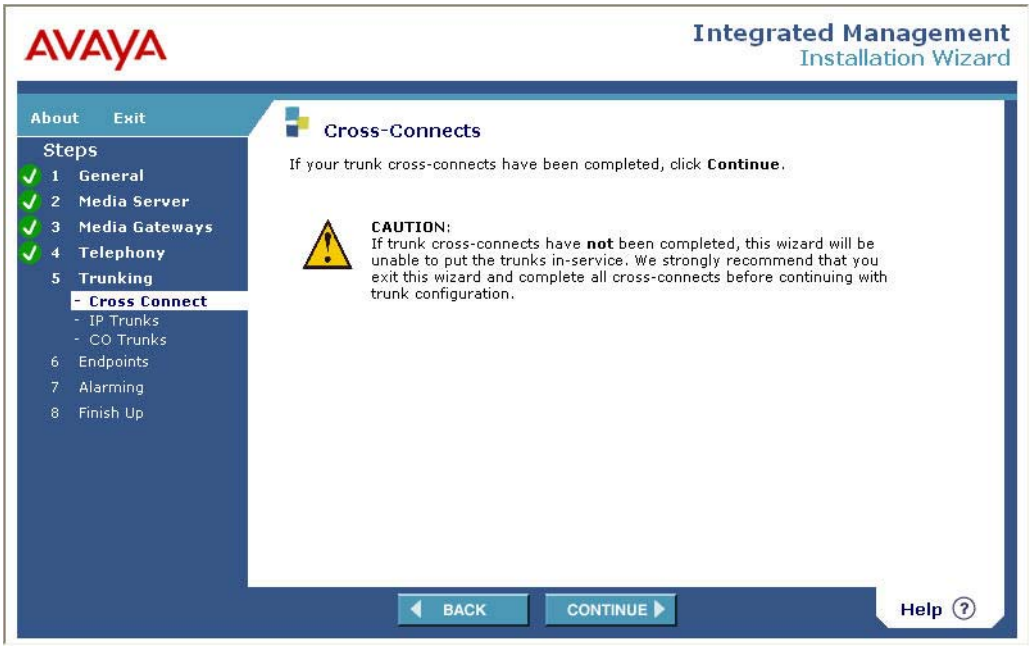


Trunk configuration

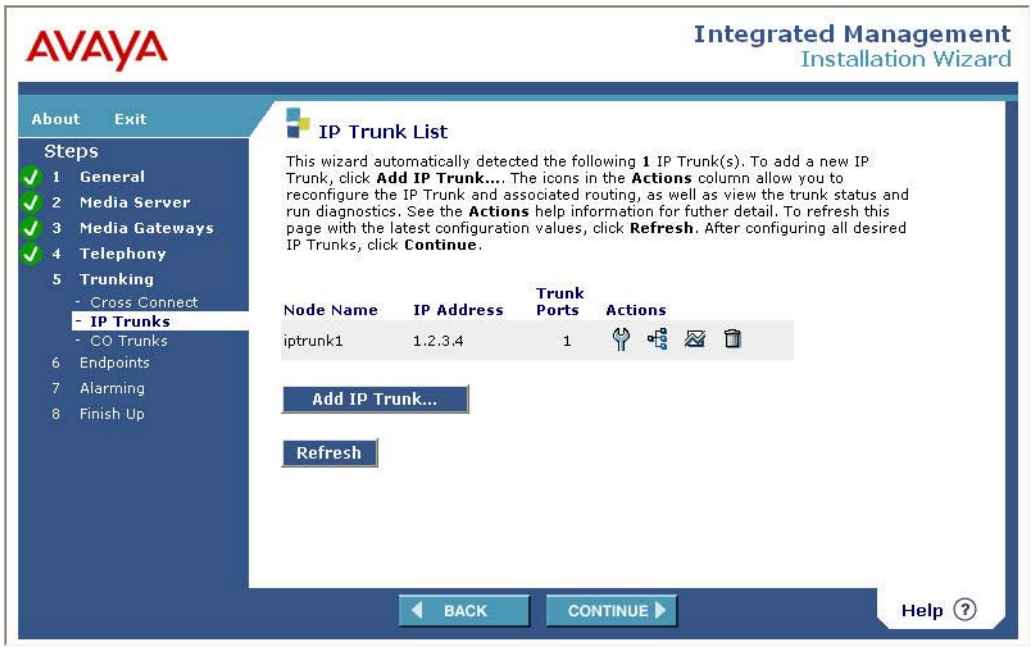
For trunk configuration:

1. To configure the G250's trunk parameters, do one of the following:
   - From the Import Name/Number List screen, click **Continue**, or
   - Click **Trunking** from the main menu.

   The Cross-Connects screen appears. If your trunk cross-connects have been completed, click **Continue** to proceed with trunk configuration. If your trunk cross-connects have not been completed, it is strongly recommended to exit the Avaya IW and complete all cross-connects before proceeding with trunk configuration.



2. Click **Continue**. The IP Trunk List screen appears. This screen displays all IP trunks configured on the G250. To refresh this list, click **Refresh**.



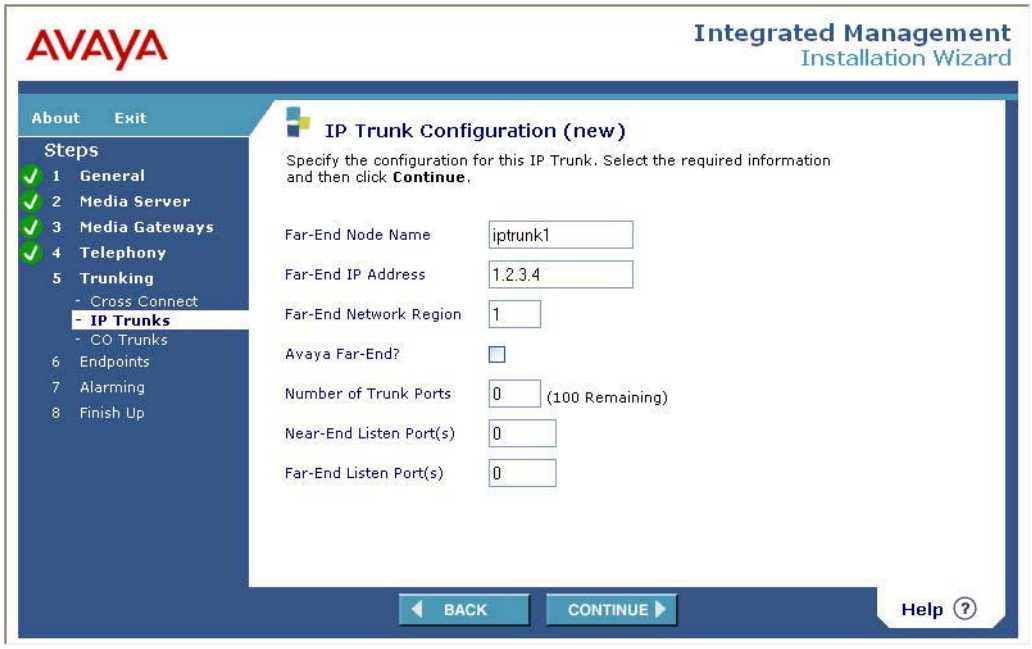
3. You can perform the following actions in the IP Trunk List screen:
   - Adding a trunk
   - Modifying trunk parameters
   - Modifying IP route configuration
   - Displaying trunk status
   - Removing a trunk

   To proceed to the CO Trunk List screen for configuring a trunk media module, click **Continue**. See Configuring a trunk media module on page 159.

Adding a trunk

To add a new trunk:

1. Click **Add IP Trunk**. The IP Trunk Configuration screen appears.



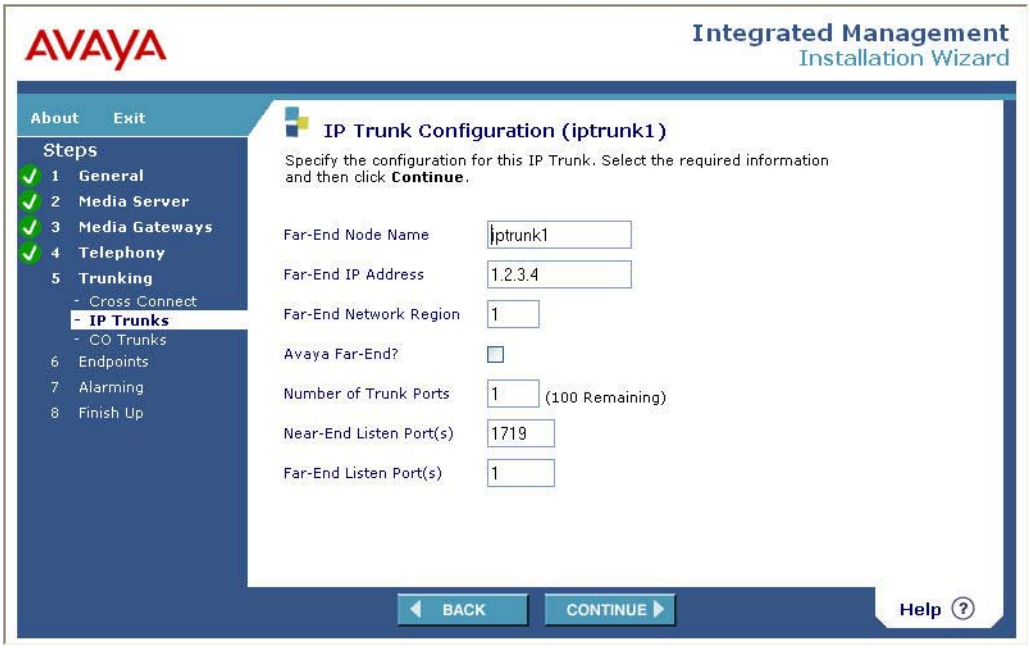
2. Enter the required information in the IP Trunk Configuration screen and click **Continue**. The IP Trunk List appears, with the new trunk included in the list of trunks. To add an additional trunk, click **Add IP Trunk** and repeat this step. When you are finished adding trunks, click **Continue** or select an action from the **Actions** column to modify an existing trunk.

Modifying trunk parameters

To modify the trunk's parameters:

1. Click the configuration icon in the **Actions** column of the IP Trunk List screen.

The IP Trunk Configuration screen appears, with the trunk's current parameters displayed.



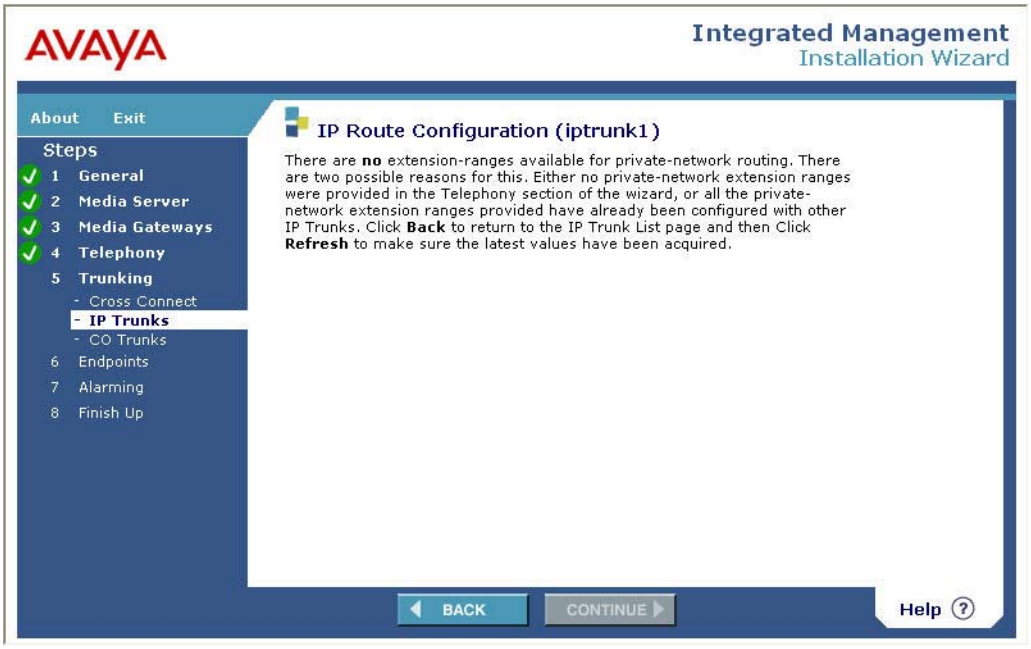
2. Modify the trunk parameters and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See Configuring a trunk media module on page 159.

Modifying IP route configuration

To modify the trunk's IP route configuration:

1. Click the IP route icon in the **Actions** column of the IP Trunk List screen.

The IP Route Configuration screen appears.



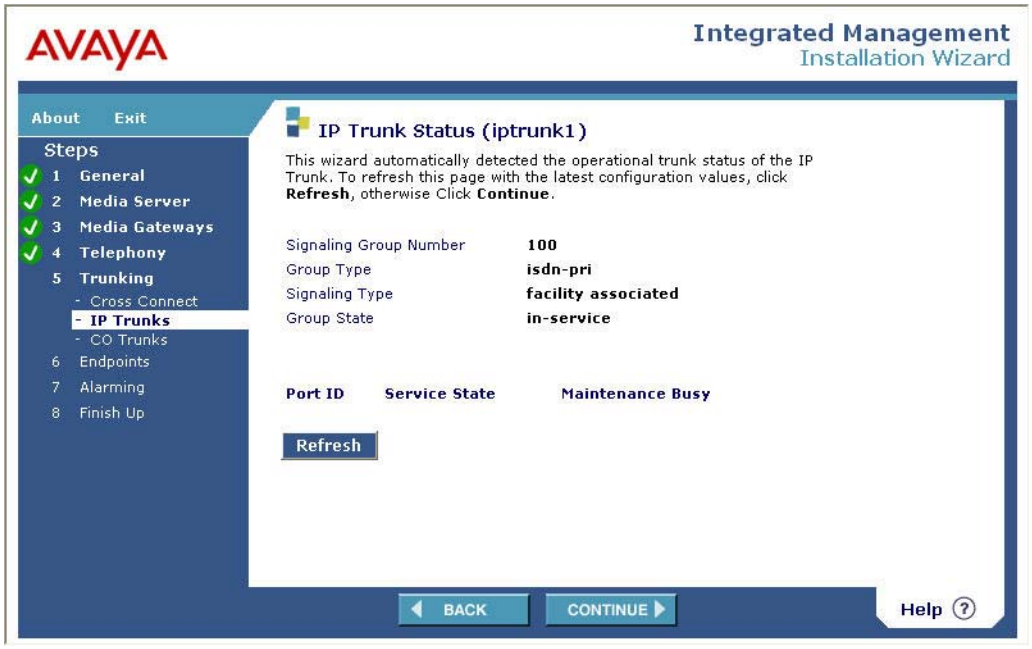
2. The IP Route Configuration screen displays the extension ranges available for private-network routing. Modify these ranges, if any, and click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See Configuring a trunk media module on page 159.

Displaying trunk status

To display the trunk's IP route configuration:

1. Click the trunk status icon in the **Actions** column of the IP Trunk List screen.

The IP Trunk Status screen appears.



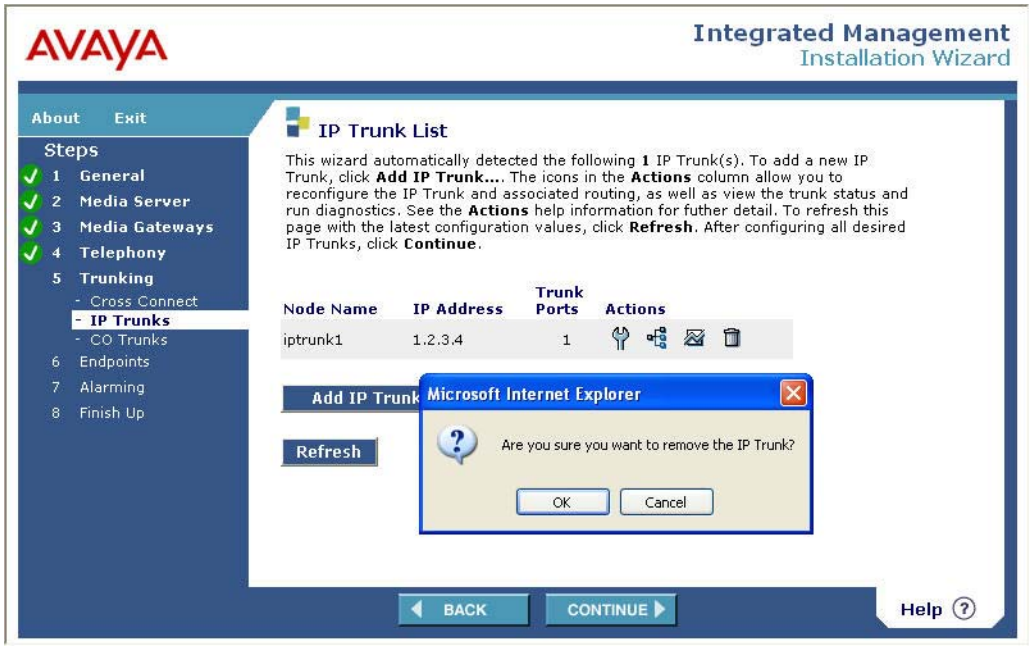
2. The IP Trunk Status screen displays the operational status of the trunk. To refresh the information, click **Refresh**. Otherwise, click **Continue**. The IP Trunk List appears. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen. See Configuring a trunk media module on page 159.

Removing a trunk

To remove a trunk:

1. Click the trunk's remove icon in the **Actions** column of the IP Trunk List screen.

A message appears asking if you want to remove the trunk.



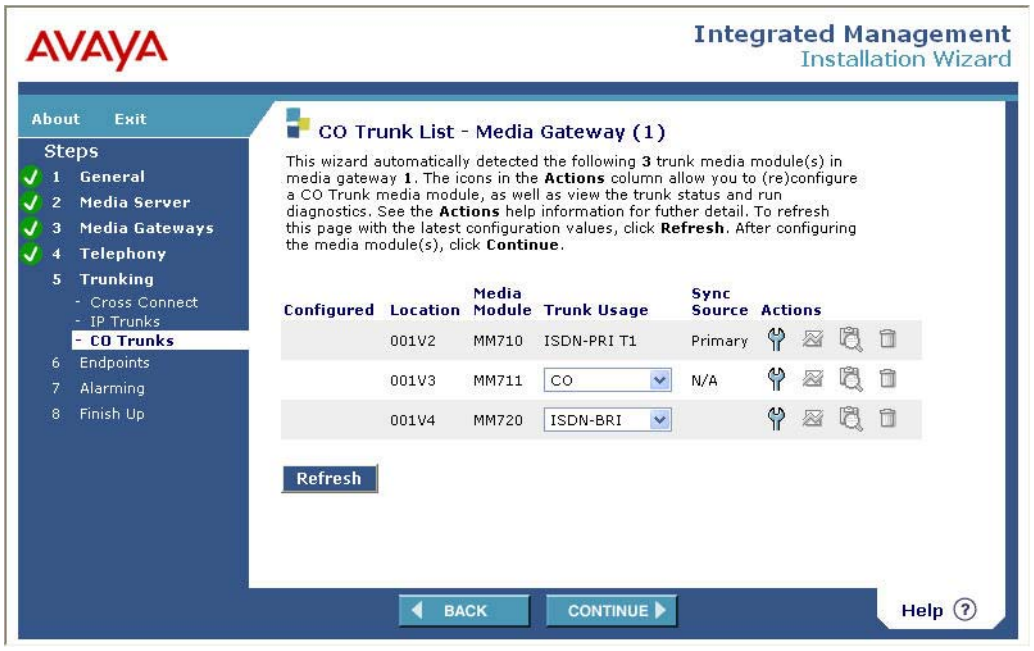
2. Click **OK** to remove the trunk. Select an additional action from the **Actions** column, or click **Continue** to proceed to the CO Trunk List screen.

Configuring a trunk media module

To configure a trunk media module, do one of the following:

- Click **Continue** from the IP Trunk List screen, or
- Click **Trunking>CO Trunks** from the main menu.

The CO Trunk List screen appears. This screen lists trunk media modules detected in the G250 and allows you to configure a media module and run diagnostics. To configure or run diagnostics on a trunk media module, click the Actions icon for the module.

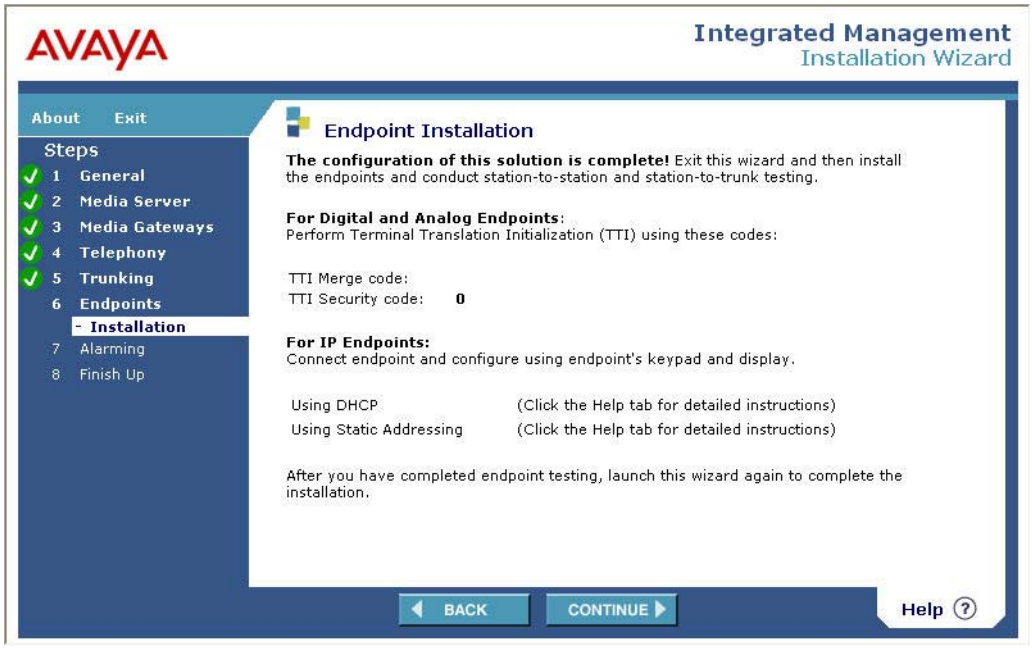


Endpoint installation

For instructions on endpoint installation, do one of the following:

- Click **Continue** from the CO Trunk List screen, or
- Click **Endpoints** from the main menu.

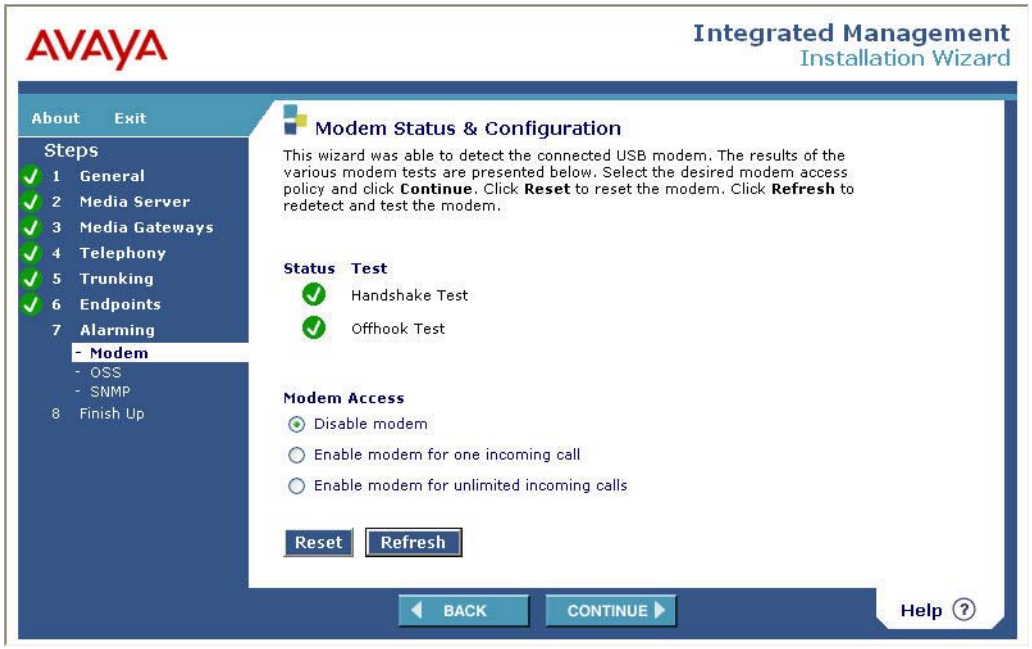
The Endpoint Installation screen appears. You can access endpoint installation information from this screen.



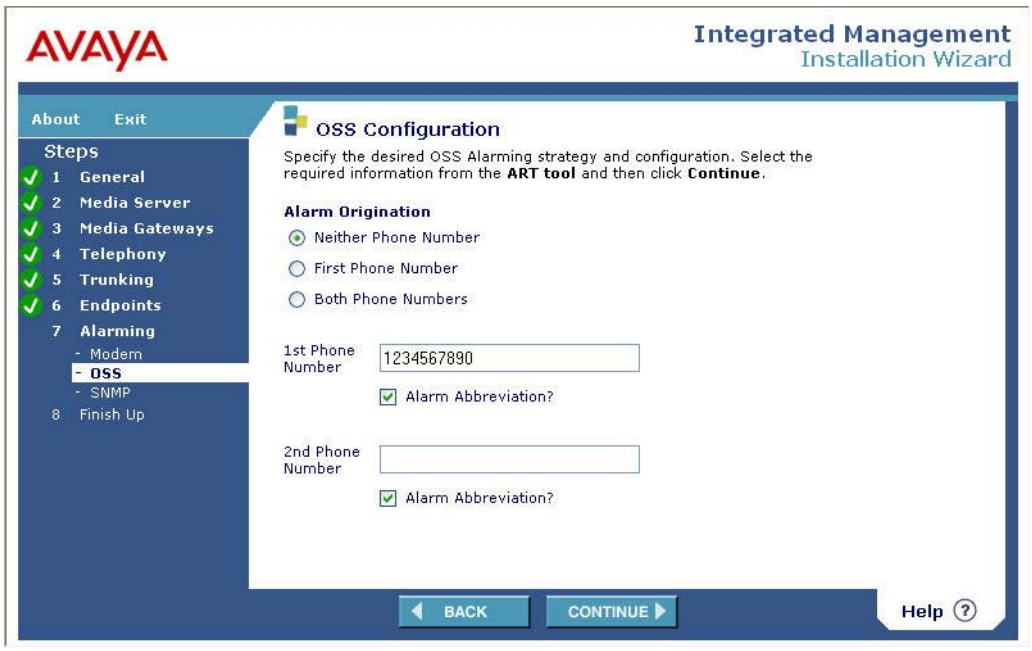
Alarm configuration

To display modem status and configure alarms:

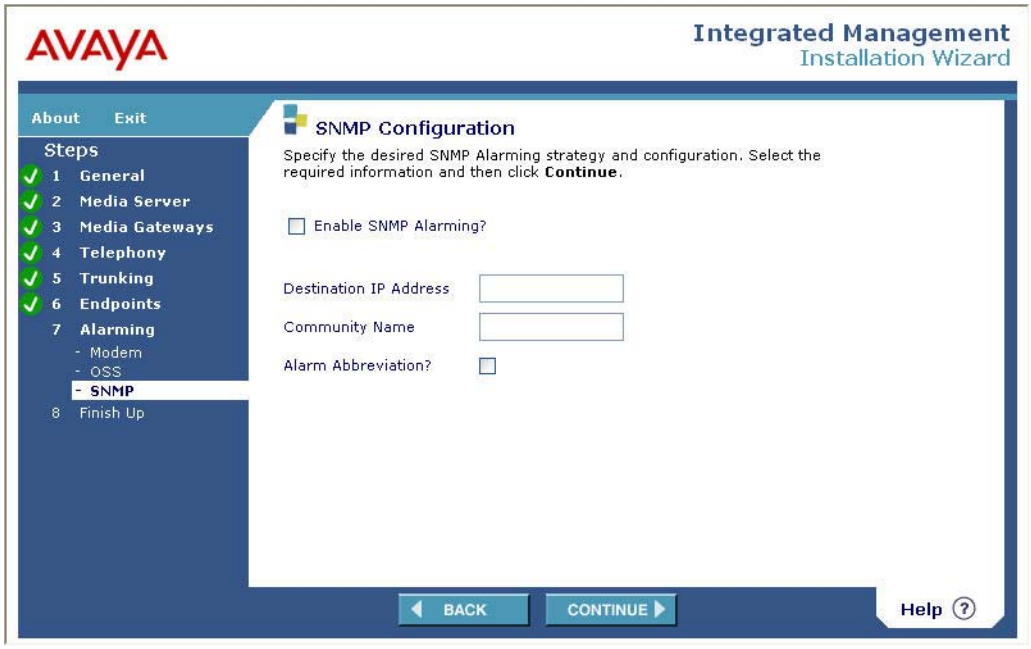
1. Click **Alarming** from the main menu. The Modem Status & Configuration screen appears. This screen detects any modem connected to the G250. The screen also displays the results of tests performed on the modem. You can perform the following actions from this screen:
   - Click **Reset** to reset the modem.
   - Click **Refresh** to re-detect and test the modem.
   - Select the appropriate modem access policy in the **Modem Access** area and click **Continue**.



2. Click **Continue**. The OSS Configuration screen appears. Enter the required information from the ART tool. For information on using the ART tool, see *Run the Automatic Registration Tool (ART) for the RAS IP address* on page 22.



3. Click **Continue**. The SNMP Configuration screen appears. Check Enable SNMP alarming if you want to enable the sending of SNMP traps to the INADS. In the Destination IP Address field, enter the INADS IP address. In the Community Name field, enter an SNMP community access string. Check the Alarm abbreviation checkbox if you want to enable SNMP alarm abbreviation.

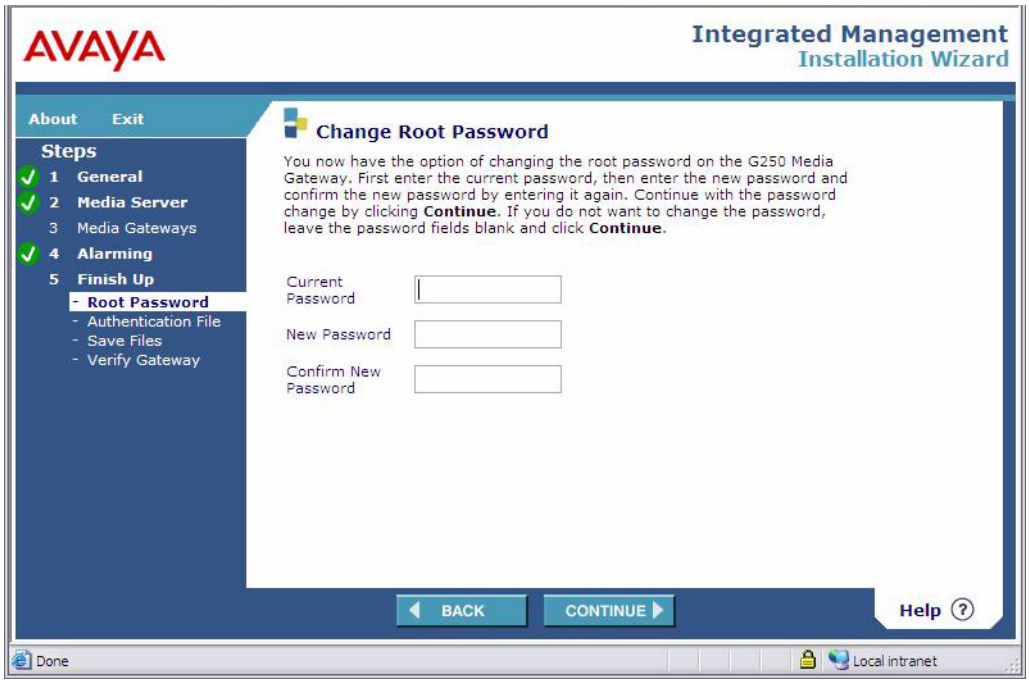


Password and final screens

To change your password (optional) and complete the installation:

1. Click **Continue** from the SNMP Configuration screen.

   The Change Root Password screen appears. This screen allows you to change the root password on the G250.



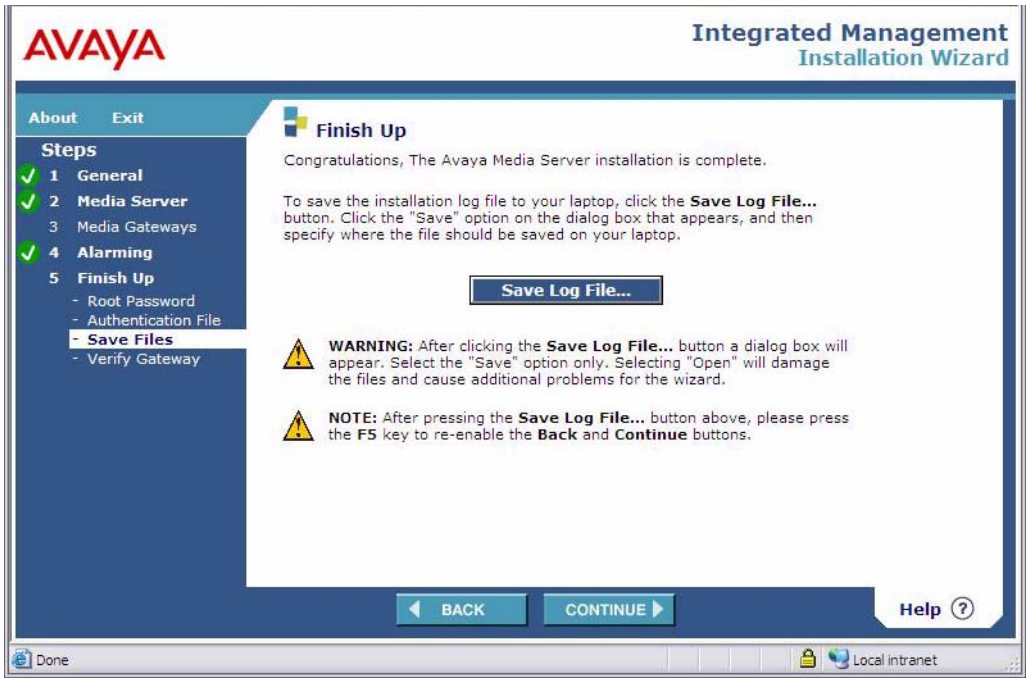
2. Click **Continue**. The Finish Up screen appears. This screen allows you to save the installation log file to your laptop. To save the installation log file:

   a. Click **Save Log File**. A dialog box appears.

   b. Click **Save**.

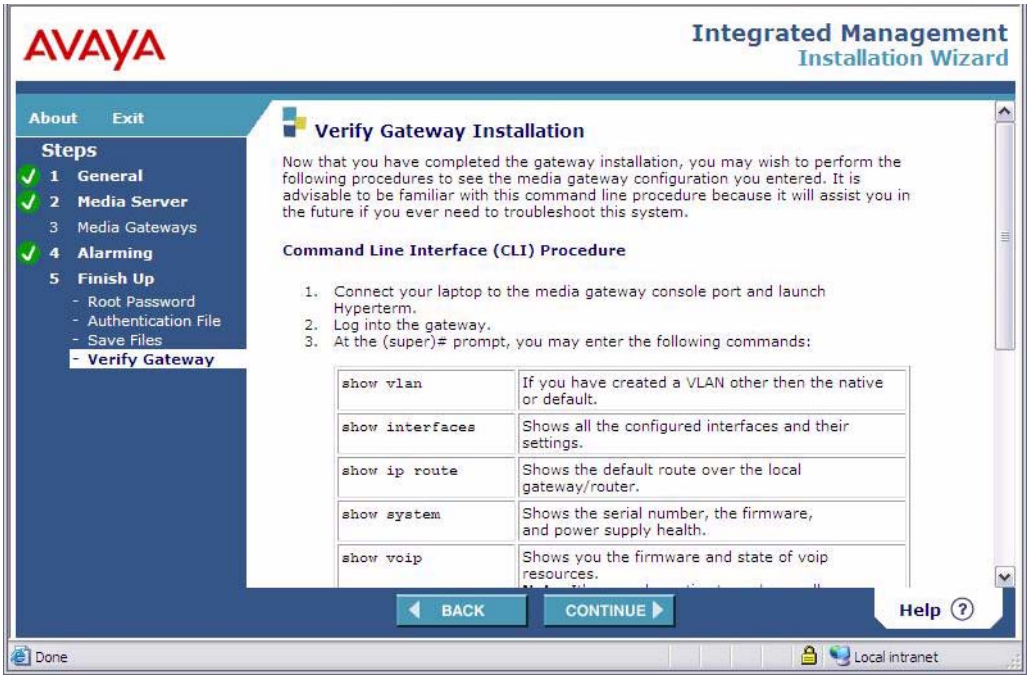
   WARNING:
   Do not click **Open**. Clicking **Open** will damage the log file and may cause other problems to the Avaya IW.

   c. Press **<F5>** to restore the **Back** and **Continue** buttons to the Finish Up screen.

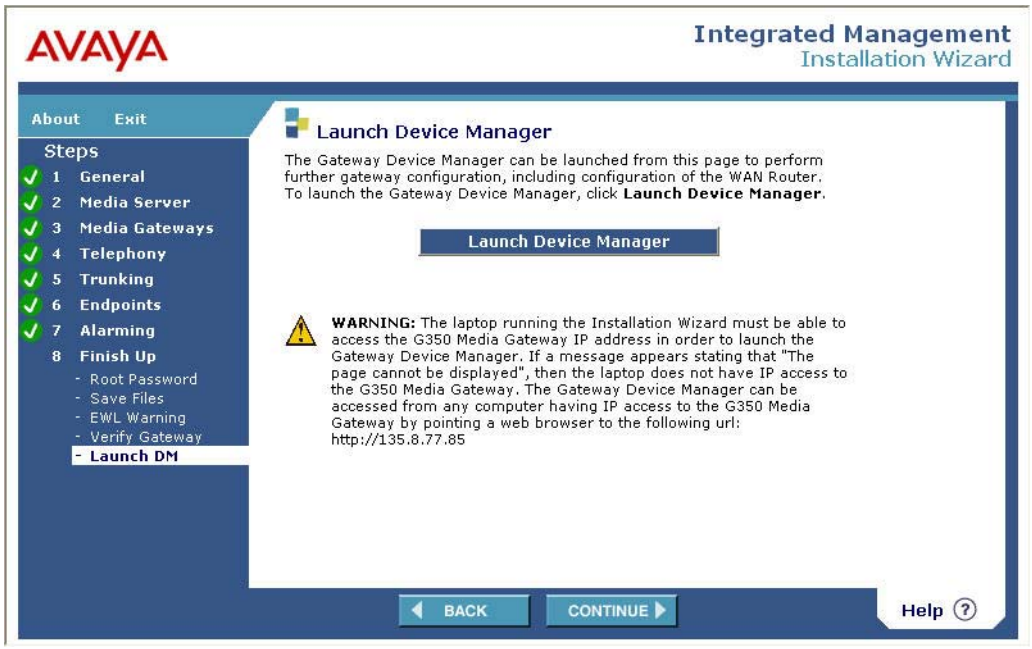


3. Click **Continue**. If you have not installed an allocation license file, a warning appears reminding you to install this file.

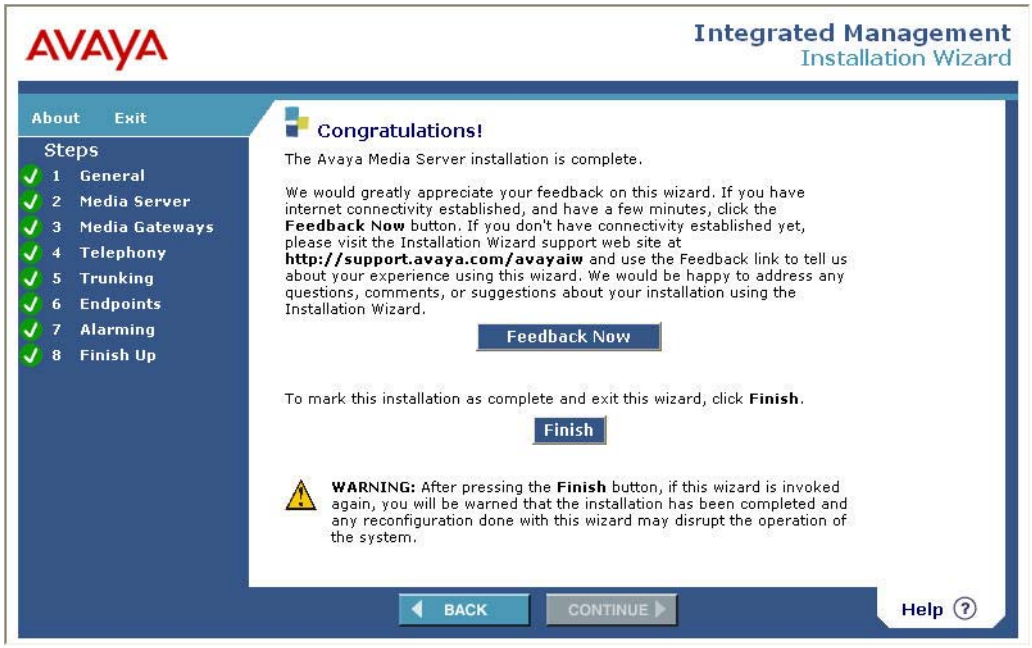
4. Click **Continue**. The Verify Gateway Installation screen appears. This screen displays a list of CLI commands that you can use to verify the G250 configuration. The following figure shows a portion of the Verify Gateway Installation screen.



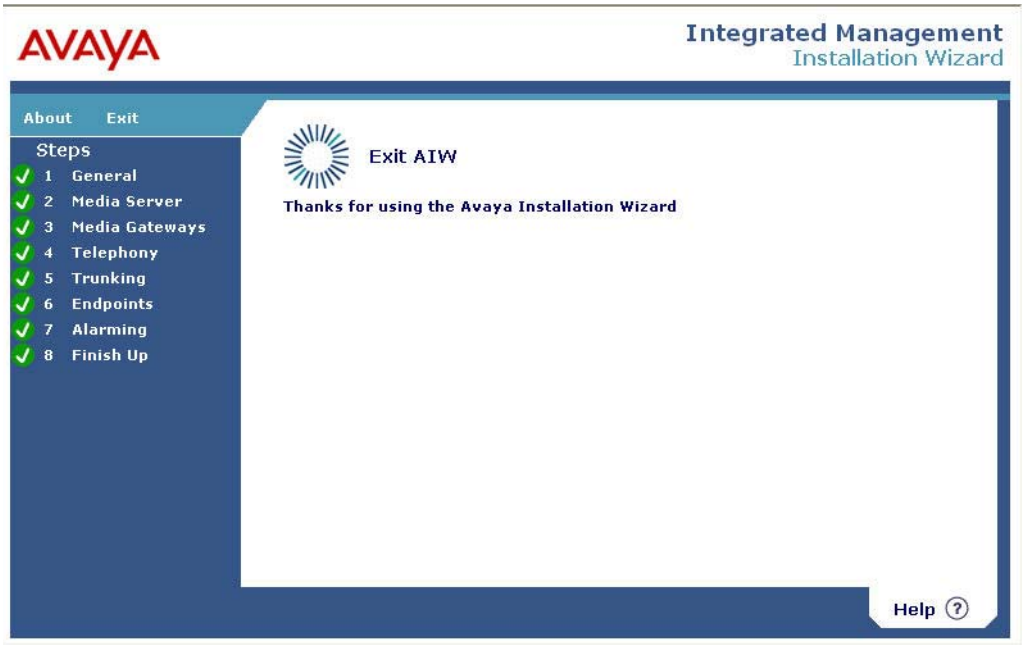
5. Click **Continue**. The Launch Device Manager screen appears. This screen allows you to launch the Gateway Device Manager, an application that allows you to configure the WAN Router and perform other advanced configuration tasks.



6. Click **Continue**. The Congratulations! screen appears to inform you that the installation is complete. To exit the Avaya IW, click **Finish**.



7. The Exit AIW screen appears.



Appendix D: Running the Gateway Installation Wizard (GIW)

If you did not install an S8300B in the G250, you can use the Gateway Installation Wizard (GIW) to perform the configurations required to complete the installation. GIW prompts you for all the configurations required to complete the installation. If you have an EPW (see Obtain the Electronic Preinstallation Worksheet (EPW) on page 24), you will be able to upload configuration parameters from the EPW to GIW as part of your GIW session.

GIW includes the option to enable a modem connected to the S8300B. This appendix describes how to run GIW, and how to connect and test a modem if you choose to enable the modem.

Perform the following steps to run GIW and perform the configuration:

1. Run the Gateway Installation Wizard (GIW) on page 169.
2. Connect a modem, if necessary on page 187.
3. Test the modem connection, if necessary on page 187.

Run the Gateway Installation Wizard (GIW)

Run Gateway Installation Wizard (GIW) to perform a basic configuration of the G250. The configuration can include:

- Configuring the Primary Management Interface (PMI)
- Setting SNMP communities and trap destinations
- Upgrading firmware
- Enabling a modem on the G250

To run GIW:

1. Prepare a PC with a CD-ROM drive and a TFTP server on the network. This may be needed for installing software and firmware upgrades.

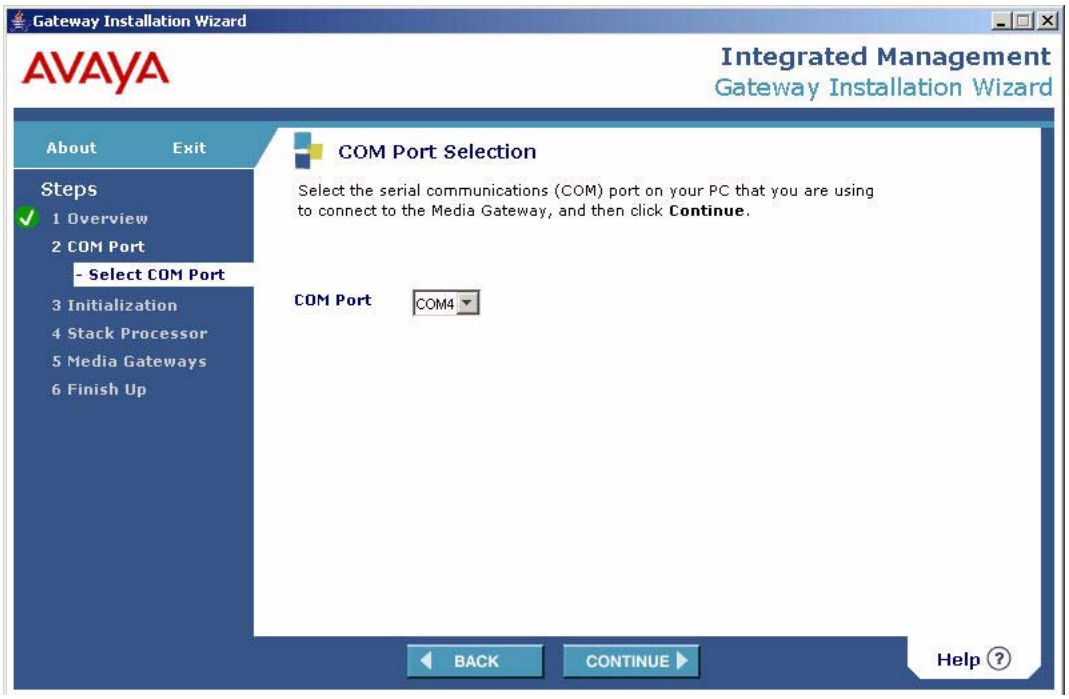
   Note:

   When uploading firmware from the S8300B using TFTP, you may need to enable TFTP service in the Set LAN Security parameters of your web server.

Note:

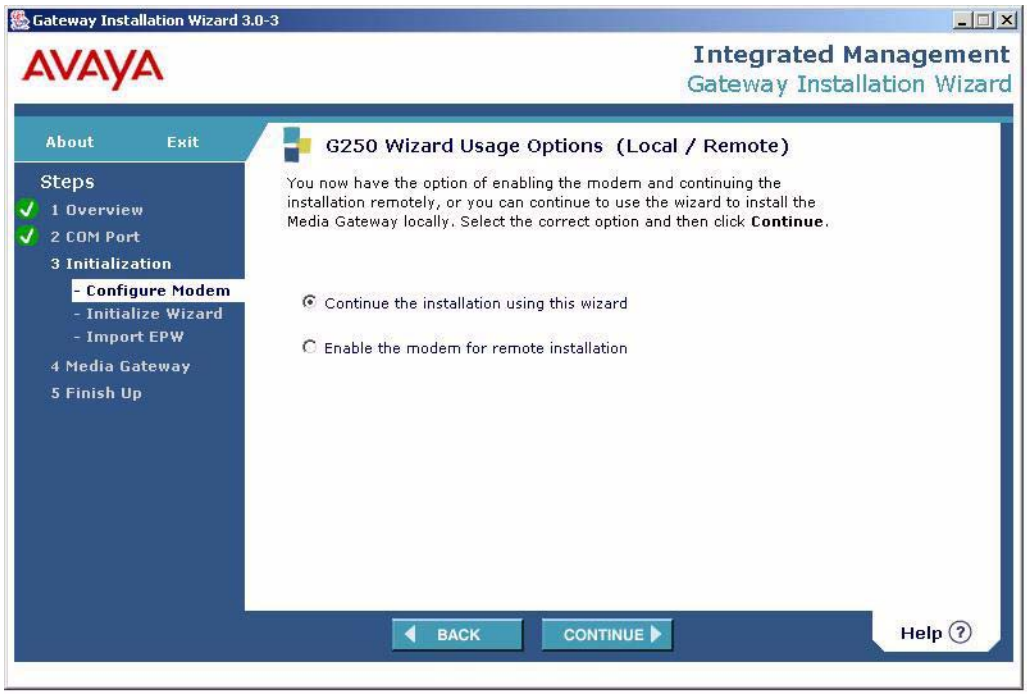
Firmware upgrades for the G250 and media modules can either be installed from CD or downloaded from the Web. For information about downloading firmware upgrades from the Web to the TFTP server, see {cross reference to be inserted, should point to section on Download G250 firmware to a local TFTP Server in Uploading firmware chapter}.

2. Download GIW (Gateway Installation Wizard) from the Avaya website (support.avaya.com/avayaiw) to the laptop computer. The laptop should be running Windows 2000 or Windows XP to support GIW.
3. Plug one end of the provided flat RJ-45 to RJ-45 cable into the provided DB-9 adapter.
4. Plug the RJ-45 connector at the other end of the cable into the CON port of the G250.
5. Plug the DB-9 end of the flat cable into the COM port of the laptop computer.
6. From your laptop computer, double-click the GIW icon to run GIW. The Overview screen appears.
7. Click **Continue**. The COM Port Selection screen appears.



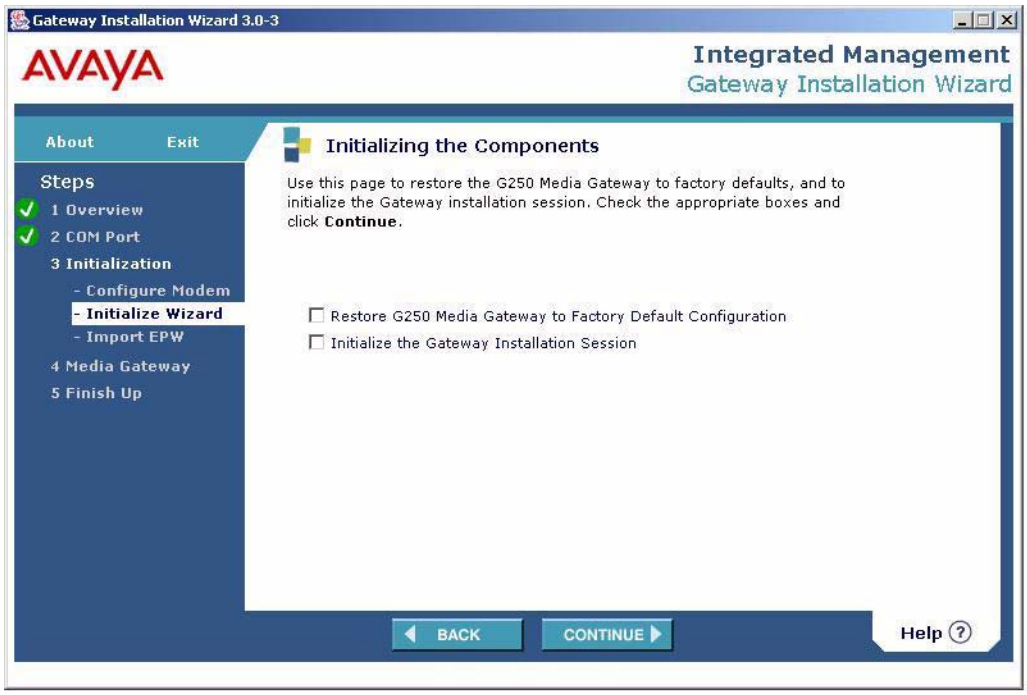
8. Select the COM port on the laptop that you are using to connect to the G250.

9. Click **Continue**. The G250 Wizard Usage Options screen appears.



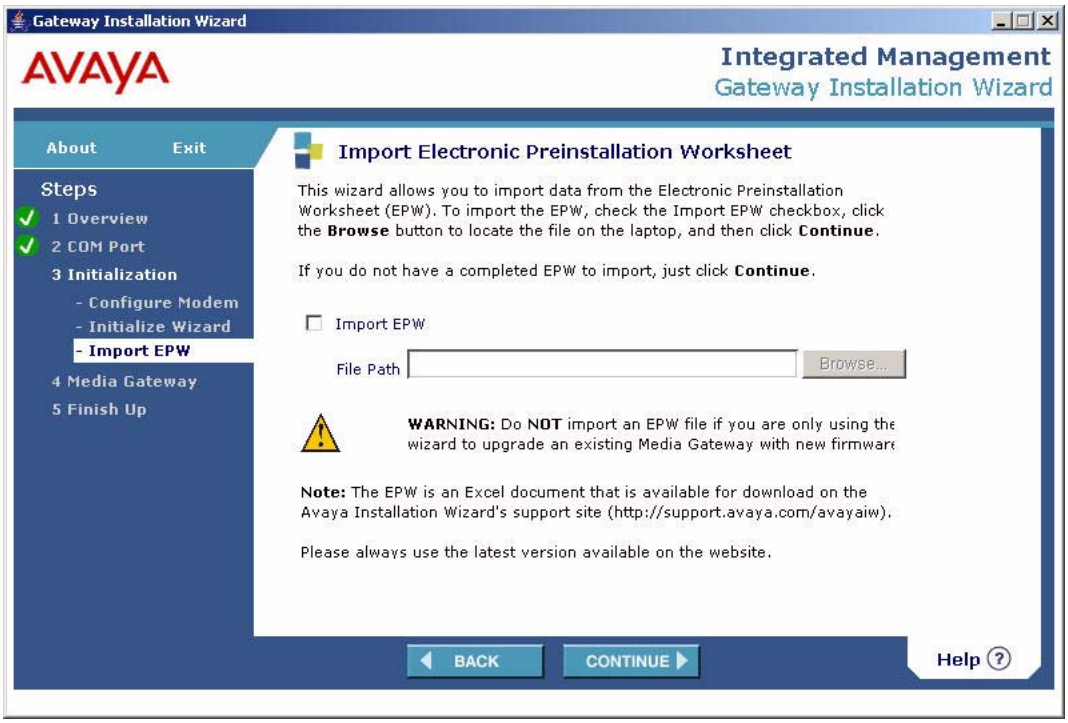
10. Select **Continue the installation using this wizard**.

11. Click **Continue**. The Initializing the Components screen appears.



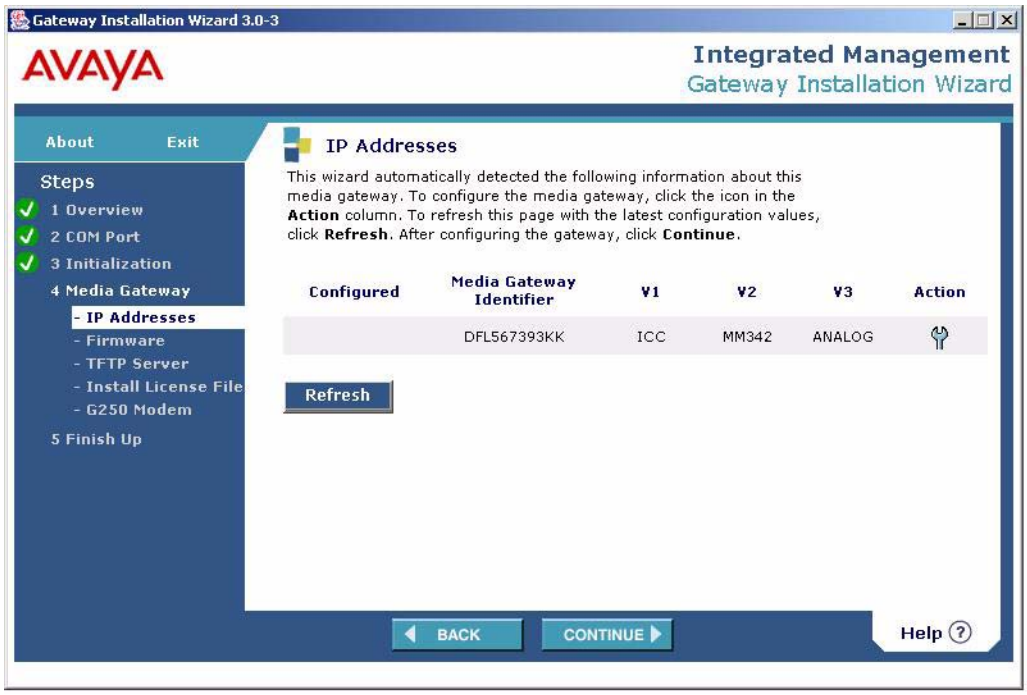
12. Check **Initialize the Gateway Installation Session**.

13. Click **Continue**. The Import Electronic Preinstallation Worksheet screen appears.



14. If you have an EPW on your laptop (see Obtain the Electronic Preinstallation Worksheet (EPW) on page 24), check **Import EPW**. If you are using GIW to upgrade files, do not check **Import EPW**.
15. Browse to the EPW file on your laptop. Any values that are included in the EPW will appear as default values from now on as you move through this wizard.

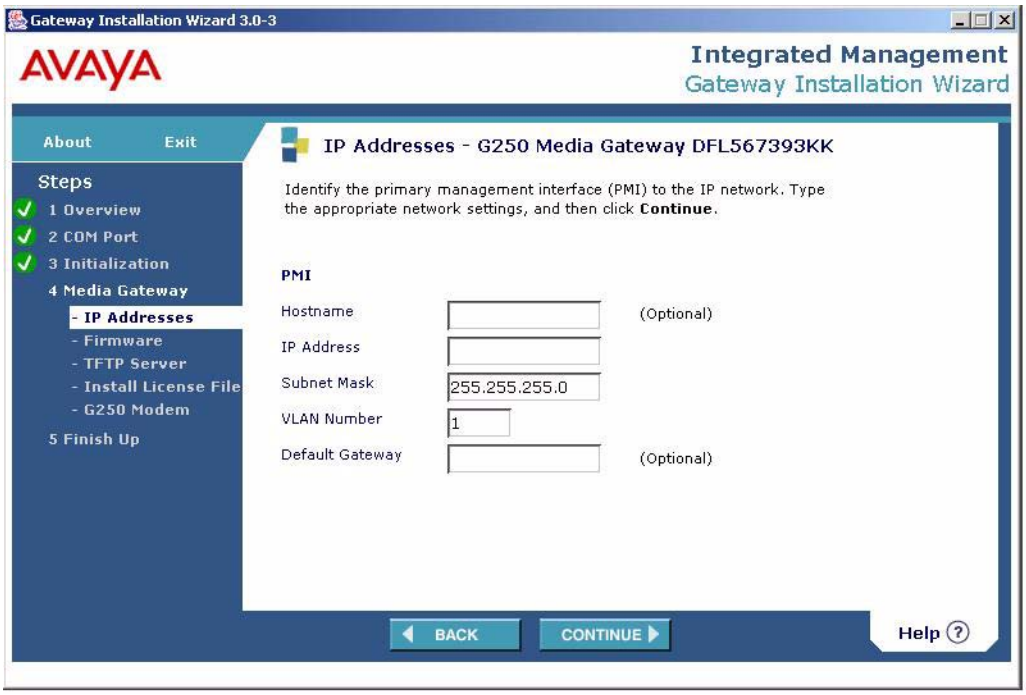
16. Click **Continue**. The IP Addresses screen appears.



The IP Addresses screen displays information about the G250 automatically detected, such as what media modules are installed in the media modules slots.

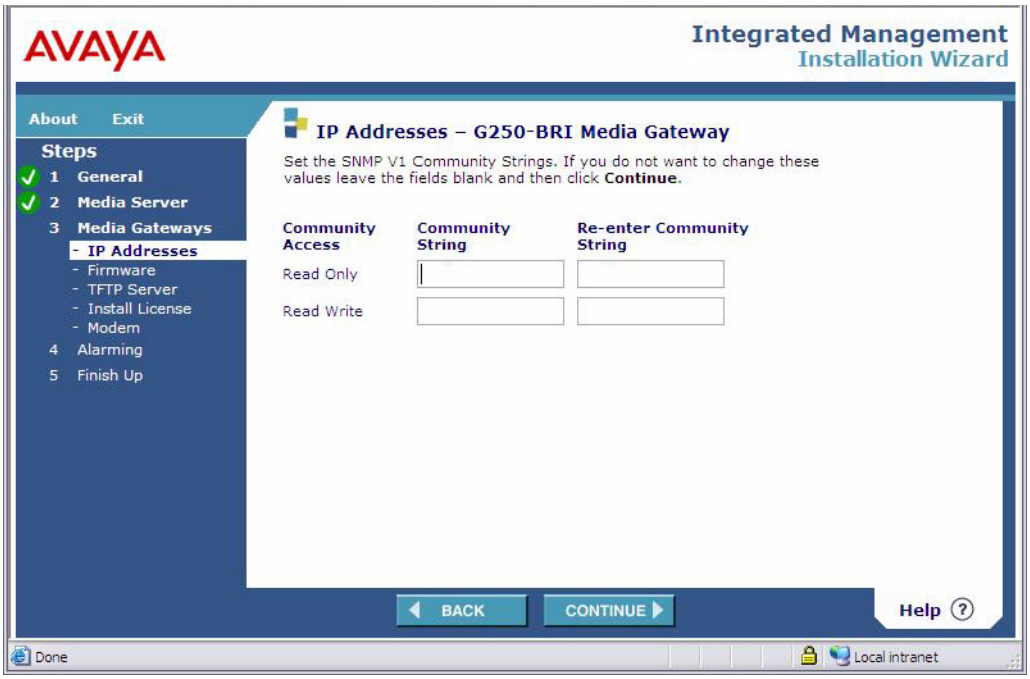
17. If you are using GIW only to upgrade firmware, continue with step 30.

18. Click the icon in the Action column. The PMI screen appears.



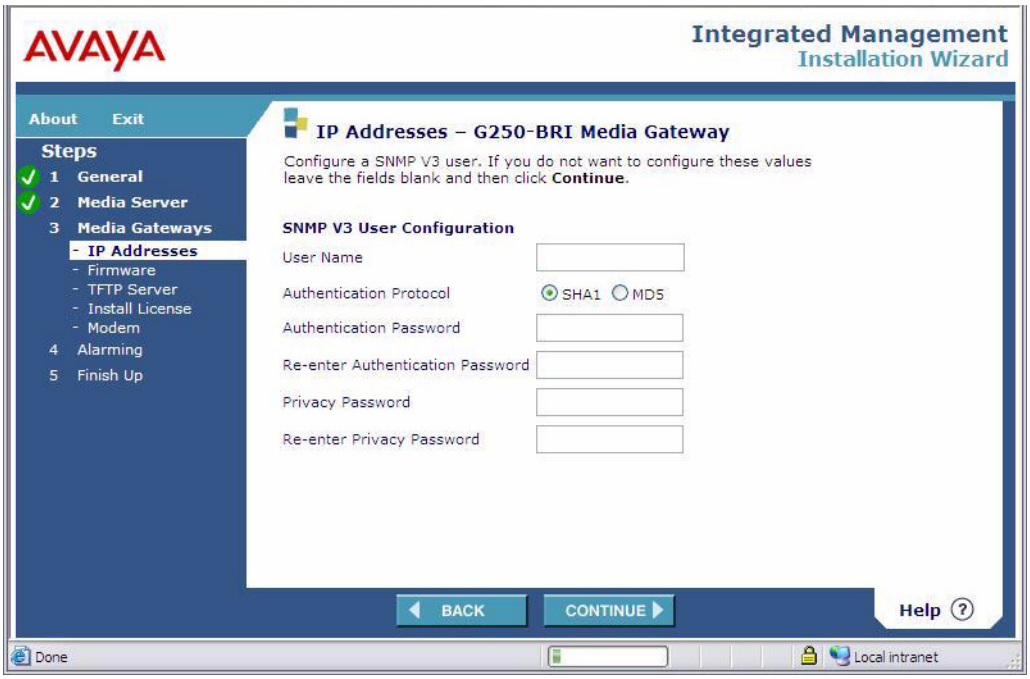
19. In the PMI screen, specify the details of the Primary Management Interface (PMI) for the G250. The PMI is used as the IP address of the G250 for specific management functions. If you do not know which interface to designate as the PMI, check with your project manager.

20. Click **Continue**. The SNMP screen appears.



21. In the SNMP V1 screen, specify SNMP V1 community strings for Read Only and Read Write access.

22. Click **Continue**. The SNMP V3 screen appears.



23. If you want to configure an SNMP V3 user on the G350, do the following:

    a. In the User Name field, enter a string of up to 32 characters representing the SNMP V3 user.

    b. Select the authentication protocol by which the SNMP V3 user should be authenticated (SHA1 or MD5).

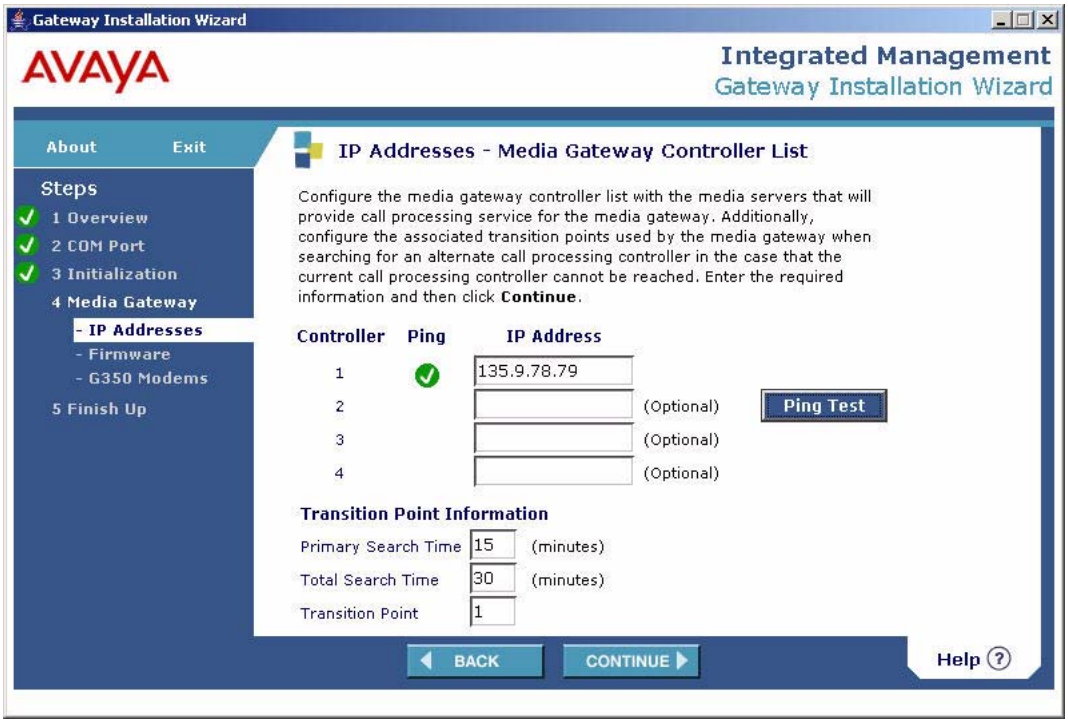
    c. In the Authentication Password field, enter a string of between 8 and 64 characters specifying the user's authentication password. The authentication password is transformed using the authentication protocol and the SNMP engine ID to create an authentication key.

    d. In the Re-enter Authentication Password field, enter the authentication password again for verification.

    e. In the Privacy Password field, enter a string of between 8 and 64 characters specifying the SNMP V3 user's privacy password.

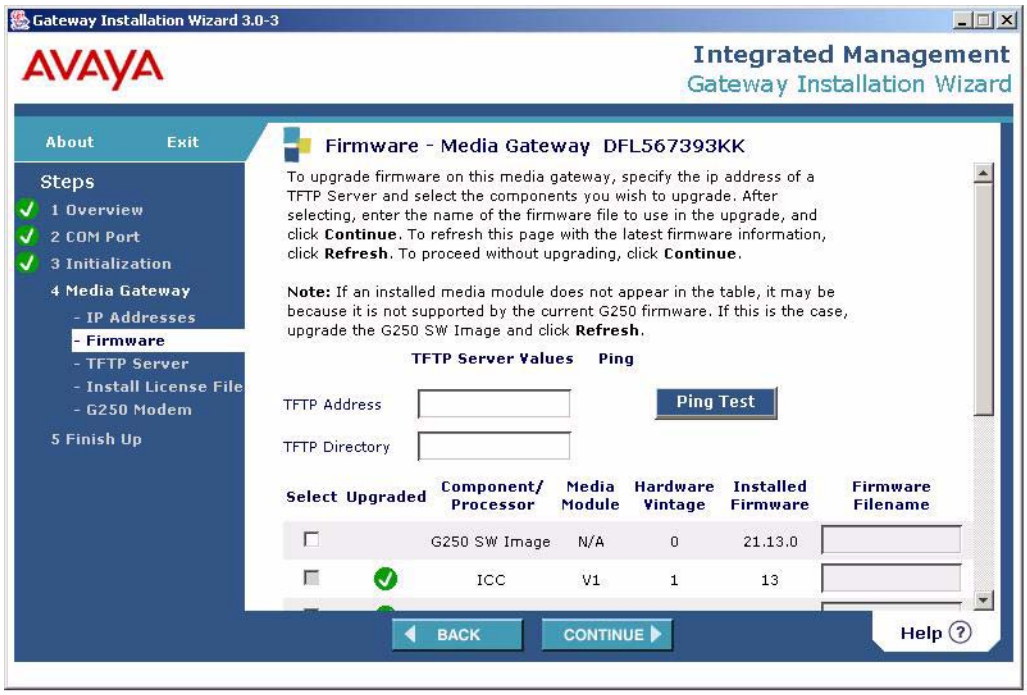
    f. In the Re-enter Privacy Password field, enter the privacy password again for verification.

24. Click **Continue**. The Media Gateway Controller List screen appears.



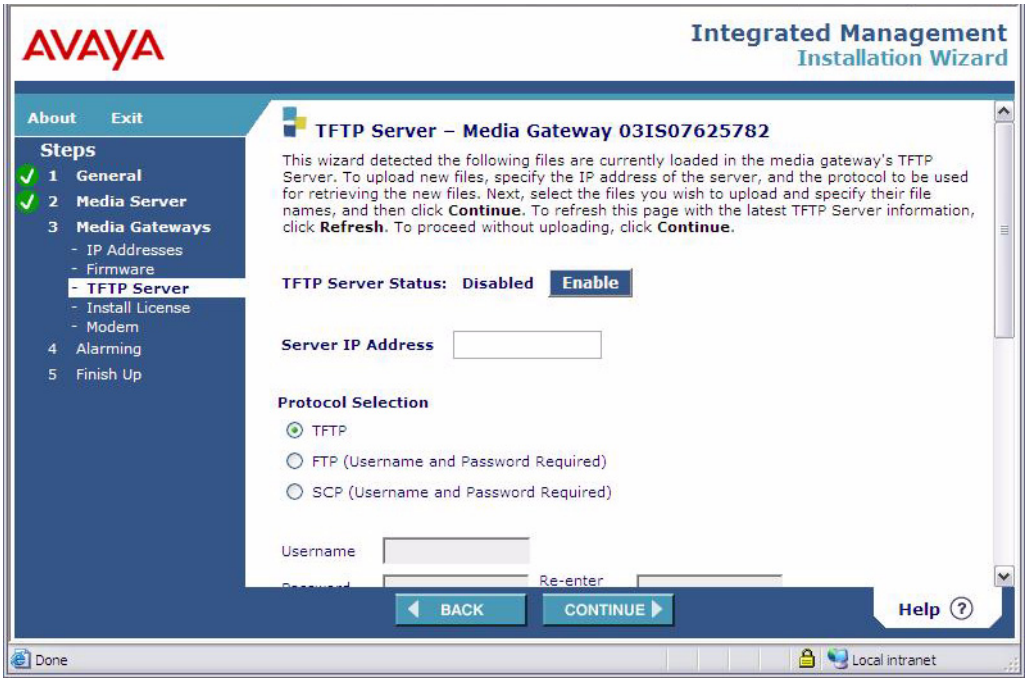
25. In the Media Gateway Controller List screen, specify the IP address of the primary MGC (Media Gateway Controller) in the first IP address box.
26. Specify the IP addresses of up to three additional MGCs, optionally, in the subsequent boxes.
27. Specify Transition Point information.
28. Click **Ping Test** to test the accessibility of each MGC.
29. Click **Continue**. You return to the IP addresses screen.

30. Click **Continue**. The Firmware screen appears.



31. Upload any firmware upgrades you need to install to your TFTP server.
32. In the TFTP Address field, enter the address of your TFTP server.
33. In the TFTP Directory field, enter the name of the directory on the TFTP server in which the upgrade files are located.
34. In the table, check the **Select** box for all firmware components you want to upgrade. The current version of each component is listed to help you confirm the need for upgrade.
35. Enter the filename of each firmware upgrade file you want to install in each line of the table where you checked the **Select** box.

36. Click **Continue**. The firmware is upgraded and the TFTP Server screen appears. The TFTP Server screen enables you to upload firmware and configuration files for IP phone upgrades to the G250 TFTP server.



37. If you want to upload configuration and firmware files for IP phones to the G350 TFTP Server, do the following:

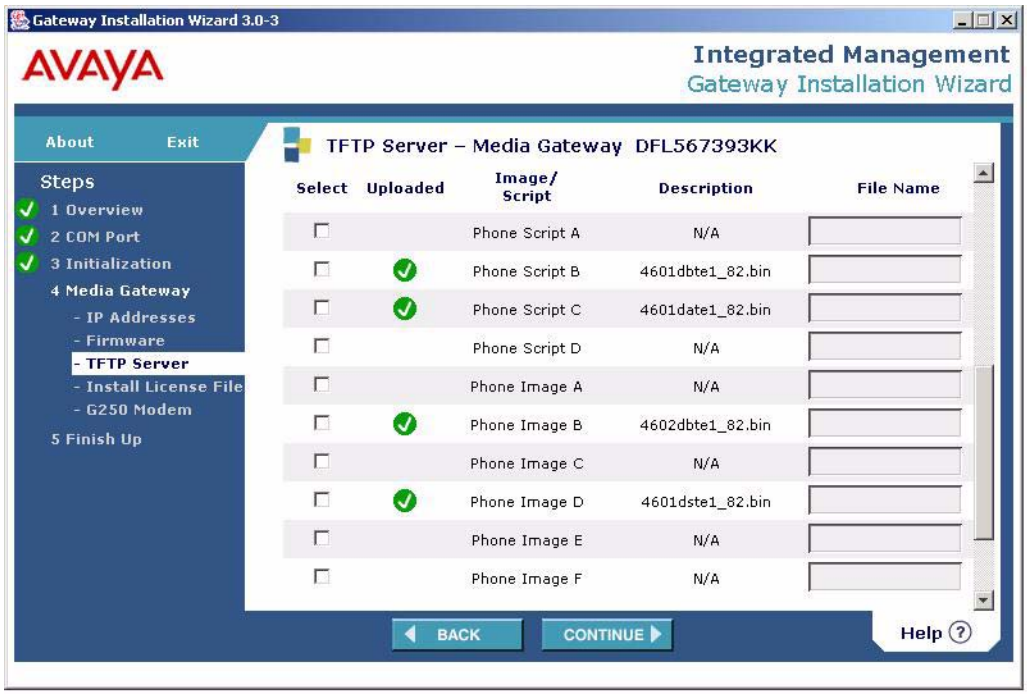
    a. In the Server IP Address field, enter the IP address of the machine hosting the files that are to be uploaded.

    b. Select the file transfer protocol (TFTP, FTP, or SCP) you want to use to upload the files from the host machine. TFTP is selected by default.

    c. The use of the SCP protocol is limited to copying files of 1 MB or less. Therefore, an SCP server can be used for copying the script files, which do not exceed 128 KB, but cannot be used for copying image files.

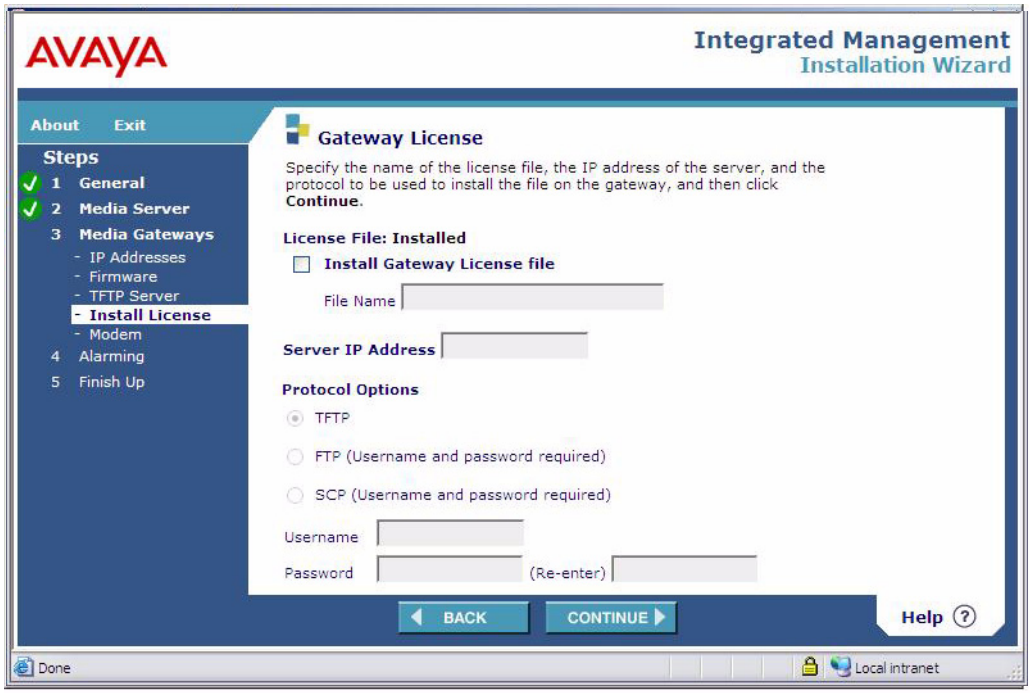
    d. If you selected FTP or SCP, enter the username and password in the Username and Password fields, and re-enter the password for confirmation in the Re-enter Password field.

38. Click **Continue**.



39. In the Select column, check any files you wish to upload. If you selected SCP as your upload protocol, the checkboxes for the phone images are disabled. If a green circled checkmark is displayed in the Uploaded column, the file has already been uploaded.

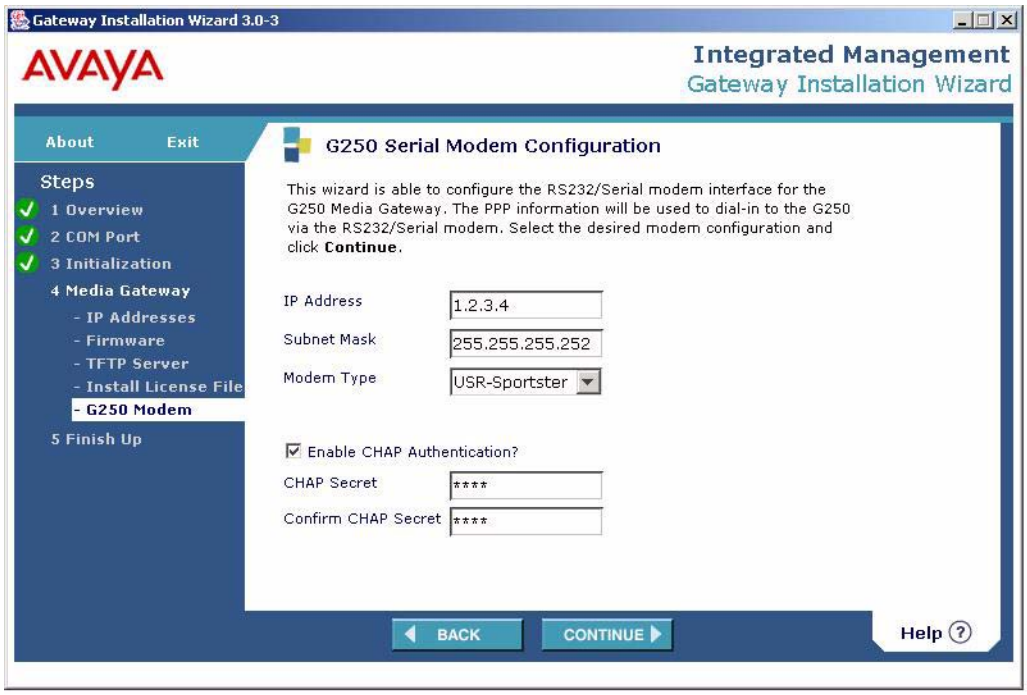
40. Click **Continue**. The files are uploaded and the Gateway License screen appears.



41. Click **Continue**. G250 Modem Type Selection screen appears. If you are using GIW only to upgrade firmware, click **Continue** until you reach the Finish Up screen. Skip the next steps until step 52.

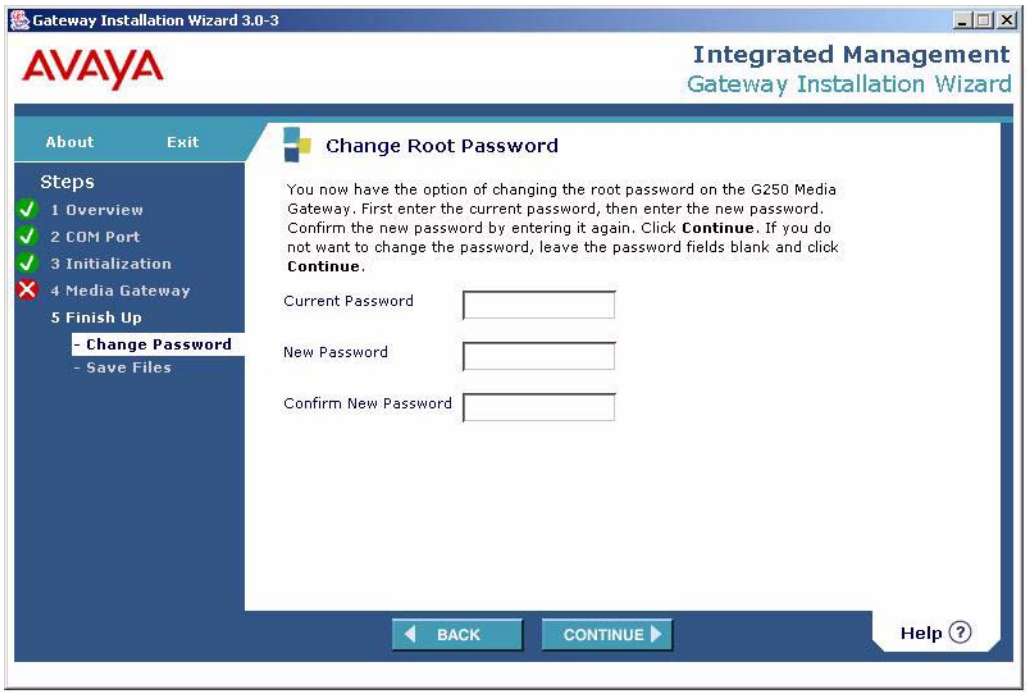
42. If you do not need to connect a modem to the G250, select **None**.
43. If you do need to connect a modem to the G250, select the type of modem you want to connect.

44. Click **Continue**. The appropriate modem configuration screen appears.



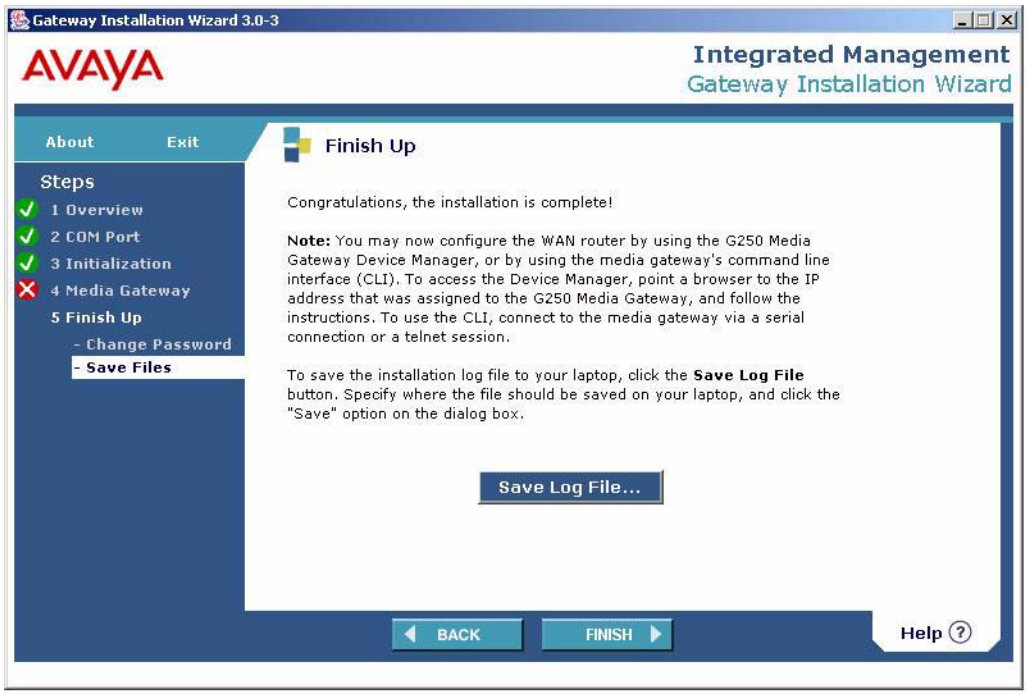
45. In the IP Address field, enter the RAS IP address of the modem obtained using the ART tool. See Run the Automatic Registration Tool (ART) for the RAS IP address on page 22.
46. Enter the Subnet Mask.
47. Check **Enable CHAP Authentication**.
48. In the CHAP Secret field, enter the CHAP secret key obtained using the ART tool. See Run the Automatic Registration Tool (ART) for the RAS IP address on page 22.
49. In the Confirm CHAP Secret field, reenter the CHAP secret key.

50. Click **Continue**. The Change Root Password screen appears.



51. If you would like to change the password on the G250 Media Gateway, enter the current password in the Current Password field, enter a new password in the New Password field, and re-enter the new password in the Confirm New Password field.

52. Click **Continue**. The Finish Up screen appears.



You have completed GIW. Follow the on-screen instructions if you want to save the installation log file. Further configurations, as described in this screen, can now be performed either remotely, via a modem that you enabled with GIW, or locally.

Connect a modem, if necessary

If you enabled a serial modem on the G250 during your GIW session, you can now connect the modem.

To connect a serial modem:

1. Connect the serial modem to a working telephone line.
2. Connect the provided DB-25 adapter to the modem.
3. Disconnect the flat cable from the COM port of the laptop computer.
4. Connect the flat cable to the DB-25 connector on the modem.

Test the modem connection, if necessary

If the modem is successfully initialized, the MDM LED on the G250 front panel lights. If you connected a modem, check that the MDM LED is alight and dial into the modem to verify that you can authenticate to the modem.

Index

F

G

H

I

L

M

O

P

R

S

T

U

W