Installing and Configuring Avaya Midsize Business Template

Release 5.2
June 2011

© 2012 Avaya Inc.

All Rights Reserved.

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

Copyright

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

the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Third-party components

For the Midsize Business Template specific Third Party open source, license text files are available in the following directory on each of the Virtual Machine's: /Licenses/. In addition, the license text file applicable to the Midsize Business Template Installation Wizard is available in the following directory within the preweb.war and post-install.tar files which form part of the Midsize Business Template distribution: /Licenses/.

For more information regarding the Third-Party components and terms for Midsize Business Template, see http://support.avaya.com/Copyright.

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

Avaya Aura is a trademark of Avaya.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

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

Contents

Chapter 1: Midsize Business Template installation overview 7
Installation checklist for Midsize Business Template 8
Chapter 2: Downloading Midsize Business Template license and installer files 11
Licensing Midsize Business Template components 11
Downloading and managing Midsize Business Template files 12
Chapter 3: Selecting a template to install 15
Search Local and Remote Template field descriptions 16
Search Local and Remote Template button descriptions 18
Chapter 4: Using the pre-installation wizard 19
System and browser requirements for installation 19
Installing Midsize Business Template using the standalone pre-installation wizard 19
Loading existing EPW file 20
Load Files field descriptions 21
Load Files button descriptions 21
Chapter 5: Using the Midsize Business Template embedded installation wizard 23
Configuring Midsize Business Template using the embedded installation wizard 23
Network settings 24
Configuring network settings 24
Customer login 30
Creating customer login 30
Selecting country 31
(Optional) Configuring DHCP 32
DHCP field descriptions 33
VPN access 33
(Optional) Configuring VPN access 33
Configuring alarm identities 35
Alarming field descriptions 35
Gateways configuration 35
Configuring gateways 36
(Optional) Configuring SIP 38
SIP field descriptions 39
Station and voicemail configuration 39
Configuring station and voice mail 43
Station and Voice Mail Configuration field descriptions 43
Station and Voice Mail Configuration button descriptions 44
Trunks configuration 44
Configuring trunks 46
Trunks field descriptions 47
Trunks button descriptions 48
Reviewing summary 49
Confirming installation 50
Chapter 6: Installing MBT with minimal configuration 53
Installing minimally configured MBT 53
Configuring network settings 53

Network Settings field descriptions for the embedded installation wizard 54
Creating customer login 57
Customer Login field descriptions 57
Reviewing summary 59
Confirming installation 60
Chapter 7: (Optional) Configuring Media Services 63
Configuring Media Services integrated announcement 63
Chapter 8: Registering the system 65
Chapter 9: Troubleshooting MBT installation 67
DVD does not read 67
Troubleshooting steps 67
Media services not working 67
Troubleshooting steps 67
Service port not working 67
Troubleshooting steps 68
System time drifts over a period of weeks 68
Troubleshooting steps 68
Appendix A: Installation prerequisites for MBT -Worksheets 69
Hardware requirement worksheet 69
Installation prerequisites for MBT – mandatory items worksheet 69
Installation prerequisites for MBT – optional items worksheet 70
IP addresses worksheet for MBT with Media Services 72
IP addresses worksheet for MBT without Media Services 73
VPN gateway worksheet 74
Appendix B: Post Installation Tasks for MBT 75
Communication Manager checks and tests 75
Communication Manager Messaging checks and tests 75
Application Enablement Services checks and tests 76
SIP Enablement Services checks and tests 76
Utility Services checks and tests 77
Remote access checks and tests 78
Alarming checks and tests 78
Media Services checks and tests 78
Appendix C: Digit treatment 81
Incoming digit treatment 81
Appendix D: LSP Configuration 83
Installing and configuring S8510 or S8800 server 83
Licensing LSP through lsp-config 84
Creating a super-user login 85
Configuring the server manually 86
Updating the SAMP firmware 87
Configuring the modem 87
Enabling network time servers 88
Configuring the server as an LSP 89
Administering the main server 90
Rebooting the server 91
Index 93

Chapter 1: Midsize Business Template installation overview

The high-level steps for installing the Avaya Midsize Business Template are as follows:

- (Optional) Download the MBT standalone pre-installation wizard and use it to generate an EPW (Electronic Preinstallation Worksheet)) configuration file.
- Download licenses for MBT components, for example Communication Manager from PLDS.
- Using the System Platform Management Console, select from where the Midsize Business Template will be installed: directly from a DVD or from Avaya's PLDS (Product Licensing Delivery System) web site (http://plds.avaya.com). Choose the specific Midsize Business Template to install, either with or without Media Services, depending on what has been purchased. Copy it to a USB flash drive or burn it to a dual layer DVD.
- Install the Avaya Aura™ System Platform software on an S8510 Server or an S8800 Server. See *Installing and Configuring Avaya Aura™ System Platform* for more information.
- Configure the SAL gateway included in System Platform for remote support and alarming.
- Configure MBT using either the MBT embedded installation wizard or using the EPW configuration file created earlier using the MBT standalone pre-installation wizard.
- Verify that the MBT installation wizard completed successfully by checking the install/upgrade log under the **Virtual Machine Management** menu in the System Platform Management Console.
- Verify that the MBT components are running by checking the Manage page on System Platform Management Console.
- (If applicable) Verify that Media Services configuration is working by making an internal call and making a call to voicemail.
- (Optional) Connect the second server (same type) with System Platform installed on it and configure/enable High Availibility Failover.

Midsize Business Template can be supplied on DVD. Alternately, using Avaya's PLDS (Product Licensing Delivery System Web site at http://plds.avaya.com), an ISO image can be downloaded allowing creation of an Midsize Business Template dual layer DVD or extracting Midsize Business Template files to a USB stick. Midsize Business Template can also be installed directly from Avaya's PLDS site using the System Platform PLDS option.

You can configure MBT in two ways: either using the standalone pre-installation wizard before the installation or the embedded installation wizard at the time of installation. Both versions of the installation wizard contain the same configuration functionality.

Note:

Using the standalone pre-installation wizard saves you time during the MBT installation as all your settings are saved in the EPW (Electronic Preinstallation Worksheet) file. During installation, the embedded installation wizard uploads the EPW file and configures MBT as a part of its installation.

After the installation wizard has the system configuration values, the virtual machines are copied to the system and configured. When this is completed, you can complete any further configuration. These additional configuration steps include configuring SAL and installing the licenses to the System Platform WebLM server.

Installation checklist for Midsize Business Template

Use the following checklist to install Midsize Business Template.

Task	Notes	✔
Generate an EPW file using the Midsize Business Template standalone pre-installation wizard. See Installing using standalone pre-installation wizard on page 19.		
Download the required licenses from PLDS. See Licensing of components on page 11.		
Do one of the following steps: • Use the Midsize Business Template supplied on DVD. • Use Avaya's PLDS (Product Licensing Delivery System Web site at http://plds.avaya.com) and download an ISO image to create an Midsize Business Template dual layer DVD. • Extract Midsize Business Template files to a USB stick. • Install Midsize Business Template directly from Avaya's PLDS site using the System Platform PLDS option. See Downloading and managing Midsize Business Template files on page 12.		
Gather the required information relating to installation, such as IP addresses, Alarm Ids, ABIT file, and user name and password.		

Task	Notes	✔
See: • Hardware requirement worksheet on page 69 • Installation prerequisites for MBT – mandatory items worksheet on page 69 • Installation prerequisites for MBT – optional items worksheet on page 70 • IP addresses worksheet for MBT with Media Services on page 72 • IP addresses worksheet for MBT without Media Services on page 73		
Select either a Midsize Business Template template with Media Services or a Midsize Business Template template without Media Services to install. See Selecting a template to install on page 15.		
Configure Midsize Business Template components. See Configuring using embedded installation wizard on page 23.		
Perform post-installation tasks. See: • Communication Manager checks and tests on page 75 • Communication Manager Messaging checks and tests on page 75 • Application Enablement Services checks and tests on page 76 • SIP Enablement Services checks and tests on page 76 • Alarming checks and tests on page 78 • Remote access checks and tests on page 78 • Utility Services checks and tests on page 77 • Media Services checks and tests on page 78		

Task	Notes	✔
Configure SAL for remote access and alarming. Registering the system on page 65		

Chapter 2: Downloading Midsize Business Template license and installer files

Licensing Midsize Business Template components

The high level steps for installing Midsize Business Template licenses are as follows:

- Access the WebLM server on System Platform Console Domain.

  Note:

  The default user ID and password of the WebLM server are **admin** and **weblmadmin** respectively. You must change the default password after the first login.

- Log into WebLM server and obtain the primary system ID (which is same as Console Domain's (cdom) virtual MAC address) from under Weblm system properties. The primary system ID is used for generating the licenses.
- Download licenses for Midsize Business Template components from PLDS.
- Install the licenses on the System Platform WebLM server.

Avaya provides the Midsize Business Template licenses through the PLDS (Product Licensing Delivery System Web site), http://plds.avaya.com.

After downloading the licenses from the PLDS, you must install them on the System Platform WebLM server.

Note:

You must generate the Avaya WebLM license using the virtual MAC address of the System Platform Console Domain (cdom). This is a system generated MAC address and NOT the same as the real MAC address of eth0. Communication Manager, AES, and Media Services are all licensed against this MAC address.

Since this MAC address is generated dynamically by System Platform, it is not possible to determine the address before the System Platform installation.

The system runs without licensing for a 30 day grace period. So, if you cannot get a license at the time of installation, you still have 30 days to acquire the license and install it on the system. Applications licensed through PLDS for Midsize Business Template are:

- Communication Manager and Communication Manager Messaging (same license)
- Application Enablement Services
- Media Services (if installed)

Note:

SIP Enablement Services (SES) is embedded and does not need a separate license to be installed.

Downloading and managing Midsize Business Template files

Procedure

1. Enter **http://plds.avaya.com** in your web browser to open the PLDS (Product Licensing and Delivery System) Web site.
2. Click **Log in with my password**.
3. Enter your login and password details.

   Your login id is your e-mail address.
4. Click **Log In**.
5. On the **Home** page, expand **Asset Mgmt** and click **View Downloads**.
6. On the **Downloads** page, enter your company's name in the **%Company** field.
7. In the **Application** drop down menu, choose the template or application to run on System Platform, for example, **Midsize Business Template**.
8. Click **Search Downloads**.
9. Locate the MBT.iso file and click **Download**.

   The MBT.iso file contains the installer files for Midsize Business Template.
10. On the **About the Download Manager** page, click **Click to download your file now**.

    Note:

    If you receive an error message about Active X, perform the instructions on the screen to get the required version of Active X installed on your computer or laptop, and then continue with the download.
11. When the system displays the security warning page, click **Install**.

    When the install is complete, PLDS displays the downloads again with a check mark next to the download which is successfully completed.
12. Extract the MBT.iso file to your computer or laptop.

13. Burn a dual layer DVD of the installer files or copy the installer files to a USB flash drive to use for installation.

Chapter 3: Selecting a template to install

After installing System Platform, install Midsize Business Template.

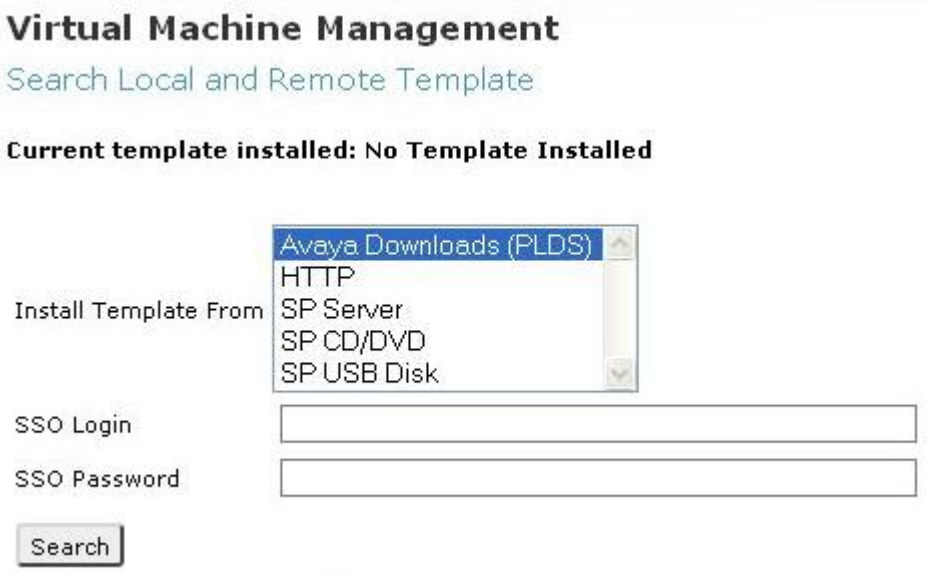
Note:

This operation is not supported on the system running in High Availability Failover Mode. To proceed with the installation, stop the High Availability Failover Mode.

See the System Platform High Availability Failover section in *Installing and Configuring Avaya Aura™ System Platform* for more information.

Procedure

1. Log on to System Platform Management Console.
2. Click **Virtual Machine Management** > **Solution template**.
   The system displays the **Virtual Machine Management** page. Use this page to select an MBT template either with Media Services (MBT.ovf file) or without Media Services (MBT_without_Media_Services.ovf file) to run on System Platform.



Important:

System Platform creates an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any connection to your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration screen. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is not connected to your LAN, this address conflict

could result in the failure of System Platform or an installed template to route packets correctly.

Before installing a template, check the Network Configuration page on the System Platform Management console (**Server Management > Network Configuration**) to view the addresses allocated on the bridge named “avprivate”.

3. Select a location from the list in the **Install Templates From** box. See Search Local and Remote Template field descriptions on page 16 for more information on the available location options.

   (Optional) If the template installation files are located in a different server (for example, Avaya PLDS or HTTP), you may be required to configure a proxy depending on your network.

4. Click **Search** to display a list of template descriptor files (each available template has exactly one template descriptor file).
5. On the Select Template page, click the required template, and then click **Select** to continue. The system displays the Template Details page with information on the selected template and its Virtual Appliances.
6. Click **Install** to start the template installation.
   The system displays the Electronic Pre-installation Worksheet (EPW) upload page.
7. Do one of the following:
   - If you have an EPW file that you generated using the Midsize Business Template standalone pre-installation wizard, upload the EPW file and then select the **continue with EPW file** option.
   - If you do not have an EPW file, select the **Continue without EPW file** option.

Search Local and Remote Template field descriptions

Use the Search Local and Remote Template page to select the template to install on System Platform, to upgrade an installed template, or to delete an installed template.

Name	Description
Install Template From	Locations from which you can select a template and install it on System Platform. Available options are as follows: **Avaya Downloads (PLDS)** The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list will contain all the templates to which your company is entitled. Each line in the list begins with the

Name	Description
	“sold-to” number to allow you to select the appropriate template for the site where you are installing. Hold the mouse pointer over the selection to view more information about the “sold-to” number. **HTTP** The template files are located on an HTTP server. You must enter the template URL information. **SP Server** The template files are located in the `/vsp-template` file system in the Console Domain of the System Platform server. **SP CD/DVD** The template files are located on a CD or DVD in the CD/DVD drive on the server. **SP USB Disk** The template files are located on a USB flash drive connected to the server.
SSO Login	Active only when you select the **Avaya Downloads (PLDS)** option to search for a template. Login id for logging on to Single Sign On.
SSO Password	Active only when you select the **Avaya Downloads (PLDS)** option to search for a template. Password for Single Sign On.

Search Local and Remote Template button descriptions

Name	Description
Install	Installs the solution template. This button is displayed only if no template is currently installed on System Platform.
Configure Proxy	Active only when you select the HTTP option to search for a solution template. Lets you configure a proxy for the HTTP address. If necessary, configure a proxy for Secure Access Link (SAL) and alarming functions to access the internet.
Upgrade	Upgrades the installed solution template from the selected template location option. This button is displayed only if a template is installed on System Platform.

Name	Description
Delete	Deletes the currently installed and active template. This button is displayed only if a template is installed on System Platform.

Search Local and Remote Template button descriptions

Name	Description
Upgrade	Upgrades the installed solution templates from the selected template location option.
Configure Proxy	Active only when you select the HTTP option to search for a solution template. Lets you configure a proxy for the HTTP address.
Install	Installs the solution template.
Delete Installed Template	Deletes the currently installed template.

Chapter 4: Using the pre-installation wizard

System and browser requirements for installation

Ensure that you have one of the following browsers installed on your computer or laptop for running the installation wizards for Midsize Business Template:

- Internet Explorer 6.x or 7.x
- Firefox 2.x or 3.x

Also, ensure that the following requirements are fulfilled:

- Java SE 5.0 or later installed on the computer or laptop from where you are going to run the installation wizard
- The computer or laptop has Windows XP installed
- TCP port 31005 is free

Note:

If the TCP port 31005 is in use, edit the configuration file installer.properties at `C:\Program Files\Avaya\MBT Pre-installation Wizard` and restart the wizard to use the new port.

Installing Midsize Business Template using the standalone pre-installation wizard

Installing Midsize Business Template using the standalone pre-installation wizard comprises the following steps:

1. Loading existing EPW file on page 20
2. Configuring network settings on page 24
3. Creating customer login on page 30
4. Selecting country on page 31
5. (Optional) Configuring DHCP on page 32
6. (Optional) Configuring VPN access on page 33

7. Configuring alarm identities on page 35
8. Configuring gateways on page 36
9. (Optional) Configuring SIP on page 38
10. Configuring station and voice mail on page 43
11. Configuring trunks on page 46
12. Reviewing summary on page 49

The Midsize Business Template standalone pre-installation wizard is a Windows executable that can be used to create or modify a configuration file for later use during the Midsize Business Template installation. The standalone pre-installation wizard starts in your default Web browser and provides the same configuration pages as the embedded installation wizard. The only difference is that the initial and final steps of loading and saving the file containing the Midsize Business Template configuration parameters (called an EPW file). The last step in the standalone pre-installation wizard allows you to save the configuration in the EPW file. The system loads this file during installation. You can save both partial and complete configurations. If you did not enter a mandatory field, you must enter the value when using the embedded wizard before installation completes at site.

Note:

You must determine whether the final installation will include Media Services when using the standalone pre-installation wizard. The Media Services network values will be displayed or hidden based on your choice of installing or not installing Media Services.

You can find the details for the common steps in the chapter Configuring using embedded installation wizard on page 23.

Loading existing EPW file

Procedure

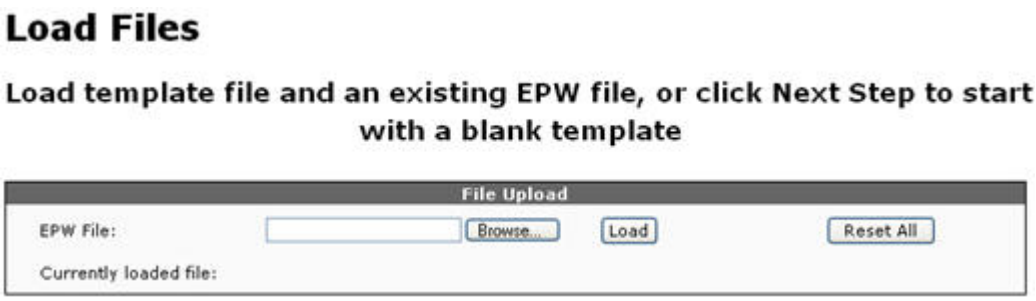
Perform one of the following tasks:

- Click **Browse** to select an existing EPW file and then click **Load** to upload the file.

  Note:

  If you are creating an EPW file for the first time, then go to the next step to start with a blank template.

- Click **Next Step** to go to the Network Settings page and create a new EPW file.



Next steps

Configure network settings.

Load Files field descriptions

Name	Description
EPW File	Existing EPW file that you can select to load.
Currently loaded file	File name of the currently loaded EPW file.

Load Files button descriptions

Button	Description
Browse	Opens a dialog box to help navigate to the folder containing the EPW file.
Load	Loads the selected EPW file.
Reset	Clears the **EPW File** entry.

Chapter 5: Using the Midsize Business Template embedded installation wizard

Configuring Midsize Business Template using the embedded installation wizard

Select **Manage Template** from the System Platform Management Console. Then select the media location for the Midsize Business Template image. If you configured this system beforehand using the standalone pre-installation wizard, upload that file in the system. If you did not use the standalone pre-installation wizard, select the option to continue without the EPW file. The System Platform downloads the files and launches the embedded installation wizard.

Note:

You must enable pop-ups in your Web browser.

The Midsize Business Template installation using the embedded installation wizard comprises the following steps:

1. Configuring network settings on page 24
2. Creating customer login on page 30
3. Selecting country on page 31
4. (Optional) Configuring DHCP on page 32
5. (Optional) Configuring VPN access on page 33
6. Configuring alarm identities on page 35
7. Configuring gateways on page 36
8. (Optional) Configuring SIP on page 38
9. Configuring station and voice mail on page 43
10. Configuring trunks on page 46
11. Reviewing summary on page 49
12. Confirming installation on page 50

Network settings

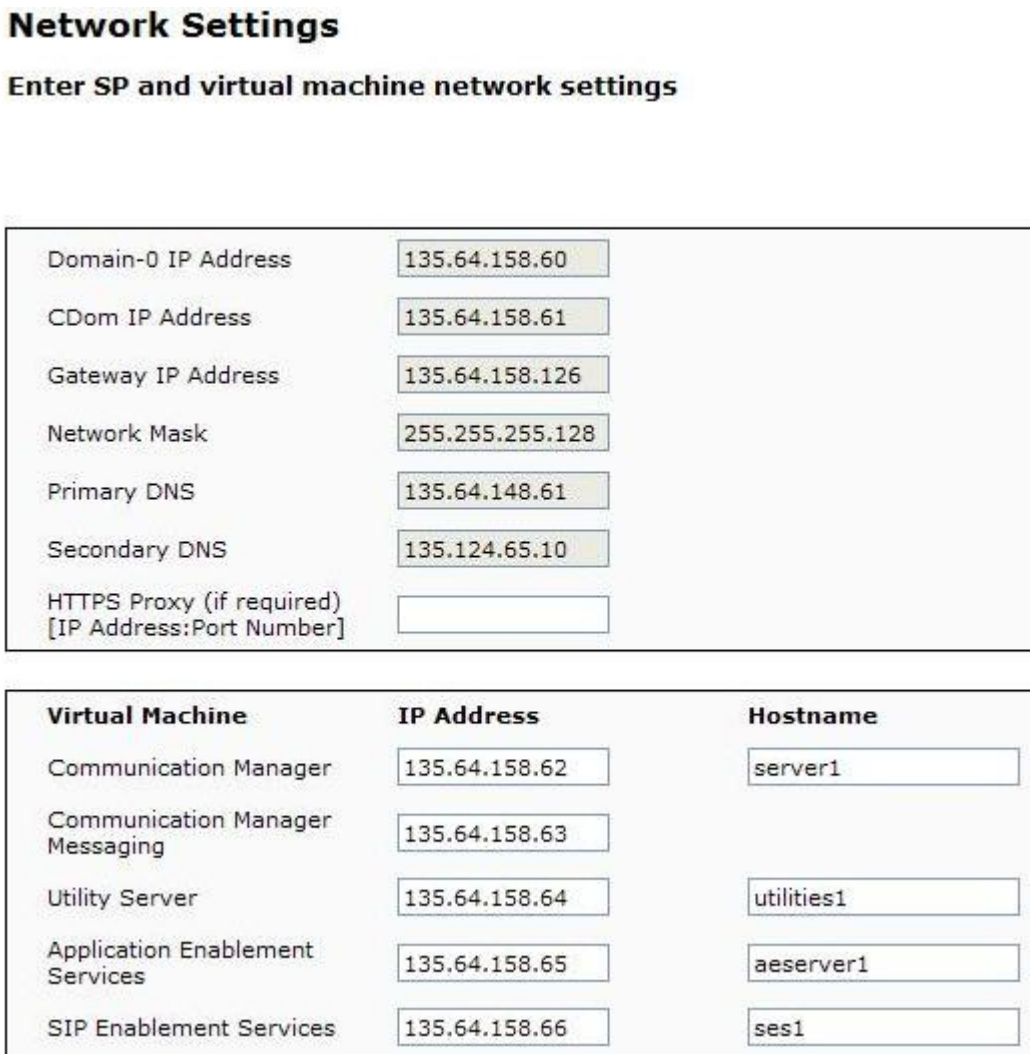
The Network Settings page allows configuration of the virtual machine IP addresses and hostnames and other IP addresses used by the system such as DNS and proxy settings. The IP addresses for System Domain (Dom-0), Console Domain, Gateway, Communication Manager, Communication Manager Messaging, Utility Services, AES,SES, and Media Services must be configured to be on the same network.

SAL uses DNS and if System Platform has already configured a value for DNS, SAL will use that value. The proxy, if in use, is used for alarming. If System Platform has configured a proxy, the same will be used.

Configuring network settings

Procedure

On the Network Settings page, complete the fields to configure all the network parameters.



Next steps

Create customer login.

Network Settings field descriptions for standalone pre-installation wizard

Name	Description
Domain-0 IP Address	The IP address of the System Domain (Dom-0). This will be compared to the IP address used when System Platform is installed. This is used as a check to ensure the correct EPW file is being used during installation.

Name	Description
C-dom IP Address	This will be compared to the IP address used when System Platform is installed. This is used as a check to ensure the correct EPW file is being used during installation.
Gateway IP Address	The gateway IP address.
Network Mask	The network mask address.
DNS	The DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center. **Important:** When you enter a DNS server address, it overwrites any value that was configured through the System Platform Management Console. If you have already configured a DNS on System Platform, then you do not have to specify any values here, as MBT Installation Wizard does not try to overwrite values configured through System Platform. If you are using the Embedded Installation Wizard, the wizard does not allow you to edit any values that you have previously (for example, through System Platform) configured. If you are using the standalone pre-installation wizard, the values you enter through the wizard are overwritten by the values you have already configured through System Platform.
HTTPS Proxy	The proxy server address, if the network to which the Midsize Business Template is connected requires a proxy server to route its internet traffic. **Important:** If you have already configured a proxy address on System Platform, then you do not have to specify any values here, as the Midsize Business Template Installation Wizard does not overwrite values configured through System Platform. If you are using the Embedded Installation Wizard, the wizard does not allow you to

Name	Description
	edit any values that you have previously (for example, through System Platform) configured. If you are using the standalone pre-installation wizard, the values you enter through the wizard are overwritten by the values you have already configured through System Platform.
Virtual Appliance	The IP address and host name for the following: • Communication Manager • Communication Manager Messaging • Utility Services • Application Enablement Services • SIP Enablement Services • Media Services
IP Address	The required IP address for Media Services TN2302B media processors. Four IP addresses should be entered: one for each TN2302B IP interface in Media Services. **Note:** The Embedded Midsize Business Template Installation Wizard prompts you for the Media Services IP addresses only if you select a template containing Media Services. The standalone pre-installation wizard always prompts for these IP addresses as it is not possible to determine in advance which template will be selected. Media Services TN2501 Announcement circuit pack also has an IP interface but it cannot be configured through the installation wizard. You can configure it using Communication Manager maintenance tools such as SAT. See Adding a TN2501AP VAL circuit pack section of the Announcement chapter in the *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)* book for more information.

Network Settings field descriptions for the embedded installation wizard

Name	Description
Domain-0 IP Address	The IP address of the System Domain (Dom-0). This was set during the installation of System Platform. If you want to change this IP address, you must do it from the Network Properties page on the Console Domain. This is a display-only field.
C-dom IP Address	The Console Domain IP address. This was set during the installation of System Platform. If you want to change this IP address, you must do it from the Network Properties page on the Console Domain. This is a display only field.
Gateway IP Address	The gateway IP address.
Network Mask	The network mask address.
DNS	The DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center. **Important:** When you enter a DNS server address, it overwrites any value that was configured through the System Platform Management Console. If you have already configured a DNS on System Platform, then you do not have to specify any values here, as MBT Installation Wizard does not try to overwrite values configured through System Platform. If you are using the Embedded Installation Wizard, the wizard does not allow you to edit any values that you have previously (for example, through System Platform) configured. If you are using the standalone pre-installation wizard, the values you enter through the wizard are overwritten by the values you have already configured through System Platform.

Name	Description
HTTPS Proxy	The proxy server address, if the network to which the Midsize Business Template is connected requires a proxy server to route its internet traffic. **Important:** If you have already configured a proxy address on System Platform, then you do not have to specify any values here, as the Midsize Business Template Installation Wizard does not overwrite values configured through System Platform. If you are using the Embedded Installation Wizard, the wizard does not allow you to edit any values that you have previously (for example, through System Platform) configured. If you are using the standalone pre-installation wizard, the values you enter through the wizard are overwritten by the values you have already configured through System Platform.
Virtual Appliance	The IP address and host name for the following: • Communication Manager • Communication Manager Messaging • Utility Services • Application Enablement Services • SIP Enablement Services • Media Services
IP Address	The required IP address for Media Services TN2302B media processors. Four IP addresses should be entered: one for each TN2302B IP interface in Media Services. **Note:** The Embedded Midsize Business Template Installation Wizard prompts you for the Media Services IP addresses only if you select a template containing Media Services. The standalone pre-installation wizard always prompts for these IP addresses as it is not possible to determine in advance which template will be selected.

Name	Description
	Media Services TN2501 Announcement circuit pack also has an IP interface but it cannot be configured through the installation wizard. You can configure it using Communication Manager maintenance tools such as SAT. See Adding a TN2501AP VAL circuit pack section of the Announcement chapter in the *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)* book for more information.

Customer login

On the Customer Login page, complete the fields to specify the user credentials for Communication Manager and SIP Enablement Services. This login will be added to Communication Manager and SES to enable the administration of these systems. Extra customer logins can be added as required after the installation wizard completes.

Creating customer login

Procedure

On the Customer Login page, complete the fields to specify the user credentials for Communication Manager and SIP Enablement Services.



Next steps

Select country (if you are using the full installation wizard).

(Optional) Review summary (if you are using the minimal installation wizard).

Customer Login field descriptions

Name	Description
Login name	A user name. This login acts as a fail-safe access option for Communication Manager and SIP Enablement Services if the system loses connectivity with the LDAP authentication server hosted on System Domain (Dom-0). The system does not allow you to add the following as user names to avoid conflict with other accounts on the system: • `root` • `sroot` • `craft` • `init` • `inads` • `cust` • `admin`
Password	A password for the user login.
Re-type password	Re-typing the password confirms that there is no error in typing.

Selecting country

About this task

The country setting is used by the wizard to set parameters such as location parameters, loss plan, ARS access code, feature access codes, tone plan, and trunk parameters.

Procedure

On the Country page select the country you are in from the **Select Country** drop down menu.



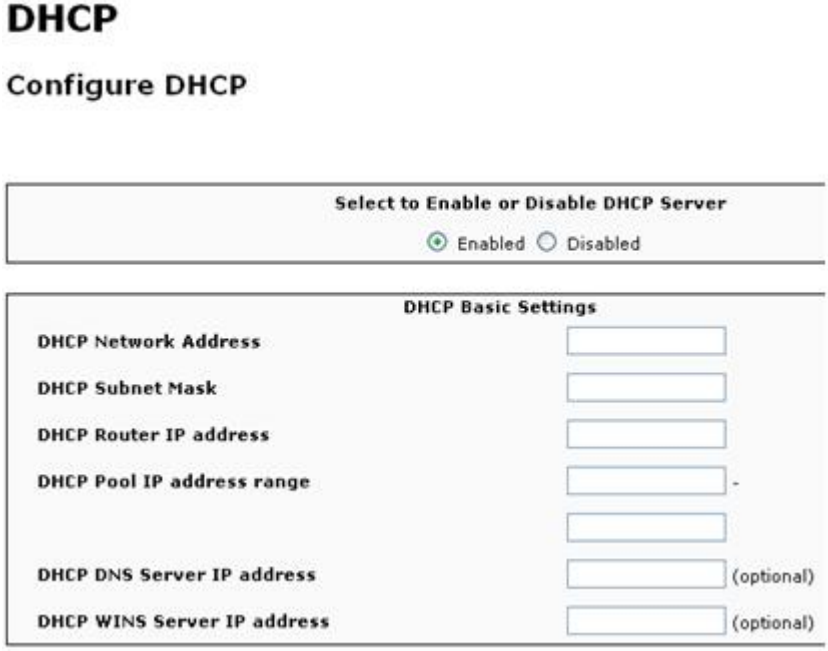
Next steps

Configuring DHCP.

(Optional) Configuring DHCP

Procedure

1. On the DHCP page, select the **Enabled** option to enable the DHCP Server.



Note:

If you plan to use an external DHCP server, then you must select the **Disabled** option. If required, you can access additional and more advanced DHCP configuration options through the web console of Utility Services after completing the installation.

2. Complete the fields in the DHCP Basic Settings to configure a DHCP server to use with Avaya IP phones.

Next steps

Configure VPN access.

DHCP field descriptions

Name	Description
Enable DHCP	When selected, enables the internal DHCP server. If you are using an external DHCP server, then do not select.
DHCP Network Address	The network IP address for the DHCP subnet.
DHCP Subnet Mask	The subnet mask associated with the network.
DHCP Router address	The IP address of the router on the DHCP subnet.
DHCP Pool IP address range	The range of IP addresses to be used within the DHCP pool.
DHCP DNS Server IP address	(Optional) The IP address of a DNS server if used.
DHCP WINS Server IP address	(Optional) The IP address of a WINS server if used.

VPN access

You only need to configure this page if your VPN gateway is on the same network as the Midsize Business Template server. If the VPN gateway is on a different network, you may need to contact the customer IT department to ensure that VPN traffic is routed correctly.

(Optional) Configuring VPN access

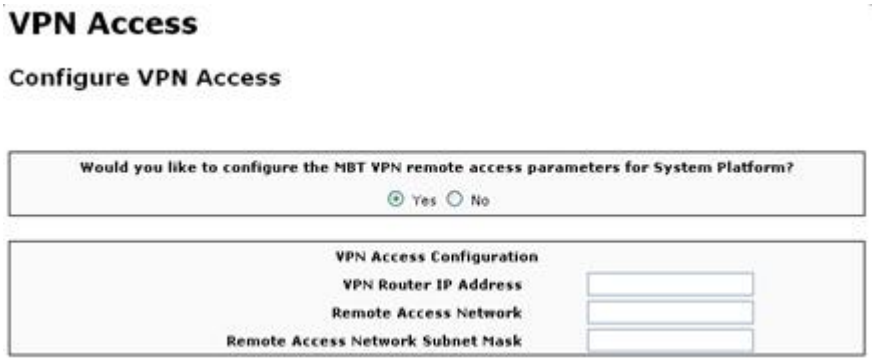
About this task

The VPN Access page allows configuration of the routing required on the applications to support remote access through a VPN. If you plan to access the system through a VPN box

local to the MBT system, you should enter the required details on this page. These values will be used to add static routes into the system to route traffic down the VPN tunnel to the remote network.

Procedure

1. On the VPN Access page, select the **Yes** option to configure MBT VPN remote access parameters for System Platform.



2. Complete the fie
3. Complete the fields to configure MBT to allow VPN access.

Next steps

Configure alarm identities.

VPN Access field descriptions

Name	Description
Select to Enable or Disable VPN access	Enables or disables VPN access.
VPN Router IP Address	The IP address of the external VPN gateway device.
Remote Access Network	The IP address of the network (that is, the Avaya Business Partner's home network) from which MBT will be accessed.
Remote Access Network Subnet Mask	The subnet mask associated with the network (that is, the Avaya Business Partner's home network) from which MBT will be accessed.

Configuring alarm identities

Procedure

1. On the **Alarming** page, select the **Yes** option to configure the Midsize Business Template alarm ID parameters for System Platform. The alarm IDs will be populated to the respective machines. This page will not enter alarm IDs in SAL and will need to be entered separately.
2. Specify the **Alarm Id**s for Communication Manager, Communication Manager Messaging, SIP Enablement Services, and Application Enablement Services.

   Note:

   You should be provided with Avaya alarm IDs from the Avaya Services team.

Next steps

Configure gateways.

Alarming field descriptions

Name	Description
Alarm Id	The alarm ID for Communication Manager, Communication Manager Messaging, Application Enablement Services, and SIP Enablement Services. **Note:** Ensure that you have received the alarm ids from the Avaya Services team.

Gateways configuration

This section of the wizard deals with the configuration of external Avaya gateways. Media Services is automatically added if that is a part of the template. The wizard will configure the required information into Communication Manager. The gateways themselves will still need to be configured.

The locations of any DS1 cards in the system should be indicated using the check boxes. The DS1 information will be used to configure trunks and the gateway section should be completed before the trunk section.

Configuring gateways

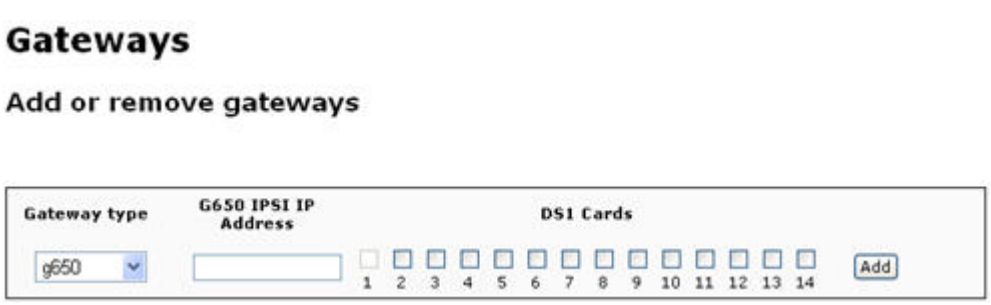
Procedure

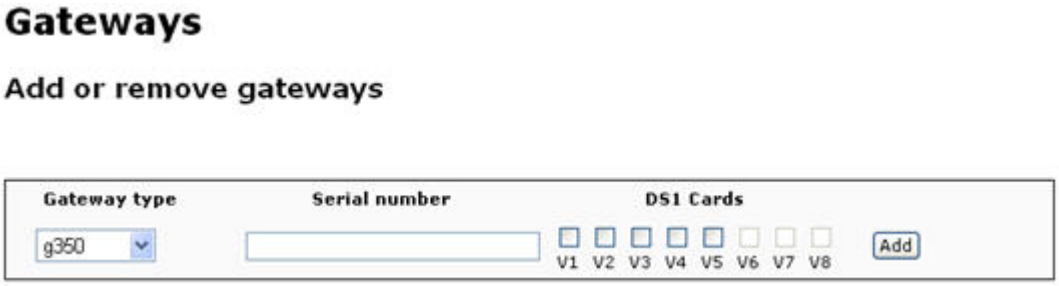
1. Complete the fields in the Gateways page to configure a media gateway on Communication Manager.

   Note:

   Depending on your selection in the **Gateway type** field, you will see different fields on the Gateways page. Shown below are two illustrations of the Gateways page: for G650 and G350 gateways.

   If the Midsize Business Template you selected earlier includes the Media Services component, the wizard transfers the configurations automatically, and you do not need to provide a **Serial number**. The software-only Media Services IP gateway configuration appears as a G650 Port Network on Communication Manager. See *Avaya Aura™ Solution for Midsize Enterprises Overview* and *Configuring the Avaya G650 Media Gateway on Communication Manager (03-300685)* available on the Avaya Support Web site, http://support.avaya.com for more information.





2. Click **Add**.

Next steps

Configuring SIP.

Gateways field descriptions

Names	Descriptions
Gateway type	The required gateway type.
Serial number	The serial number of the selected gateway. You can change the 12–digit serial number later through Communication Manager, if required. **Note:** The media gateway serial number can be found on the gateway label or by issuing a `show system` command on the gateway command line interface (CLI).
DS1 Cards	Use the check boxes to indicate which slots in the gateway will be populated with DS1 cards (for example, MM710 or TN464). A DS1 card is required for each trunk you would like to configure. **Important:** The slot selected on the wizard must match the physical slot the board will be inserted in.
G650 IPSI IP Address	The IP server interface IP address for the selected gateway type. For G650 cabinets, you enter the IPSI IP address.

Gateways button descriptions

Button	Description
Add	Adds the gateway.

(Optional) Configuring SIP

About this task

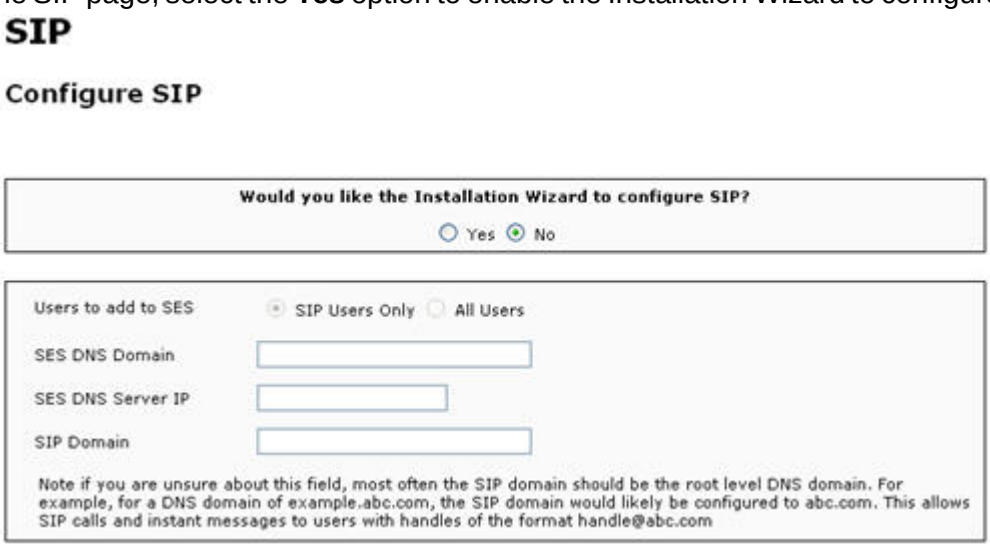
This page enables configuration through the SES wizard. If **Yes** is selected, the wizard will run the initial configuration on SES with the values provided. The wizard will either add all users listed in the abit.txt file to SES to allow the use of Instant Messaging or just the users specifically set to a port type of SIP in the abit.txt.

Important:

Do not import the configuration from a standalone SIP Enablement Server into the Midsize Business Template SIP Enablement Server. The configurations are not compatible and will prevent the Midsize Business Template SIP Enablement Server from operating.

Procedure

1. On the SIP page, select the **Yes** option to enable the Installation Wizard to configure SIP.



2. Complete the fields to configure SIP Enablement Services to support SIP endpoints or trunks.

Next steps

Configure stations and voice mail.

SIP field descriptions

Name	Description
Would you like the Installation Wizard to configure SIP?	Selecting **Yes** allows the Installation Wizard to configure the SIP based on your specifications in the page.
Users to add to SES	**SIP Users Only** Selects only the SIP users. **All Users** Selects all the users.
SES DNS Domain	Allows the DNS domain of the SES server to be different from the domain of the System Platform server. For example, the System Platform domain might be `emea.avaya.com` but that of SES might be `ses.sipserviceprovider.com`.
SES DNS Server IP	Allows SES to use a SIP provider DNS which may be different from the enterprise DNS set on the network page.
SIP Domain	The domain name of the enterprise you want to use for SIP communications. **Tip:** If you are not sure about what values to enter in this field, you can enter the root-level DNS name of your enterprise domain.

Station and voicemail configuration

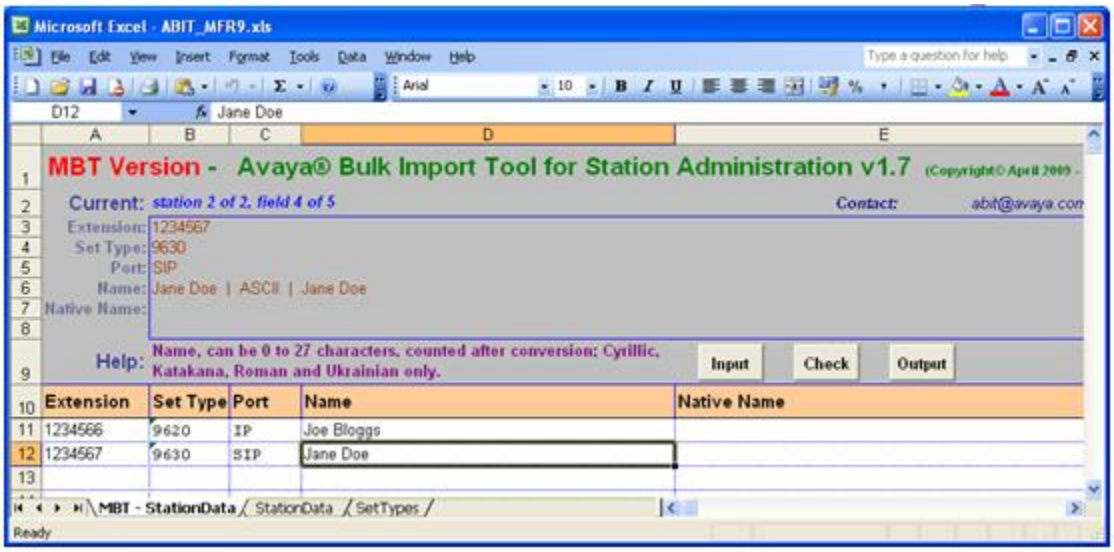
The Station and Voicemail Configuration screen enables you to perform the following tasks:

- Select the required dial plan length (3, 4, 5, 6 or 7 digits) for the system.
- Upload an Avaya Bulk Import Tool (ABIT) text file containing Midsize Business Template user data. The ABIT text file is generated by an ABIT Excel spreadsheet that you can either download from the link in the installation wizard or from the Avaya Support site,

support.avaya.com. After populating the spreadsheet with the relevant user data, click the **Output** button to generate the ABIT text file to upload to the installation wizard.

- Select the appropriate Communication Manager Messaging voicemail language from the list of supported languages (the language for the country selected is displayed as the default but this can be changed).

The following graphic shows an exaple of ABIT file.



Ensure that you have the latest version of the ABIT file (v 1.7) and have selected the *MBT – StationData* tab at the bottom of the worksheet (if selected, the system displays the *MBT version* title in red text in the top left corner of the screen.)

Avaya recommends that you use the *MBT* tab in the new version of the spreadsheet as it ensures that the MBT specific validation rules are applied to the ABIT data. This helps to avoid configuration problems later on in the installation process.

The following section provides a description of the fields in the ABIT file, and the procedure to populate them.

Extension

Enter the extension numbers you wish to add to the system. Always ensure that the extension number length is consistent with the dial-plan length configured in the Wizard. The wizard supports dial plan lengths between 3 and 7 digits and number ranges beginning with the numbers 1 to 7. Leading digits 8 and 9 are currently reserved for system use (that is, Facility Access Codes).

Set Type

Enter the set type of any station that is supported by the version of Communication Manager you are using (in this case Communication Manager 5.2). Version 1.7.1 of the ABIT file has an additional SetTypes tab that contains a list of all the set types supported by the installation wizard.

Port

For H.323 endpoints enter `ip` or `IP`, for SIP endpoints enter `sip` or `SIP`, and for x-port stations enter `x` or `X`.

Name

Enter a standard ASCII string to identify the station/user. In the case of Communication Manager, this string is used to populate the station name field directly; however, in the case of SIP Enablement Services, the wizard attempts to split the name into a first name and a last name using either the first white space character or a comma (if present) as the delimiting characters. In the case of a white space, all of the characters before the first white space will be used as the first name and all of those after (including any subsequent white spaces) will be used as the last name. Subsequent whitespaces in the last name will be replaced with an underscore '_' character. If a comma is found in the string, this will take precedence over any other whitespaces. Any characters before the comma will be used as the last name and any characters after the comma will be used as the first name. White spaces both before and after the comma will be replaced with an underscore '_' character. The following table shows an example:

Name string in ABIT	SES First Name	SES Last Name
Fred Bloggs	Fred	Bloggs
Fred Bloggs Senior	Fred	Bloggs_Senior
Fred	Fred	_
Bloggs, Fred	Fred	Bloggs

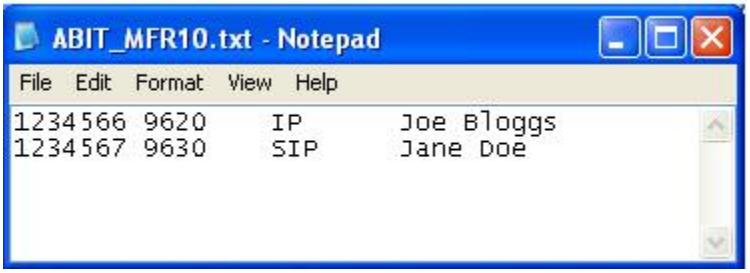
Note:

If a string is present in the **Native Name** field of the ABIT then this is used to populate the SES first name and last name fields in preference to any strings found in the standard name field. The installation wizard applies the same rules as those described above to native name field in this instance.

Native Name

Allows the user to enter a *native name* using the additional character sets supported by Unicode. In the case of Communication Manager, this string is applied directly, in the case of SES the rules described in the previous section (**Name**) are used to derive the first and last name fields. If a string is present in the native name filed it will take precedence over any strings found in the 'name' field for populating the SES first and last name fields.

After completing the fields when you click the **Output** button, the spreadsheet generates a text file similar to the following. You can uploaded this text file to the installation wizard.



The installation wizard uses the ABIT file to configure the following:

- Voicemail

  The wizard configures a CMM voicemail box for all stations in the ABIT. The default PIN for all mailboxes is ‘2580’. Avaya strongly recommends that you change this PIN when logging in to CMM for the first time.

- H323 endpoints

  If the port type is set to *IP*then the installation wizard configures an H.323 endpoint on Communication Manager. The default station security code for all H.323 endpoints is 123456.

- SIP endpoints

  If the port type is set to *SIP*the installation wizard configures a SIP extension on Communication Manager, adds an OPS entry to the *off-pbx-station mapping*form on Communication Manager and also adds a SIP user to SES. The default station security code for all SIP endpoints is 123456.

Firmware Selection for SIP and H323 Endpoints

This section describes how IP phones should be configured in order to select the appropriate firmware (i.e. H323 or SIP) if you are using the Midsize Business Template in-built DHCP Server. If you are not using the Midsize Business Template built-in DHCP server and File server, ignore this section.

By default Avaya IP phones (46xx and 96xx) are shipped with the default settings configured to download H323 firmware. If you include ‘SIP’ stations in your ABIT file (using the ‘SIP’ port type) additional configuration will be required on the IP phones themselves in order to designate which phones pick up H323 firmware and which pick up SIP firmware. The process for 46xx and 96xx phones is different, the instructions for these respective phone types is described below:

- 46xx IP Phones

  The version of firmware (that is, SIP or H.323) that the phone downloads can be controlled using the ‘SIG’ setting on the phone. By default, the SIG setting configured on 46xx phones when they ship is ‘0’ (H323). In order to force 46xx phones to download SIP firmware the SIG value must be changed to ‘2’ (SIP)

- 96xx IP Phones

  The upgrade scripts shipped with the 96xx phones do not recognize the SIG setting on the phones. You cannot use the SIG setting to control which version of firmware (i.e. H323 or SIP) is downloaded. Instead, SSON is used to determine the type of firmware that the

phones download. By default, all phones use the value 242 (H323), if you require a particular phone (or phones) to use SIP firmware then the SSON value on those phones must be changed to 250.

Configuring station and voice mail

Procedure

1. On the Station and Voice Mail Configuration page, select the required **Dial plan length** for the dial plan.



2. Click **Browse** to locate an ABIT.txt file (an Avaya Bulk Import Tool (ABIT) text file containing MBT user data).
3. Click **Load**.
4. Select a language from the **Select a Voice Mail language to load** drop down menu.

Next steps

Configure trunks

Station and Voice Mail Configuration field descriptions

Name	Description
Dial plan length	Number of digits in the dial plan.
ABIT.txt file	Name of the Avaya Bulk Import Tool file.
Currently loaded file	Name of the currently loaded Avaya Bulk Import Tool file.

Name	Description
Select a Voice Mail language to load	The language choice for voice mail.

Station and Voice Mail Configuration button descriptions

Name	Description
Browse	Enables selecting the Avaya Bulk Import Tool file.
Load	Loads the selected Avaya Bulk Import Tool file.
Unload	Unloads the currently selected Avaya Bulk Import Tool file.

Trunks configuration

The Trunks page of the wizard will administer ISDN PRI trunks appropriately for your country of installation within Communication Manager.

The countries currently supported are: US, UK, Germany, Russia, France, Spain, Mexico, Brazil, Australia, New Zealand, Italy, and Japan.

Systems being installed in countries not on the above list will need to administer ISDN trunking though the SAT interface of Communication Manager.

The trunks administered will be added to route pattern 1. If extra routing is required, this should be administered through the SAT interface of Communication Manager after the post installation wizard has completed. The first step is to select a DS1 board from the drop down list in the ISDN Trunks section for the trunk you want to configure through the wizard and click **Add**. The wizard will then assign a trunk number. Repeat this step for all DS1 cards you want the wizard to configure trunks for. Incoming call handling treatment allows mapping of incoming numbers from the PSTN to extensions.

Incoming call handling treatment allows mapping of incoming numbers from the PSTN to extensions.

Trunk Number: The number of the trunk group for which incoming call handling is being administered.

Number Length: The number of digits received from the network.

Number Digits: The actual digits received from the network. If this is shorter than*Number Length* then it represents a block of numbers, whose leading digits match *Number Digits*.

Otherwise it represents a single number received from the network. If *Number Digits* is left blank, it will match all incoming digits up to a maximum of *Number Length*.

Delete: The number of digits which Communication Manager needs to delete from the beginning of the number received from the network.

Insert: The digits which Communication Manager needs to prefix to the number received from the network, after *Delete* leading digits have been deleted.

For example, if you wanted incoming number 720-555-3434 to route to extension 3434 you would enter:

Number length as 10

Number digits as 720555

Delete 6

Add < leave blank >

If you wanted incoming digits 123456 to route to extension 5456 you would enter:

Number length as 6

Number digits as 123

Delete 3

Add 5

Note:

In Germany, digits are received from the network in overlap mode. See Incoming digit treatment on page 81 for further details.

Public Unknown Numbering:

Public unknown numbering is used to send the user's calling ID number out to the PSTN when they make an outgoing call. For example, the extension 2424 dials out and the call ID sent out is 720 555 2424.

Dial Plan Length: The length of Communication Manager extension numbers.

Ext Code: The leading digit(s) of Communication Manager extension numbers.

Trk Grp(s): If this field is populated, calls carried on this (these) trunk group(s) have the wizard data *CPN Prefix* prefixed to the calling station's extension number and sent out as Calling Party Number. If the field is not populated, all trunk calls include this Calling Party Number.

CPN Prefix: These digits are prepended to the calling station's extension number and the result is checked to see if it is greater than *CPN Len*. If it is greater, then the excess digits are removed from the beginning of the calling station's extension before the prefixing is done. The resulting digits are used as Calling Party Number of the call.

Total CPN Len: The maximum allowed length of a Calling Party Number. The wizard administers *Dial Plan Length* in the *Ext Len* field in the public-unknown-numbering form of Communication Manager, and the remaining values in the public-unknown-numbering form fields of the same name. So, from the above example, the extension 2424 dials out and the call ID sent out is 720 555 2424.

Dial Plan Length 4

Ext Code 2

Trk Grp(s)

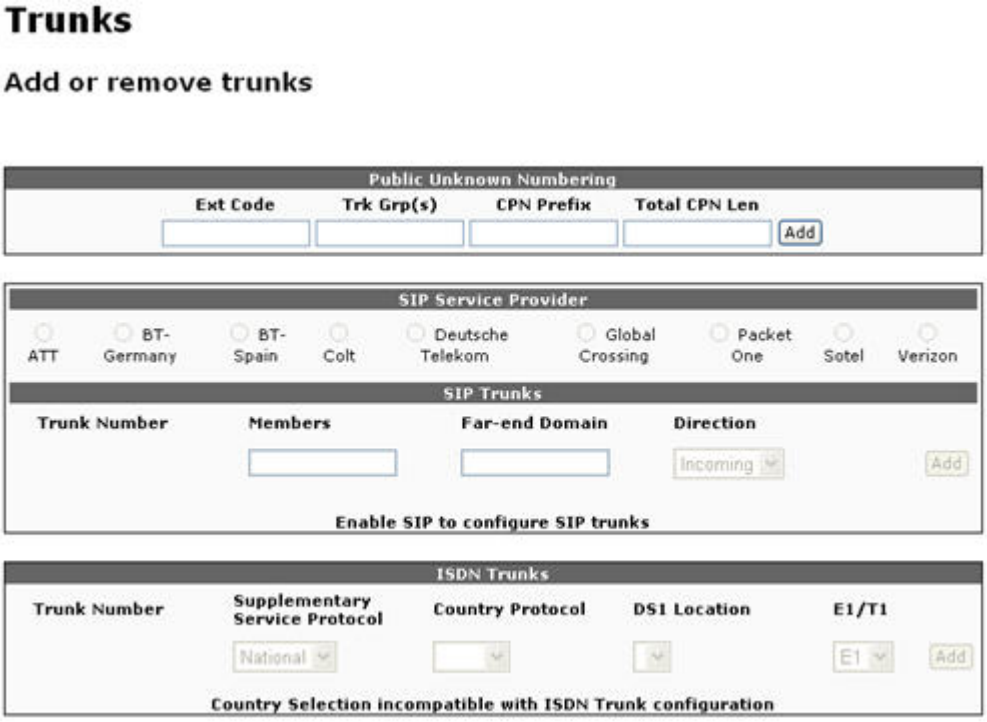
CPN Prefix 720555

Total CPN Len 10

Configuring trunks

Procedure

On the Trunks page, complete the fields to configure trunk groups.



Next steps

Review summary.

Trunks field descriptions

Name	Description
Ext code	Extension number to be associated with a trunk group.
Trk Grp(s)	Trunk group associated with a set of extension numbers.
CPN Prefix	Digits to be prefixed to the extension number to make a Calling Party Number (CPN).
Incoming Call Handling Treatment	
Trunk Number	The number of the trunk group for which incoming call handling is being administered.
Number Length	The number of digits received from the network.
Number Digits	The actual digits received from the network. If this is shorter than **Number Length** then it represents a block of numbers, whose leading digits match **Number Digits**. Otherwise it represents a single number received from the network.
Delete	The number of digits which Communication Manager needs to delete from the beginning of the number received from the network.
Insert	The digits which Communication Manager needs to prefix to the number received from the network, after **Delete** leading digits have been deleted.
Add	Adds the country information to the configuration database.
	When the country selected is **USA** in the Country page, the Trunks page presents an additional drop-down list for selecting the DS1 protocol version. The supported values are mapped as follows: • a AT&T TR 41449/41459 • b Bellcore TR 1268; NIUF.302; ANSI T1.607

Name	Description
	• c NORTEL DMS-250 BCS36/IEC01 • d Telecordia SR-4287

Trunks button descriptions

Button	Description
Add on **Public Unknown Numbering**	Adds an extension number to the configuration database.
Add on **ISDN Trunks**	Adds a country information to the configuration database.

Reviewing summary

Procedure

The Summary page provides an overview of the configuration data already gathered by the wizard. This page displays the values you have not yet set in red.

Summary

Network Settings	
Domain-0 Address	135.9.184.150
CDom Address	135.9.184.151
Gateway Address	135.9.184.254
Network Mask	255.255.255.0
Primary DNS	135.9.1.2
Secondary DNS	Not set
HTTPS Proxy	Not set

Virtual Machine	IP Address	Hostname
CM	135.9.184.152	cm1
CMM	135.9.184.153	
Utility Server	135.9.184.154	util1
AES	135.9.184.155	aes1
SES	135.9.184.156	ses1
Media Services	135.9.184.157	ms1

	IP Address
Media Services Medpro 1	135.9.184.158
Media Services Medpro 2	135.9.184.159
Media Services Medpro 3	135.9.184.160
Media Services Medpro 4	135.9.184.161

Next steps

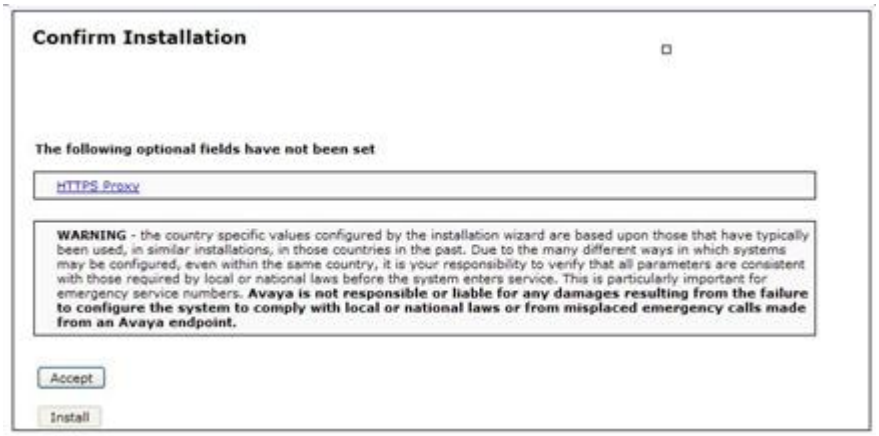
Confirm installation.

(Optional) Save configuration (if you are using standalone pre-installation wizard).

Confirming installation

Procedure

1. On the Confirm Installation page, click **Accept** to accept the warning message. The system enables the **Install** option.



2. Click **Install** to start installing the template.

Result

After proceeding from the configuration section of the wizard the installation then downloads, starts and configures the virtual machines. The screen is updated with the progress of each section. This process takes approximately 30 - 90 minutes depending on system size (average time is about 40 minutes). During this time the system requires no extra input and you can spend this time in deploying the phones or administering the gateways.



09:53:50	-- Download/Install aes	Complete	100	6m 53s
10:00:43	-- Download/Install ses	Complete	100	3m 37s
10:04:20	-- Download/Install utility_server	Complete	100	3m 35s
10:07:56	Assign Dedicated NIC	Complete	100	57s
10:08:53	-- Download/Install cobar	Complete	100	3m 52s
10:12:58	Start all VMs	Complete	100	1m 18s
10:14:16	Wait until system and all VMs are stabilised	Complete	100	1m 4s

Run post-install plugin if present
- CM:Configuring CM
- CM:Checking ssh connection to CM
- US:Configuring Utility Server
- US:Checking ssh connection to US
- SES:Configuring SES
- SES:Checking ssh connection to SES
- AES:Configuring AES
- AES:Checking ssh connection to AES
- CMM:Configuring CMM
- CMM:Downloading Language rpm
- CM:Connecting to CM
- SES:Connecting to SES
- US:Copying authentication file to US
- AES:Checking AES database is up
- CM:Waiting for CM to come up.
- SES:Waiting for SES to come up.
- US:Installing authentication file
- AES:Adding switch
- CM:CM is up.
- CM:Adding tmpuser login to CM
- US:Authentication file loaded.
- US:Configuring phone settings file
- SES:Waiting for SES to come up.
- CM:Adding customer login to CM
- SES:Waiting for SES to come up.
- AES:Adding switch password
- AES:Adding switch connection
- US:Finished phone settings file configuration.
- US:Configuring ESD settings file
- CMM:Loading and Installing Language rpm
- CM:Copying authentication file to CM
- SES:SES is up.
- SES:Adding Customer login
- CM:Installing authentication file
- AES:Restarting MVAP service
- CM:Saving CM translations

Note:

Do not attempt to configure the virtual machines (for example, Communication Manager using SAT) while the post installation process is in progress. All the applications are configured at this stage. Attempting to configure the system too early may result in your changes being lost or the wizard being blocked from completing its tasks.

If there is any error during the process, the system displays the error on screen in bold letters together with a warning symbol in the extreme right column in the screen. Investigate such a message immediately. The error may be very minor and may not effect the overall success of the installation or may require some corrective action which may be a reinstallation.

After system loads the machines and configures them, you can proceed to test the installation.

Next steps

Perform post-installation tasks for MBT.

(Optional) Check the troubleshooting steps if the installation is not successful.

Chapter 6: Installing MBT with minimal configuration

Installing minimally configured MBT

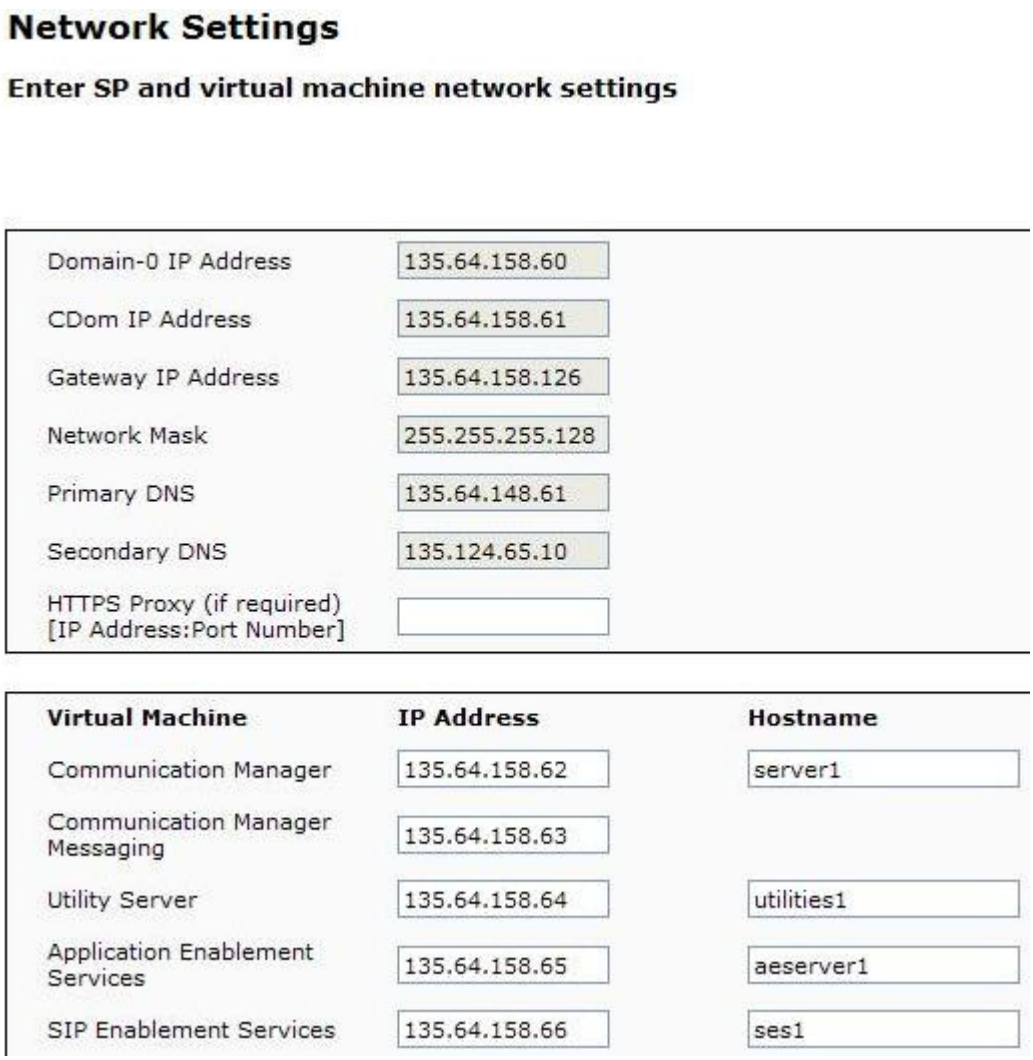
Advanced users can administer the system through other means (such as provision) or by restoring a previous MBT save file. In this case, they must select the **Configuration** option in the navigation pane of the wizard. When this is selected, many of the installation wizard sections will disappear and these parameters will no longer be configured by the wizard. The minimal MBT installation comprises the following steps:

1. Configuring network settings on page 24
2. Creating customer login on page 30
3. Reviewing summary on page 49
4. Confirming installation on page 50

Configuring network settings

Procedure

On the Network Settings page, complete the fields to configure all the network parameters.



Next steps

Create customer login.

Network Settings field descriptions for the embedded installation wizard

Name	Description
Domain-0 IP Address	The IP address of the System Domain (Dom-0). This was set during the installation of System Platform. If you want to change this IP address, you must do it from the

Name	Description
	Network Properties page on the Console Domain. This is a display-only field.
C-dom IP Address	The Console Domain IP address. This was set during the installation of System Platform. If you want to change this IP address, you must do it from the Network Properties page on the Console Domain. This is a display only field.
Gateway IP Address	The gateway IP address.
Network Mask	The network mask address.
DNS	The DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center. **Important:** When you enter a DNS server address, it overwrites any value that was configured through the System Platform Management Console. If you have already configured a DNS on System Platform, then you do not have to specify any values here, as MBT Installation Wizard does not try to overwrite values configured through System Platform. If you are using the Embedded Installation Wizard, the wizard does not allow you to edit any values that you have previously (for example, through System Platform) configured. If you are using the standalone pre-installation wizard, the values you enter through the wizard are overwritten by the values you have already configured through System Platform.
HTTPS Proxy	The proxy server address, if the network to which the Midsize Business Template is connected requires a proxy server to route its internet traffic. **Important:** If you have already configured a proxy address on System Platform, then you do not have to specify any values here, as the

Name	Description
	Midsize Business Template Installation Wizard does not overwrite values configured through System Platform. If you are using the Embedded Installation Wizard, the wizard does not allow you to edit any values that you have previously (for example, through System Platform) configured. If you are using the standalone pre-installation wizard, the values you enter through the wizard are overwritten by the values you have already configured through System Platform.
Virtual Appliance	The IP address and host name for the following: • Communication Manager • Communication Manager Messaging • Utility Services • Application Enablement Services • SIP Enablement Services • Media Services
IP Address	The required IP address for Media Services TN2302B media processors. Four IP addresses should be entered: one for each TN2302B IP interface in Media Services. **Note:** The Embedded Midsize Business Template Installation Wizard prompts you for the Media Services IP addresses only if you select a template containing Media Services. The standalone pre-installation wizard always prompts for these IP addresses as it is not possible to determine in advance which template will be selected. Media Services TN2501 Announcement circuit pack also has an IP interface but it cannot be configured through the installation wizard. You can configure it using Communication Manager maintenance tools such as SAT. See Adding a TN2501AP VAL circuit pack section of the Announcement chapter in the *Avaya Aura™ Communication*

Name	Description
	Manager Feature Description and Implementation (555-245-205) book for more information.

Creating customer login

Procedure

On the Customer Login page, complete the fields to specify the user credentials for Communication Manager and SIP Enablement Services.



Next steps

Select country (if you are using the full installation wizard).

(Optional) Review summary (if you are using the minimal installation wizard).

Customer Login field descriptions

Name	Description
Login name	A user name. This login acts as a fail-safe access option for Communication Manager and SIP Enablement Services if the system loses connectivity with the LDAP authentication server hosted on System Domain (Dom-0). The system does not allow you to add the following as user names to

Name	Description
	avoid conflict with other accounts on the system: • root • sroot • craft • init • inads • cust • admin
Password	A password for the user login.
Re-type password	Re-typing the password confirms that there is no error in typing.

Reviewing summary

Procedure

The Summary page provides an overview of the configuration data already gathered by the wizard. This page displays the values you have not yet set in red.

Summary

Network Settings	
Domain-0 Address	135.9.184.150
CDom Address	135.9.184.151
Gateway Address	135.9.184.254
Network Mask	255.255.255.0
Primary DNS	135.9.1.2
Secondary DNS	Not set
HTTPS Proxy	Not set

Virtual Machine	IP Address	Hostname
CM	135.9.184.152	cm1
CMM	135.9.184.153	
Utility Server	135.9.184.154	util1
AES	135.9.184.155	aes1
SES	135.9.184.156	ses1
Media Services	135.9.184.157	ms1

	IP Address
Media Services Medpro 1	135.9.184.158
Media Services Medpro 2	135.9.184.159
Media Services Medpro 3	135.9.184.160
Media Services Medpro 4	135.9.184.161

Next steps

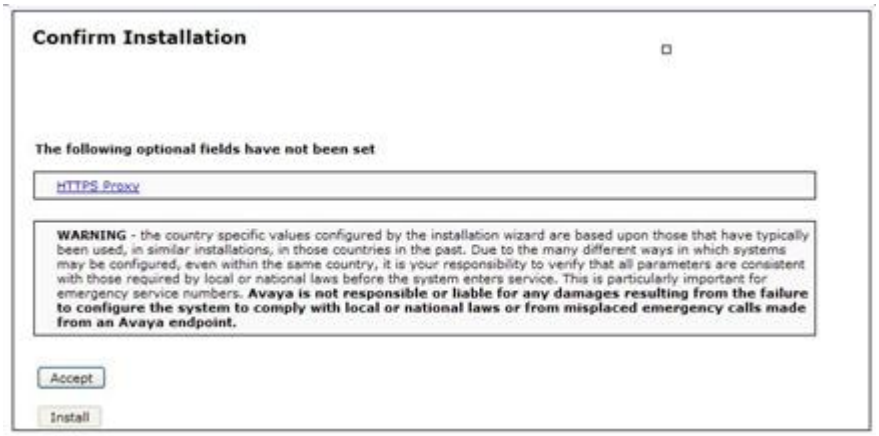
Confirm installation.

(Optional) Save configuration (if you are using standalone pre-installation wizard).

Confirming installation

Procedure

1. On the Confirm Installation page, click **Accept** to accept the warning message. The system enables the **Install** option.



2. Click **Install** to start installing the template.

Result

After proceeding from the configuration section of the wizard the installation then downloads, starts and configures the virtual machines. The screen is updated with the progress of each section. This process takes approximately 30 - 90 minutes depending on system size (average time is about 40 minutes). During this time the system requires no extra input and you can spend this time in deploying the phones or administering the gateways.



09:53:50	-- Download/Install aes	Complete	100	6m 53s
10:00:43	-- Download/Install ses	Complete	100	3m 37s
10:04:20	-- Download/Install utility_server	Complete	100	3m 35s
10:07:56	Assign Dedicated NIC	Complete	100	57s
10:08:53	-- Download/Install cobar	Complete	100	3m 52s
10:12:58	Start all VMs	Complete	100	1m 18s
10:14:16	Wait until system and all VMs are stabilised	Complete	100	1m 4s

Run post-install plugin if present
- CM:Configuring CM
- CM:Checking ssh connection to CM
- US:Configuring Utility Server
- US:Checking ssh connection to US
- SES:Configuring SES
- SES:Checking ssh connection to SES
- AES:Configuring AES
- AES:Checking ssh connection to AES
- CMM:Configuring CMM
- CMM:Downloading Language rpm
- CM:Connecting to CM
- SES:Connecting to SES
- US:Copying authentication file to US
- AES:Checking AES database is up
- CM:Waiting for CM to come up.
- SES:Waiting for SES to come up.
- US:Installing authentication file
- AES:Adding switch
- CM:CM is up.
- CM:Adding tmpuser login to CM
- US:Authentication file loaded.
- US:Configuring phone settings file
- SES:Waiting for SES to come up.
- CM:Adding customer login to CM
- SES:Waiting for SES to come up.
- AES:Adding switch password
- AES:Adding switch connection
- US:Finished phone settings file configuration.
- US:Configuring ESD settings file
- CMM:Loading and Installing Language rpm
- CM:Copying authentication file to CM
- SES:SES is up.
- SES:Adding Customer login
- CM:Installing authentication file
- AES:Restarting MVAP service
- CM:Saving CM translations

Note:

Do not attempt to configure the virtual machines (for example, Communication Manager using SAT) while the post installation process is in progress. All the applications are configured at this stage. Attempting to configure the system too early may result in your changes being lost or the wizard being blocked from completing its tasks.

If there is any error during the process, the system displays the error on screen in bold letters together with a warning symbol in the extreme right column in the screen. Investigate such a message immediately. The error may be very minor and may not effect the overall success of the installation or may require some corrective action which may be a reinstallation.

After system loads the machines and configures them, you can proceed to test the installation.

Next steps

Perform post-installation tasks for MBT.

(Optional) Check the troubleshooting steps if the installation is not successful.

Chapter 7: (Optional) Configuring Media Services

Use this section only if you have installed MBT with Media Services.

The MBT installation wizard performs the basic configuration of Media Services during MBT installation. If you want to configure advanced features of Media Services and test the Media Services configuration, see the Administering Media Services section in *Administering Avaya Aura™ Solution for Midsize Enterprise* for the detailed procedures.

Note:

Media Services has a dedicated Ethernet port. Check that a CAT5 Ethernet cable is connected to the Media Services port in the server. See the Connecting to server and network section in *Installing and Configuring Avaya Aura™ System Platform* for more information.

Configuring Media Services integrated announcement

About this task

Media Services offers an integrated announcement feature. This feature is not configured by the MBT installation wizard. To use the Media Services integrated announcement feature, you must configure the feature.

See the Administering Media Services section in *Administering Avaya Aura™ Solution for Midsize Enterprise* for the detailed procedures.

Chapter 8: Registering the system

About this task

Registering System Platform and applications in the solution template ensures that Avaya has a record of the system and it is ready for remote support if needed.

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In the context of System Platform, managed devices are the components of System Platform and of the applications that are included in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

Note:

- For a description of any elements you must register along with your Solution Template, refer to your Avaya Aura® solution documentation.
- For solutions being deployed in a System Platform High Availability configuration, you must register two VSP solution elements, one for the primary server and one for the secondary server in the HA pair. For a description of any other solution elements you must register for the various System Platform High Availability deployments, refer to your Avaya Aura® solution documentation.

Registrations are performed in two stages: before installation of System Platform, the solution template, and SAL Gateway and after installation. The first stage of registration provides you with the SE IDs and Product Identifications required to install the products. The second stage of the registration makes alarming and remote access possible.

Procedure

1. Access the registration form and follow the instructions. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Avaya Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.
2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date.

   Provide the following:

   - Customer name
   - Avaya Sold-to Number (customer number) where the products will be installed

- Contact information for the person to whom the registration information should be sent and whom Avaya can contact if any questions arise
- Products that are included in the solution template and supporting information as prompted by the form

Avaya uses this information to register your system. When processing of the registration request is complete, Avaya sends you an e-mail with an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices.

3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

Chapter 9: Troubleshooting MBT installation

DVD does not read

Troubleshooting steps

About this task

The DVD may be corrupted or the DVD player may be failing.

Procedure

Burn another DVD or try loading the files from a USB flash drive.

Media services not working

Troubleshooting steps

Procedure

Check that the eth3 dedicated NIC connection is connected on the right network.

Service port not working

Troubleshooting steps

Procedure

1. Recheck the connection process.
2. Ensure that web browser proxy is turned off.

System time drifts over a period of weeks

Troubleshooting steps

Procedure

Use an NTP clock source through system platform to time sync.

Appendix A: Installation prerequisites for MBT -Worksheets

Hardware requirement worksheet

Requirement	Description	✔
Bootable DVD or USB flash drive	Contains the MBT installer files provided by Avaya or downloaded from PLDS (Product Licensing and Delivery System) Web site, http://plds.avaya.com.	✔
CAT5 Ethernet cable for gateway configuration.	See Connecting to server and network section in *Installing and Configuring Avaya Aura™ System Platform* for more information.	
Verify that an S8510 Server or S8800 Server with System Platform, or two S8510 Servers or S8800 Servers with System Platform and other required configuration are available for simplex and High Availability Failover configuration respectively.	See *Installing and Configuring Avaya Aura™ System Platform* for more information.	

Installation prerequisites for MBT – mandatory items worksheet

Note:

Contact Avaya Services team to get the Alarm IDs for System Platform, Communication Manager, Communication Manager Messaging, Application Enablement Services, and SIP Enablement Services.

Requirement/ component/machine name	Value/requirement	Notes
Subnet mask		
Default gateway IP address		
DNS server IP address		
Gateway Serial Numbers		
Alarm ID for System Platform		
Alarm ID for Communication Manager		
Alarm ID for Communication Manager Messaging		
Alarm ID for Application Enablement Services		
Alarm ID for SIP Enablement Services		
List of adjuncts to be integrated with Midsize Business Template		

Installation prerequisites for MBT – optional items worksheet

Requirement/ component/machine name	Value/requirement	Notes
IP address and port number of the Web proxy server		If your access to internet is through a proxy server. This is particularly important for SAL (alarming and remote access).
Range of IP addresses for IP phones		If you plan to use DHCP server on the Midsize Business TemplateUtility Services.

Requirement/ component/machine name	Value/requirement	Notes
ABIT file		If you plan to use ABIT for importing station data. You can download the ABIT files from the standalone pre-installation wizard or Avaya Support Web site. Enter ABIT in the **Search** field to search for the ABIT file. Ensure that the **MBT – Station Data** tab is selected when entering data for an Midsize Business Template system.
DNS domain name		If you want to specify the hostnames in the *long* format.
Customer SIP domain		If you plan to use SIP Enablement Services.
Customer SES DNS domain		If you plan to use SIP Enablement Services.
Topology map of customer's network.		
User name and password for *admin*		For customer access to System Platform and Midsize Business Template through internal LDAP
User name and password for *cust*		For customer access to System Platform and Midsize Business Template through internal LDAP
User name and password for accessing Communication Manager		Required to allow direct access without using internal LDAP.
User name and password for accessing SIP Enablement Services		Required to allow direct access without using internal LDAP.
Documentation minimums		

IP addresses worksheet for MBT with Media Services

Requirement/ component/machine name	Value/requirement	Notes
System Domain (Dom-0) IP address		
Console Domain IP address		
Communication Manager IP address		
Communication Manager Messaging IP address		
Utility Services IP address		
Application Enablement Services IP address		
SIP Enablement Services IP address		
Media Services IP address		
Medpro IP address 1		
Medpro IP address 2		
Medpro IP address 3		
Medpro IP address 4		
System Domain (Dom-0) IP address for High Availability Failover configuration		
Console Domain IP address for High Availability Failover configuration		
Media Gateway IP address		Write one IP address per Media Gateway.

IP addresses worksheet for MBT without Media Services

Requirement/ component/machine name	Value/requirement	Notes
System Domain (Dom-0) IP address		
Console Domain IP address		
Communication Manager IP address		
Communication Manager Messaging IP address		
Utility Services IP address		
Application Enablement Services IP address		
SIP Enablement Services IP address		
System Domain (Dom-0) IP address for High Availability Failover configuration		
Console Domain IP address for High Availability Failover configuration		
Media Gateway IP address		Write one IP address per Media Gateway.

VPN gateway worksheet

Requirement/ component/machine name	Value/requirement	Notes
Public IP address for VPN gateway		Modems are not supported on System Platform. Business Partners who require remote access to the system and do not have a method already set up will need to use a VPN gateway to access the system.
Private IP address for VPN gateway		

Appendix B: Post Installation Tasks for MBT

Communication Manager checks and tests

Task	Notes	✔
Verify the server health, status and major/minor alarms.		
Verify date and time.		
Verify the Communication Manager version and service pack activation.		
Verify License Mode: Normal.		

Communication Manager Messaging checks and tests

Task	Notes	✔
Dial into voice mail and verify that the correct language file (that is, US English, UK English, German and so on) has been installed.		
Call busy/unattended station and leave a voice mail.		
Verify that MWI light is on when voice mail is left.		
Verify that voice mails can be retrieved successfully through TUI.		
Verify that voice mails can be retrieved successfully through the Message Manager (if applicable).		
Verify IMAP integration (if applicable).		

Application Enablement Services checks and tests

Task	✔
Check the status with **Switch Conn Summary** under **Status and Control**. Verify that the status of **Connection State** is set to **Talking**.	

SIP Enablement Services checks and tests

Applicable only if SIP Enablement Services is enabled.

Task	Notes	✔
Go to Maintenance page, and then click on **Process Status** and verify that all the processes are **UP**.		
Make a call to from a SIP endpoint to a non-SIP endpoint (assuming SIP endpoint are installed).		
Make call to from a non-SIP endpoint to a SIP endpoint (assuming SIP endpoint are installed).		
Make external call through a SIP trunk from a non-SIP endpoint (assuming SIP trunk configured).		
Make an external call through a SIP trunk to from a SIP endpoint (assuming SIP trunk configured).		
Make call to a busy SIP endpoint and leave a voice mail. Verify that the MWI light is on when the voice mail is left..		

Utility Services checks and tests

Task	Notes	✔
If internal DHCP server is being used: Verify through the Utility Services web console that the DHCP server is running.		
If internal IP phone file server is being used: Click on the **File Server** link to verify through the Utility Services web console that the IP phone file server is running (if internal IP phone file server is being used).		
If internal DHCP server is being used: Connect an IP phone to part of the network served by the Utility Services's DHCP server. Verify that the phone comes up and make a test call. If the phone doesn't come up correctly, reset it to factory defaults and try again.		
If internal DHCP and IP phone file server are being used: - Connect an IP phone to part of the network served by the Utility Services's DHCP server. Verify that the phone comes up and make a test call. View the file server log files from the Utility Services's web console and verify that the correct upgrade and setting files were both served to the IP address of the phone by the file server		
MyPhone: Verify that WML features work correctly on IP phones (if this feature has been enabled in MyPhone admin).		
MyPhone: Verify that the LDAP server is correctly configured on the MyPhone admin page and that the WML directory feature works as expected from IP phones (if this feature has been enabled in MyPhone admin).		
MyPhone: Verify that the MyPhone user link is accessible from Utility Services main page.		

Remote access checks and tests

Task	Notes	✔
Verify that the Midsize Business Template system is accessible through Secure Access Link and the VPN Gateway (if applicable).		

Alarming checks and tests

Applicable only if Alarming is enabled.

Task	Notes	✔
Verify that all Secure Access Link alarming parameters are configured correctly and generate test alarms. The tests procedures for each of the components that support alarming are as follows: Communication Manager and SIP Enablement Services: Type the command ‘testinads’ in the Command Line Interface and check Maestro for an alarm report. Application Enablement Services: Type ‘logger -t mon -i "High CPU" ‘ in the Command Line Interface and check Maestro for an alarm report. System Platform: Generate an alarm through the System Platform Management Console on Console Domain and check Maestro for an alarm report.		

Media Services checks and tests

Note:

The following checks and tests are applicable only if Media Services is enabled.

Task	Notes	✔
Verify License Mode: Normal. Access the WebLM server on the System Platform Console Domain and verify under Licensed Products that the Media Services feature was licensed and the license was acquired.		
Verify that Media Services is connected to Communication Manager. Run the **`list ipserver-interface`** command on SAT and verify that the value for **Serv State** field is set to *IN*.		
Run the **`list config`** command and verify that all the required packs are present.		
Verify that the network connectivity is present. Ping the IP address of each TN2302B media processor from a computer on the same subnetwork.		
Establish three to six party conferences between IP phones and IP trunks or disable shuffling on the ip-network-region screen and place test calls between two IP stations. Enable shuffling again after the test.		

Appendix C: Digit treatment

Incoming digit treatment

Incoming digits are sent by the trunk group's digit treatment processing to the ARS digit-conversion form of Communication Manager. Here, the digits are converted to Communication Manager extension numbers. The values administered by the wizard in the ARS digit-conversion form are derived from the wizard values as follows:

ars digit-conversion form *"Matching Pattern"* = "*" + wizard *"Number Digits"*

ars digit-conversion form *"Min"* = length of data in wizard *"Number Digits"* + 1

ars digit-conversion form *"Max"* = wizard *"Number Length"* + 1

ars digit-conversion form *"Del"* = wizard *"Delete"* + 1

ars digit-conversion form *"Replacement String"* = wizard *"Insert"*

Note:

For Germany, the data entered in the wizard is not actually associated with the trunk group in the *"Trunk Number"* field, since incoming digit routing is performed in the ARS digit-conversion form of Communication Manager.

The character "*" must not be prefixed to the digits entered in the *"Number Digits"* field in the pre-installation wizard. The character is automatically prefixed by the post-installation wizard when it adds the *"Number Digits"* data to the ars digit-conversion form. The "*" character is used to separate entries used for incoming digit processing from those used for outgoing ARS digit processing.

The wizard field *"Insert"* should be left empty.

You must correctly enter the total length of the incoming number which is to be routed.

You must enter data (*"Trunk Number"*, *"Number Length"*, *"Number Digits"*, *"Delete"*, and *"Insert"*) for as many incoming ISDN mappings as may be needed. The wizard will then add each mapping to the ARS digit-conversion form of Communication Manager.

Appendix D: LSP Configuration

Installing and configuring S8510 or S8800 server

About this task

Communication Manager within Midsize Business Template is licensed differently than standalone Communication Manager. As such, the setup process for LSPs subtending from an MBT Communication Manager main is slightly different. Those differences are covered in this section.

Note:

To install a new S8510 or S8800 server as an LSP, first complete the tasks in *Quick Start for Hardware Installation: Avaya S8500 Server*.

Complete the steps below as described in the S8500 installation documentation:

- Install the S8510 or S8800 server hardware in the 19-inch rack
- Connect the cables between the server and the network of the customer
- Connect the SAMP card and the modem
- Configure SNMP and the Ethernet switch
- Install Communication Manager
- Configure the S8510 or S8800 server

When you have completed these tasks, proceed with the following tasks:

Procedure

1. Licensing LSP through lsp-config on page 84.
2. Creating a super-user login on page 85.
3. Configuring the server manually on page 86.
4. Updating the SAMP firmware on page 87.
5. Configuring the modem on page 87.
6. Enabling network time servers on page 88.
7. Configuring the server as an LSP on page 89.

Licensing LSP through lsp-config

Procedure

1. Log in to the LSP command line interface.
2. Type **`lspconfig S M P`**.

   where

   `S` is the system ID (SID). The SID is the same as the SID of the main server. To check the SID on the main server, use the command **`systemid -x`**.

   `M` is the module ID (MID). MIDs for LSPs are assigned sequentially starting at 2. The main server has a MID of 1. The MID must be unique for the main server and all LSPs.

   `P` is the numeric platform type of the LSP. The numeric platform value to be used for LSP are as follows:

LSP Platform Type	Value of *platformtype* Command Argument
S8300 LSP in G250	19
S8300 LSP in G350	10
S8300 LSP in G430	27
S8300 LSP in G450	23
S8300 LSP in G700	9
S8500 LSP	21

3. Verify the SID by using one of the following methods:
   - From the command line interface, type **`statuslicense –v`**
   - From the SAT terminal, access the Optional Features form by typing **`display system-parameters customer-options`**. The SID is displayed on page one of the form.

   Note:

   The Universal Install/SAL Product Registration Request form requires the SID and MID for the main server and the LSP.
4. Reboot the LSP using one of the following commands:
   - From the command line type **`stop -r`**.
   - From the SMI Server Administration interface:

i. Select **Server** > **Shutdown Server** in the navigation pane.

ii. Ensure that **Delayed Shutdown** and **Restart server after shutdown** are selected on the Shutdown Server page.

iii. Click **Shutdown**.

iv. Click **OK** when prompted to confirm shutdown.

5. After the server restarts completely, log in to the command line interface, and type **`loadpwd`** to load the password file.

Creating a super-user login

About this task

Note:

Make sure you have a login name and password that the customer would like for the super-user login. If you are a business partner, you can also repeat this procedure to add the dadmin login.

Make sure the customer can change this login, its password, or its permissions later.

Procedure

1. On the System Management Interface, click **Administration > Server (Maintenance) > Administrator Accounts**.
2. Select **Add Login**.
3. Select **Privileged Administrator** and click **Submit**.
   The Administrator Accounts -- Add Login: Privileged Administrator screen appears.
4. In the **Login name** field, type a login name for the account.
5. In the **Primary group** field, **susers** appears.
6. In the **Additional groups (profile)** field, **prof18** appears (prof18 is the code for the customer super-user).
7. In the **Linux shell** field **/bin/bash** appears.
8. In the **Home directory** field, **/var/home/login name** appears (login name is the name you choose in step 4).
9. Skip the **Lock this account** and **Date on which account is disabled-blank to ignore** fields.
10. In the **Select type of authentication section**, choose **Password**.

Note:

Do not lock the account or set the password to be disabled.

11. In the **Enter key or password** field and the **Re-enter key or password** field, enter the password.
12. In the **Force password/key change on next login section**, leave the default to **no**.
13. Click **Submit**.

Configuring the server manually

About this task

Note:

If you are configuring the server as a main server, the license files and the authentication files must be downloaded on the server.

Important:

Be sure to set the date, time, and time zone *before* manually configuring the server. Failure to do so may cause network problems.

Procedure

1. From the Main Menu, under Server, click **Server Date/Time**.
2. In the Server Date/Time window, verify the date and time are correct. If the date and time are incorrect, do the following steps:
   - Enter the date in the format *mm/dd/yyyy*.
   - Enter the time in 24 hour format *(hh:mm)*.
   - Enter the time zone.
   - Click **Submit**.
   - Reboot the server. For more information, see Rebooting the server on page 91.

Updating the SAMP firmware

About this task

You might need to update the SAMP firmware if the most current version is not installed. Information about the versions that require updates should be included in your project planning information.

For how to update SAMP software, see *Using the Avaya Server Availability Management Processor (SAMP)*.

Procedure

1. Check the firmware version by doing the following steps:
   - Use SSH to access the server and log in.
   - Type `sampcmd samp-update status`.
   - Check the firmware version displayed..
2. If you need to update the firmware, on the Server Administration Interface under Miscellaneous, click **Download Files**.
3. Enter the information to copy the firmware file to the server.
4. Use SSH to access the server and log in.
5. Start the update process by typing`sampupdate`.
   The update process takes approximately 5 minutes.

Configuring the modem

Procedure

1. From the **Installation** menu of the System Management Interface, click **Configure Server**.
2. Click **Continue** until you get to the Specify how you want to use this wizard page.
3. Select **Configure individual services** and click **Continue**.
4. On the menu on the left, click **Set Modem Interface**.
5. Select **Change Modem Setting** and click **Continue**.

6. In the Extra Modem Initialization Commands window, type the initialization commands that are appropriate for your modem and the country of operation. Click **Help** for help on what to enter.
   For example, to change the country code to Japan, type `AT%T19,0,10`.
7. Click **Change**.
   The system displays a message that indicates that a modem route was added successfully.
8. Click **Close Window**.

Enabling network time servers

About this task

Important:

Avaya strongly recommends that you enable Network Time Protocol (NTP) and configure at least one network time server. If a network time server is not used, the Date/Time settings on the server must be reset regularly, at least monthly, using the System Management Interface. The network time strategy is determined by the network administrator.

With NTP, you can specify one, two, or three network time servers to provide the accurate time of day data to the clocks on the servers. The network time servers, in turn, get their source timing from one of several highly accurate time services that are available on the Internet.

To use a network time server, the NTP service must be enabled. The Avaya Installation Wizard prompts you to enable the NTP service. If you do not use the Installation Wizard, use the Configure Server function on the System Management Interface to configure the network time servers.

Procedure

1. From the **Installation** menu of the System Management Interface, click **Configure Server**.
2. On the Review Notices page and the Backup Up Data page, click **Continue**.
3. On the Specify how you want to use this wizard page, select **Configure individual services** and then click **Continue**.
4. In the menu on the left of the Configure Server page, click **Configure Timer Server**.
5. Enter the NTS information on the **Configure Time Server** screen and click **Change**.
6. On the main menu, under Security, click **Firewall**.
7. In the "Output from Server" column, select **ntp 123/udp**.

Note:

It is not necessary to enable the "Input to Server" ntp service. If this service is already enabled, you do not need to disable it.

When the Avaya Installation Wizard prompts you for information about the network time servers, enter the DNS name or the IP address for the primary network time server and the secondary and the tertiary time servers if any. If you enter a DNS name instead of an IP address for the network time server, you must specify the IP address of the DNS server on the DNS/ DHCP Web page.

Configuring the server as an LSP

About this task

Note:

Do not install the license file and the authentication file until you administer the primary controller. For more information, see Administering the main server on page 90.

Procedure

1. Open the Server Administration Interface and from the **Installation** menu, click **Configure Server**.
2. Select **Set Date and Time Zone**. You must set the time of the LSP to the same time zone as the primary controller even if the LSP is physically located in a different time zone.
3. Click **Continue** until you get to the How do you want to use the Wizard page.
4. Select the **Configure Individual Services**.
5. Select **Set Identities**
   - Enter the host name for the LSP..
   - In the **ID** field, check the Server ID (SVID) value. The primary controller is set to SVID 1. If the primary controller is a duplicated S8700-series Server, the server IDs are SVID 1 and SVID 2. The ID for an LSP must be greater than 2 and less than or equal to 256. Gaps in the numbering are allowed. For example, SVIDs can be 10, 20, 30, and so on.
   - In the **Control Network A** field, select the default **Ethernet 0**.
   - In the **Services Port** field, select the default **Ethernet 1**.
   - In the **Corporate LAN** field, select the default **Ethernet 0**.

- In the **Control Network B** field, select the default **unused**.
- In the **Assign a Processor Ethernet Interface** field, select **Corporate LAN**.

6. Click **Continue**.
7. On the Configure Interfaces Web page, enter the following IP addresses:
   - In the **IP address server1** field, enter the IP address for the LSP.
   - In the **Gateway** field, enter the IP address for the LAN gateway.
   - In the **Subnet mask** field, enter the subnet mask for the LSP
8. In the **Speed** field, select **Autosense**.
9. Click **Change**.
10. From the list in the left margin, select **Configure LSP/ESS**.
    - Select **This is a local survivable processor (LSP)**.
    - In the **Registration address** field, enter the IP address of a C-LAN that is administered and enabled in the translations of the primary controller. If the primary controller is an S8510 or S8800 server, this address can be the IP address of the Processor Ethernet of the primary controller.
    - In the **File Synchronization address at the main cluster** field, enter the physical IP address or addresses of the primary controller servers. These addresses must be connected to the corporate LAN. The IP address cannot be the address of a port that is assigned to a control network if the control network is dedicated to the IPSI connection. If the control network or the control networks are dedicated, enter the IP address of the port that is assigned to the corporate LAN.
11. Click **Change** to save your changes.

Administering the main server

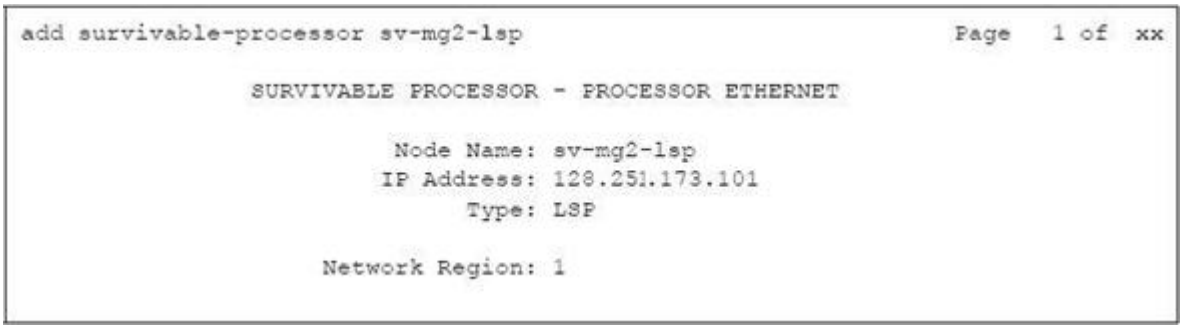
About this task

You must administer the primary controller so that the controller can identify and communicate with the S8510 or S8800 LSP.

Procedure

1. At the SAT command line, type change node-names ip name and press Enter, where name is the name of the LSP.
2. In the Name column, type the name of the LSP.
3. In the IP Address column, type the IP address of the LSP.

4. At the SAT command line, type add survivable-processor name and press Enter, where name is the LSP name from the Node Names screen. The system displays the Survivable Processor screen.



5. The Type field is automatically populated with LSP. LSP appears in the field if the node name is not associated with ESS.
6. Enter a network region for the LSP. The default is 1. However, a different network region might be better suited for the LSP to provide media gateway and IP telephone support.
7. On pages 2 and 3 of the screen, add any adjuncts that the LSP can support if a failover from the primary controller occurs.

   For how to administer the Survivable Processor form, see *Administrator Guide for Avaya Aura™ Communication Manager (03-300509)*.

Rebooting the server

Procedure

1. Click **Server > Shutdown Server**.
2. Select **Delayed Shutdown** and **Restart server after shutdown** .
3. Click **Shutdown**.
   You will be logged off the server when it reboots. When you are waiting for the system to reboot, enter `ping -t 192.11.13.6` from a command prompt window on your services laptop computer to start a continuous ping command.

Index

A

Alarm Id 35
alarming 35
    configuring 35
alarming checks and tests 78
alarming field descriptions 35

B

browser requirements 19

C

C-dom IP Address 25, 28, 54
Communication Manager checks and tests 75
configuring 23
    using embedded install wizard 23
configuring Media Services 63
configuring Media Services integrated announcement 63
configuring modem 87
configuring S8510 server 83
configuring S8800 server 83
configuring server 86, 89
    as LSP 89
country 31
    selecting 31
customer login 30, 57
    creating 30, 57
customer login field descriptions 31, 57

D

DHCP 32
    configuring 32
DHCP DNS Server IP address 33
DHCP field descriptions 33
DHCP leases display button descriptions 21
DHCP network address 33
DHCP pool IP address range 33
DHCP router address 33
DHCP subnet mask 33
DHCP WINS Server IP address 33
DNS 25, 28, 54
Domain-0 IP Address 25, 28, 54
DVD does not read 67

E

Embedded MBT Installation Wizard 19
EPW file 15, 20
    loading 20

G

Gateway IP Address 25, 28, 54
gateway type 37
gateways 36
    configuring 36
gateways button descriptions 37
gateways configuration 35
gateways field descriptions 37

H

hardware requirements 69
HTTPS Proxy 25, 28, 54

I

incoming digit treatment 81
installation 19, 50, 60
    confirming 50, 60
    using pre-installation wizard 19
installation checklist 8
installation prerequisites 11
IP Address 25, 28, 54
ip addresses for MBT installation 72, 73
    with Media Services 72
    without Media Services 73

L

legal notices 2
licensing 11
load files field descriptions 21
local and remote template 18
local survivable processor 84
    configuring 84
login name 31, 57
LSP 84

configuring 84

M

main server 90
administering 90
mandatory items for installing MBT 69
MBT 78
MBT.iso file 12
Media Services checks and tests 78
Midsize Business Template installation 7
minimal MBT installation 53
using embedded installation wizard 53

N

Network Mask 25, 28, 54
network settings 24, 53
Network Settings field descriptions 25, 28, 54
network time server 88
enabling 88
notices, legal 2

O

optional items for installing MBT 70

P

password 31, 57
PLDS 7, 12
preparing for installing midize business template 15
Product Licensing and Delivery System 12

R

re-type password 31, 57
rebooting server 91
registration 65
of system 65
remote access 78
Remote Access Network 34
Remote Access Network Subnet Mask 34

S

SAL 78
SAL Gateway 65
registering 65
SAMP firmware 87
updating 87
Search Local and Remote Template page 16
field descriptions 16
serial number 37
SES checks and tests 76
SIP 38
configuring 38
SIP domain 39
SIP Enablement Services 76
SIP field descriptions 39
solution template 65
registering applications 65
Standalone MBT Installation Wizard 19
station 43
configuring 43
station and voicemail configuration 39
station configuration 43, 44
summary 49, 59
reviewing 49, 59
super-user 85
System Platform 65
registering 65
system requirements 19

T

troubleshooting 67, 68
DVD does not read 67
media services not working 67
service port not working 67
system time drifts over a period of weeks 68
trunks 46
configuring 46
trunks button descriptions 48
trunks configuration 44
trunks field descriptions 47

U

Utility Server checks and tests 77

V

Virtual Appliance 25, 28, 54
Virtual Machine 15
Virtual Machine Management page 16
field descriptions 16
voice mail 43
configuring 43
voice mail configuration 43, 44
VPN access 33

configuring 33
VPN Access field descriptions 34
VPN gateway for MBT installation 74
VPN Router IP Address 34

W

WebLM 7