Installing, Configuring, and Upgrading to Avaya Communication Manager Express

03-602251
Issue 1.1
Release 5.1
October 2008

© 2008 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the documents, *Avaya Support Notices for Software Documentation*, 03-600758, and *Avaya Support Notices for Hardware Documentation*, 03-600759.

These documents can be accessed on the documentation CD and on the Web site, http://www.avaya.com/support. **On the Web site, search for the document number in the Search box.**

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Trademarks

Avaya, Communication Manager Express, MultiVantage, and INTUITY are trademarks of Avaya Inc. Some MultiVantage Express applications use the Open Source Indy Sockets library. License terms for this library are available at http://www.indyproject.org/License/index.en.iwp.

All non-Avaya trademarks are the property of their respective owners.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya’s Web site at: http://support.avaya.com/ThirdPartyLicense/

The Third Party open source copyright license text file is available in the following directory on the installation DVD:

<DVD_ROM_Drive>:/licenses

For more information regarding the Third-Party components and terms for Communication Manager Express 5.1, see http://support.avaya.com/Copyright.

Avaya support

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

Contents

Chapter 1: Introduction 7
Purpose, scope, and audience of this guide 7
Organization of this book 7

Chapter 2: Installation and configuration overview 9
Introduction 9
Installation prerequisites 10
Hardware installation overview 11
H.248 Media Gateway and LSP hardware installation 12
G450 Media Gateway hardware installation 12
Software installation and configuration overview 12
Progress indicators 12
Important configuration notes 14
SPIRIT alarming overview 15

Chapter 3: Installing the Communication Manager Express software 17
Installing the software from the DVD 17
Setting up the configuration process 20
Logging on 21
Verifying the server date and time 21
Selecting the configuration type 23

Chapter 4: Configuring Communication Manager Express—new installation 27
Completing the configuration steps 27
Step 1. Login to wizard 27
Step 2. Selecting a country 28
Step 3. Installing the RFA files and customer login 28
Step 4. Setting up the IP telephone settings and DHCP 30
Step 5. Activating alarming and VPN access 33
Step 6. Installing the gateways 36
Step 7. Selecting a template 37
Step 8. Configuring SIP 40
Step 9. (Optional) Loading the user data 41
Step 10. Save and Back up 42
Step 11. Post-installation configuration 44

Chapter 5: Upgrading MVE R2.x to CME 5.1 47
Installing the software from the DVD 48
Completing the configuration steps 49
Step 1. Login to the wizard 49

Step 2. Selecting a country 49
Step 3. Installing the RFA files and customer login 49
Step 4. Activating alarming and VPN access 51
Step 5. Loading the backup file 53
Step 6. Configuring SIP 55
Step 7. (Final step) Save and back up 56
Step 8. Post-installation configuration 57

Chapter 6: System logins and access 59
System logins 59
Modem and Services port (eth1) access to machines 60
Port redirection 60
Port switching 61
Administering through customer LAN 64

Appendix A: Troubleshooting installation problems 65
Solving wizard navigation and installation step errors 65

Appendix B: How to manually add SIP configuration to CM 69
Changes to CM to support SIP 69
Locations 69
Network Region 69
Route Pattern. 70
SIP Signaling Group 70
SIP Trunk Group 71
Node Names 73
Off-PBX Configuration Set 73

Appendix C: Upgrading MVE R1.x to CME 5.1 75
Backing up MultiVantage Express data for an upgrade 75
Pre-upgrade tasks 75
Backing up the Communication Manager, AUDIX, and VM2 data 76
Preparing Communication Manager, AUDIX, and VM2 backup files 76
Preparing the VM2 backup files. 77
Copying the backup files to an external device 78
Backing up AE Services data 79
AE Services backup 79
Recording the customer IP addresses and logins 79
IP addresses 79
Logins 80
Setting up customer super-user login 80

Restoring MVE R 1.x data for upgrades 81
Post-upgrade procedures 83

Appendix D: Installing and configuring G450 gateway—an overview 85
Example of basic G450 running configuration. 86

Index 87

Chapter 1: Introduction

This chapter describes the audience, purpose, and organisation of the *Installing, Configuring, and Upgrading to Avaya Communication Manager Express* document.

Purpose, scope, and audience of this guide

This document is for technicians and administrators as a reference to:

- Install and configure CME 5.1
- Upgrade from MultiVantage Express (MVE) 1.*x* and 2.*x* to CME 5.1

The applications that each virtual machine supports are standard, and the normal processes to access and maintain these applications are retained wherever possible. This guide does not explain these normal processes. This guide describes only the processes which vary from the standard processes to support CME.

The technicians and administrators who use this guide must:

- refer to the supporting documentation of the products as necessary

  Important:
  The complete supporting documentation is available on the CME supplemental DVD

- have prior training on the Communication Manager (CM), IA770, and SES products

Organization of this book

The procedure to install and configure a CME system is similar to the procedure to upgrade from an existing MVE system to the CME system.

- The procedure to install and configure a CME system is presented in chapters 2 and 3.

- The procedure to upgrade from the MVE system to the CME system is presented in chapter 5 and appendix C.
- Information about system logins and access is presented in Chapter 6.

Chapter 2: Installation and configuration overview

This chapter presents an overview of the simplified installation process of CME. This chapter contains the following sections:

- Introduction on page 9
- Installation prerequisites on page 10
- Hardware installation overview on page 11
- Software installation and configuration overview on page 12
- SPIRIT alarming overview on page 15

Introduction

To install a CME 5.1 system, (chapters 2, 3, and 4):

1. Install the hardware, including the server and the gateways.
2. Install the CME software.
3. Configure the system using the default configuration template.
4. Further customization.

To upgrade an existing MVE system to CME 5.1 (chapter 5 and appendix C):

1. Back up the existing MVE system data.
2. Install the new server hardware.
3. Install the CME software.
4. Configure the system using the MVE backup file through the wizard.

Installation prerequisites

- CM license file for CME 5.1 platform type MVE
- CM password file for CME 5.1 platform type MVE
- (Optional) Solution Elements file
- Six IP addresses on the same network for the following CME elements:
  - Base server, Communication Manager, System Management, Application Enablement Services (AES), AUDIX, and SIP Enablement Services (SES)
- Customer network mask
- Subnet mask
- Default gateway IP address
- (Optional) Customer DNS server IP address
- IP addresses for the gateways
- (Optional) If you plan to use DHCP on CME for the IP telephones, a range of IP addresses
- (Optional) If you plan to import user data, Avaya Bulk Import Tool (ABIT) file
- A cross-over cable or a serial cable for the G450 implementation
- (Optional) Customer SIP domain
- (Optional) Customer SIP DNS
- For alarming through HTTPS, IP address and port number of the customer's Web proxy server

Important:
To enable the SPIRIT (Serviceability through Product Integrated Remote Intelligent Agents and Transport) alarming, you must perform the following during the installation process:

a. Configure a valid DNS server

b. Configure a valid HTTPS proxy address and port (if applicable)

Hardware installation overview

CME 5.1 requires the S8510 server. The server hardware installation follows the standard sequence of Avaya S8510 server deployment. Figure 1 shows the back view of the S8510 with the USB and Ethernet ports labeled. For more information, see *Installing the Avaya S8510 Server Family and Its Components*.

Important:
CME 5.1 uses an Avaya S8510 server with 4-GB of memory. You cannot install the software on a system that does not have the required amount of memory.

Figure 1: S8510–back view

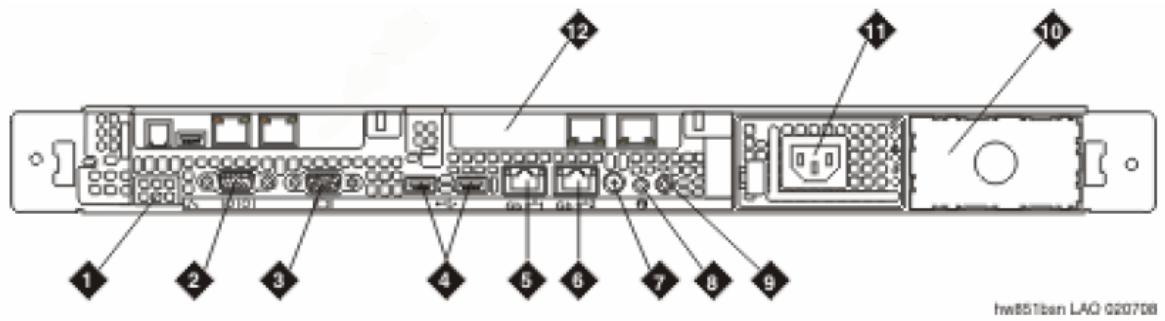


Figure notes:

1. Remote access controller (unused)
2. Serial connector
3. Video connector (for optional use of monitor)
4. USB ports (for optional use of modem, mouse and keyboard)
5. GB-1 Customer LAN (Eth 0)
6. GB-2 Services port (Eth 1)
7. System status indicator connector
8. System ID button
9. System status LED
10. Bay for optional redundant power supply
11. Power supply
12. Dual NIC (NIC should be in this PCI slot on the server)

H.248 Media Gateway and LSP hardware installation

If you are installing an H.248 media gateway, with or without a Local Survivable Processor (LSP), see one of the following installation and quick start documents:

- *Quick Start for Hardware Installation: Avaya G450 Media Gateway*, 03-602053.
- *Installing and Upgrading the Avaya G450 Media Gateway*, 03-602054.
- *Installing and Upgrading the Avaya G700 Media Gateway* and *Avaya S8300 Media Server*, 555-234-100.
- *Quick Start for Hardware Installation: Avaya S8300 Media Server and Avaya G700 Media Gateway,* 555-233-150.
- *Installation and Upgrade for the Avaya G250 Media Gateways,* 03-300434.
- *Quick Start for Hardware Installation: Avaya G250 Media Gateway*, 03-300433.
- *Installing and Upgrading the Avaya G350 Media Gateway*, 03-300394.
- *Quick Start for Hardware Installation: Avaya G350 Media Gateway*, 03-300148.

G450 Media Gateway hardware installation

If you are installing a G450 media gateway, see *Quick Start for Hardware Installation: Avaya G450 Media Gateway,* 03-602053 and *Installing and Upgrading the Avaya G450 Media Gateway,* 03-602054.

Software installation and configuration overview

This section presents an overview of the installation and configuration process for the CME 5.1 software.

Progress indicators

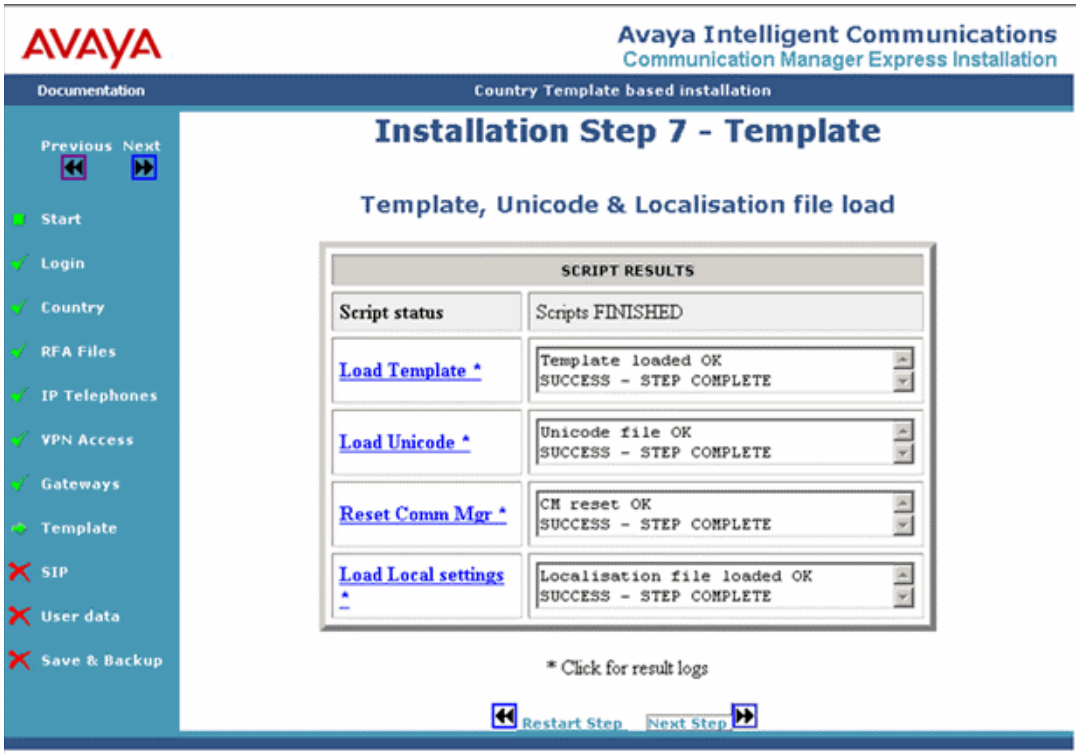
During the installation process, the system runs several predefined scripts. The browser display shows the status of these scripts. The status display is refreshed every 10 seconds.

Important:
Do not attempt any additional action until the script installation is complete. Allow 30 to 60 seconds for an action to complete.

You can see the status of progress through the installation steps on the left navigation menu. You can restart an individual step if needed. If restarting the step causes an error, restart the wizard from the beginning. Although you can go back to any previous step, you must continue from that step forward in strict sequence only. Avaya recommends that if a step fails, you restart the wizard from the beginning.

When the wizard is configuring the system, a progress indicator is displayed. If the progress indicator icon is displayed, the wizard is still active. The user must wait till the progress indicator icon disappears to proceed to the next step. When a step is complete, SUCCESS – STEP COMPLETE is displayed in the status box of that step. The following figure displays the successful completion of all the scripts.

Figure 2: Successful completion of the scripts



If you want to view the log files associated with a step, click on the name of the installation step. The name of the installation step is followed by * in the SCRIPT RESULTS box. The log files provide useful information to troubleshoot a step that did not complete properly or does not display the success message.

Important configuration notes

The Terminal Translation Initialization (TTI) merge code of ***69** and separate code of **#69** are predefined as the feature access codes.

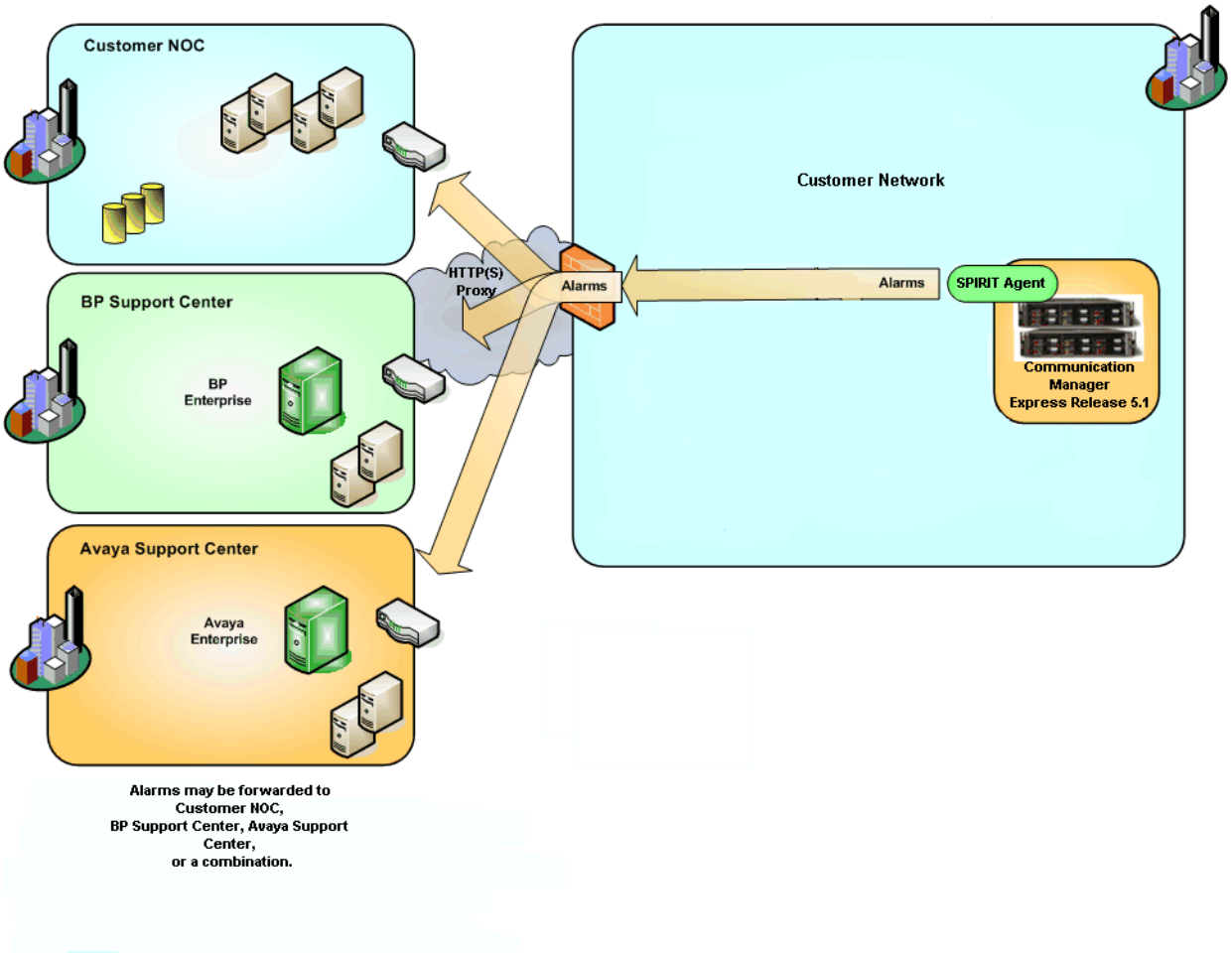
After the wizard finishes all the steps, you must complete the site-specific programming such as adding public access trunks and associated routing to the system.

SPIRIT alarming overview

Serviceability through Product Integrated Remote Intelligent Agents and Transport (SPIRIT) is a solution that improves service methods and processes and provides better remote management capability for CME. SPIRIT enables collection of inventory and automatic creation of service tickets. SPIRIT implementation is composed of a SPIRIT Agent and a SPIRIT Enterprise server. A SPIRIT Agent is a Java application that helps to monitor and manage CME on your network. To enable SPIRIT alarming, you must choose one of the following:

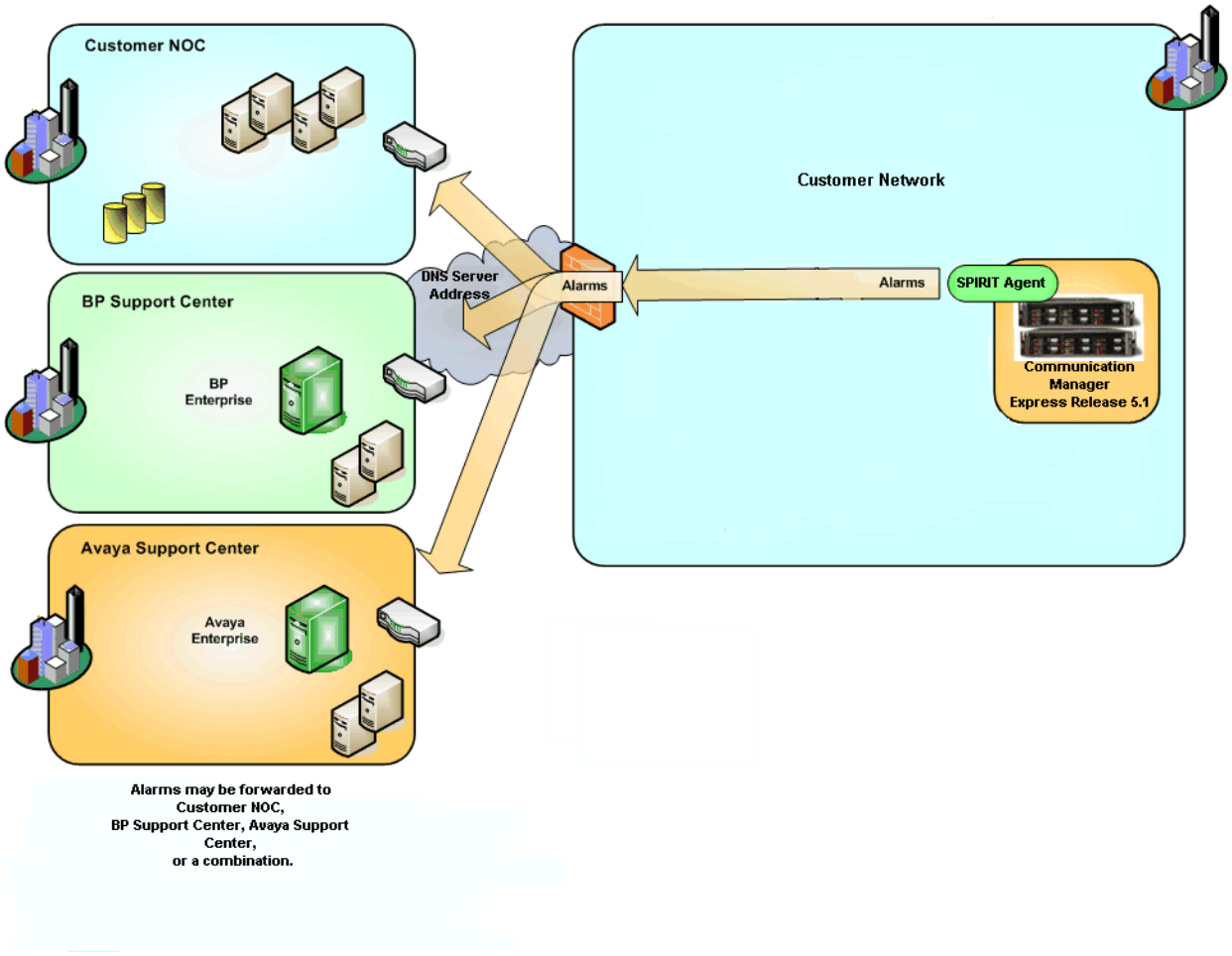
- If you have an HTTP(S) proxy server, configure a valid HTTP(S) proxy address and port (if applicable) and a DNS server.

Figure 3: Alarming through HTTP(S) proxy



- If you do not have an HTTP(S) proxy server (that is, you are directly connected to the Internet), configure a valid DNS server. For example, https://alarming.esp.avaya.com

Figure 4: Alarming through DNS server



Chapter 3: Installing the Communication Manager Express software

The procedures in this chapter are for installing a CME 5.1 system.

If you are upgrading an existing MultiVantage Express system to CME 5.1, see the following:

- **Upgrade from MVE R2.*x* to CME 5.1: Chapter 5: Upgrading MVE R2.x to CME 5.1 on page 47.**
- **Upgrade from MVE R1.*x* to CME 5.1: Appendix C: Upgrading MVE R1.x to CME 5.1 on page 75.**

This chapter describes how to install the server software—the operating system, the virtualization software, and the application software on the virtual machines—from the installation DVD on the new server after you have installed the hardware. After installing the server software, you can log in and complete the initial administration and configuration steps described in Chapter 4: Configuring Communication Manager Express—new installation on page 27.

Installing the software from the DVD

Tip:
During this procedure, when you are waiting for the system to restart, enter **`ping -t 192.11.13.6`** from a command prompt window on your services laptop computer to start a continuous ping command.

To begin the installation:

1. Connect your services laptop computer to the services port (GB-2 Services port) on the back of the server. See Figure 1: S8510–back view on page 11.
2. Attach the power cord to the S8510 server and plug it into the AC outlet.
3. Turn on power to the S8510 server and insert the installation DVD into the DVD-ROM drive.

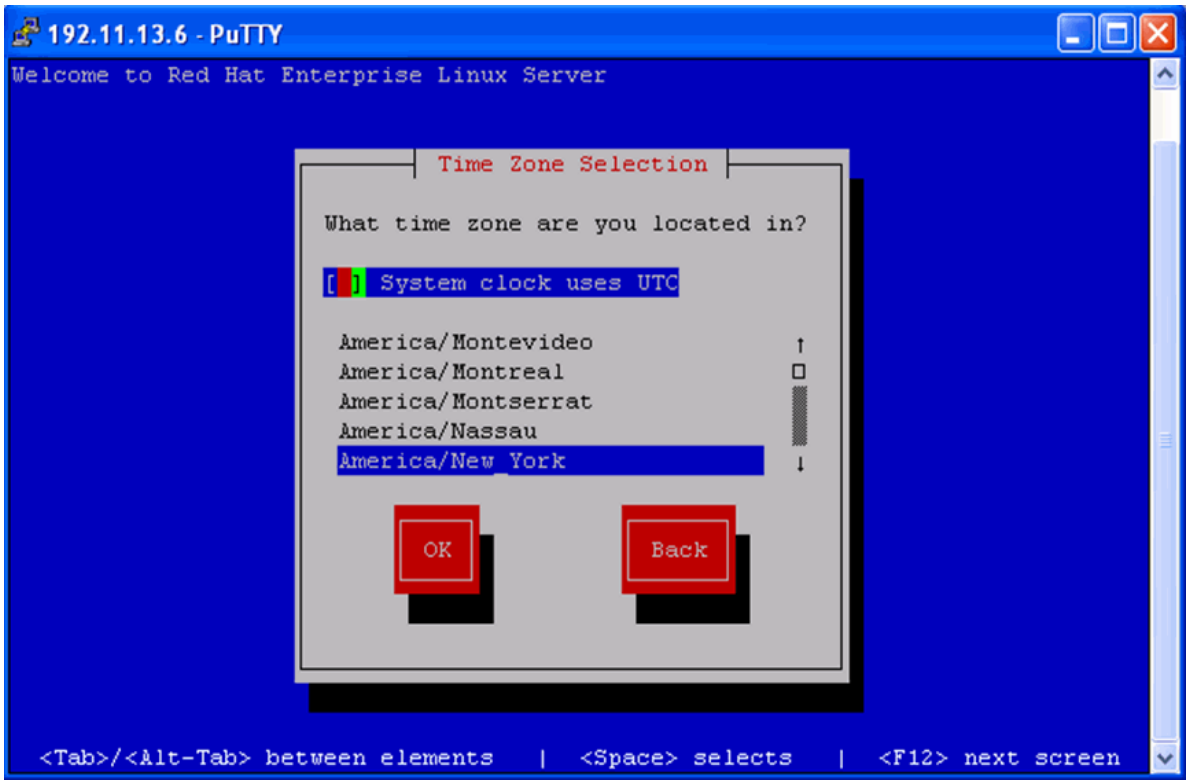
4. Use PuTTY (or other Terminal client) to start a **Telnet** (do not use **SSH**) session from your services laptop computer to 192.11.13.6 on port 23. In PuTTY, set the Window Translation character set to 'UTF-8'. This ensures the boxes within the setup windows are displayed correctly.
   PuTTy is a free Telnet and SSH client for Windows and UNIX platforms which can be downloaded from:
   http://www.putty.org/

   Note:
   Do not use the Windows telnet client because it does not support the correct emulation for the installation steps and causes the server to reboot.

   After your computer connects to the server, the system displays the Linux Server time zone selection screen. (Figure 5: Time Zone Selection on page 18).

5. Press the Tab key on your computer to get to the list of time zones. Scroll through the list and select the appropriate time zone for this installation. Press the Tab key on your computer and select **OK** and press the space bar.

Figure 5: Time Zone Selection



6. Several progress screen are displayed during the installation.

7. The installation takes approximately 5 minutes. When the installation is complete, the Linux screen closes and the system ejects the DVD from the DVD-ROM drive. The server reboots automatically in approximately 5 minutes and is ready to start the installation of the VM software.

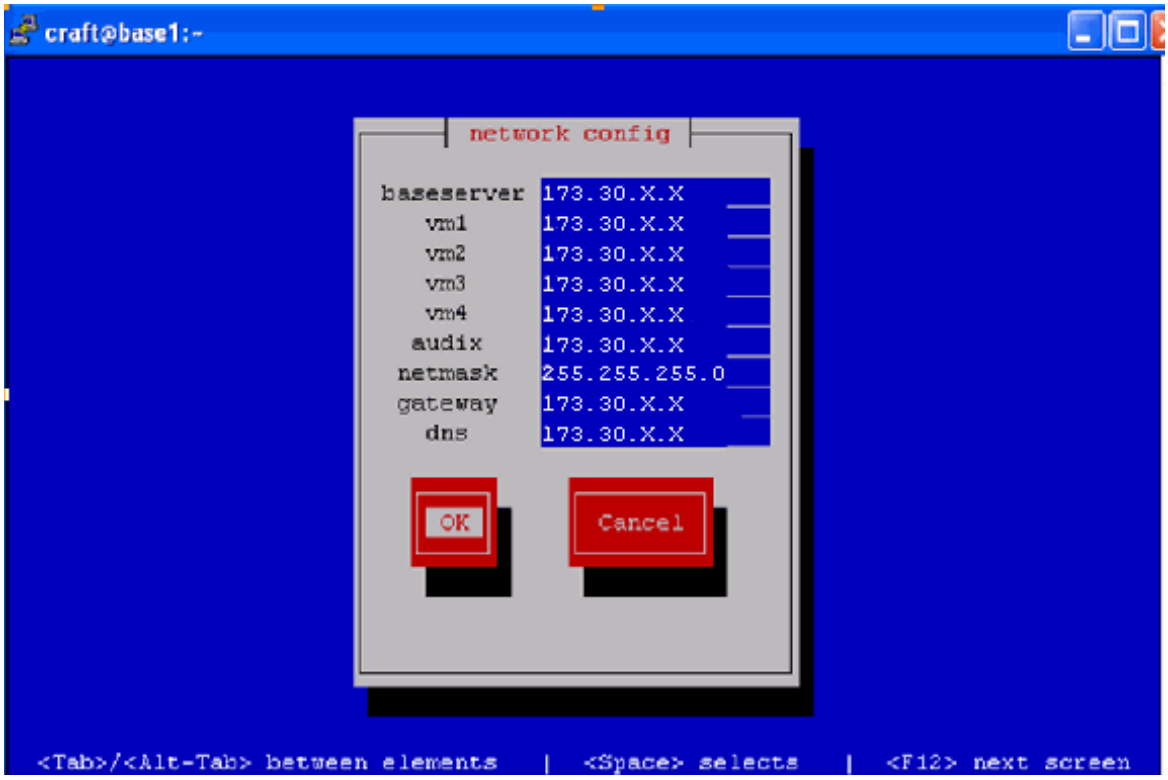
   Important:
   Before reinserting the DVD in the DVD-ROM drive in the next step, ensure that the server reboots completely. If you insert the DVD before the server reboots completely, the installation process restarts from the beginning.

8. After the reboot is complete, reinsert the CME software DVD in the DVD-ROM drive.
9. From your services laptop computer, use PuTTY to start an **SSH** (do not use **Telnet**) session to 192.11.13.6, port 22, and log in as **craft** using the initial craft password (**craft01**).
10. At the command line prompt, enter the command **`cmesetup`**.

    Note:
    The message 'Unable to connect to the Xend' might appear as the virtual machines are not yet installed. This is normal and you can ignore it.

11. When the system prompts, enter the current time and date.
12. When the IP address configuration screen is displayed, enter the customer network IP addresses (Figure 6: Base server network IP address configuration on page 20.)

Figure 6: Base server network IP address configuration



It is important that you enter the correct IP addresses at this stage. It is not recommended to change the IP addresses after this stage because it might require significant re-programming of the system.

Note:
The default IP addresses are in the 172.30.*x.x* private Internet address space. Change the default IP addresses to the IP addresses supplied by the customer.

After you select **OK**, the DVD proceeds to install the software and the virtual machines. This process takes approximately 15–20 minutes.

13. When the software installation is complete, the system ejects the DVD from the DVD-ROM drive and reboots. Remove the DVD and make sure that you store it carefully for future use.

Setting up the configuration process

After you have installed the core system software on the server, log on to the Maintenance Web Pages on the base server and start the configuration process.

Note:
In this chapter, the term installation as used on the Web pages has the same meaning as the term configuration as used in the text.

Logging on

To log on to the base server Maintenance Web Pages:

1. Open a browser on your services laptop computer that is connected to the services port (eth1) on the S8510 and enter **`https://192.11.13.6:11443`**. The system displays the logon screen.

   Note:
   You must use ’https’ not ’http’.

2. Log on to the server as **craft** using the initial craft password (**craft01**).

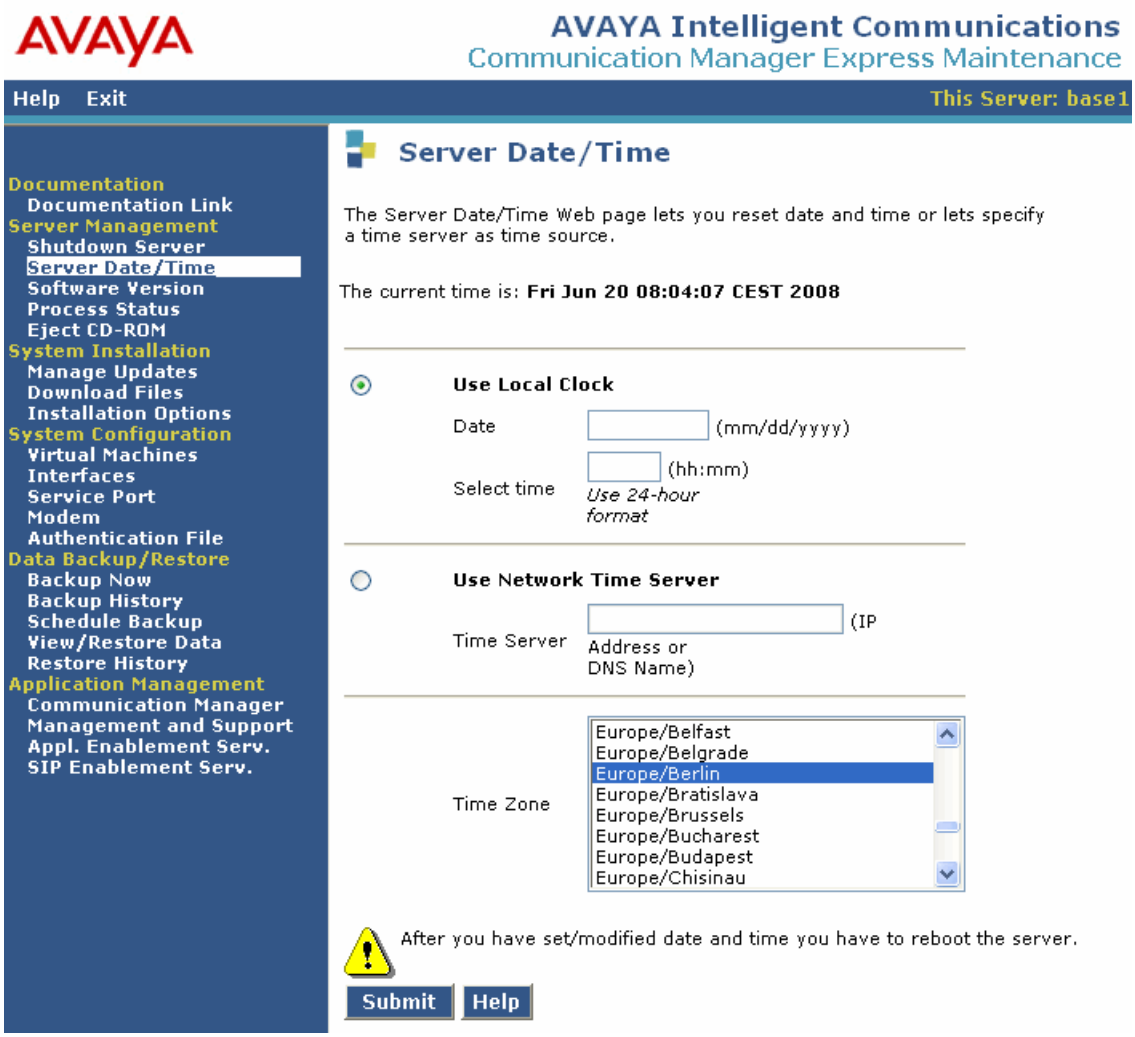
   The system displays the main screen with the copyright notices. This screen provides access to all the remaining server partitions and functions from the left navigation menu.

Verifying the server date and time

1. On the left navigation menu, click **Server Date/Time**.

   The system displays the Server Date/Time screen (Figure 7: Server Date/Time screen on page 22).

Figure 7: Server Date/Time screen



2. Verify the current date and time displayed at the top of the screen. If the date and time are correct, proceed to Selecting the configuration type on page 23.

   If the date or time needs to be changed, select **Use Local Clock** and enter the current date and time and click **Submit**.

   To commit the date or time changes, perform the following actions:

   a. On the left navigation menu, in the Server Management section, click **Shutdown Server**.

   b. Select **Immediate Shutdown** and **Restart server after shutdown**.

   c. Click **Submit**. The server reboots. This process takes several minutes. After the reboot completes, log on to the base server again.

   To check the virtual machine status:

a. Click **Process Status**. The system displays the Process Status screen.

b. Select **Summary** and **Display Once**.

c. Click **View**. The system displays the View Process Status Results screen.

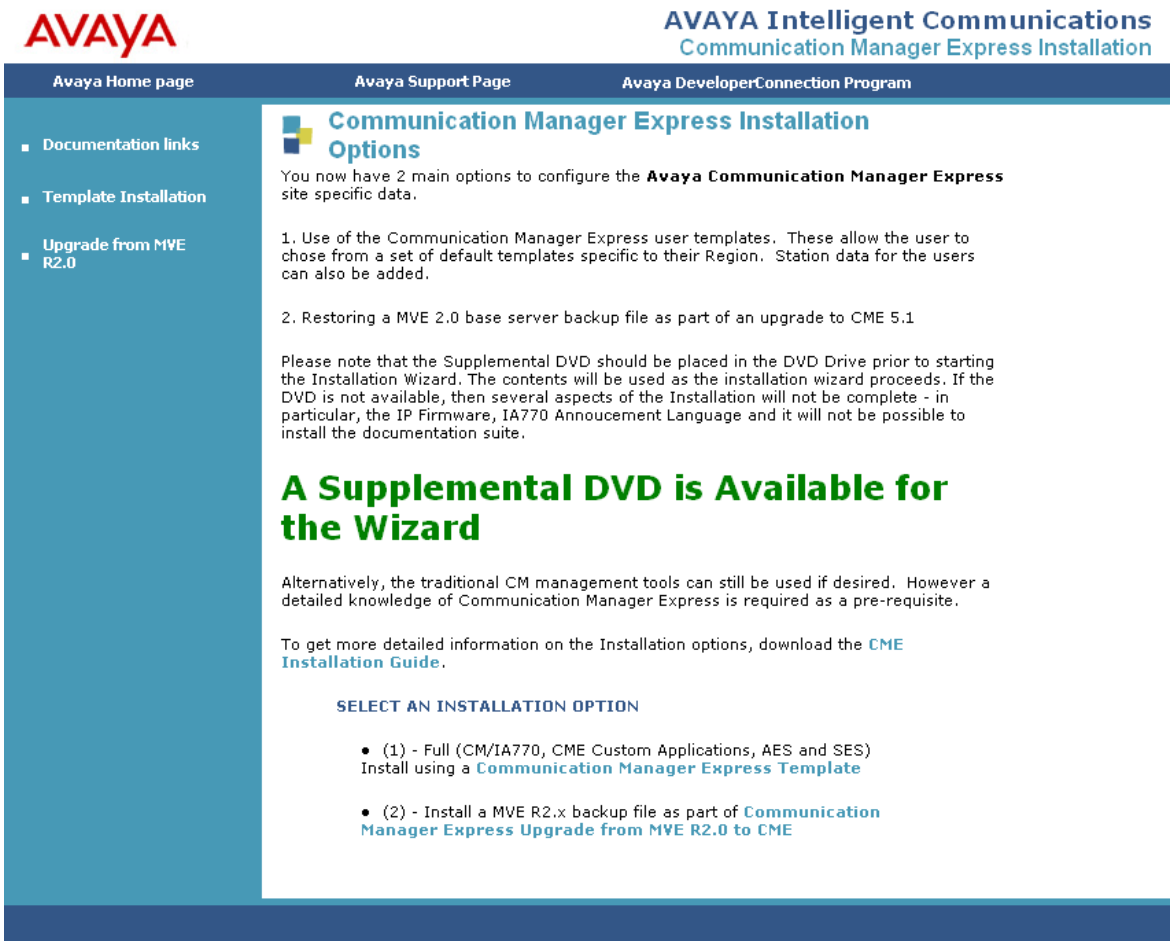
Selecting the configuration type

To select the configuration type, perform the following actions:

1. Insert the CME Supplemental DVD into the DVD-ROM drive on the server.
2. On the left navigation menu, in the System Installation section, click **Installation Options**.

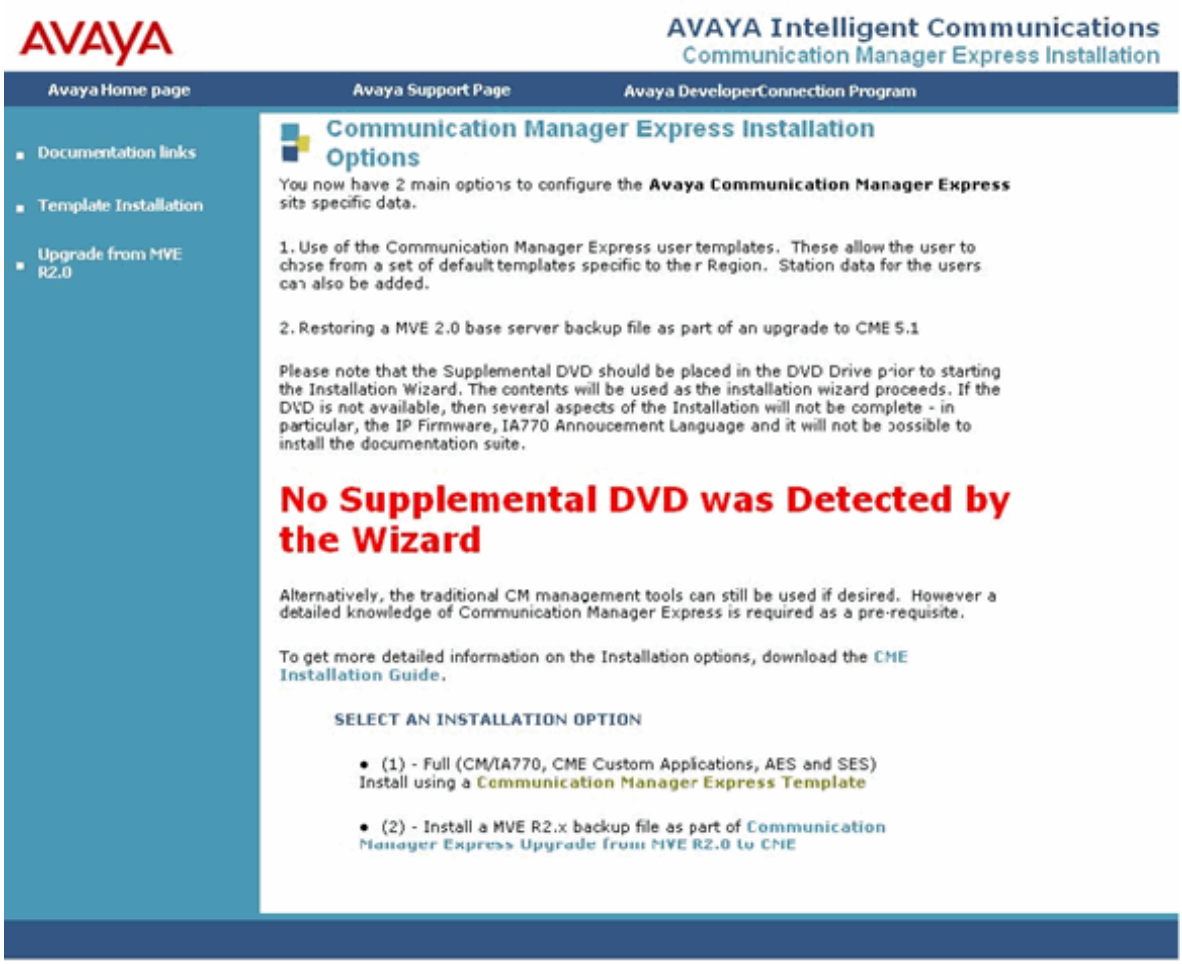
   The system displays the Communication Manager Express Installation Options screen (Figure 8).

Figure 8: CME Configuration Options screen–Supplemental DVD inserted



If you have not inserted the CME Supplemental DVD, you get a warning screen (Figure 9). However, you can proceed with the installation process.
If the supplemental DVD is not inserted before proceeding with the installation process, the IP phone firmware is not loaded and the AUDIX announcement language is automatically set to US English.
Avaya recommends you to insert the supplemental DVD and then proceed with the installation process.

Figure 9: CME Configuration Options screen–Supplemental DVD not inserted



Note:

If the browser times out, wait for 60 seconds and try again as the virtual machine may still be in the process of booting up. If you cannot access the system after three attempts, see the troubleshooting section of the *Administering and Maintaining Communication Manager Express* guide.

For a new installation, proceed to the configuration steps described in Chapter 4: Configuring Communication Manager Express—new installation on page 27.

For an upgrade from MVE R2.*x* to CME 5.1, proceed to the configuration steps described in Chapter 5: Upgrading MVE R2.x to CME 5.1 on page 47.

For an upgrade from MVE R1.*x* to CME 5.1, proceed to the configuration steps described in Appendix C: Upgrading MVE R1.x to CME 5.1 on page 75.

Chapter 4: Configuring Communication Manager Express—new installation

The procedures in this chapter are for installing a new CME 5.1 system.

If you are upgrading an existing MultiVantage Express system to CME 5.1, see the following:

- **Upgrade from MVE R2.*x* to CME 5.1: Chapter 5: Upgrading MVE R2.x to CME 5.1 on page 47.**
- **Upgrade from MVE R1.*x* to CME 5.1: Appendix C: Upgrading MVE R1.x to CME 5.1 on page 75.**

This chapter describes the steps to load configuration information on the CME virtual machines. On the left navigation menu of the Communication Manager Express Installation Options screen (see Figure 8: CME Configuration Options screen–Supplemental DVD inserted on page 23 and Figure 9: CME Configuration Options screen–Supplemental DVD not inserted on page 24), select **Template Installation** to start the CME 5.1 installation wizard.

Alternatively, you can select **Communication Manager Express Template** in the SELECT AN INSTALLATION OPTION section of the Communication Manager Express Installation Options screen.

Completing the configuration steps

Perform the following steps in sequence to complete the software configuration. You can see the status of progress through the installation steps on the left navigation menu.
If any of the steps fail to complete successfully, see Appendix A: Troubleshooting installation problems on page 65.

Step 1. Login to wizard

After you select the template Installation option, the system prompts you to log on with an Avaya Communication Manager login. Use the username as **craft** and the initial password as **craft01**.

Important:
If you have already run the wizard and installed the authentication file prior to the current installation, use the customer login (username and password) you added in step 3 instead of **craft** and **craft01**.

Step 2. Selecting a country

On the Country Selection screen, choose a country by clicking the appropriate flag. Selecting a flag configures the system with the following parameters specific to the country selected:

- Telephone display language
- Voice mail language
- Tone plan and ARS table
- Feature access codes
- Companding

Click **Next Step**. The system displays the Load the RFA License & Password Files screen.

Step 3. Installing the RFA files and customer login

After you select the country setting, you must load the RFA license file and the RFA authentication file from your laptop computer to the server. You must also create a super-user customer login to access Communication Manager at this time. The **dadmin** login may be added as the customer login if it is enabled in the RFA licence file. See Figure 10: Load license & password files and create customer login on page 29.

Note:
The CME 5.1 license file is used for Communication Manager and INTUITY AUDIX 770 (IA770). CME 5.1 requires no other RFA license files as AES and SES are already licensed within the CME 5.1 bundle.

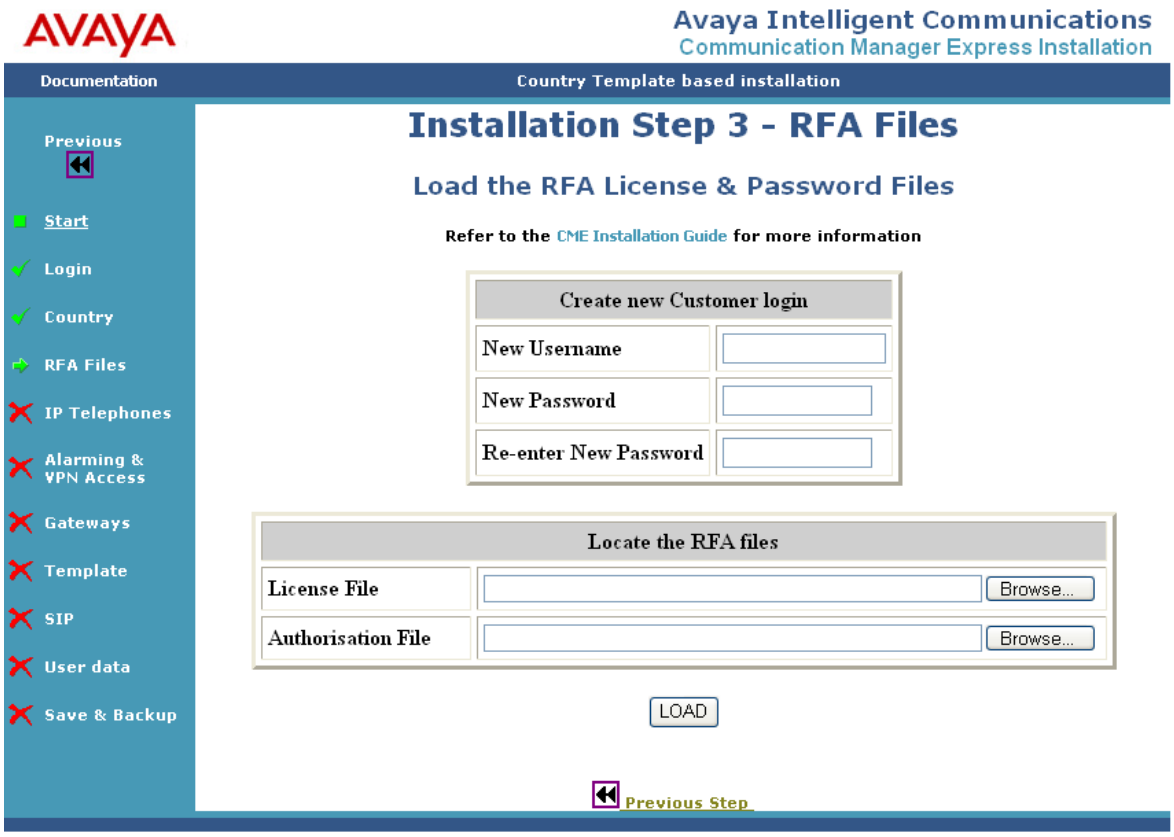
To create a customer login for Communication Manager, perform the following actions:

1. In the **New Username** box, enter the user name.
2. In the **New Password** box, enter the new password.

   The username and password must conform to the normal requirements for Communication Manager logins.
3. In the **Re-enter New Password** box, re-enter the new password.

Important:
Make sure you record the new username and password that you entered. You cannot retrieve them from the system later.
If the new username and password are lost, you need to re-configure the system. In addition, if you restart the wizard after this step, use the new customer login and password to log on to the wizard instead of **craft** and **craft01**.

Figure 10: Load license & password files and create customer login



To load the RFA files:

1. Locate the license file by clicking **Browse** next to the License File box.
   The system displays the Choose File window.
2. Locate the license file on your laptop and click **Open**.
3. Locate the authorisation file by clicking **Browse** next to the Authorisation File box.
   The system displays the Choose File window.
4. Locate the authorisation file on your laptop and click **Open**.
5. Click **Load**.

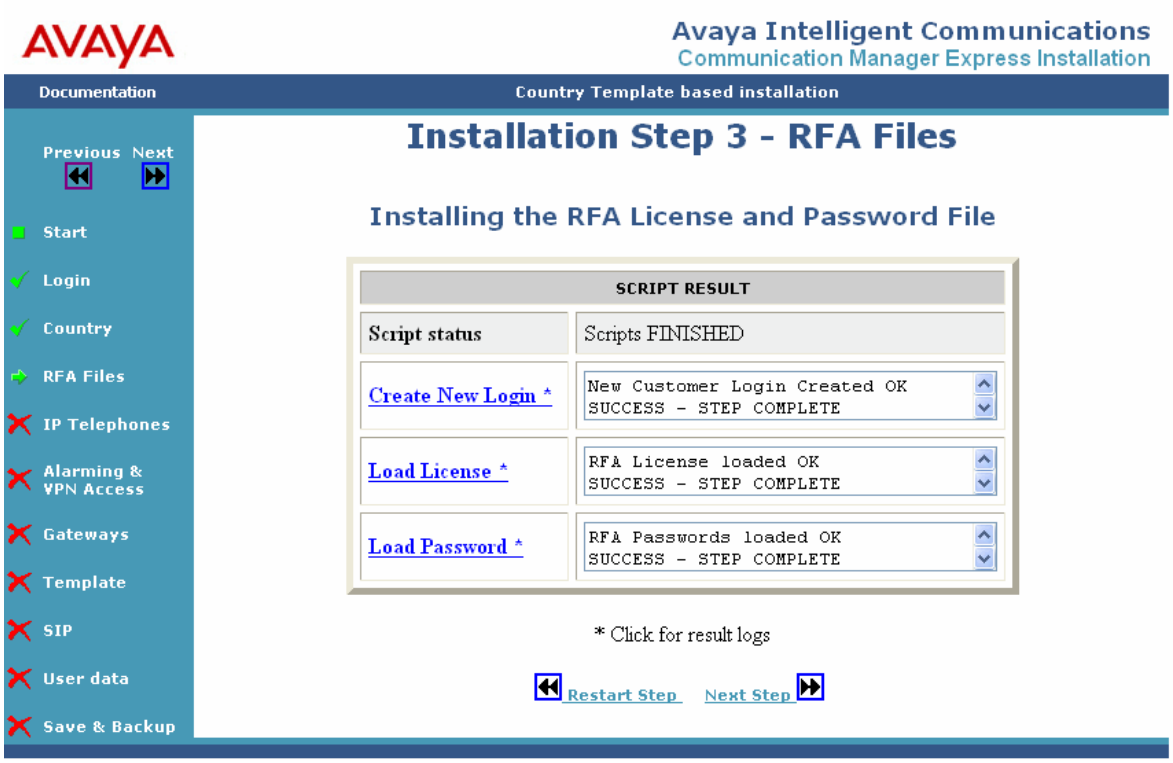
6. On the next screen, verify the files and click **Confirm**.

Note:
If you select an incorrect file, click **Cancel** to start the step again.

The system displays the SCRIPT RESULT screen. After the script loads the RFA files and creates the login, the SCRIPT RESULT screen shows `OK SUCCESS - STEP COMPLETE` for each item. (Figure 11: Script Result screen for RFA files and new login on page 30).

The license and authentication files load immediately. If you restart the wizard after this step, use the new customer login and password to log on to the wizard.

Figure 11: Script Result screen for RFA files and new login

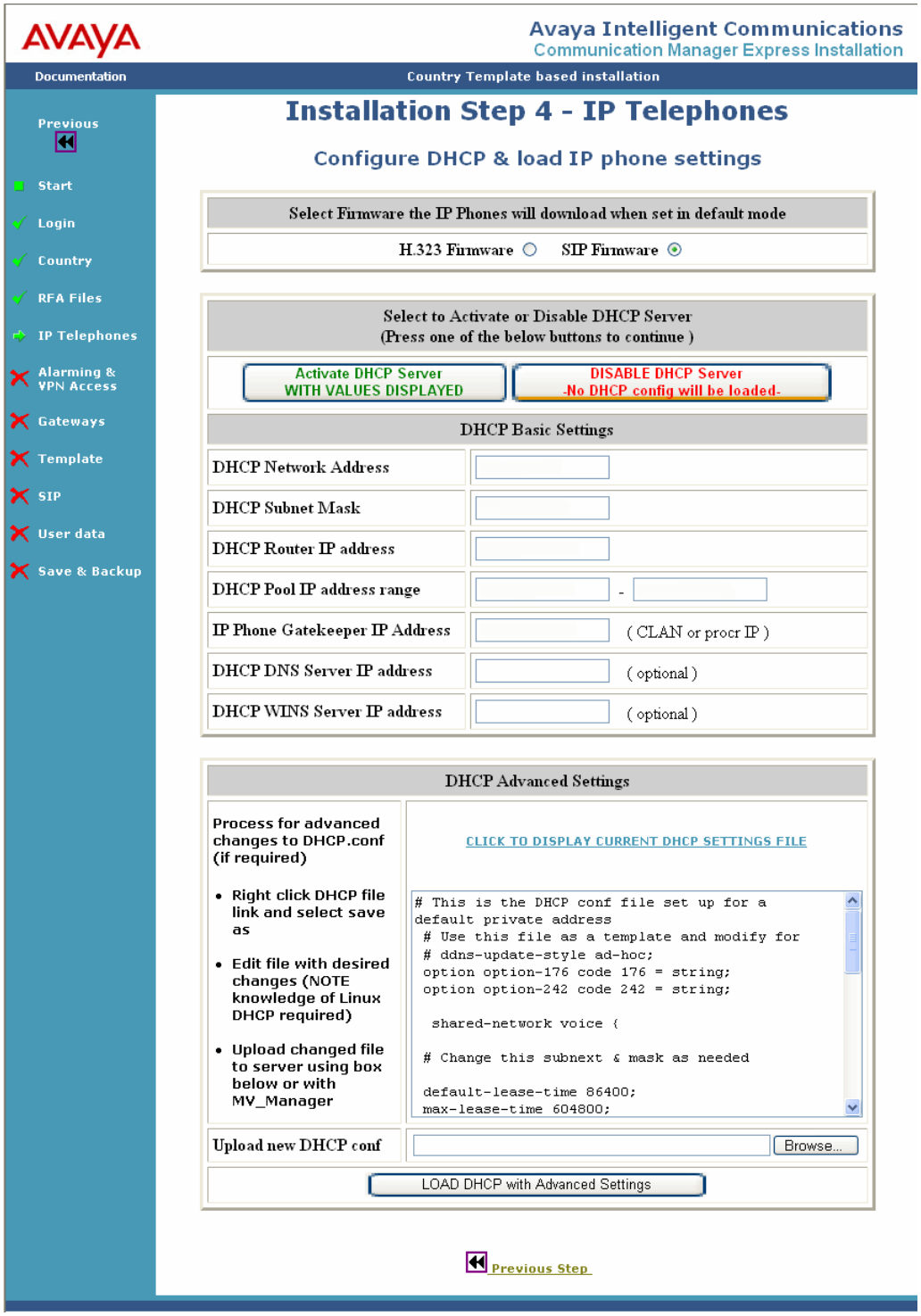


7. Click **Next Step**.

Step 4. Setting up the IP telephone settings and DHCP

In this step, you modify and install the configuration files that support IP telephones and DHCP.

Figure 12: IP Phone firmware and DHCP settings page



To install the IP telephones on CME, perform the following actions:

1. On the first Web page of Step 4, select the appropriate firmware.
   The system displays the H.323 firmware as selected by default. You can select the SIP firmware, if required. The selected firmware is loaded on the CME file server as either SIP phones or H.323 phones.
   You can also have both H.323 and SIP stations on the same customer network.To do so, set the SIG value on the IP phone and restart the phone. This action converts the phone to have both H.323 and SIP stations.
   For example, if a customer has 90 H.323 and 10 SIP stations, you would select H.323 phones on this screen and then set SIG value of the 10 SIP phones to SIP and reboot them.
2. On the next screen, change the DHCP basic settings, if required.
   The system displays the values based on the IP address of the server. You must check if the values displayed are correct.
   The DHCP settings can be changed after the installation by using the MV_Manager administration pages.
3. Click **Activate DHCP Server WITH VALUES DISPLAYED**.

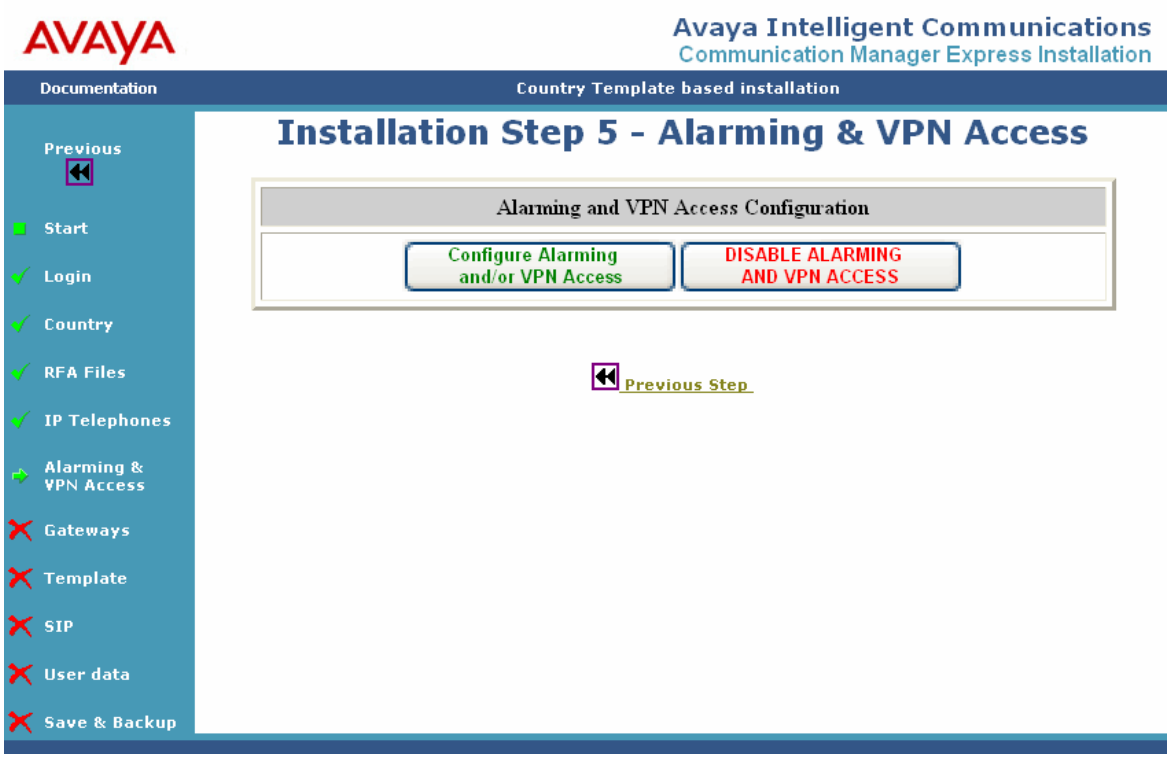
   Important:
   To modify the DHCP advanced settings, download the sample dhcpd.conf file from the DHCP Advanced Settings section. Edit the settings as required and then upload the file to the system.
   Knowledge of Linux dhcpd configuration is required to use the advanced DHCP settings option.
4. Click **Confirm**. The DHCP script results are automatically loaded.

Note:
You must disable DHCP if the customer already has a DHCP server on the network. Running two DHCP servers simultaneously on the same network can lead to IP-address related problems.

5. Click **Next Step**.

Step 5. Activating alarming and VPN access

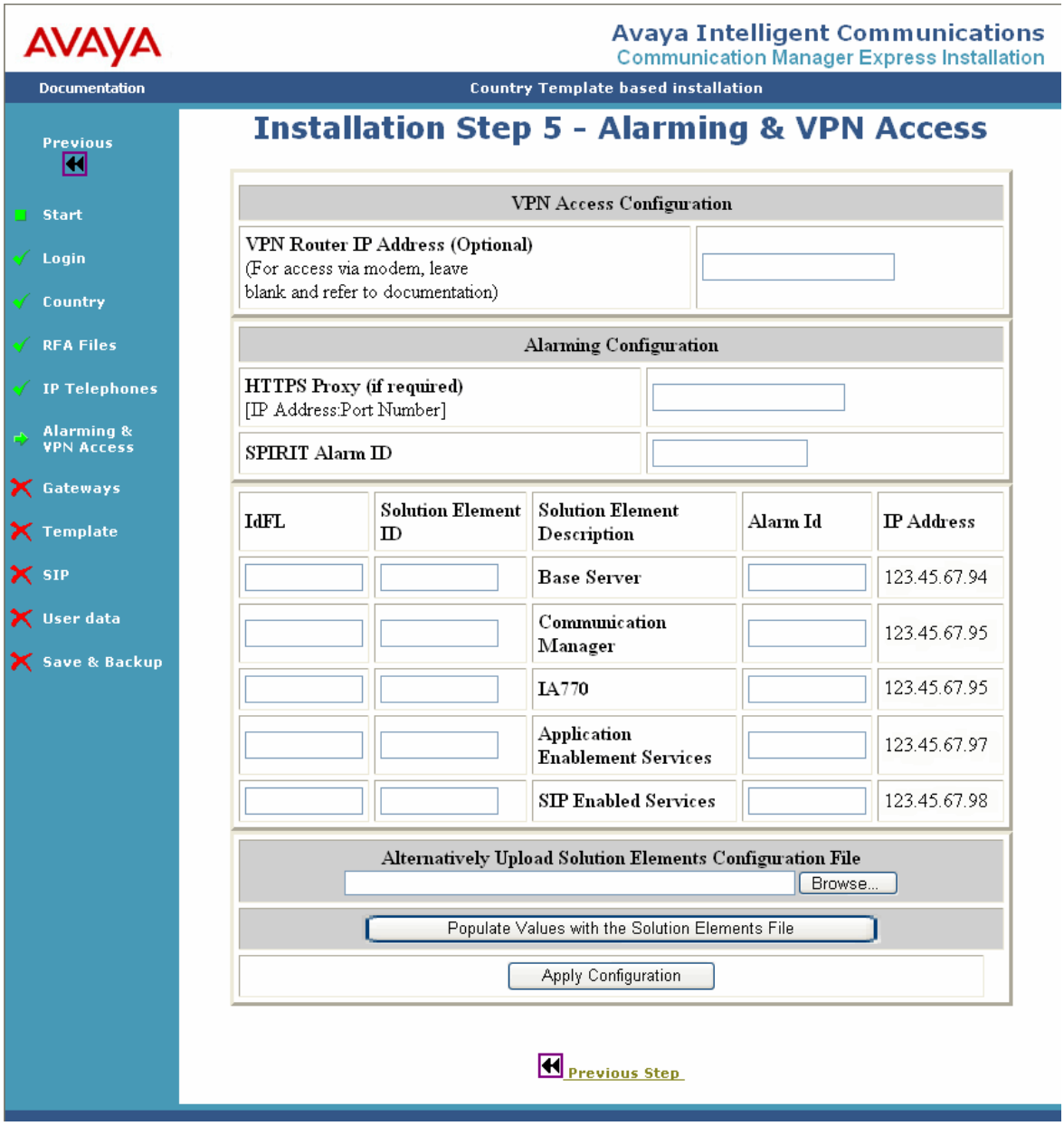
Figure 13: Alarming and VPN Access



1. To activate the alarming concentrator and VPN or either one of them, click **Configure Alarming and/or VPN Access**. The system displays the page to configure VPN access and alarming.

   Important:
   Even if you do not need VPN access, you must click **Configure Alarming and/or VPN Access** to enable alarming. If you click **DISABLE ALARMING AND VPN ACCESS**, alarming is not enabled.

Figure 14: Alarming and VPN configuration



2. If you have a VPN router, enter the IP address of the VPN router in the **VPN Router IP Address (optional)** box.
3. In the **HTTPS Proxy (if required) [IP Address:Port Number]** box, enter the IP address of the proxy server if the customer is using a proxy server to access the internet.
   For example, 123.45.67.89:8000

4. If you have a Solution Elements configuration file, you can use it to populate the remaining values. Otherwise, proceed to step 5. To populate the values by using the Solution Elements configuration file, perform the following actions:
   a. Click **Browse** and locate the Solution Elements configuration file.
   b. Click **Populate Values with the Solutions Element File**. The values are automatically populated in the alarming configuration fields.
   Modify the values, if required.
   c. Proceed to step 9.

Note:
The Solution Elements configuration file is provided by Avaya to the installing technician along with the RFA license and authentication files.

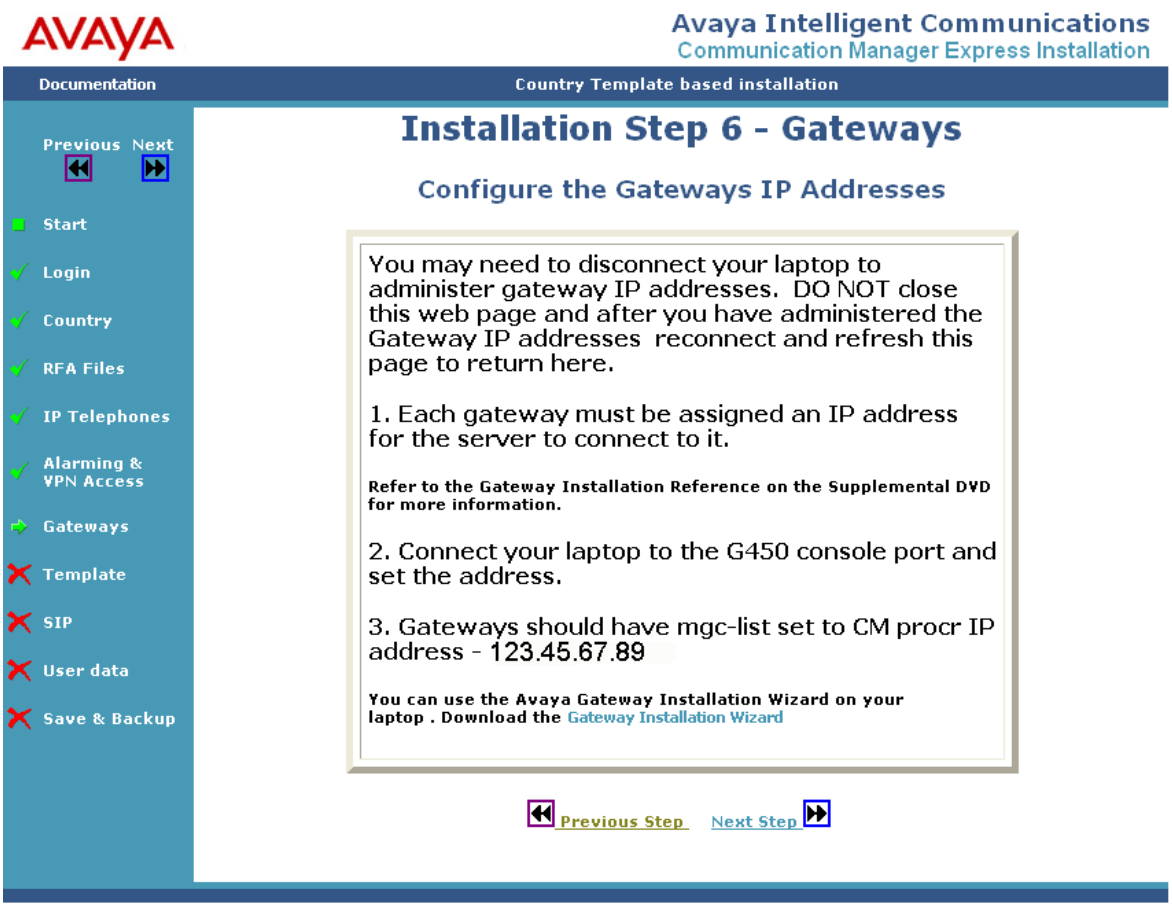
5. In the **SPIRIT Alarm ID** box, enter the SPIRIT Alarm ID.
6. In the **IdFL** boxes, enter the values listed in the following table:

Solution Element Description	Value
Base Server	base1
Communication Manager	cm1
IA770	ia770
Application Enablement Services	aes1
SIP Enabled Services	ses1

7. Enter the solution element ID of the base server, CM, IA770, AES, and SES in the appropriate boxes.
8. Enter the alarm ID of the base server, CM, IA770, AES, and SES in the appropriate boxes.
9. Click **Apply Configuration**.

Step 6. Installing the gateways

Figure 15: Step 6



To install the gateways, you must connect your laptop to the H.248 gateways and follow the instructions on the Configure the Gateways IP Addresses page.

Important:
Do not close the Web page when you disconnect the laptop from CME. After you configure the gateways, reconnect the laptop to CME and refresh the Web page. If the Web page closes, restart the installation wizard by using the customer login used at the RFA step.

For more information, see Appendix D: Installing and configuring G450 gateway—an overview on page 85.

Click **Next Step**.

Important:
If you want to use the gateway installation wizard, click **Gateway Installation Wizard**. You can either save the file at a location or directly run it. Follow the instructions on the wizard to install the G450 gateway.

Step 7. Selecting a template

For the template configuration, you must select the dial plan length and the type of gateways to install.

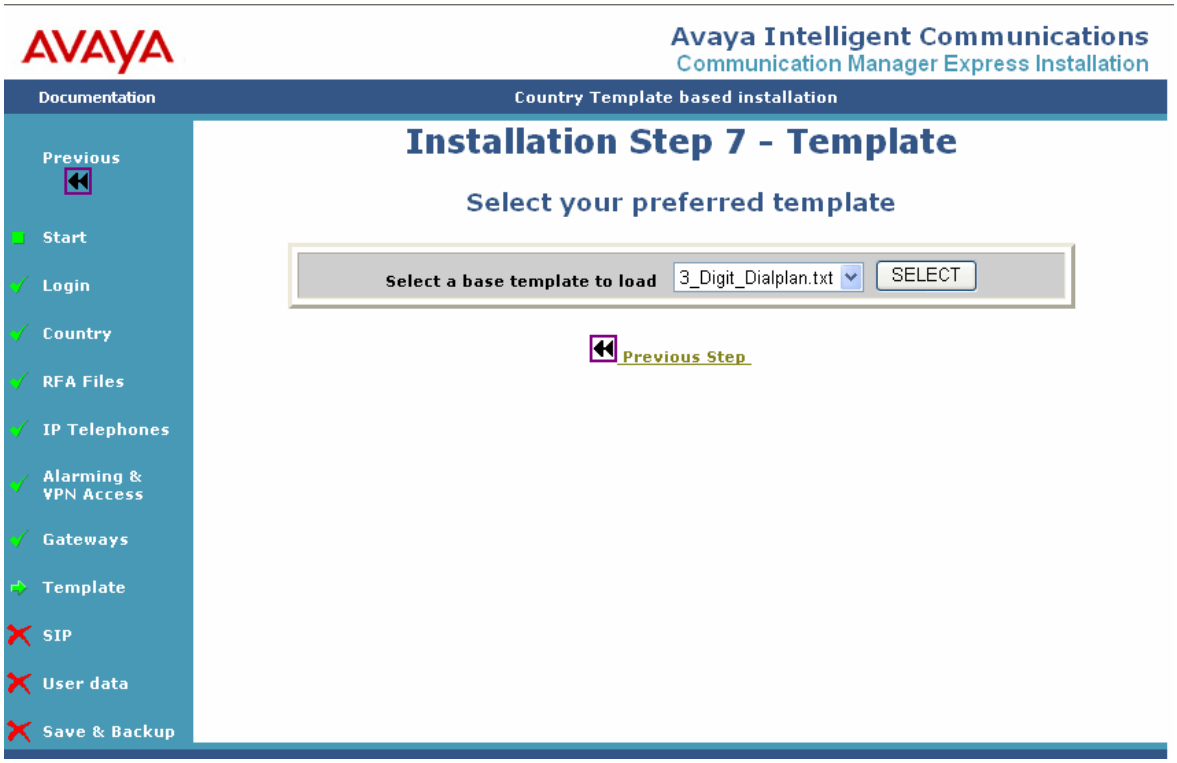
Note that:

- CME supports 3, 4, and 5 digit dial plan templates.
- For the H.248 gateways, the number of gateways that you select is added to the configuration.
- You must enter the serial numbers of the gateways. If incorrect serial numbers are entered at this stage, the gateways are unable to register with CM until you add the serial numbers through the SAT.

To select the template, perform the following actions:

1. On the first screen of step 7, select the appropriate base template in **Select a base template to load**. Click **SELECT**. (Figure 16.)

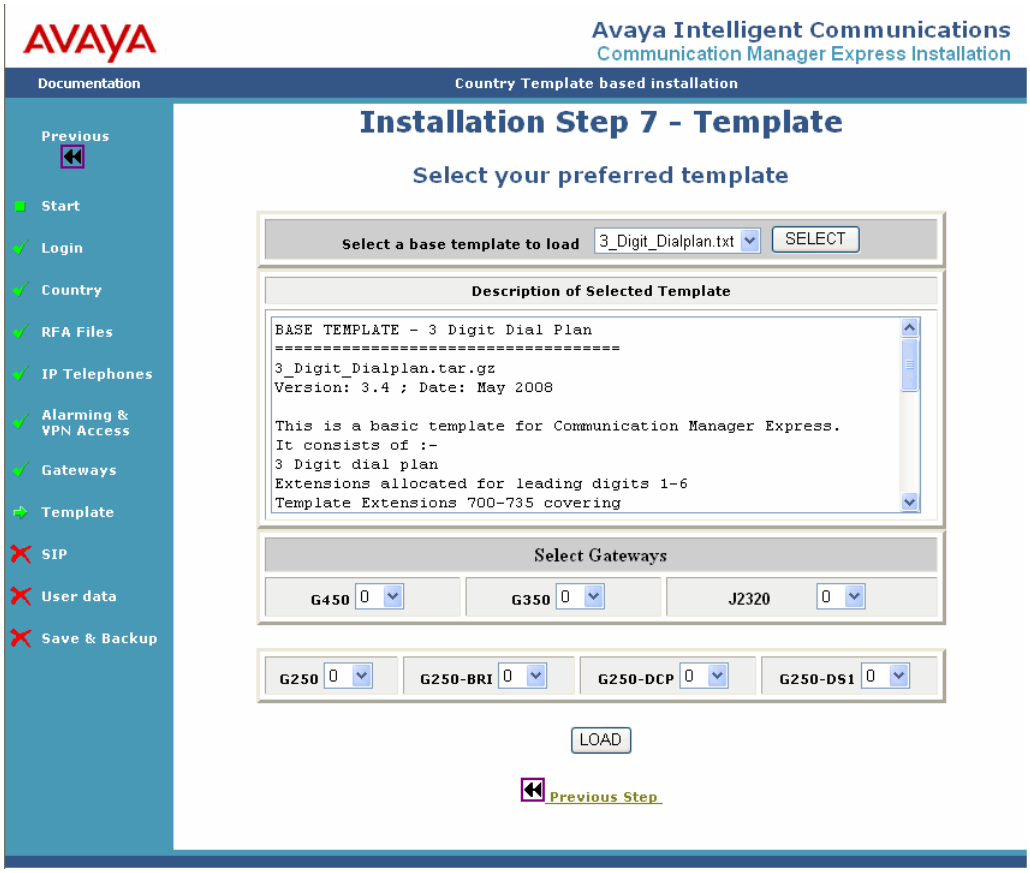
Figure 16: Select configuration template



2. On the second Web page of step 7, the system displays a description of the core configuration parameters in the Description of Selected Template box, as shown in Figure 17: Configuring from a template, screen 2 of 4 on page 39).
   Based on the country selected for the configuration, the second section of the template sets several other parameters. For details about these defaults, see *Administering and Maintaining Communication Manager Express*.

   At the bottom of the screen, select the number of each type of gateway that is connected to the CME server.

Figure 17: Configuring from a template, screen 2 of 4



3. Click **LOAD**.

   The system displays the data selected for loading the server and the serial numbers of the selected gateways.

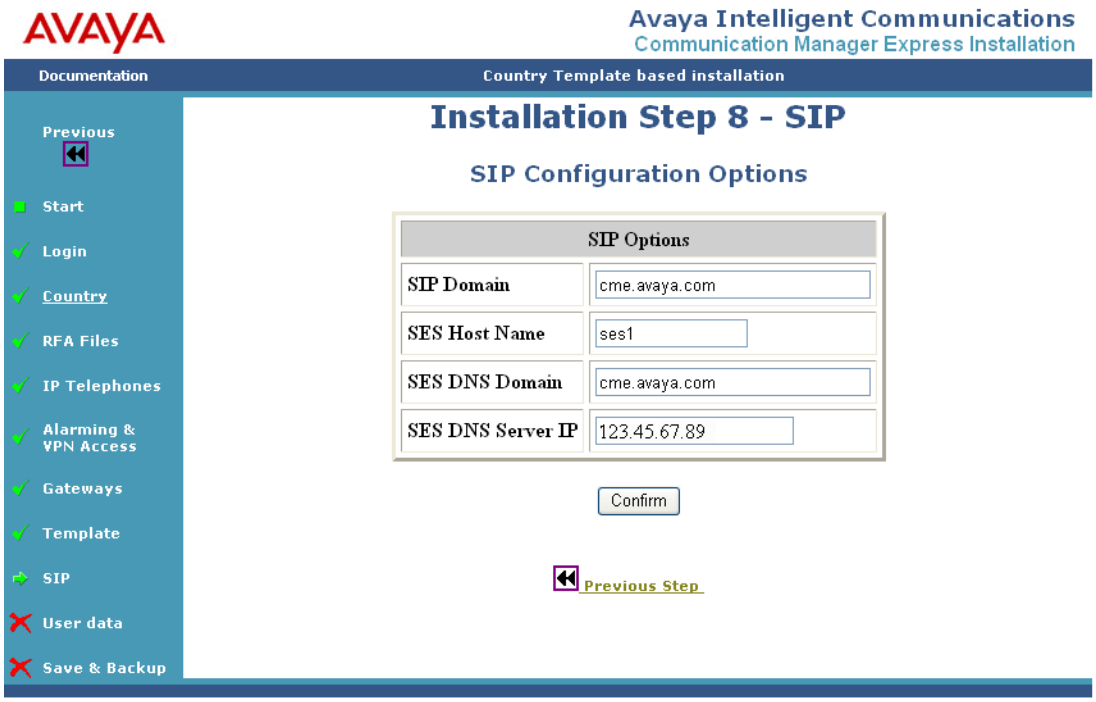
4. Click **Confirm**. The system loads the template, unicode, and localisation files and displays the script results.

   Tip:
   If you want to restart the step, click **Cancel**.

5. Click **Next Step**.

Step 8. Configuring SIP

In this step, SIP is configured on the CME system. The SIP Configuration Options page automatically displays the default SIP configuration values. If the customer wants the CME system to communicate with other SIP systems, you must change the SIP configuration values to the SIP details of the customer. Otherwise, retain the default values.
You can also change the SIP configuration values after the installation process by using the CM SAT and the SES Web pages. However, this process might require you add all the SES SIP users to the system again.



To configure SIP,

1. Click **Confirm**. The system displays the SIP options to be installed.
2. Click **Confirm**. The system loads the SIP configuration and displays the script results.

Tip:
If you want to restart the step, click **Cancel**.

3. Click **Next Step**.

Step 9. (Optional) Loading the user data

You can load the user data from an ABIT.txt file. The ABIT.txt file contains the voice mail users and extensions(Figure 18: Loading the ABIT file on page 41).

Alternatively, you can use Avaya Site Administration (ASA) to install the user data after the CME Installation wizard completes.

Figure 18: Loading the ABIT file



1. To load an ABIT file, click **Browse**. Locate the ABIT file and click **Open**.

   The user data must be in the Avaya 'ABIT' format as generated by the Avaya Bulk Import Tool. This tool is a Microsoft Excel spreadsheet. To download the Avaya Bulk Import Tool, click **ABIT** on the Load user data (optional) screen. You must then complete the spreadsheet with the basic user details.
   To make sure that the data for all the users is imported, verify the following on the ABIT spreadsheet:

- The telephone types are valid.
- The port type for the IP telephones is **IP**.
- The port type for the DCP or analog telephones is **x**. If the exact G450 hardware ports are not installed and configured in your template, use the TTI installation.

- The voice mail extension range covers the full range that is expected for all the future uses, including automated attendant.
- The SIP stations must be entered with a station and port value of 'SIP'.

The stations are added to the system with the following defaults:

- CM and SES default user passwords—123456
- IA770 subscriber password—2580

Note:
The users can change these passwords after the installation by using either MyPhone (for CM and SES) or AUDIX TUI (for AUDIX passwords).

2. Select one of the following options:
   - **Duplicate existing stations (recommended choice)**
     If you want the CME template stations to create new stations. The stations are automatically configured with a coverage path to the IA770. By default, this option is selected.
   - **or load using Defaults**
     If you want to create the stations through the CM 'add station' command and include minimum station configuration. A coverage path to AUDIX is not configured.
     For example, if an external voice mail already exists or you want to use ASA to alter the stations after the installation is complete, you would select this option.
3. From the **Select a Voice Mail language to load** list, select the language to be used. By default, the system offers an announcement set appropriate to the country selected in step 2.

Note:
You must insert the supplemental DVD to populate the list of voice mail languages. Otherwise, US English voice mail is loaded.

4. Click **LOAD**. The system displays the data selected.
5. Verify that the correct files have been selected on the User data loaded & ready to execute screen and click **Confirm**.
6. The Script Results screen shows `OK SUCCESS – STEP COMPLETE` after the user data is loaded.
7. Click **Next Step**. The system takes you to the final step.

Step 10. Save and Back up

This step loads AES, saves translations, and activates security. You have the option to copy the documentation suite from the supplemental DVD. To complete this step, click **Continue** on the first Web page of the Final Step.

1. Click **Continue**.

2. Select the appropriate option to copy documentation suite.

   Note:
   Copying the documentation suite takes approximately 20 minutes and can be performed by using the Application server Web pages after the wizard completes.

3. Click **Confirm**. The Configuring AES, Saving Translations & Activating Security script results are loaded.
   At this stage, the wizard is complete. Avaya recommends to perform a system back up at this point to restore the server for future use.
4. Click **Backup**. The system displays the Proceeding to Base server to perform a system Backup page.
5. Click **Proceed to Backup on Baseserver**. The system displays the base server home page.
6. Log on to CME base server.
7. On the left navigation menu in the Data Backup/Restore section, click **Backup Now**. The system displays the Backup Now Web page.

You can save and backup the data by selecting one of the following methods:

Important:
Avaya recommends to create the backups on off-server locations like flash card or network backup server. Backups to the local hard drive may be lost in the event of a hardware failure.
Complete system backups are performed from the base server. Typically, the system backup size is 80 MB. However, on very busy systems, the size can go up to 500 MB. You must note this specification to make sure that enough free space is available to create backups on flash cards or network servers.

- Network Device method
  To store the backup data on a network device, perform the following actions:
  a. Select **Network Device**.
  b. From the **Method** drop-down, select the appropriate data transfer method.
  c. In the **User Name** box, enter the user name of the account on the backup server.
  d. In the **Password** box, enter the password of the account on the backup server.
  e. In the **Host Name** box, enter the host name or IP address of the backup server.
  f. In the **Directory** box, enter the path where you want to store the backup data.
  g. Click **Start Backup**.
- Local Directory method
  To store the backup data on a local directory, perform the following actions:
  a. Select **Local Directory**.
  b. In the **Local Directory** box, enter the path where you want to store the backup data.

c. Click **Start Backup**.

- Local Compact Flash Card method
  To store the backup data on a flash memory device, perform the following actions:

  a. Select **Local CompactFlash Card**.

  b. If you want to format your flash memory device, select **Format CompactFlash**.

  c. In the **Retain data sets at destination** box, enter the number of data sets (backup) to be stored.
  Choose the number of data sets to be stored depending on the capacity of your flash device. Typically, a data set is more than 60 MB. If the flash device has stored the maximum number of data sets, backing up a new data set replaces the oldest data set.

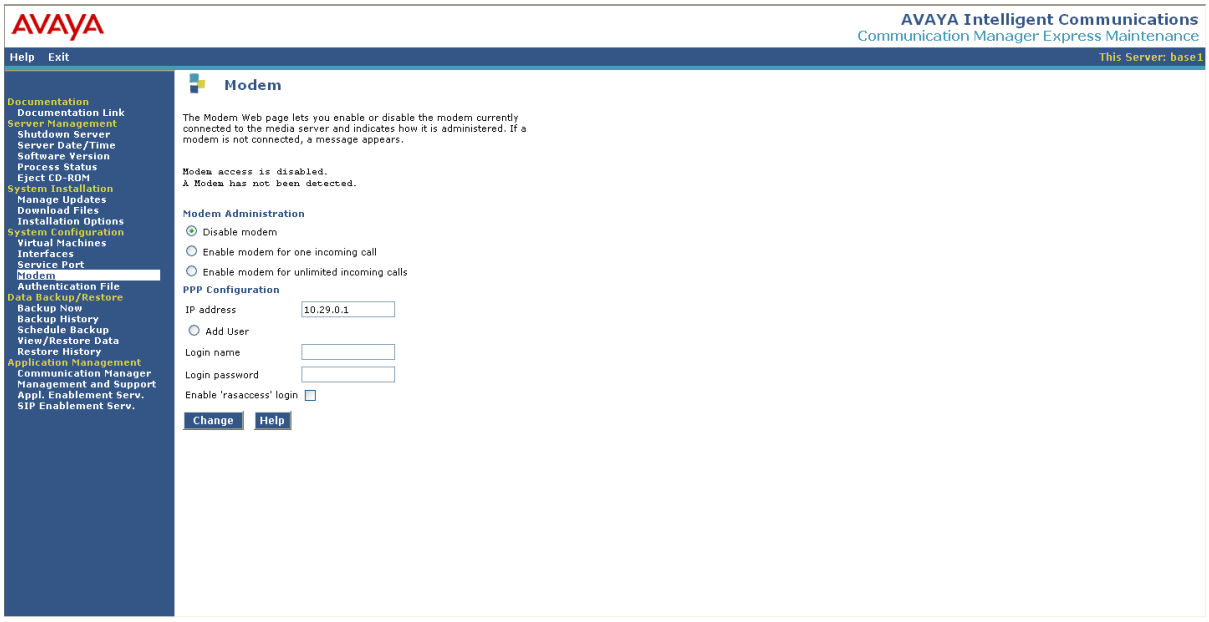
  d. Click **Start Backup**.

Step 11. Post-installation configuration

Activating modem

If you want the CME system to have modem access, you must configure it now. To configure modem access, perform the following actions on to the base server maintenance Web pages:

Figure 19: Activating modem



1. On the left navigation menu, in the System Configuration section, click **Modem**. The system displays the Modem page.

2. On the Modem Administration section, select the required option.
   If you want to administer modem for one incoming call, select **Enable modem for one incoming call**.
   If you want to administer modem for unlimited incoming calls, select **Enable modem for unlimited incoming calls**.

   Note:
   The system displays **Disable modem** as selected by default.

3. On the PPP Configuration section, in the **IP address** box, enter the IP address that the server would use for a modem PPP session.
4. If you want to add an additional remote user to the system, select **Add User**.
   This user can start a PPP session to the server through the modem. Business partners and customers who want to use their own remote users can enter them here.
5. Enter the login name of the new remote access user in **Login name**.
6. Enter the login password for the new remote access user in **Login password**.
7. To enable Avaya Services to access the system remotely, select **Enable 'rasaccess' login**.

The wizard is now complete and you can perform the post-installation configuration tasks, such as additional station changes and extra trunk administration.

CM is configured through ASA (You can download ASA from the application server)

SES is configured through the SES Web pages.

If you have copied the documentation suite during the installation process, the entire documentation is available on the application Web pages.

Modifying the SPIRIT parameters

You can modify the SPIRIT parameters after the installation process is complete. The following are the requirements to modify the SPIRIT parameters:

a. SPIRIT configuration file in ART syntax
b. Proxy IP and port (optional)
c. VPN gateway IP (optional)
d. SPIRIT alarm ID

To modify the SPIRIT parameters, log on to the base server as any user and enter the following command:

`spirit_setup configfile <VPN_ROUTER> <PROXY_IP> <SPIRIT_ALARM_ID>`

Note:
If the VPN router or Proxy IP is not available, you must use "" (empty string) as the value.

Chapter 5: Upgrading MVE R2.x to CME 5.1

CAUTION:
If you are upgrading from MVE R1.*x* to CME 5.1, you must follow the backup and restore procedure outlined in Appendix C: Upgrading MVE R1.x to CME 5.1 on page 75.

To upgrade MVE R2 to CME 5.1, perform the following actions:

8. Perform a complete system backup from the Base server Web pages. To do so, perform the following actions:
   a. On the left navigation menu in the Data Backup/Restore section, click **Backup Now**. The system displays the Backup Now Web page.
   b. Save and backup the data by selecting Network Device method.
      To store the backup data on a network device:
      1. Select **Network Device**.
      2. From the **Method** drop-down, select the appropriate data transfer method.
      3. In the **User Name** box, enter the user name of the account on the backup server.
      4. In the **Password** box, enter the password of the account on the backup server.
      5. In the **Host Name** box, enter the host name or IP address of the backup server.
      6. In the **Directory** box, enter the path where you want to store the backup data.
      7. Click **Start Backup**.
9. After you save the backup file, copy the backup file from the backup server to your laptop computer. You will upload this file to the new CME server through the installation wizard Web pages.

Note:
The file preview.txt within the backup zipped file contains the IP addresses of the R2 system which must be reused on the CME 5.1 system.

10. Login to the Base server by using the following command:

```
cat etc/opt/mve/network.conf
```

Record the IP addresses displayed in the /etc/opt/mve/network.conf file in the following table:

Table 1: IP Address Table

IP Address	Used for
	Base Sever
	VM1
	VM2
	VM3
	AUDIX
	Default Gateway (GWIP)
	Subnet Mask

You must enter the IP addresses during the DVD installation. The IP addresses must be the same as the IP addresses for the previous release. However, you need an extra IP address for the SES server.

Note:

The base server backup file contains a file called 'preview.txt'. This file contains the IP addresses used on the system. You can use the preview.txt file to record the system IP addresses.

After you back up the system data, you are ready to upgrade MVE R2.*x* to CME 5.1. The upgrade procedure installs the new main server software from the DVD.

Installing the software from the DVD

After you complete the backup of the MVE system and note the IP addresses of the current MVE system, follow the instructions mentioned in chapter 3, Installing the Communication Manager Express software (Installing the software from the DVD on page 17). After completing the instructions in the Installing the software from the DVD section, proceed to the following section.

Completing the configuration steps

Perform the following steps in sequence to complete the software configuration. On the left navigation menu, you can see the status of progress through the steps. You can restart an individual step if needed. Although you can go back to any previous step, you must continue from that step forward in strict sequence only.

To complete the software configuration, see Selecting the configuration type on page 23. Select **Upgrade from MVE R2.0**. This starts the upgrade wizard.

Alternatively, you can select **Communication Manager Express Upgrade from MVE R2.0 to CME** in the SELECT AN INSTALLATION OPTION section of the Communication Manager Express Installation Options page.

Step 1. Login to the wizard

To log on to the wizard, use **craft** as the user name and **craft01** as the password.

Step 2. Selecting a country

For more information, see Step 2. Selecting a country on page 28. As this is an upgrade, many of the country specific settings are already in the translation backup files and are not changed by the wizard.

Step 3. Installing the RFA files and customer login

After you select the country setting, you must load the RFA license file and the RFA authentication file from your laptop computer to the server. You can also create a super-user customer login to access Communication Manager at this time. See Figure 20: Load license and password files and create customer login on page 50.

Note:
The Communication Manager Express license file is used for Communication Manager and INTUITY AUDIX 770 (IA770). CME requires no other RFA license files.

To create a customer login for Communication Manager, perform the following actions:

1. In the **New Username** box, enter the new user name.

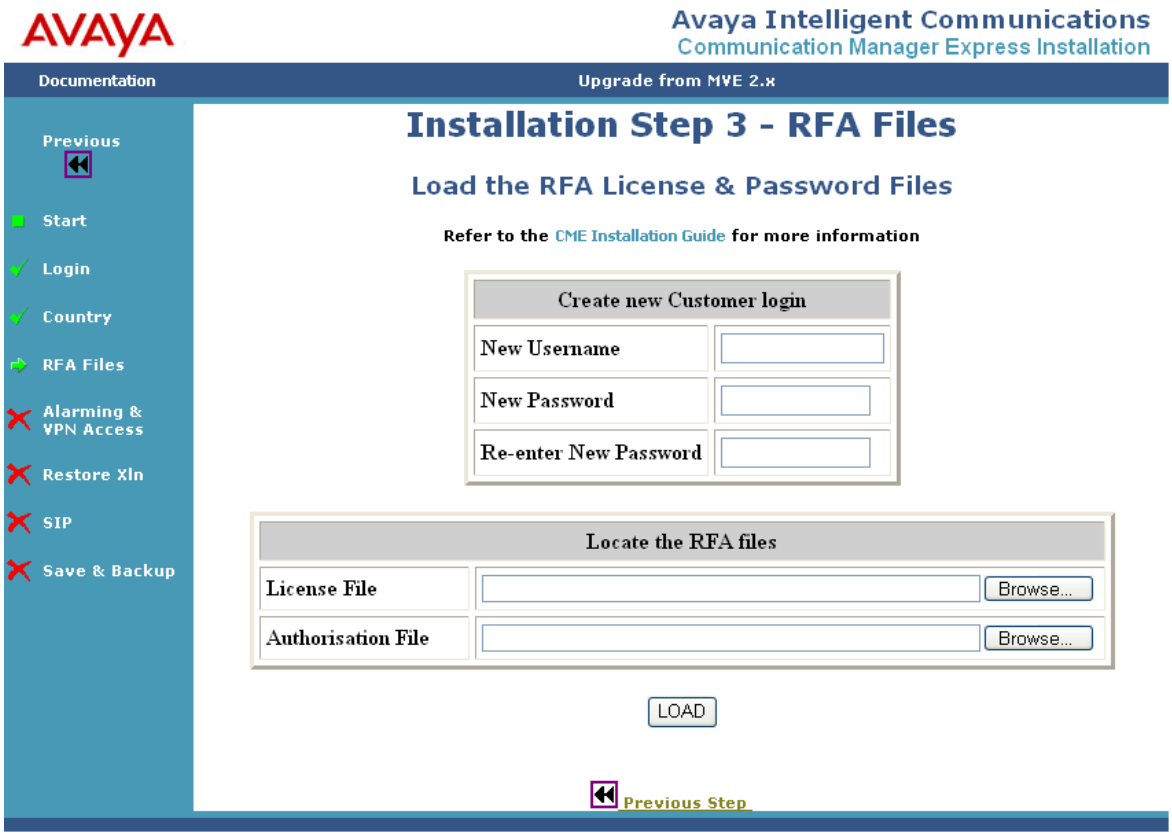
2. In the **New Password** box, enter the new password.

   The username and password must conform to the normal requirements for Communication Manager logins.

3. In the **Re-enter New Password** box, re-enter the new password.

Important:
Make sure you record the new username and password that you entered. You cannot retrieve them from the system later.
If the new username and password are lost, you need to re-configure the system.

Figure 20: Load license and password files and create customer login



To load the RFA files:

1. Locate the license file by clicking **Browse** next to License File box.
   The system displays the Choose File window.
2. Locate the license file on your laptop and click **Open**.
3. Locate the authorisation file by clicking **Browse** next to Authorization File box.
   The system displays the Choose File window.
4. Locate the authorisation file on your laptop and click **Open**.

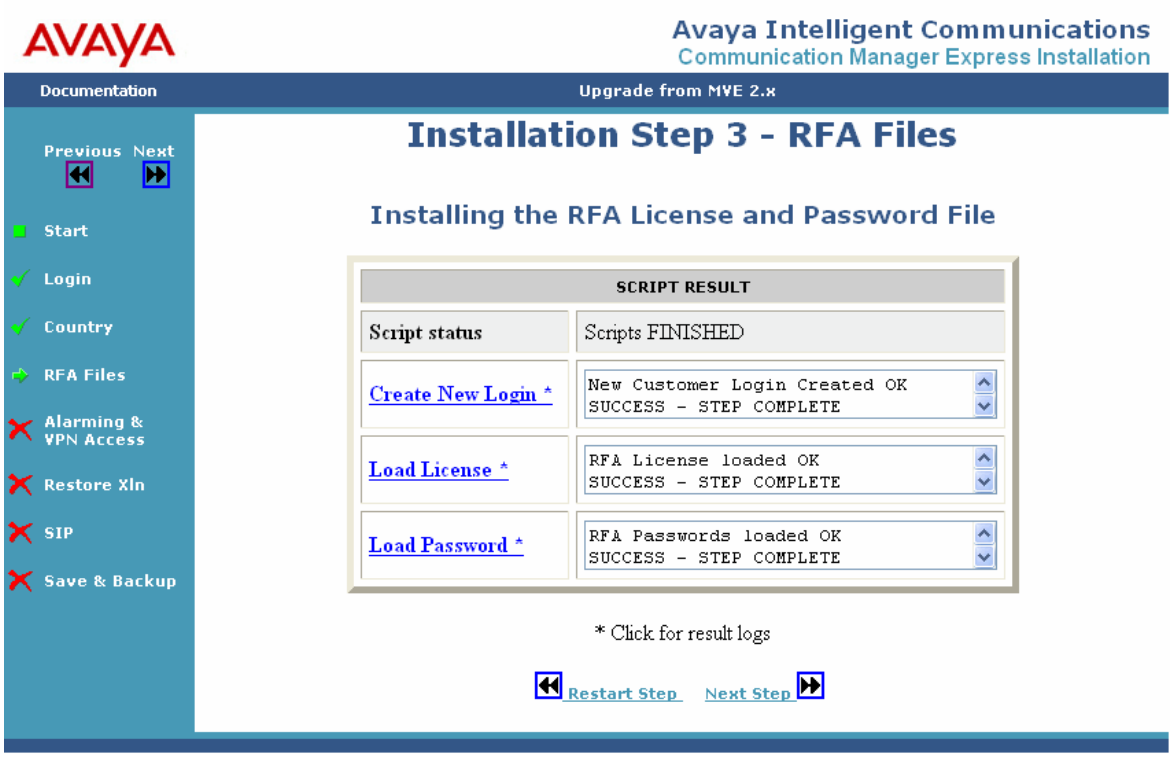
5. Click **Load**.
6. On the next screen, verify the files and click **Confirm**.

Note:
If you select an incorrect file, click **Cancel** to start the step again.

The system displays the SCRIPT RESULT screen. After the script loads the RFA files and creates the login, the SCRIPT RESULT screen shows `OK SUCCESS - STEP COMPLETE` for each item. (Figure 21: Script Result screen for RFA files and new login on page 51).

The license and authentication files load immediately. If you restart the wizard after this step, use the new customer login and password to log on to the wizard.The new login is activated when the configuration steps are complete.

Figure 21: Script Result screen for RFA files and new login



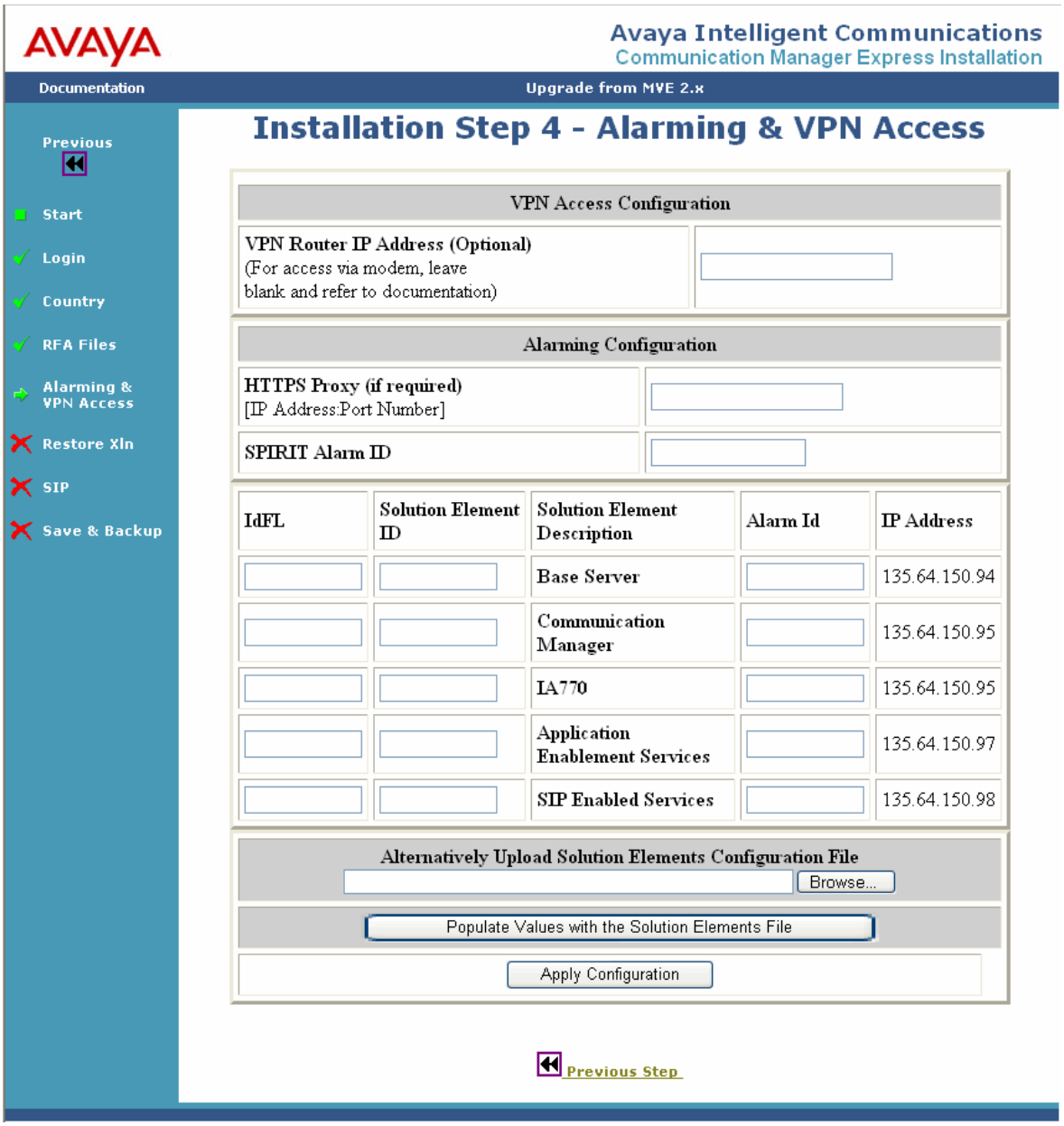
7. Click **Next Step**.

Step 4. Activating alarming and VPN access

In this step, you activate alarming and VPN access.
To activate the alarming concentrator and VPN or either one of them, click **Configure Alarming and/or VPN Access**. The system displays the screen to configure VPN access and alarming.

Important:
Even if you do not need VPN access, you must click Configure Alarming and/or VPN Access to enable alarming. If you click **DISABLE ALARMING AND VPN ACCESS**, alarming is not enabled.

Figure 22: Alarming and VPN configuration



1. If you have a VPN router, enter the IP address in the **VPN Router IP Address (optional)** box. Otherwise proceed to step 3.

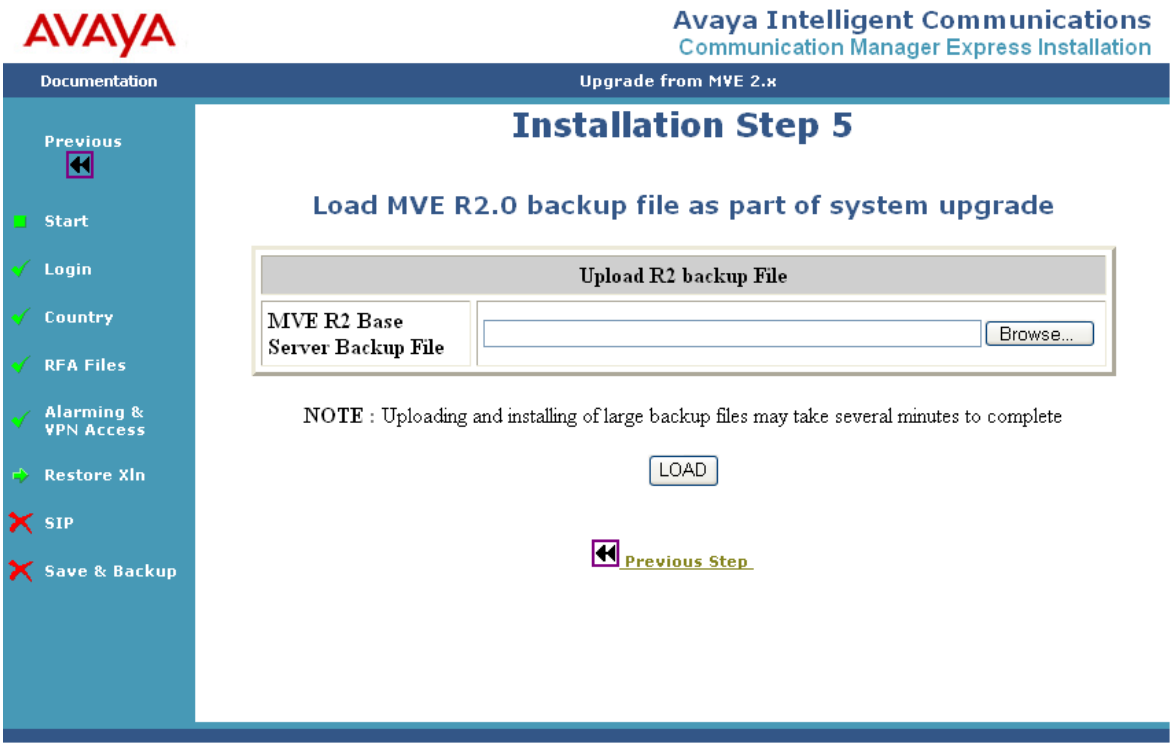
2. If the customer uses a proxy server to access the internet, enter the IP address of the proxy server in the **HTTPS Proxy (if required)** box.
3. If you have a Solution Elements configuration file, you can use it to populate the remaining values. Otherwise, proceed to step 4.
   To populate the remaining values by using the Solution Elements configuration file, perform the following actions:
   a. Click **Browse** in the Alternatively Upload Solution Elements Configuration File section and locate the Solution Elements configuration file.
   b. Click **Populate Values with the Solutions Element File**. The values are automatically populated in the alarming configuration fields.
      You can modify the values, if required.
   c. Proceed to step 8

   Note:
   The Solution Elements configuration file is provided by Avaya to the installing technician along with the RFA license and authentication files.
4. In the **SPIRIT Alarm ID** box, enter the SPIRIT Alarm ID.
   The SPIRIT ID is the product ID of the platform.
5. In the **IdFL** boxes, enter the FL ID.
6. Enter the solution element ID of the baser server, CM, IA770, AES, and SES in the appropriate boxes.
7. Enter the alarm ID of the baser server, CM, IA770, AES, and SES in the appropriate boxes.
8. Click **Apply Configuration**.
9. On the next screen, click **Confirm**. The system displays the configuration script results.
10. Click **Next Step**.

Step 5. Loading the backup file

In this step, you load the MVE R.2 backup data onto the CME system.

Figure 23: Loading the backup data



To load the backup file, perform the following actions:

1. Click **Browse** next to **MVE R2 Base Server Backup File** box to locate the backup file. The system displays the Choose File window.
2. Locate the backup file on your laptop and click **Open**.
3. Click **Load**.
4. On the next screen, verify the files and click **Confirm**. The system displays the configuration script results.

   Note:

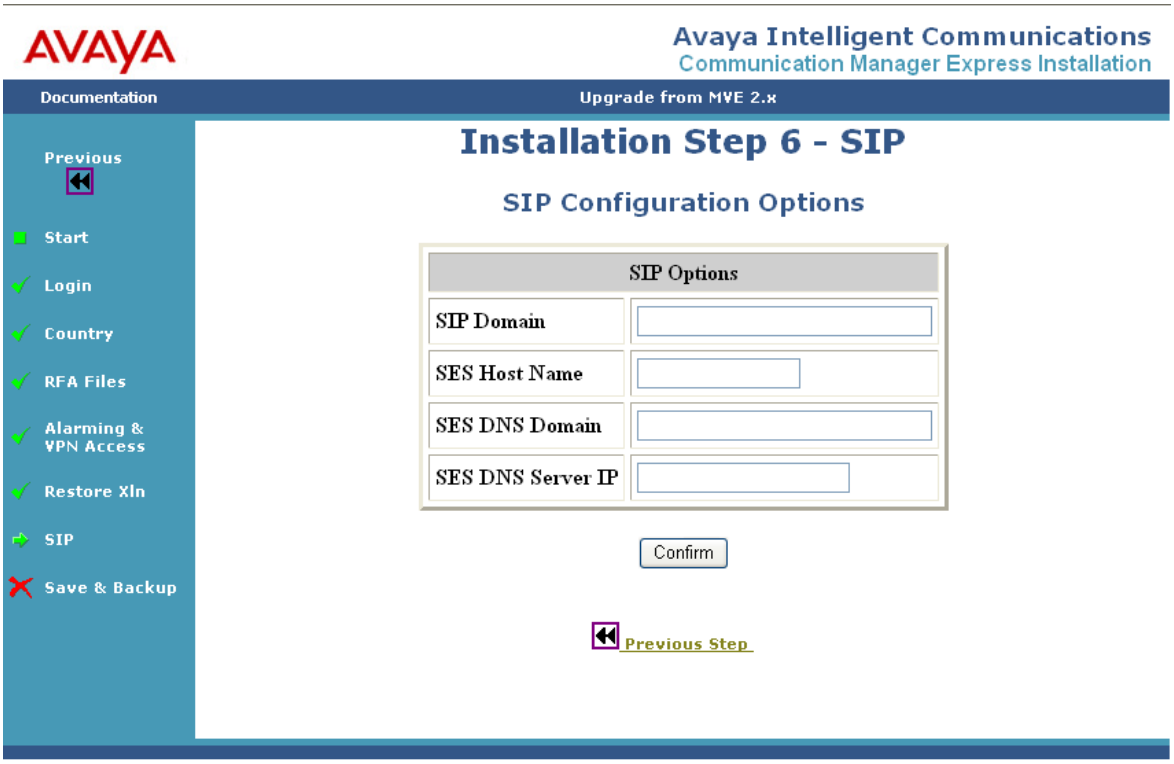
   The installation wizard attempts to add a SIP trunk (trunk and signaling group 98 with a TAC of #98) between CM and SES. If the SIP trunk is already present in the system, this step fails. You must manually add the SIP trunk after the installation wizard completes.For more information, see Appendix B: How to manually add SIP configuration to CM on page 69.

5. Click **Next Step**.

Step 6. Configuring SIP

In this step, SIP is configured on the CME system. The SIP Configuration Options screen automatically displays the default SIP configuration values. If the customer wants the CME system to communicate with other SIP systems, you must change the SIP configuration values to the SIP details of the customer. Otherwise, retain the default values.
You can also change the SIP configuration values after the installation process by using the CM SAT and the SES Web pages. However, this process might require you add all the SES SIP users to the system again.

Figure 24: SIP configuration



To configure SIP,

1. Click **Confirm**. The system displays the SIP options to be installed.
2. Click **Confirm**. The system loads the SIP configuration and displays the script results.
3. Click **Next Step**.

Step 7. (Final step) Save and back up

This step loads AES, saves translations, and activates security. You also have the option to copy the documentation suite from the supplemental DVD.

Note:
After saving the AES configuration, you can modify the basic install according to the requirements of the customer.

To complete this step, perform the following actions:

1. Click **Continue**. The system displays the next Web page.
2. Select the appropriate option to copy documentation suite.
3. Click **Confirm**. The Configuring AES, Saving Translations & Activating Security script results are loaded.



Tip:
To view the updated script results, click **Refresh**.

4. Click **Backup**. The system displays the Proceeding to Base server to perform a system Backup screen.
5. Click **Proceed to Backup on Baseserver**. The system displays the base server home page.
6. Log on to CME Base server.
7. On the left navigation menu in the Data Backup/Restore section, click **Backup Now**. The system displays the Backup Now Web page.

You can save and backup the data separate from the Avaya server by selecting one of the following methods:

- Network Device method
  To store the backup data on a network device, perform the following actions:
  a. Select **Network Device**.
  b. From the **Method** drop-down, select the appropriate data transfer method.
  c. In the **User Name** box, enter the user name of the account on the backup server.
  d. In the **Password** box, enter the password of the account on the backup server.
  e. In the **Host Name** box, enter the host name or IP address of the backup server.
  f. In the **Directory** box, enter the path where you want to store the backup data.
  g. Click **Start Backup**.
- Local Directory method
  To store the backup data on a local directory, perform the following actions:
  a. Select **Local Directory**.

b. In the **Local Directory** box, enter the path where you want to store the backup data.

c. Click **Start Backup**.

- Local CompactFlash Card method
  To store the backup data on a flash memory device, perform the following actions:

  a. Select **Local CompactFlash Card**.

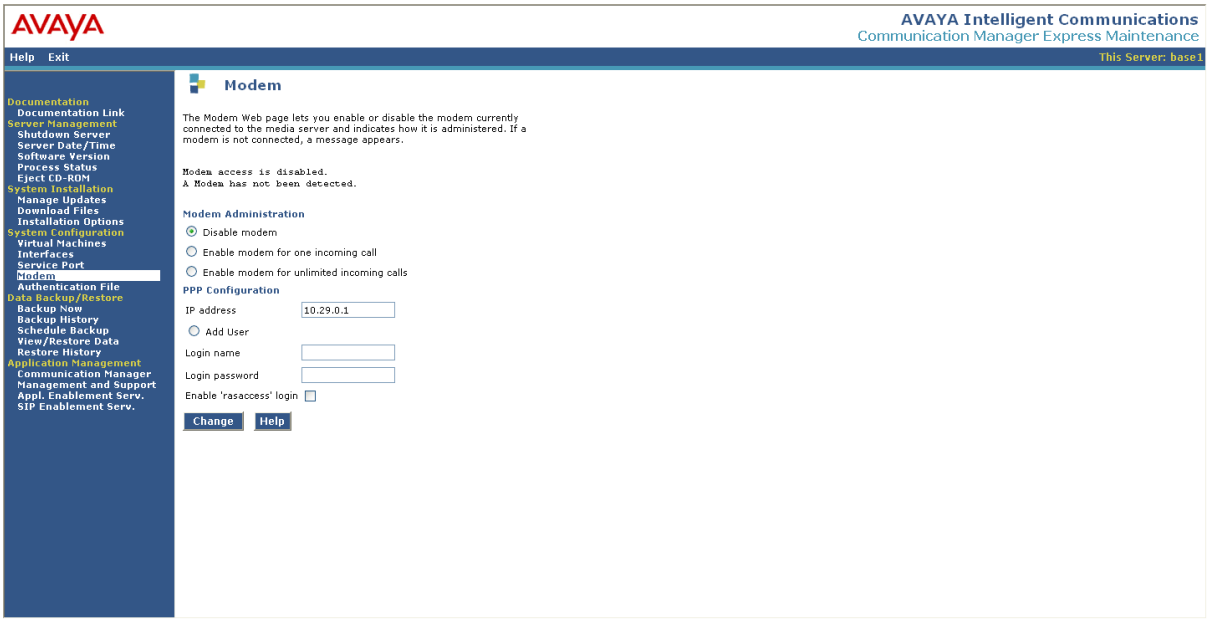
  b. If you want to format your flash memory device, select **Format CompactFlash**.

  c. In the **Retain data sets at destination** box, enter the number of data sets (backup) to be stored.
  Choose the number of data sets to be stored depending on the capacity of your flash device. Typically, a data set is more than 60 MB. If the flash device has stored the maximum number of data sets, backing up a new data set replaces the oldest data set.

  d. Click **Start Backup**.

Step 8. Post-installation configuration

If you want the CME system to have modem access, you must configure it now. To configure modem access, perform the following actions on to the base server maintenance Web pages:



1. On the left navigation menu, in the System Configuration section, click **Modem**. The system displays the Modem page.

2. In the Modem Administration section, select the required option.
   If you want to administer modem for one incoming call, select **Enable modem for one incoming call**.
   If you want to administer modem for unlimited incoming calls, select **Enable modem for unlimited incoming calls**.

   Note:
   The system displays **Disable modem** as selected by default.

3. On the PPP Configuration section, in the **IP address** box, enter the IP address that the server would use for a modem PPP session.
4. If you want to add an additional remote user to the system, select **Add User**.
   This user can start a PPP session to the server through the modem. Business partners and customers who want to use their own remote users can enter them here.
5. Enter the login name of the new remote access user in **Login name**.
6. Enter the login password for the new remote access user in **Login password**.
7. To enable Avaya Services to access the system remotely, select **Enable 'rasaccess' login**.

The wizard is now complete and you can perform the post-installation configuration tasks, such as additional station changes and extra trunk administration.

CM is configured through ASA (You can download ASA from the application server)

SES is configured through the SES Web pages.

If you have copied the documentation suite during the installation process, the entire documentation is available on the application Web pages.

Chapter 6: System logins and access

System logins

- Access to CME is provided by the Base server for the local services and remote maintenance connections.
- Password access to CME uses standards similar to Communication Manager.
- Before you install the RFA password file using the wizard, the default system password apply. After the password file is installed, most of the machines will have the Access Security Gateway (ASG) security access mechanisms for the services logins.

The following table lists the login details for the various machines:

CM	
Service login	ASG
Customer login	Added through the CM Web page
First customer login	Added by wizard
SES	
Service login	ASG
Customer login	Added through the SES Web page
First customer login	Added by the wizard
Base Server	
Service login	ASG
Customer login	Use the customer login added to CM
First customer login	Added by the wizard
Modem users	Added through the base server Web pages
AES	

Service login	Non-ASG. This password is changed by the Avaya Password Change System
Customer login	AES
First customer login	Craft
Application Server	
Service login to shell	ASG
Customer login to shell	None. All the administration tasks are performed through the Web interface
Customer logins to the Web application	CM logins are used. Any non-ASG login on CM can be used. Logins added to CM through the CM Web pages also allow access to the application server pages.
Service login to the Web application	None. The non-ASG login must be added to CM through the service login.

Note:
The craft login directly on the services port requires a password. An ASG response is not required.

Modem and Services port (eth1) access to machines

Port redirection

The CME hardware has one physical services port and five virtual machines. You can access the virtual machines through the services port. The services port provides access to the virtual machines through port redirection together with a port switching method for ports 22 and 443 (shell and https).

The following table lists the port numbers of the machines that you can access through the services port or modem:

Machine name	Web access URL	Shell access port
Base server (Dom 0)	Use port switching to access through 443	11022
CM (VM1)	Use port switching to access via 443	5022 (Direct SAT)11122 (Shell)
Application server (VM2)	https://192.11.13.6:12443	12022
AES (VM3)	Use port switching to access via 443	13022
SES (VM4)	Use port switching to access via 443	14022

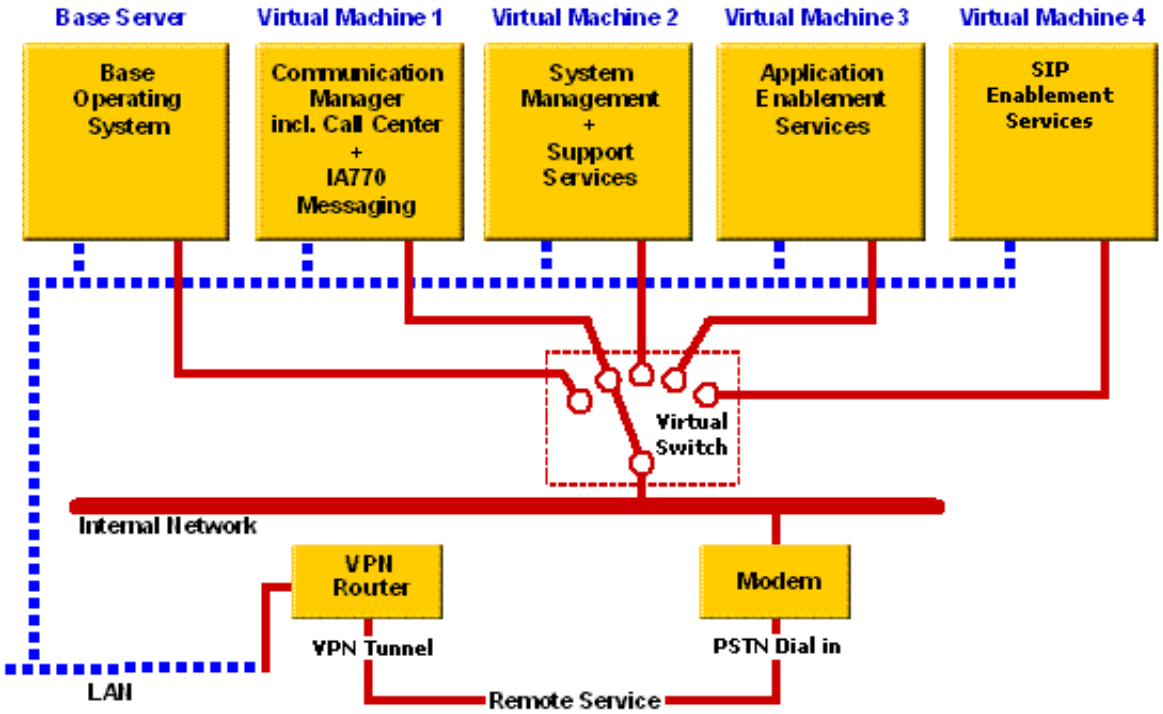
Port switching

Some Web pages of the virtual machines do not work with the port redirection method. In such a situation, the system allows you to switch the ports 443 or 22 between machines through a virtual port switch from the base server.

It is recommended that you use the port switching method to access the base server, CM, AES and SES Web pages when accessing through the services port or the modem.

The system has a method to allow port 443 or port 22 to be moved between machines through a virtual port switch from the base server.

Figure 25: The Xen network environment—port switching



This is controlled from the base server either from the shell using the following commands or through the base server Web pages.
Services port refers to both the modem PPP link and eth1 on the server.

You can use the following shell commands to switch the ports listed in the table:

Shell command	Port switching
[craft@base1 ~]$setshell -?	Would display command help
[craft@base1 ~]$setshell 1	Would move 192.11.13.6:22 to point at port 22 on CM
[craft@base1 ~]$setweb 3	Would move 192.11.13.6:443 to point at port 443 on AES
[craft@base1 ~]$getshell	Would display the machine port 22 is currently set to
[craft@base1 ~]$getweb	Would display the machine port 443 is currently set to

The machine numbers are as follows:

Base server	0
CM	1
Application server	2
AES	3
SES	4

Alternatively, you can use the routing switch function from the base server Web page. To do so, on the left navigation menu, in the System Configuration section, click **Service Port**.

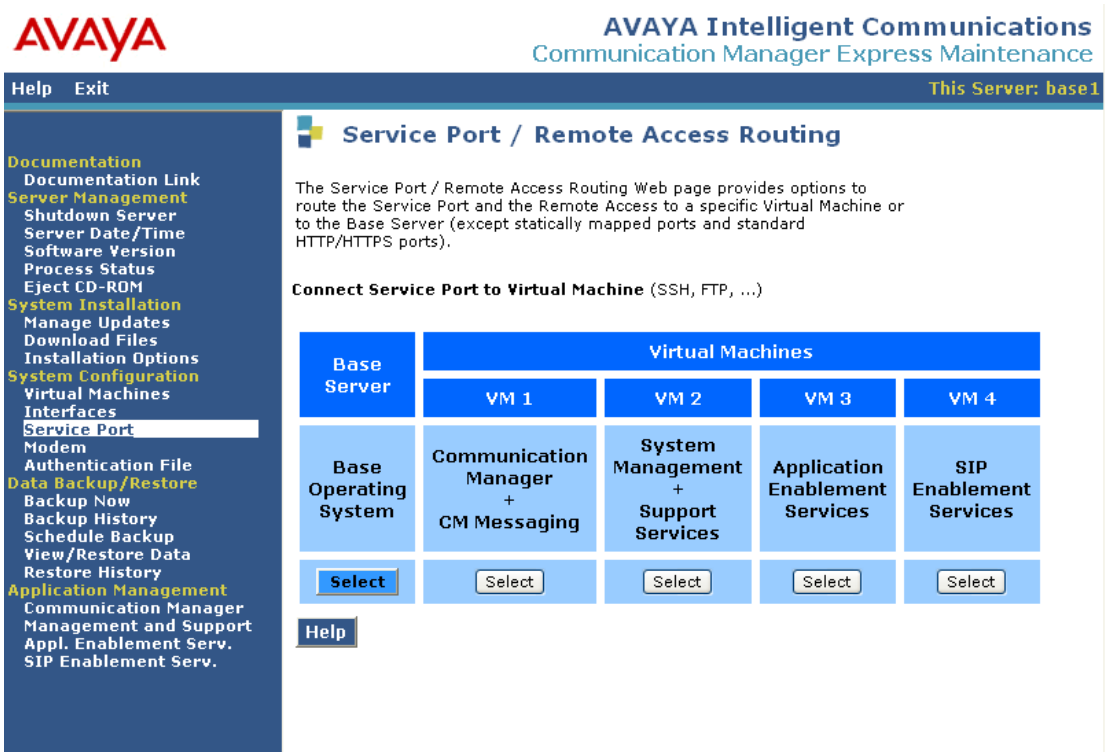
You can access the Web page switching function by using the links in the left navigation menu (Application Management section)

For example, you can click **Communication Manager** to move the Web port switch to CM and open a new window.

Note:

You must use the shell command “setweb 0” from the base server to move the base server Web pages back to port 443.

Figure 26: The Virtual Machine Services Port and Remote Access Routing



Administering through customer LAN

To access the Web pages on a virtual machine through the customer LAN, use the following URL format:

https://<VM_IP_address>

Where <VM_IP_address> is the network IP address for the virtual machine being accessed.

To establish a secure shell session to a virtual machine, you must type the virtual machine IP address into the SSH client.

Note:

Port switching has no effect on the Customer LAN interfaces. All machines are accessed normally through the customer LAN IP addresses regardless of the setting of the virtual port switch.

Appendix A: Troubleshooting installation problems

This appendix provides instructions on how to troubleshoot the common installation problems.

Solving wizard navigation and installation step errors

You can troubleshoot the following common installation problems by proceeding with the relevant troubleshooting instructions:

- If incorrect data is entered into the installation wizard:
  You must restart the installation steps by either clicking **Cancel** or by navigating back through the wizard pages by using the left navigation menu. However, it is recommended that you restart the wizard from the first step, and thus ensure that the system is reset.
- If installation step is incomplete:
  You must examine the script log file to know the cause of the error. If the error is minor, you can continue with the installation.
  For example, a single station may not add to AUDIX correctly because of an incorrect entry in the ABIT file. In this situation, you can continue with the installation and correct the entry in the ABIT file after the installation is complete.
  However, if it is a serious error, you must restart the step or restart the wizard from the first step.
  For example, if all the stations fail to add because of a problem in the ABIT file, you must correct the ABIT file and upload to the system again and then continue with the installation.

For the wizard to continue and complete the installation process, some steps must pass successfully.
For example, the installations of the customer login addition, licence file, and authentication file installation must complete successfully for the wizard to continue to the next step. Note that the next button is not displayed if these steps do not complete successfully. So problems with the license or authentication file must be corrected before continuing with the installation. Click the name of the script to access the log file and see if there are any error messages. The log file also displays why the step has not completed successfully.

Solutions to common installation errors

The following table lists the common installation errors.

Problem	Solution
The option to proceed to the next step does not appear on the wizard.	1. If the progress indicator circle is displayed, the installation wizard is still active and configuring the system. You are able to move to the next step only when the progress indicator circle disappears. 2. If a mandatory installation step has not completed successfully, check the logs and correct the problem before re-running the step and continuing with the installation process.
After navigating back to a previous installation step in the wizard, a subsequent step does not complete correctly.	Restart the wizard from the beginning.
Not able to use maximum number of stations in the Communication Manager license file.	The installation wizard uses a number of template stations. After a successful installation, you must remove the template stations to free up resources for new stations. The template stations are 700-735 for the 3 digit template, 1900-1934 for the 4 digit template, and 19000-19034 for the 5 digit template.
Not able to use the maximum number of trunk members in the Communication Manager license file.	The default CME configuration has a SIP trunk between CM and the SES server that consists of 255 trunk members. However, you can reduce the number of trunk members in a SIP trunk. Reducing the trunk members affects the number of SIP endpoints that will use CME. Trunk Group 3 is the CM to SES SIP trunk for all installation wizard templates.
Cannot login in to the wizard	1. If the RFA authentication file is already installed on CM; you must use the login you added to the system in step 2 to log on to the wizard. 2. If there is a problem with the CM virtual machine, you must check if CM is running correctly. 3. If your login is locked due to password attempts that exceed the limits, you must wait for approximately 10 minutes for the lockout to automatically reset and then log on again.

Problem	Solution
No AUDIX announcement language displayed in the add user data step.	1. If the supplemental DVD is not in the DVD-ROM drive, you must insert the supplemental DVD into the DVD-ROM drive and refresh the page. 2. If the Supplemental DVD is in the DVD-ROM drive, remove the disk and check for damage. You can add AUDIX announcement in the normal way. To do so, after the installation is complete, download the files from http://support.avaya.com through the AUDIX administration Web pages.
AUDIX does not start automatically.	Check the system is in license normal mode and start AUDIX manually by using the maintenance Web pages. Also, check if you have installed the chosen announcement set on the system correctly.

Appendix B: How to manually add SIP configuration to CM

Changes to CM to support SIP

This section describes how to manually add SIP configuration to CM if the automatic SIP trunk addition in the upgrade wizard fails.

Locations

```
display locations                                          Page   1 of   4
                                LOCATIONS

              ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc  Name           Timezone Rule  NPA  ARS  Atd      Disp   Prefix   Proxy Sel
 No                   Offset             FAC  FAC      Parm              Rte Pat
 1:  Main           + 00:00   0                         1                  3
```

Network Region

```
display ip-network-region 1                                Page   1 of  19
                            IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain:cme.avaya.com
    Name: CM Express
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Route Pattern

```
display route-pattern 3                                        Page   1 of   3
                   Pattern Number: 3   Pattern Name: SIP Trunk
                            SCCAN? n     Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
   No          Mrk Lmt List Del  Digits                          QSIG
                            Dgts                                  Intw
1: 3    0                                                         n   user
2:                                                                n   user
3:                                                                n   user
4:                                                                n   user
5:                                                                n   user
6:                                                                n   user

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
   0 1 2 M 4 W     Request                                Dgts Format
                                                       Subaddress
1: y y y y y n  n           rest                                     none
2: y y y y y n  n           rest                                     none
3: y y y y y n  n           rest                                     none
4: y y y y y n  n           rest                                     none
5: y y y y y n  n           rest                                     none
6: y y y y y n  n           rest                                     none
```

SIP Signaling Group

```
display signaling-group 3
                              SIGNALING GROUP

 Group Number: 3              Group Type: sip
                      Transport Method: tls




  Near-end Node Name: procr                Far-end Node Name: ses1
Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                    Far-end Network Region: 1
      Far-end Domain: mve.avaya.com

                                          Bypass If IP Threshold Exceeded? n

        DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
                                                   IP Audio Hairpinning? n
        Enable Layer 3 Test? n
Session Establishment Timer(min): 3
```

SIP Trunk Group

```
display trunk-group 3                                        Page   1 of  21
                              TRUNK GROUP

Group Number: 3                    Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SES            COR: 1        TN: 1        TAC: *03
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                    Signaling Group: 3
                                                  Number of Members: 30
```

```
display trunk-group 3                                        Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name? y

                                        Redirect On OPTIM Failure: 5000

           SCCAN? n                              Digital Loss Group: 18
                     Preferred Minimum Session Refresh Interval(sec): 600
```

```
display trunk-group 3                                        Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: internal
                                                      Maintenance Tests? y



                    Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

```
display trunk-group 3                                        Page   4 of  21
                            PROTOCOL VARIATIONS

                      Mark Users as Phone? n
           Prepend '+' to Calling Number? n
     Send Transferring Party Information? n
                Network Call Redirection? n
            Telephone Event Payload Type:
```

```
display trunk-group 3                                        Page   5 of  21
                               TRUNK GROUP
                                    Administered Members (min/max):   1/30
GROUP MEMBER ASSIGNMENTS                Total Administered Members:  30

       Port             Name
 1: T00043              SIP Trunk
 2: T00044              SIP Trunk
 3: T00045              SIP Trunk
 4: T00046              SIP Trunk
 5: T00047              SIP Trunk
 6: T00048              SIP Trunk
 7: T00049              SIP Trunk
 8: T00050              SIP Trunk
 9: T00051              SIP Trunk
10: T00052              SIP Trunk
11: T00053              SIP Trunk
12: T00054              SIP Trunk
13: T00055              SIP Trunk
14: T00056              SIP Trunk
15: T00057              SIP Trunk
```

```
display trunk-group 3                                        Page   6 of  21
                               TRUNK GROUP
                                    Administered Members (min/max):   1/30
GROUP MEMBER ASSIGNMENTS                Total Administered Members:  30

       Port             Name
16: T00058              SIP Trunk
17: T00059              SIP Trunk
18: T00060              SIP Trunk
19: T00061              SIP Trunk
20: T00062              SIP Trunk
21: T00063              SIP Trunk
22: T00064              SIP Trunk
23: T00065              SIP Trunk
24: T00066              SIP Trunk
25: T00067              SIP Trunk
26: T00068              SIP Trunk
27: T00069              SIP Trunk
28: T00070              SIP Trunk
29: T00071              SIP Trunk
30: T00072              SIP Trunk
```

Node Names

```
display node-names ip
                                    IP NODE NAMES
    Name              IP Address
IA770               172.30.0.5
MV_BCMS             172.30.0.2
MV_CDR              172.30.0.2
aeserver1           172.30.0.3
default             0.0.0.0
procr               172.30.0.1
ses1                172.30.0.4*

*enter public IP address of SES
```

Off-PBX Configuration Set

```
display off-pbx-telephone configuration-set 1




                               CONFIGURATION SET: 1

           Configuration Set Description: SES Link
                     Calling Number Style: network
                      CDR for Origination: phone-number
      CDR for Calls to EC500 Destination? y
             Fast Connect on Origination? n
            Post Connect Dialing Options: dtmf
           Cellular Voice Mail Detection: none
                           Barge-in Tone? n
             Calling Number Verification? y
Call Appearance Selection for Origination: primary-first
                         Confirmed Answer? n
```

Appendix C: Upgrading MVE R1.x to CME 5.1

Backing up MultiVantage Express data for an upgrade

You must complete the backup procedure described in this chapter before upgrading the MultiVantage Express software.

To upgrade, use the existing license and authentication files. You must have a copy of each of these files on your laptop computer before starting the upgrade.

Important:
Avaya recommends that you read the Communication Manager Express release notes before you upgrade MVE to CME. The release notes describe the new platform changes that may be overwritten by performing the restore of Communication Manager and AUDIX. The release notes are available on the Avaya Support Web site (http://support.avaya.com).

Pre-upgrade tasks

You must complete the following tasks before starting the upgrade procedures.

- Disable scheduled maintenance
- Check for translation corruption (use SAT newterm)
- Save translations by performing the following actions:
  a. Start an SSH session to Communication Manager that runs the existing MVE R1.x.
  b. Log on to MVE and open a SAT session.
  c. To check for translation corruption, enter **`newterm`**.
  If corruption is reported, do not continue with the upgrade and contact your services manager.
  d. If no corruption is reported, enter **`save translation`**.
- Ensure that the original backup of AUDIX data, including the subscriber names, is available for recovery purposes, if needed.

Backing up the Communication Manager, AUDIX, and VM2 data

Important:
The following procedures provide instructions for backing up on your service laptop computer. However, a customer server that can connect to CME over the LAN is the preferred destination for the backup files. Before you start this procedure, check with the customer to see if a server is available for the backup. In most cases, the commands to back up files to a customer server are the same as the commands to back up to the laptop, with the appropriate address changes.

You must delete any customer files from your laptop computer after the files have been restored to the CME server.

This section describes the procedures to back up:

- Communications Manager data on VM1
- AUDIX data on VM1
- MV_CDR/Call Accounting and MyPhone data on VM2 (the Postgres data base)
- DHCP data on VM2 (dhcpd.conf file)

The backup procedure consists of two steps:

- create the backup files and copy them to /var/home/ftp/pub on VM1
- copy the five backup files to an external device

If AE Services is used for applications other than the MyPhone application, you must use a separate backup procedure described in Backing up AE Services data on page 79.

Preparing Communication Manager, AUDIX, and VM2 backup files

To copy the Communication Manager and AUDIX data files to the /var/home/ftp/pub directory on VM1, perform the following actions:

1. Connect your services laptop computer to the services port on the S8510. See Figure 1: S8510–back view on page 11.
2. On the Backup Now Web page in the Backup Method section, select **Network Device** and do the following:
   - from the **Method** drop-down, select the appropriate data transfer method
   - in the **User Name** box, enter the user name of the account on the backup server
   - in the **Password** box, enter the password of the account on the backup server
   - in the **Host Name** box, enter the host name or IP address of the backup server
   - in the **Directory** box, enter the path where you want to store the backup data
3. Click **Start Backup**.

4. Click **Check Status** to see the backup status. After the backup is complete, the system displays Backup Successful messages for both ACP and AUDIX.

Preparing the VM2 backup files

To prepare the VM2 backup file, perform the following steps:

1. Create the Postgres backup files:
   a. Use PuTTY to open an SSH session to **192.11.13.6**, port **12022,** on VM2 and log in as **craft** or **dadmin**.
   b. At the Linux bash prompt, enter
   `/usr/bin/pg_dump –h localhost –U mvuser –F c –f /tmp/<ca_filename> MVCA`,
   where **`<ca_filename>`** is a file name you choose for the CDR/Call Accounting backup file.

   The MV_CA database is backed up on the /tmp directory on VM2.

   c. At the Linux bash prompt, enter
   `/usr/bin/pg_dump –h localhost –U mvuser –F c –f /tmp/<fm_filename> followme`,
   where **`<fm_filename>`** is a file name you choose for the MyPhone/FollowMe backup file.
2. Copy the Postgres and DHCP backup files to VM1:
   a. Use PuTTY to open an SSH session to **`192.11.13.6`**, port **22**, on VM1 and log in as **craft** or **dadmin**.
   b. Change directory to /pub:
   Enter **`cd /var/home/ftp/pub`**.
   c. Open an SFTP session to VM2:
   Enter **`sftp craft@172.29.29.2`**.
   d. Change directory to /tmp:
   Enter **`cd /tmp`**.
   At this point, the ’remote’ directory is /tmp on VM2 and the ’local’ directory is /var/home/ftp/pub on VM1.
   e. Copy Postgres files to VM1
   Enter **`get <ca_filename>`**
   Enter **`get <fm_filename>`**,
   where **`<ca_filename>`** and **`<fm_filename>`** are the filenames you chose for the CDR/Call Accounting and MyPhone backup files, respectively.
   f. Copy the DHCP configuration file to VM1:
   Enter **`get /etc/dhcpd.conf`**.
   g. Enter **`quit`** to close the SFTP session to VM2.

Copying the backup files to an external device

Important:
You must copy the backup files to an external destination. Otherwise, the files are lost when the upgrade software is installed.

1. Make sure that the backup files are copied to /pub:
   a. Enter **`cd /var/home/ftp/pub`**.
   b. Enter **`ls -at`**.
   c. Make sure that the backup files are in the /pub directory and have the current date and time:

Backup file for	Filename
Communication Manager	Example: **xln_server1_121500_20070622. tar.gz**
AUDIX	Example: **audix-tr-name-msg_server1121540_20070622.tar.gz**
CDR/Call Accounting	Name that you chose ***<ca_filename>***
MyPhone	Name that you chose ***<fm_filename>***
DHCP	**dhcpd.conf**

2. To copy the backup files to a customer server or to the services laptop by using the PSFTP, perform the following actions:
   a. Go to the backup location:

      If backing up to the Services laptop, open the command window and change directory to the backup directory on your laptop computer.

   b. In the PuTTY list of programs, click **PSFTP**. The system opens the PSFTP command window.
   c. Enter **`open 192.11.13.6`**.
   d. Enter **`cd /var/home/ftp/pub`**.
   e. Enter **`get <backup_filename>`**,

      where **<backup_filename>** is the one of the five backup filenames. Note that you must use the complete filenames in the **`get`** command—PSFTP does not support wild carding.

   f. Repeat step d. for the other four backup files.
   g. Enter **`quit`**.
3. Verify that the files were successfully copied to the external destination.

Backing up AE Services data

AE Services backup

If you use AE Services (AES) for anything other than the MyPhone application, you must backup up the AES files.
However, if you use AES *only* for MyPhone, skip this backup procedure and proceed to Recording the customer IP addresses and logins on page 79.

To back up the AES data on your laptop computer:

1. To open the CTI OAM main menu on VM3, open a Web browser and enter https://192.11.13.6:8443
2. Click **AE Services Administration**.
3. Log in as craft with the initial password.
4. Click **CTI OAM Admin**.
5. Select **Maintenance** then **Backup Database**.

   OAM displays the Database Backup screen with the following message:

   The backup file can be downloaded from **here**.
6. Click **here**.

   The system displays the File Download dialog box which identifies the file name (mvapdb*ddmmyyyy*.tar) and prompts you to save the file.
7. Click **Save**.

   The system displays the Save As dialog box.
8. Browse to the location on the computer (for example, C:\mve_backup) that you want to use for storing the AES database backup, and click **Save**.
9. If possible, copy the AES backup file to a customer server.

Recording the customer IP addresses and logins

IP addresses

To record the system IP addresses, perform the following actions:

1. Use PuTTY to open an SSH session to **192.11.13.6**, port **11022** on the base server.
2. Enter **`cd /etc/opt/mve/`**
3. Enter **`cat network.conf`**

4. Record the IP addresses displayed in the network.conf file in the following table:

IP Address	Used for
	Base Server
	VM1
	VM2
	VM3
	AUDIX
	Default Gateway (GWIP)
	Subnet Mask

Important:
These IP addresses will be entered during the DVD installation. The IP addresses must be the same as the IP addresses for the previous release.

Logins

Perform the following steps to record the customer logins:

1. Use PuTTY to open an SSH session to **192.11.13.6**, port **22**, on VM1.
2. Enter **`cat /etc/passwd`** to display the password file.
3. Select the contents of the password file and copy to a Notepad text file to record the login information.

Setting up customer super-user login

If requested by the customer, perform the following steps to set up a customer super-user login:

1. Using the Web browser, open the Maintenance Web Interface on VM1:

   Enter https://192.11.13.6 in the address bar of the browser window. Log in and click **Launch Maintenance Web Interface**.
2. In the Security section on the left navigation menu, click **Administrator Accounts**.
3. In the Select Action section, select **Add Login** and select the required login type.
4. Click **Submit**.
5. On the Add Login screen, enter the required fields and click **Submit**.

Restoring MVE R 1.x data for upgrades

If you are upgrading the MVE software, complete the following procedure to restore the previously backed up XLN and AUDIX data:

1. After you complete the installation and configuration procedures, use the Communication Manager Web pages on VM1 to restore the Communication Manager and AUDIX translations that you saved in Backing up MultiVantage Express data for an upgrade on page 75.
   a. On the left navigation menu, click **Download Files**.
   b. Select **File(s) to download from the machine I'm using to connect to the server**.
   c. Click the first **Browse** button and browse to the location on the Services laptop where you saved the backup files and select the tar.gz file for xln_server1.
   d. Click the second **Browse** button and browse to the location on the Services laptop where you saved the backup files and select the tar.gz file for AUDIX.

      Important:
      Do not select the Install this file on the local server check box.

   e. Click **Download**.
   f. After the files are copied to the /var/home/ftp/pub directory, the Download Files Results Web page will display the *.tar.gz files and their size. Make sure that the file names and sizes are correct.
2. Restore the AUDIX backup file:
   a. Stop the AUDIX messaging application.
   b. Select **View/Restore Data** under 'Data Backup/Restore'.
   c. On the View/Restore Data Results Web page, select the *.tar.gz file for AUDIX that you want to restore.
   d. Click **Restore**.
   e. Click **Check Status** and, if necessary, click **Refresh** until the restore is finished.
      If the AUDIX restore is not successful, you must start Messaging and use ASA to import a the original AUDIX subscriber data back into the IA770.
   f. Restart the AUDIX messaging application.
3. Restore the Communication Manager (XLN) backup file:
   a. Select **View/Restore Data** under 'Data Backup/Restore'.
   b. On the View/Restore Data Results Web page, select the *.tar.gz file for XLN of CM that you want to restore.
   c. Click **Restore**.

d. Click **Check Status** and, if necessary, click **Refresh** until the restore is finished.

e. Make sure that CM re-reads the restored translations by resetting the system by entering the following command at the SAT prompt:
`reset system 4`
The system reboots.

4. Restore AE Services configuration data, if any.

a. From the base server Maintenance Web pages, enter **`http://<IP_address_VM3>/MVAP`**, where **`<IP_address_VM3>`** is the IP address of virtual machine 3.

b. Click on AE Server Administration and log in to AE Services using the initial craft login.

c. From the CTI OAM main menu, select **Maintenance** > **Restore Database**.

d. Click **Browse** and locate the AE Services database backup file that you intend to use (mvapdb10082007.tar.gz, for example). Continue with Step c after you have selected the backup file.

e. Click **Restore**.

OAM displays the Restore Database Configuration screen, with the following message. 'A database restore is pending'. You must restart the Database Service and the AE Server for the restore to take effect.

f. Click **Restart Services**.

AE Services restarts the Database Service and the AE Server, completing the restore process.

5. Restore the Postgres database and the DHCP configuration file:

a. Connect your Services laptop to the Services port on the S8500.

b. Open a PSFTP session to VM2 on port 12022 and log in as craft or dadmin:

`open 192.11.13.6 -P 12022`

c. Enter **`cd /tmp`**.

d. Enter **`lcd <path_to_backup_directory>`**, where <path_to_backup_directory> is the full path name to the directory that contains the backup files.

e. Enter **`put <filename>`**, where **`<filename>`** is the Postgres backup file name.

f. Repeat step **e** for each backup file.

g. Enter **`cd /etc`**.

h. Enter **`put dhcpd.conf`**.

i. If the files were successfully transferred, enter **`bye`**.

j. Use SSH to connect to **192.11.13.6**, port **12022** on VM2.

k. Enter
/usr/bin/pg_restore –h localhost –U mvuser –c –d MVCA /tmp/ <*ca_backup_filename*>

The MV_CA database is restored.

l. Enter
/usr/bin/pg_restore –h localhost –U mvuser –c –d followme tmp/ <*fm_backup_filename*>

The FollowMe database is restored.

6. Stop messaging and perform the SAT command **reset system 4** to allow the restored Communication Manager translations to be enabled.

   Stopping messaging allows the application to shut down gracefully. Reset system 4 enables the restored Communication Manager translations.

7. Restore the following settings, which are lost during an upgrade:

   a. Use the VM1/Communication Manager Web Pages, under Configure Server, to set the modem RAS IP address and enable modem for 'all incoming calls'.

   b. Reestablish the original customer logins using the SAT login commands.

Post-upgrade procedures

To complete the upgrade procedure, you must follow these steps:

1. Verify that Communication Manager translations were restored correctly and that all processes, including AUDIX, are running and the system is stable on the new software load.
2. Check the Avaya Communication Manager Express Downloads Web site for any Service Packs or Messaging RFUs that need to be applied.
3. Perform save translations.
4. Back up new system files using the steps in Backing up MultiVantage Express data for an upgrade on page 75. Select the Full Backup option.
5. Connect the power cord to the SAMP.
6. Perform system testing including alarm dial out and remote access.
7. Schedule periodic future backup procedures.

Appendix D: Installing and configuring G450 gateway—an overview

This appendix provides an overview of the G450 gateway installation and configuration steps. For more information, see *Quick Start for Hardware Installation: Avaya G450 Media Gateway, 03-602053* and *Installing* and *Upgrading the Avaya G450 Media Gateway, 03-602054*.

To install and configure the G450 gateway, perform the following actions:

1. Connect your laptop computer to the G450 gateway by using an Ethernet crossover cable or a serial cable.
2. Use PuTTy or similar Telnet or SSH client session from your services laptop computer to 192.11.13.6 on port 23 and log in as root with password (root).
3. Change the root password if prompted.
4. At the command prompt, enter the following commands:
    1. `G450-???(super)#`**`ip license-server`**
       If this is the primary (the serial number is in the license) gateway.
    2. `G450-???(super)#`**`set mgc list <CM_IP_address>`**
       where, <*CM_IP_Address*> is the IP address of CM that is listed in the installation wizard in the Gateway step.
    3. `G450-???(super)#`**`interface Vlan 1`**
    4. `G450-???(super)#`**`ip address <IP_address> <subnet_mask>`**
       For example, ip address 123.45.67.89 255.255.255.0
       where, 123.45.67.89 is the IP address for the G450 Gateway
    5. `G450-???(super)#`**`pmi`**
       Message about PMI set and reboot of gateway required
    6. `G450-???(super)#`**`exit`**
    7. `G450-???(super)#`**`ip route 0.0.0.0 0.0.0.0 <IP_address>`**
       where, <*IP_address*> is the IP address that the G450 uses as a default gateway.
    8. `G450-???(super)#`**`copy run start`**
    9. `G450-???(super)#`**`reset`**
5. Log in as root with the new password.
6. Upgrade the gateway if required as outlined in the G450 instruction manual. The application server has the gateway firmware available via TFTP and HTTP

Avaya recommends that you visit http://support.avaya.com for the latest firmware binaries.

Example of basic G450 running configuration

To see the contents of the G450 basic configuration file, enter the following command at the command prompt:

G450-???(super)#**show run**

```
! version 27.26.0
Config info release 27.26.0 time "03:05:51 12 JAN 1970 " serial_number 08IS05164
872
set logging file enable
set logging file condition all Error
set logging file condition BOOT Debug
!
no ip telnet
no snmp-server community
!
ds-mode t1
!
interface Vlan 1
 icc-vlan
 ip address 10.10.10.206    255.255.255.0
 pmi
 exit
!
interface FastEthernet 10/3
 exit
!
interface FastEthernet 10/4
 exit
!
interface Console
 exit
!
interface USB-Modem
 shutdown
 exit
!
set mgc list 10.10.10.200
set mediaserver 10.10.10.200 10.10.10.200 23 telnet
set mediaserver 10.10.10.200 10.10.10.200 5023 sat
rtp-stat qos-trap
no rtp-stat fault
ip license-server
!#
!# End of configuration file. Press Enter to continue.
```

Index

A

ABIT text file 41
AE Services
  backup 79
alarming and VPN access 33

B

backup
  AE Services 79
  AUDIX 76
  Communication Manager 76
backup file
  load 53
backup methods
  local compact flash card 44
  local directory 43
  network device 43

C

configuration
  from template 37
  important notes 14
  post-installation 44
  selecting the type 23
  SIP 40, 55
country selection 28

D

DHCP 30

G

G450 media gateway 12
gateway installation references 12
gateway installation wizard 37
gateways
  H248 37
  installing 36

H

H.248 media gateway installation reference 12
hardware installation 11

I

installation
  gateways 36
  hardware 11
  prerequisites 10
IP addresses
  recording 79
IP telephone, settings 30

L

loading user data 41, 43
local compact flash card 43
local directory 43
logins
  recording 80
  super-user 80

P

port redirection 60
port switching 61
post-installation 44
pre-upgrade tasks 75
progress indicators 12

R

references, gateway installation 12
RFA files 28, 49

S

S8510 server 11
solution elements configuration file 53
SPIRIT alarming 10

T

template configuration 37
Terminal Translation Initialization 14

U

user data, loading 41, 43