Installing and Configuring Avaya Aura™ System Platform

Release 6.0
June 2010

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

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product 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, AND 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). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (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(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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://www.avaya.com/support/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 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://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya Aura is a registered trademark of Avaya.

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

PuTTY is copyright 1997-2009 Simon Tatham.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: System Platform installation overview

Installation Process

Installation of System Platform consists of the following tasks:

1. Install the server hardware.
2. Connect the server to the customer's network.
3. Connect the two servers if using the High Availability Failover option.

   Connect both the servers with a Gigabit-certified Ethernet cable on the same ports on both machines.
4. Install the System Platform software on the server. If using the High Availability Failover option, install the System Platform software on the secondary server too.
5. Install the solution template.

   Important:

   If you are using the High Availability Failover option, do not install a solution template on the server that will serve as standby. If you do, you will not be able to start High Availability Failover. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability Failover.
6. Configure the Secure Access Link (SAL) gateway that is included in System Platform for remote support and alarming.

   Note:

   On High Availability Failover systems, configure the SAL Gateway only on the primary server. When you enable High Availability Failover, SAL Gateway will propagate to the standby server.
7. Configure High Availability Failover if using the option.

Software installation

To install System Platform, you must first download the ISO image from the Avaya PLDS Web site and then burn the ISO image to a DVD. Avaya recommends that you verify that the ISO image is not corrupt before you start the installation.

You can install the System Platform software by using either a:

- Laptop connected to the services port on the server.
- Video monitor, keyboard, and mouse connected to the appropriate ports on the server.

Note:

During the installation, you will need to boot the servers. The S8800 and the S8300D server takes in excess of 7 minutes to boot. The server is ready to boot when the power-on LED changes from a fast flashing state to a slow flashing state.

It is possible to complete the installation by using only a keyboard and monitor. If you do not have a mouse, use the Tab key to navigate between fields.

If you use a laptop to install the software, you must have a PuTTY SSH client and Telnet application installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server.

Use the provided worksheets and checklists during installation.

Related topics:

Configuring the laptop for direct connection to the server on page 20

Chapter 2: Installation requirements for System Platform

What Avaya provides

Avaya provides the following items for installing System Platform:

- One or two servers. One is for a standard configuration, and two are for High Availability Failover configuration.
- Slide rails to mount the servers in a rack.
- System Platform installation software.
- Other hardware as ordered, such as an uninterruptible power supply (UPS). UPS is a required component.
- Product registration form. The form is available on http://support.avaya.com. Click **More Resources** > **Equipment Registration (Partners only)**. Download the **Universal Install/SAL Product Registration Request Form** under **Non-Regional (Product) Specific Documentation**.

Note:

Avaya provides the System Platform installation software, which the customer must write on DVDs as a prerequisite to installing System Platform.

What customer provides

The customer must provide the following items for installing System Platform.

- Standard equipment rack properly installed and solidly secured.
- USB keyboard, USB mouse, and VGA monitor or laptop with an Ethernet crossover cable.

  Note:

  Depending on the capabilities of the network interface card in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.
- Gigabit-certified Ethernet cable for High Availability Failover.

- DVDs written with the software for installing .
- A computer that can route to the System Platform server that has Internet Explorer 7 or Firefox 2 or Firefox 3 installed on it.
- Filled-out worksheets with the system and network information needed for installation and configuration.
- (Optional) EPW and ABIT files.
- Access to the customer network.
- (Optional) VPN Gateway for providing remote access to Avaya Partners.

Note:

The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, uautf, uk, and us.

Avaya Partners must arrange for their own IP-based connectivity (for example, B2B VPN) to provide remote services. Modem connectivity is not supported.

Chapter 3: Preinstallation tasks for System Platform

Preinstallation checklist for System Platform

The preinstallation checklist given below will help to ensure that the installation is carried out efficiently. Before starting the installation, make sure that you complete the tasks from the preinstallation checklist.

No.	Task	Notes	✔
1	Complete and submit the Universal Install/SAL Product Registration Request form. When opening the Excel based form, click **Enable Macros**; otherwise, the form automation will not work. Submit the completed form using the built in e-mail button. See Registering the system on page 12. **Note:** Allow 48 business hours for a reply.	**Important:** Make sure that you perform this task at least 48 hours before installing System Platform and any solution template.	
2	Gather the required information relating to installation, such as IP configuration information, DNS addresses, and NTP server addresses. See Installation worksheet for System Platform on page 65.		
3	Download the System Platform installer ISO image file from PLDS. See Downloading software in PLDS on page 14.		
4	Download the appropriate solution template and licenses from PLDS. See Downloading software in PLDS on page 14.		
5	Verify that the downloaded ISO images match the images on the PLDS Web site.		

No.	Task	Notes	✔
	See Verifying the ISO image on a Linux-based computer on page 14 and Verifying the ISO image on a Windows-based computer on page 15.		
6	Write the ISO images to separate DVDs. See Writing the ISO image to DVD on page 16.		

Registering the system

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 applications that are included in a specific 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.

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 that you will need to install the products. The second stage of the registration makes alarming and remote access possible.

1. Download and follow the instructions in the registration form. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Equipment Registration (Partners only)**. At the bottom of the page, under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.

   The registration form consists of two pages.

2. Complete the first page and submit it at least two business days before the planned installation date to avoid delays.

   You need to 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 the SE IDs and Product ID numbers that you must enter in SAL Gateway to add managed devices.

3. Complete and submit the second page after the installation is complete.

Related topics:

SAL Gateway on page 39

Registering for PLDS

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site (https://plds.avaya.com).
   You will be redirected to the Single sign-on (SSO) Web site.
2. Log in to SSO using SSO ID and Password.
   You will be redirected to the PLDS registration page.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Link ID, send an e-mail to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License Authorization Code (LAC)
4. Click **Submit**.
   Avaya will send you the PLDS access confirmation within one business day.

Downloading software in PLDS

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Select **Assets** from the Home page and select **View Downloads**.
4. Search for the downloads available using one of the following methods:
   - By Actual Download name
   - By selecting an Application type from the drop-down list
   - By Download type
   - By clicking **Search Downloads**
5. Click the download icon from the appropriate download.
6. When the confirmation box displays, select **Click to download your file now**.
7. If you receive an error message, click on the message, install Active X, and continue with the download.
8. When the security warning displays, click **Install**.

   When the install is complete, PLDS displays the downloads again with a checkmark next to the downloads which have been completed successfully.

Verifying the downloaded ISO image

Verifying the ISO image on a Linux-based computer

Prerequisites

Download any required software from PLDS.

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Linux-based computer.

1. Enter `md5sum filename`, where *filename* is the name of the ISO image. Include the .iso file extension in the filename.
2. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
3. Ensure that both numbers are the same.
4. If the numbers are different, download the ISO image again and reverify the md5 checksum.

Verifying the ISO image on a Windows-based computer

Prerequisites

Download any required software from PLDS.

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Windows-computer.

1. Download a tool to compute md5 checksums from one of the following Web sites:
   - http://www.md5summer.org/
   - http://zero-sys.net/portal/index.php?kat=70
   - http://code.kliu.org/hashcheck/

   Note:
   Avaya has no control over the content published on these external sites. Please use the content only as reference.
2. Run the tool on the downloaded ISO image and note the md5 checksum.
3. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
4. Ensure that both numbers are the same.
5. If the numbers are different, download the ISO image again and reverify the md5 checksum.

Writing the downloaded software to DVD

DVD recommendations

Avaya recommends use of high quality, write-once, blank DVDs, such as Verbatim DVD-R or DVD+R. Multiple rewrite DVDs are prone to error and should not be used.

When writing the data to the DVD, Avaya recommends a slower write speed of 4X or at a maximum 8X. Attempting to write to the DVD at higher or the maximum speed rated on the disc is likely to result in write errors.

Note:

If the software files you want to write on media are less than 680 Mb in size, you can use a CD instead of a DVD.

Writing the ISO image to DVD

Prerequisites

1. Download any required software from PLDS.
2. Verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

This procedure requires a computer or server that has a DVD writer and software that is capable of writing ISO images to DVD.

Important:

When the ISO image is being written to the DVD, do not run other resource-intensive applications on the computer. Any application that uses the hard disk intensively can cause a buffer underrun or other errors, which can render the DVD useless.

Write the ISO image of the installer to a DVD.

Chapter 4: Installing System Platform

Installation methods

You can install the System Platform software by using either a:

- Laptop connected to the services port on the server.
- Video monitor, keyboard, and mouse connected to the appropriate ports on the server.

Note:

It is possible to complete the installation by using only a keyboard and monitor. If you do not have a mouse, use the Tab key to navigate between fields.

If you use a laptop to install the software, you must have a PuTTY SSH client and Telnet application installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server.

Installation checklist for System Platform

Use this checklist to install System Platform.

Important:

If you are using the High Availability Failover option, install the same version of System Platform on both servers.

No.	Task	Notes	✔
1	If you are installing System Platform from a laptop, perform the following tasks: • Ensure that a Telnet and Secure Shell application are installed on the laptop. Avaya supports use of the open source Telnet/SSH client application PuTTY. • Configure the IP settings of the laptop for direct connection to the server.		

No.	Task	Notes	✔
	See Configuring the laptop for direct connection to the server on page 20. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Internet Explorer on page 21 or Disabling proxy servers in Firefox on page 21 .		
2	Connect your laptop to the services port with an Ethernet crossover cable.	If you do not have a crossover cable, you can use an IP hub. **Note:** Depending on the capabilities of the network interface card in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.	
3	Turn on the server.		
4	Place the DVD into the DVD drive on the server. See Starting the installation from your laptop on page 22 or Starting the installation from the server console on page 23 depending on your selection of installation method.		
5	If using your laptop to install System Platform, verify the media within the System Platform installation wizard. If using the server console to install System Platform, enter the **`vspmediacheck`** command and press **Enter**. The **`vspmediacheck`** command verifies that the image on the System Platform DVD is not corrupt. See Starting the installation from your laptop on page 22 or Starting the installation from the server console on page 23 depending on your selection of installation method.		
6	If using your laptop to install System Platform, establish a Telnet connection to the server. See Starting the installation from your laptop on page 22.		

No.	Task	Notes	✔
7	Select the required keyboard type. See Selecting the type of keyboard on page 24.		
8	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 25.		
9	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 25.		
10	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 28.		
11	Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 29.		
12	Configure the date and time or set up NTP server for the System Platform server. See Configuring the date and time for the System Platform server on page 29.		
13	Configure the System Platform passwords. See Configuring System Platform passwords on page 30.		
14	Verify access to the System Platform Web Console. See Verifying installation of System Platform on page 32.		
15	Check for System Platform patches at http://support.avaya.com. Install any patches that are available.		
16	Install a solution template. See Installing a solution template on page 54.	**Important:** If you are using the High Availability Failover option, do not install a solution template on the server that will serve as standby. If you do, you will not be able to start High Availability Failover. If you are using a bundled System Platform installation (with a	

No.	Task	Notes	✔
		solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability Failover.	
17	Configure the SAL gateway for remote access and alarming. See SAL Gateway on page 39.		
18	If applicable, configure System Platform High Availability Failover. See Configuring High Availability Failover on page 59.		

Connecting your laptop to the server

Configuring the laptop for direct connection to the server

You must manually configure the IP address, subnet mask, and default gateway of the laptop before you connect the laptop to the server.

Note:

The following procedure is for Windows XP. The procedure may differ slightly for other versions of Windows.

1. Click **Start** > **Control Panel**.
2. Double click **Network Connections** > **Local Area Connection**.
3. In the Local Area Connection Status dialog box, click **Properties**.
4. In the **This connection uses the following items** box, click **Internet Protocol (TCP/IP)**.
5. Click **Properties**.
6. In the Internet Protocol (TCP/IP) Properties dialog box, select **Use the following IP address** on the **General** tab.

Warning:
Do not click the **Alternate Configuration** tab.

7. In the **IP address** field, type `192.11.13.5`.
8. In the **Subnet mask** field, type `255.255.255.252`.
9. In the **Default gateway** field, type `192.11.13.6`.
10. Click **OK**.

Disabling proxy servers in Internet Explorer

To connect directly to the services port, you must disable the proxy servers in your Internet Explorer Web browser.

1. Open your Internet browser.
2. Click **Tools** > **Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**.
5. Clear the **Use a proxy server for your LAN** option. Select the option when you have to enable the proxy server.
6. Click **OK** to close each dialog box.

Disabling proxy servers in Firefox

To connect directly to the services port, you must disable the proxy servers in your Firefox Web browser.

Note:
This procedure is for Firefox on a Windows-based laptop. The procedure may differ slightly if your laptop is running Linux or another operating system.

1. Open your Internet browser.
2. Click **Tools** > **Options**.

3. Select the **Advanced** option.
4. Click the **Network** tab.
5. Click **Settings**.
6. Select the **No proxy** option.
7. Click **OK** to close each dialog box.

Starting the installation

Starting the installation from your laptop

Prerequisites

- A Telnet/SSH application such as, PuTTY is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

1. Connect your laptop to the services port with an Ethernet crossover cable.
   If you do not have a crossover cable, you can use an IP hub.

   Note:
   Depending on the capabilities of the network interface card in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.
2. Turn on the server.
3. Insert the System Platform DVD in the server's DVD drive.
   The server boots from the DVD.
4. Verify that the laptop can ping the service port by performing the following steps:
   a. Click **Start** > **Run**.
   b. Type `ping -t 192.11.13.6`

Note:

Allow sufficient time for the `ping` command to return continuous responses before proceeding to the next step.

5. Open a PuTTY session by performing the following steps:

   Important:

   If you use a Telnet client other than PuTTY, or if you forget to set the proper terminal emulation for the PuTTY client, the system might not display the Keyboard Type screen correctly. This screen problem does not affect the installation.

   a. Open the PuTTY application.
   b. In the **Host Name** field, enter `192.11.13.6`.
   c. Under **Connection type**, select **Telnet**.
   d. Under **Window** in the left navigation pane, select **Translation**.
   e. Under **Received data assumed to be in which character set** , select **UTF-8** from the list.
   f. Click **Open** to open a PuTTY session.

   The system displays the Keyboard Type screen.

Next steps

Select the required keyboard type. See Selecting the type of keyboard on page 24.

Related topics:

Connecting to the server through the services port on page 33

Starting the installation from the server console

Prerequisites

Connect a USB keyboard, USB mouse, and video monitor to the server.

1. Turn on the server.
2. Insert the System Platform DVD in the server's DVD drive.
   The server boots up from the System Platform DVD and displays the Avaya screen.
3. Within 30 seconds of the system displaying the Avaya screen, type **`vspmediacheck`** at the boot prompt and press **Enter**.

The **vspmediacheck** command verifies that the image on the System Platform DVD is not corrupt.

Important:

If you do not press **Enter** or type **vspmediacheck** within 30 seconds of the system displaying the Avaya screen, the system disables installation through the server console and enables installation through the services port. The system then displays the Waiting for Telnet connection screen, so you can connect to the server through Telnet. At this point, if you want to install through the server console, reset the server to restart the installation.

The system displays the Keyboard Type screen.

Next steps

Select the required keyboard type. See Selecting the type of keyboard on page 24.

Selecting the type of keyboard

On the Keyboard Type screen, select the type of keyboard that you have.

Note:

The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, ua-utf, uk, and us.

- The CD Found screen is displayed if you:

  - are installing System Platform from the server console and entered the **vspmediacheck** command at the boot prompt, or

  - are installing System Platform from a laptop

  See Verifying the System Platform image on the DVD on page 25.

- The System Domain Network Configuration screen is displayed if you are installing System Platform from the server console and did not enter the **vspmediacheck** command at the boot prompt. See Configuring network settings for System Domain (Domain-0) on page 25.

Next steps

- Verify that the System Platform image was copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 25.

OR

- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 25

Verifying the System Platform image on the DVD

Use this procedure to verify that the System Platform image was copied correctly to the DVD.

The CD Found screen is displayed if you:

- are installing System Platform from the server console and entered the **vspmediacheck** command at the boot prompt, or
- are installing System Platform from a laptop

On the CD Found screen, use the **Tab** key to select **OK** to test the DVD, or select **Skip** to skip the test and begin the installation immediately.

If you choose to test the DVD, the system displays another screen with a progress bar and the percentage of completion. After the test is complete, the system displays whether the image passed the test.

Note:

If the DVD you are using is corrupt, you must write a new DVD with the System Platform image. Before using the new DVD, make sure that you restart the server.

The System Domain Network Configuration screen is displayed.

Next steps

Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 25.

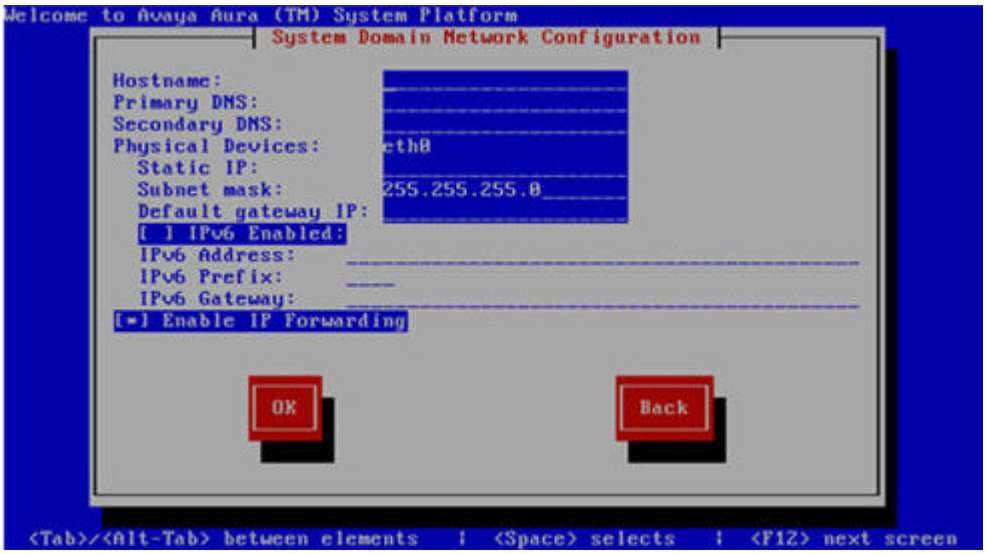
Related topics:

Writing the ISO image to DVD on page 16

Configuring network settings for System Domain (Domain-0)

1. On the System Domain Network Configuration screen, complete the following fields:

- Hostname. Enter a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
- Primary DNS
- (Optional) Secondary DNS



2. Perform the following steps to configure the interface that is connected to the customer network:
   a. Use the Tab key to highlight the **Physical Devices** field.
   b. Complete the **Static IP** field.
   c. Modify the subnet mask if necessary. The server displays a default value of 255.255.255.0.
3. Complete the **Default gateway IP** field.
4. Use the Tab key to highlight the **IPv6 Enabled** field. Press the Space bar to either enable or disable entering IP addresses in IPv6 format.
5. If you have enabled IPv6, fill in the following fields:
   - **IPv6 Address**
   - **IPv6 Prefix**
   - **IPv6 Gateway**
6. Use the Tab key to highlight the **Enable IP Forwarding** field. Press the Space bar to either enable or disable the IP forwarding as desired.

Note:
IP forwarding is enabled by default and is denoted by an asterisk (* character).

7. Use the Tab key to highlight **OK** and press **Enter** to accept the configuration.
8. If IP forwarding is enabled, a confirmation message is displayed. Use the Tab key to highlight **OK** and press **Enter**.
   The System Platform Console Domain Network Configuration screen is displayed.

Next steps

Configure network settings for Console Domain. See Configuring network settings for Console Domain on page 28.

Related topics:

System Domain Network Configuration field descriptions on page 27

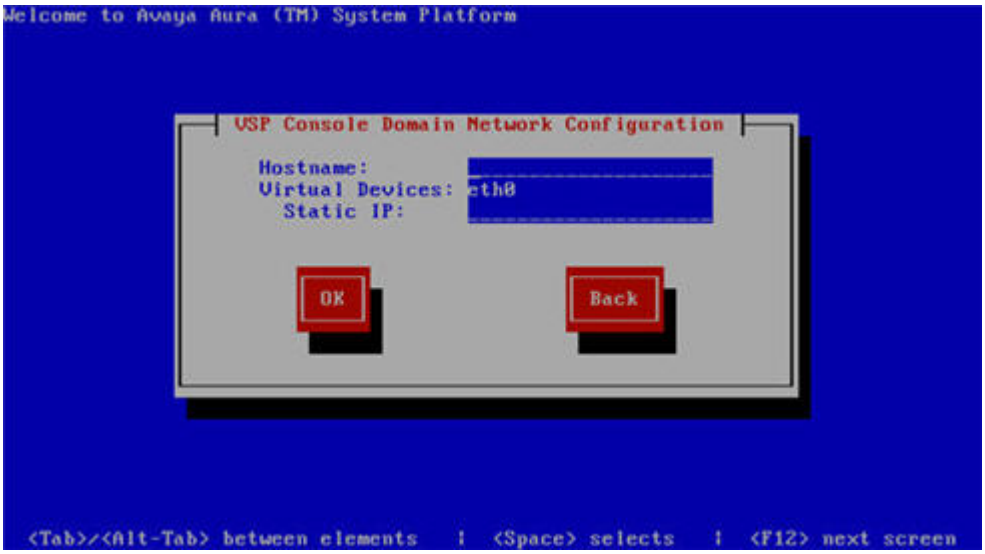
System Domain Network Configuration field descriptions

Name	Description
Hostname	The host name for System Domain (Dom-0). This must be a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
Primary DNS	The primary DNS server address.
Secondary DNS	(Optional) The secondary DNS server address.
Physical Devices	This field displays the physical Ethernet interface (NIC) that connects to the customer network. You must configure this interface for IP. The specific Ethernet interface number depends on the server model being used.
Static IP	The static IP address for the Ethernet interface that connects to the customer network.
Subnet Mask	The subnet mask for the Ethernet interface that connects to the customer network.
Default gateway IP	The default gateway IP address. This default gateway IP address will be used for all the virtual machines if you do not specify gateway IP addresses for them.
IPv6 Enabled	The indicator whether or not the IP addresses required by System Platform needs to be IPv6-compliant.
IPv6 Address	The IPv6–compliant IP address of System Domain.
IPv6 Prefix	The IPv6 prefix for **IPv6 Address**.
IPv6 Gateway	The IPv6–compliant gateway IP address of System Domain.
Enable IP Forwarding	The indicator whether or not IP forwarding is enabled. An asterisk on the left of the field denotes that IP forwarding is enabled.

Name	Description
	IP forwarding enables access through the services port to virtual machines on System Platform, including System Domain and Console Domain. IP forwarding must be enabled for both SSH and Web Console access.

Configuring network settings for Console Domain

1. On the VSP Console Domain Network Configuration screen, complete the following fields to set up the Console Domain network:
   - **Hostname**. Enter a fully qualified domain name (FQDN), for example, SPCdom.mydomainname.com.
   - **Static IP**



2. Select **OK** and press **Enter** to accept the configuration and display the Time Zone Selection screen.

Next steps

Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 29.

Related topics:

System Platform Console Domain Network Configuration field descriptions on page 29

System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	The host name for the Console Domain. This must be a fully qualified domain name (FQDN), for example, SPCdom.mydomainname.com.
Static IP	The IP address for the Console Domain. **Note:** The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System Domain (Domain-0). As System Domain acts like a bridge, the IP address that you enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).

Configuring the time zone for the System Platform server

1. On the Time Zone Selection screen, select the time zone in which the server is located.
2. Select **OK** and press **Enter** to accept the configuration and display the Date/Time and NTP setup screen.

Next steps

Configure date and time for the System Platform server. See Configuring the date and time for the System Platform server on page 29.

Configuring the date and time for the System Platform server

1. If you are not using an NTP server, set the current date and time on the Date/Time and NTP setup screen.

Tip:

Avaya recommends that you use an NTP server within your network to synchronize the time of the System Platform server.

Note:

Ensure that the time set here is correct. Changing the time in a virtual machine environment requires rebooting the virtual machines. Therefore, Avaya recommends setting the time correctly on this screen during the installation

2. If you are using an NTP server, perform the following steps on the Date/Time and NTP setup screen:
   a. Select **Use NTP** if you are using one or more NTP (Network Time Protocol) servers.
   b. In the **NTP server** fields, enter the DNS name or the IP address of your preferred NTP server(s).
3. Select **OK** and press **Enter** to accept the configuration and display the Passwords screen.

Next steps

Configure System Platform passwords. See Configuring System Platform passwords on page 30.

Configuring System Platform passwords

Prerequisites

Configure the date and time for the System Platform server.

1. On the Passwords screen, enter new passwords for all logins. You must enter each password twice to ensure that you are not making any mistakes in typing.

   If you do not enter new passwords, the defaults are used. The following table shows the default password for each login.

Login	Default password	Capability
root	root01	Advanced administrator
admin	admin01	Advanced administrator
cust	cust01	Normal administrator

Login	Default password	Capability
manager (for ldap)	root01	Administrator for the System Platform local LDAP directory. System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Important:

Avaya highly recommends that you enter new passwords instead of using the default passwords. Make a careful note of the passwords that you set for all logins. Passwords must be at least six characters long. Avaya recommends using uppercase and lowercase alphabetic characters and at least one numeral or special character.

Note:

The Avaya Services craft login uses Access Security Gateway (ASG) for authentication. If you are using the craft login, you must have an ASG tool to generate a response for the challenge that is generated by the login page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. An Avaya Services representative will use Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative will use those keys to generate the response for the challenge generated by the login page.

2. Select **OK** and press **Enter** to accept the passwords and continue the installation.

Result

The installation takes approximately 5 minutes. During this time, you can see the Package Installation page with progress bars, followed by the Running page, as the system completes the post-install scripts. After the installation is completed, the system ejects the DVD and reboots the server. If you are installing from server console, the system displays the Linux login page for System Domain (Domain-0) after the reboot.

Important:

If the DVD does not eject automatically, eject if manually. The system restarts the installation if the DVD is not ejected.

Next steps

Verify System Platform installation. See Verifying installation of System Platform on page 32.

Related topics:

Passwords field descriptions on page 32

Passwords field descriptions

Note:

Passwords must be at least six characters long. Avaya recommends using uppercase and lowercase alphabetic characters and at least one numeral or special character.

Name	Description
root Password	The password for the root login.
admin Password	The password for the admin login.
cust Password	The password for the cust login.
ldap Password	The password for the ldap login. System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Verifying installation of System Platform

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding.

Important:

You must wait approximately 15 to 20 minutes after the installation finishes to perform this procedure. The first boot process for Console Domain can take up to 20 minutes. You cannot access Console Domain until the first boot process is finished.

After completing installation of System Platform, perform this procedure to check for problems with the installation.

1. Access the System Platform Web Console. See Accessing the System Platform Web Console on page 35.
2. Perform the following steps to log in to Console Domain as `admin`:
   a. Start PuTTY from your computer.
   b. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.
   c. In the **Connection type** field, select **SSH**, and then click **Open**.
   d. When prompted, log in as `admin`, and type the password that you entered for the admin login during System Platform installation.
   e. Type `exit` to exit Console Domain.
3. Perform the following steps to log in to Console Domain as `cust`:
   a. Start PuTTY from your computer.
   b. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.
   c. In the **Connection type** field, select **SSH**, and then click **Open**.
   d. When prompted, log in as `cust`, and type the password that you entered for the cust login during System Platform installation.
   e. Type `exit` to exit Console Domain.

Important:
If you cannot log in to Console Domain as `admin` or `cust` or access the System Platform Web Console, contact Tier 3 Engineering.

Accessing System Platform

Connecting to the server through the services port

Prerequisites

- A Telnet/SSH application such as, PuTTY is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

1. Connect your laptop to the services port with an Ethernet crossover cable.

   If you do not have a crossover cable, you can use an IP hub.

   Note:

   Depending on the capabilities of the network interface card in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.

2. Start a PuTTY session.
3. In the **Host Name (or IP Address)** field, type `192.11.13.6`.

   The system assigns the IP address 192.11.13.6 to the services port.

4. For **Connection type**, select **SSH**.
5. In the **Port** field, type `22`.
6. Click **Open**.

   Note:

   The system displays the PuTTY Security Alert window the first time you connect to the server.

7. Click **Yes** to accept the server's host key and display the PuTTY window.
8. Log in as **craft**.
9. When you finish the session, type **`exit`** and press **Enter** to close PuTTY.

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Dom-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. If you disable IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.

c. In the command line, type **service_port_access enable** and press **Enter**.

2. For security reasons, always disable IP forwarding after finishing your task. Perform the following tasks to disable IP forwarding:

   a. Start an SSH session.

   b. Log in to System Domain (Domain-0) as admin.

   c. In the command line, type **ip_forwarding disable** and press **Enter**.

Accessing the System Platform Web Console

Prerequisites

If you are performing this task from a laptop that is connected to the services port, enable IP forwarding.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error, then follow the instructions in your browser to install a valid certificate on your computer.

3. Enter a valid User ID.

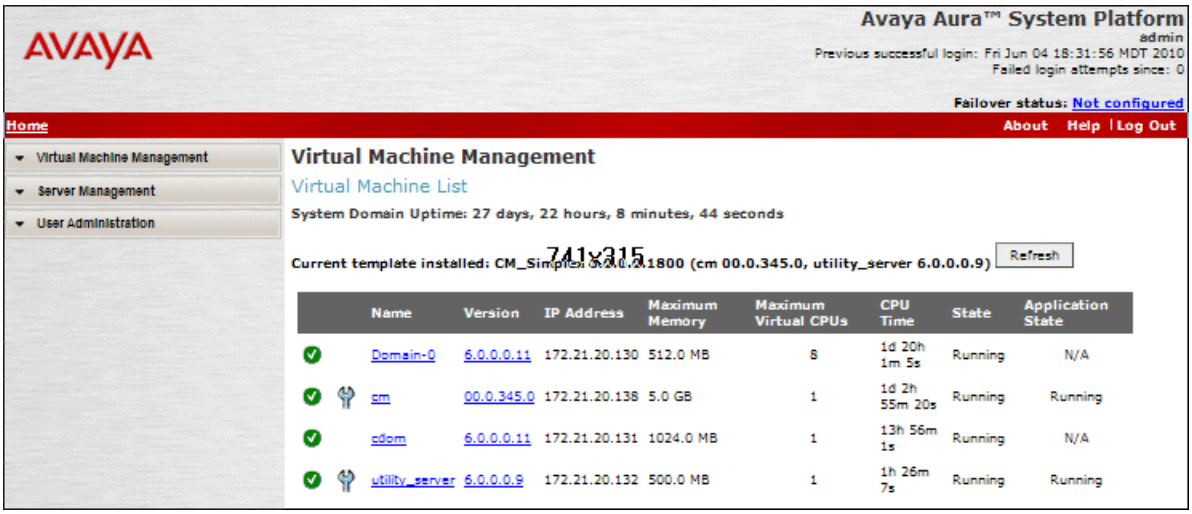
   Note:

   If you use an Avaya services login that is Access Security Gateway (ASG)-protected, you must have an ASG tool to generate a response for the challenge that is generated by the login page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. An Avaya Services representative will use Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative will use those keys to generate the response for the challenge generated by the login page.

4. Click **Continue**.

5. Enter a valid Password.

6. Click **Log On**.
   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end user license agreement.
   The system displays the Virtual Machine List page in the System Platform Web Console.



Related topics:

Enabling IP forwarding to access System Platform through the services port on page 34

Accessing the command line for System Domain

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. Alternatively, use an SSH (Secure Shell) client such as PuTTY to set up a remote connection from your computer. After logging in, the system prompts you with the Linux command prompt.

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of System Domain.

   Tip:
   You can obtain the IP address of System Domain (Domain-0) from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.

5. Once logged in, type the following command to log in as the root user: `su – root`
6. Enter the password for the *root* user.

   Tip:

   To access Console Domain from System Domain, type **`xm list`**, note the ID for *udom*, and then type **`xm console`** *`udom-id`*. When prompted, login as `admin`. Then type **`su – root`** and enter the root password to log in as root.

   To exit Console Domain and return to System Domain, press `Control+]`.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit System Domain.

Accessing the command line for Console Domain

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.

   Tip:

   You can obtain the IP address of Console Domain (cdom) from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su – root`
6. Enter the password for the *root* user.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit Console Domain.

Chapter 5: Administering SAL on System Platform

SAL Gateway

Secure Access Link (SAL) Gateway provides Avaya remote support engineers and Avaya Partners with remote access and alarming for serviceability of applications on System Platform. The Secure Access Link (SAL) Gateway application is automatically installed with System Platform. SAL Gateway software is also available separately for stand-alone deployments. See **Secure Access Link** on http://support.avaya.com. The SAL Gateway application on System Platform receives alarms from applications in the solution template and forwards them to Secure Access Core Concentrator Servers at Avaya and applicable Avaya Partners. SAL Gateway can also forward alarms to the customer's Network Management System (NMS) if configured to do so. The SAL gateway application also polls designated service providers for connection requests.

Remote Serviceability

System Platform utilizes SAL as Avaya's exclusive method for remote delivery of services. System Platform can be serviced remotely, eliminating the need for a service technician to visit the customer's site. System Platform uses the customer's existing Internet connectivity to facilitate remote support. All communication is outbound from the customer's environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS). SAL requires upload bandwidth (customer to Avaya or Avaya Partner) of at least 90 KB/s with latency no greater than 150 ms (round trip). Business Partners without a SAL Core Concentrator Server must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

Note:

Business Partners and customers must ensure that SAL is always configured and registered with Avaya during System Platform installation. Avaya support will be delayed or not possible if SAL is improperly implemented or not operational. System Platform and SAL do not support modem connections.

SAL Gateway configuration

The SAL Gateway includes a Web-based user interface that provides status information, logging information, and configuration interfaces. You must configure the SAL Gateway and other devices for alarming and remote access. The devices include System Platform's System Domain (dom 0), Console Domain (cdom), and other products that are included in the solution template that is installed. For example, virtual machines might include Communication

Manager, Communication Manager Messaging, SIP Enablement Services, and other applications that are included in the template.

To configure SAL, perform these high-level steps:

1. Register the system.

   You must submit the Universal Install/SAL Registration Request form to obtain from Avaya the information that you must enter in SAL Gateway.

   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 applications that are included in a specific 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.

2. Configure the SAL Gateway.

   The SAL Gateway provides remote access to those devices that are configured for remote access within it. It controls connections to managed elements, new or updated models, and verifies certificates for authentication.

Note:

On High Availability Failover systems, configure the SAL Gateway only on the primary server. When you enable High Availability Failover, SAL Gateway will propagate to the standby server.

Related topics:

Registering the system on page 12

Configuration prerequisites

Before configuring the SAL Gateway, you must start the registration process and receive product registration information from Avaya.

To register a product, download and complete the *Universal Install/SAL Registration Request* form and submit the form to Avaya. The form includes complete instructions. Open the Microsoft Excel form with macros enabled.

This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Equipment Registration (Partners only)**. At the bottom of the page, under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.

Note:

Start the registration process at least two business days before the planned installation date to avoid delays.

Related topics:

Registering the system on page 12

System and browser requirements

Browser requirements for SAL Gateway:

- Internet Explorer 6.x and 7.x
- Firefox 3.5

System requirements:

A computer with access to the System Platform network.

Starting the SAL Gateway user interface

1. Log in to the System Platform Web Console.
2. Click **Server Management** > **SAL Gateway Management**.
3. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
4. When the SAL Gateway displays its Log on page, enter the same user ID and password that you used for the System Platform Web Console.

Configuring the SAL Gateway

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Gateway Configuration**.
2. On the Gateway Configuration page, click **Edit**.
3. On the **Gateway Configuration** (edit) page, complete the following fields:
   - **Gateway IP Address**
   - **Solution Element ID**
   - **Gateway Alarm ID**
   - **Alarm Enabled**

   For field descriptions, see Gateway Configuration field descriptions on page 43.
4. (Optional) Complete the following fields if desired:
   - **Inventory Collection**
   - **Inventory collection schedule**
5. Click **Apply**.

   Note:
   The configuration changes do not take effect immediately. The changes take effect after you apply configuration changes on the Apply Configuration Changes page.
6. If you want to cancel your changes, click **Undo Edit**.

   The system restores the configuration before you clicked the **Edit** button.

   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Gateway Configuration field descriptions on page 43

Applying configuration changes on page 50

Gateway Configuration field descriptions

Name	Description
Gateway Hostname	A host name for the SAL Gateway. **Warning:** Do not edit this field as the SAL Gateway inherits the same hostname as the CentOS operating system that hosts both the System Platform Web Console and the SAL Gateway.
Gateway IP Address	The IP address of the SAL Gateway. This IP address is the same as that of cdom (also called VSPU).
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. If you have not obtained your System Platform Solution Element IDs, start the registration process as described in Registering the system on page 12. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.
Gateway Alarm ID	The Alarm ID of the SAL Gateway. The system uses the value in the **Gateway Alarm ID** field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.
Alarm Enabled	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
Inventory Collection	Enables inventory collection for the SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel who are working on tickets and want to review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which you want inventory collected.

Configuring a proxy server

Use the Proxy Server page to configure proxy settings if required for SAL Gateway to communicate with the Secure Access Concentrator Remote Server and the Secure Access Concentrator Core Server.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Proxy**.
2. On the Proxy Server page, complete the following fields:
   - **Use Proxy**
   - **Proxy Type**
   - **Host**
   - **Port**
3. If using an authenticating HTTP proxy server, complete the following fields:
   - **Login**
   - **Password**
4. Click **Apply**.
5. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the proxy server.

   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Proxy server field descriptions on page 45
Applying configuration changes on page 50

Proxy server field descriptions

Name	Description
Use Proxy	Check box to enable use of a proxy server.
Proxy Type	Type of proxy server that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy server.
Port	The port number of the Proxy server.
Login	Login if authentication is required.
Password	Password for login if authentication is required.

Configuring SAL Enterprise

Use the SAL Enterprise page to review settings for communication between SAL Gateway and a Secure Access Concentrator Core Server. Do not change the default settings unless you are explicitly instructed to do so.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **SAL Enterprise**.
   The SAL Enterprise page is displayed.
2. Do not change the default settings on this page.
   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.
3. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Core Servers.
   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, Avaya

recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

The system does not connect to the new Secure Access Concentrator Core Server until you restart the SAL Gateway.

Related topics:

SAL Enterprise field descriptions on page 46
Applying configuration changes on page 50

SAL Enterprise field descriptions

Name	Description
Passphrase	Default passphrase is `Enterprise-production`. Do not change the default unless you are explicitly instructed to do so. This passphrase is used to establish a channel for communication between the SAL Gateway and the Secure Access Concentrator Core Server.
Primary Enterprise	IP Address or the host name of the primary Secure Access Concentrator Core Server. The default value is `secure.alarming.avaya.com`.
Port	Port number of the primary Secure Access Concentrator Core Server. The default value is `443`.
Secondary Enterprise	This value must match the value in the **Primary Enterprise** field.
Port	This value must match the value in the **Port** field for the primary server.

Configuring Remote Access Server

Use the Remote Access page to review settings for communication between SAL Gateway and a Secure Access Concentrator Remote Server. Do not change the default settings unless you are explicitly instructed to do so.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Remote Access**.

The Remote Access page is displayed.

2. Do not change the default settings on this page unless you are explicitly instructed to do so.
3. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Remote Servers.

   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

The system does not connect to the new Secure Access Concentrator Remote Servers until you restart the SAL Gateway.

When you restart the SAL Gateway, the system terminates all active connections.

Related topics:

Remote Access field descriptions on page 47
Applying configuration changes on page 50

Remote Access field descriptions

Name	Description
Primary Server Host Name / IP Address	The IP address or host name of the primary Secure Access Concentrator Remote Server. The default value is `sl1.sal.avaya.com`.
Port	The port number of the primary Secure Access Concentrator Remote Server. The default value is `443`.
Secondary Server Host Name / IP address	This value must match the value in the **Primary Server Host Name / IP Address** field.
Port	This value must match the value in the **Port** field for the primary server.

Configuring NMS

Use this procedure to specify SNMP trap destinations. When you configure Network Management Systems (NMSs), the SAL Gateway copies traps and alarms (encapsulated in traps) to each NMS that you configure.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **NMS**.
2. On the Network Management Systems page, complete the following fields:
   - **NMS Host Name/ IP Address**
   - **Trap port**
   - **Community**
3. Click **Apply**.
4. (Optional) Use the **Add** button to add multiple NMSs.
   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Network Management Systems field descriptions on page 48
Applying configuration changes on page 50

Network Management Systems field descriptions

Name	Description
NMS Host Name/ IP Address	The IP address or host name of the NMS server.
Trap port	The port number of the NMS server.

Name	Description
Community	The community string of the NMS server. Use `public` as the **Community**, as SAL agents support only public as community at present.

Managing service control

Use this procedure to view the status of a service, stop a service, or test a service that the SAL Gateway manages.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Service Control**.
   The system displays the Gateway Service Control page. The page lists the following services:
   - **Inventory**
   - **Alarming**
   - **Remote Access**
   - **Health Monitor**

   The Gateway Service Control page also displays the status of each service as:
   - **Stopped**
   - **Running**
2. Click one of the following buttons:
   - **Stop** to stop a service.
   - **Start** to start a service that is stopped.
   - **Test** to send a test alarm to the Secure Access Concentrator Core Server.

   Important:
   Use caution if stopping the Remote Access service. Doing so will block you from accessing SAL Gateway remotely.

Applying configuration changes

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Apply Configuration**.
   The system displays the Apply Configuration Changes page.
2. Click the **Apply** next to **Configuration Changes**.
   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.

   When you click **Apply**, the system restarts the SAL Gateway and updates the Gateway with the new values you configured.

   The SAL Gateway misses any alarms that are sent while it restarts.

Configuring a managed element

Prerequisites

Complete the Managed Element Worksheet for SAL Gateway. See Managed element worksheet for SAL Gateway on page 67.

Perform this procedure for each Solution Element ID (SE ID) that is provided in the registration information from Avaya.

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway** > **Managed Element**.
2. On the Managed Element page, click **Add new**.
3. Complete the fields on the page as appropriate.
4. Click **Add**.
5. Click **Apply** to apply the changes.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page

and restarts the SAL Gateway. To minimize disruption of services and alarms, Avaya recommends that you apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Applying configuration changes on page 50
Managed Element field descriptions on page 51
Managed element worksheet for SAL Gateway on page 67

Managed Element field descriptions

Name	Description
Host Name	Host name for the managed device or any meaningful name that describes the device to your or your provider (for example, CM_Bldg5_Production).
IP Address	IP address of the managed device.
NIU	Not applicable for applications that are installed on System Platform. Leave this field clear (not selected).
Model	The model that is applicable for the managed device.
Solution Element ID	The Solution Element ID (SE ID) of the device. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
Product ID	The Product ID or the Alarm ID. 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.
Provide Remote Access to this device	Check box to allow remote connectivity to the managed device.
Transport alarms from this device	(Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server.
Collect Inventory for this device	Check box to enable inventory collection for the managed device. When this check box is selected, SAL Gateway collects inventory information about the managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel who are working on tickets and want to review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com

Name	Description
Inventory collection schedule	Interval in hours at which you want inventory collected from the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
Generate Health Status missed alarm every	Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device. You must restart the SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart and generates alarms if it does not receive a heartbeat within the configured interval.
Suspend health monitoring for this device	Check box to suspend health monitoring for the managed device.
Suspend for	Number of minutes for which you want health monitoring suspended for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Chapter 6: Installing a solution template

Template installation

After installing System Platform, install the solution templates.

After installing the templates, manage the templates from the System Platform Web Console.

Note:

The procedures for configuring a solution template differ depending on the template. See the documentation for the specific solution template for the configuration steps.

Prerequisites for installing a solution template

- Stop High Availability Failover if it is running. You cannot install a solution template if High Availability Failover is running.
- Make sure that the IP address for the *avprivate* bridge do not conflict with any other IP addresses in your network.

  Go to the Network Configuration page on the System Platform Web Console (**Server Management** > **Network Configuration**) to view the addresses that are allocated to avprivate. The range of IP addresses starts with System Domain's (Dom-0) interface on avprivate. If any conflicts exist, resolve them. Keep in mind that the template you install may take additional addresses on the private bridge.

  The avprivate bridge is 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 page. 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.

Installing a solution template

Important:

If you are using the High Availability Failover option, do not install a solution template on the server that will serve as standby. If you do, you will not be able to start High Availability Failover. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability Failover.

1. Log in to the System Platform Web Console as admin.
2. Click **Virtual Machine Management** > **Solution template**.

   The system displays the Search Local and Remote Template page. Use this page to select a template that you want to run on System Platform.
3. Select a location from the list in the **Install Templates From** box.

   Note:

   If the template installation files are located on 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 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.

   If the template you selected supports an Electronic Pre-installation Worksheet (EPW), the system prompts you to continue without an EPW or to provide an EPW file. The system also prompts you with pages that require your input such as IP addresses for the applications that are included in the template. These pages vary depending on the template that you are installing. If you provided an EPW file, some of these pages may be pre-populated with data from the EPW.

   See the respective template documentation for detailed instructions.

Related topics:

Prerequisites for installing a solution template on page 53
Search Local and Remote Template field descriptions on page 55

Search Local and Remote Template field descriptions

Name	Description
Install Template From	Lets you select from the available options to locate a template and install it on System Platform. The 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 “sold-to” number to allow you to select the appropriate template for the site where you are installing. You may hold the mouse pointer over the selection to view more information about the “sold-to” number. **HTTP** The template files are located in a 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.

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. A proxy may also be required in order for Secure Access Link (SAL) and alarming to access the internet.
Install	Installs the solution template.

Name	Description
Delete Installed Template	Deletes the currently installed template.

Chapter 7: System Platform High Availability Failover

High Availability Failover overview

The System Platform High Availability Failover is an optional feature aimed at providing service continuity. However, it does not support critical reliability. Moreover, certain solution templates (Communication Manager is one such template) do not support this feature.

Note:

System Platform High Availability Failover does not support IPv6 and cannot be configured with IPv6 addresses.

The System Platform High Availability Failover feature offers the following capabilities:

Node scores

High Availability Failover uses node scores to compute the ability of each machine to run the resources and determine which node runs the resources. If the system has no issues, and resources could run on either node, both machines have the same score. Thus System Platform uses the term “preferred node” for the machine that should run the resources when the system has no issues. The preferred node has a small score benefit. So if both machines are booted at the same time, the preferred node will run resources. The node from which you configure High Availability Failover is designated the preferred node. If you stop High Availability Failover, the currently active node becomes the preferred node.

No auto-failback

High Availability Failover does not use auto-failback to migrate resources back to the preferred node when the resources are running on the standby node and the preferred node becomes available again. Switching servers disrupts service, and if both servers are healthy, then running on the preferred node offers no increased benefit. If you want to migrate resources back to the preferred node after a failover or a switchover, you can do so by using the **Manual Switchover** option in the Failover menu at the most suitable time.

Expected failover/switchover times

High Availability Failover uses 30 seconds as a timeout interval after which the standby node will declare the active node dead and start resources (even though the active node may be not accessible, not running or blocked). Note that System Platform does not provide any Web interface to modify this interval.

For manual switchover or when the system initiates a preemptive failover, the total time between the start of the command and activating the standby node includes a graceful shutdown and restart of all resources:

- Stop of resources– Up to 5 minutes.
- Start of resources–Up to 5 minutes.
- Resulting longest switchover time–Up to 10 minutes.

For failover due to total failure of the active node, the total time between the start of the outage and the time when all resources are running on the standby node includes a detection interval timeout and the start of all resources:

- Detect active node failure–30 seconds.
- Start of resources–Up to 5 minutes.
- Resulting longest switchover time–Up to 5.5 minutes.

Note:

The switchover time is approximate and varies depending on the hardware running System Platform with no templates. The switchover is further delayed by the following factors:

- The system runs complex templates.
- The system shutdown was not proper. Therefore, the system performs an FSCK (File System Check) as it boots up and starts the virtual machines.

Requirements for High Availability Failover

The requirements for High Availability Failover are as follows:

- Two servers with exactly the same hardware configuration. The standby server cannot have less memory, number of processors, total disk space or free disk space than the primary server.
- The hardware must be supported by System Platform.
- The servers must have a spare Gigabit network interface to be dedicated exclusively to High Availability Failover services. The servers must be connected on the same ports on both machines.
- Both the servers must be in the same subnet.
- Both servers must be in close proximity so that they can be connected with the crossover cable. The Ethernet specification limit for this distance is 100 meters.
- The same version of System Platform must be installed on the active and standby nodes.
- Do not install a template on the standby node. If you do so, you will not be able to start High Availability Failover. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability Failover.

Prerequisites for configuring High Availability Failover

The prerequisites for configuring High Availability Failover are as follows:

- Connect both the servers with a Gigabit-certified Ethernet cable on the same ports on both machines.
- Ensure that your network gateway replies to ICMP requests from the System Platform nodes. The default network gateway is the ping target of the High Availability Failover heartbeat. This target cannot be configured differently.

Configuring High Availability Failover

You must have a user role of Advanced Administrator to perform this task.

1. Log in to the Web Console of the server that you want to be the preferred node.
2. Click **Server Management** > **Failover** to display the Failover page.

   The Failover page displays the current status of High Availability Failover.
3. Click **Configure Failover**.
4. On the Configure failover page, enter the appropriate information to configure High Availability Failover.
5. Click **Create**.
6. After the system completes creation of the High Availability Failover configuration, click **Start Failover Mode** and confirm the warning that is displayed.

   System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.
7. Log in to the System Platform Web Console.
8. Click **Server Management** > **Failover**.

   You can check the status of the failover components on the Failover page and ensure that Distributed Replicated Block Device (DRBD) is synchronizing the hard disks of the two servers.

   Tip:

   During the disk synchronization process, you can increase or decrease the speed of the synchronization with a slider bar on the console. The default value of this

rate is 30 MB/s. If you set the value too high, it may affect the performance of the virtual machines running on the active server.

Configure Failover field descriptions

Name	Description
Remote cdom IP address	IP Address of Console Domain on the standby node.
Remote cdom user name	User name for Console Domain on the standby node.
Remote cdom password	Password for Console Domain on the standby node.
Primary network interface	Network interface connected to the customer network.
Crossover network interface	Network interface connected to the standby server.

Chapter 8: Troubleshooting the installation

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

1. Log in to the Console Domain as admin.
2. Type `su -`
3. Enter the root password.
4. Run the following commands:

```
> ssh dom0.vsp /opt/avaya/vsp/template/scripts/udomAttachCd
> mount /dev/xvde /cdrom/
```

Cannot ping Console Domain or access the Web Console

Troubleshooting steps

1. Log in to the System Domain (Dom-0) as `admin`.
2. Enter **`su -`** to log in as root.
3. At the prompt, type **`xm list`**.

The **xm list** command shows information about the running virtual machines in a Linux screen.

You should see two virtual machines running at this time: System Domain (shown as Domain-0) and Console Domain (shown as udom in **xm list**).

A state of r indicates that the virtual machine is running. A state of b indicates that the virtual machine blocked.

Note:

The blocked state does not mean that there is a problem with the virtual machine. It only means that the virtual machine is currently not using any CPU time.

Other possible virtual machine states are:

- p: paused
- s: shutdown
- c: crashed

For more information on the information displayed, see the Linux manual page for the **xm** command.

4. On the Linux screen, type **exit** to log off as root. Type exit again to log off from System Domain (Domain-0).

Example

xm list output:

```
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0   512     2     r-----  60227.8
aes                                         15  1024     1     -b----  12674.4
cm                                          17  1024     1     -b----  14898.2
cobar                                       14   512     1     -b----   8492.7
ses                                         19  1024     1     -b----   4775.0
udom                                        16  1024     1     -b----   9071.6
utility_server                              18   512     1     -b----   1909.0
```

If High Availability Failover is enabled, the output of the **xm list** command differs for the active server and the standby server. The output for the active server is similar to that shown above.

xm list output for the standby server:

If High Availability Failover is enabled, the output for the standby is similar to the following:

```
Name                                        ID    Mem VCPUs       State    Time(s)
Domain-0                                     0    512     2      r-----  21730.2
aes                                               1024     1              2786.0
cm                                                1024     1              3023.7
cobar                                              512     1              1745.1
ses                                               1024     1              1021.7
udom                                              1024     1              2714.1
utility_server                                     512     1               400.0
```

SAL does not work

Troubleshooting steps

1. Ping the DNS server in the customer network.
2. Ping the proxy server in the customer network.
3. Ping support.avaya.com to check DNS is working.
4. Try a **wget** using the proxy from the command line to check that the proxy is working.

Example

Type a command such as `wget http://support.avaya.com`

You should get an output similar to the following:

```
HTTP request sent, awaiting response... 200 OK
```

Multiple reinstallations can result in an out of memory error

If a pre-installation Web application is used to install a template and the template is reinstalled by deleting and installing it multiple times, an out of permanent generation memory space (PermGen) error can occur.

Troubleshooting steps

Perform the troubleshooting steps given here to ensure that a PermGen error does not occur.

1. Delete the template.
2. Restart Tomcat by performing the following steps:
   a. Log in to Console Domain as admin.
   b. Type `su`
   c. Type `/sbin/service tomcat restart`
3. Start the pre-installation Web application.
4. Install the template.

Appendix A: Installation worksheet for System Platform

The System Platform installer application requires you to fill in several fields. Having the information available at the time of installation makes it go faster and ensures accuracy.

Print out the following tables and work with your network administrator to fill in the rows.

System Domain Network Configuration

Field	Value	Notes
Hostname		This is the hostname for System Domain (Dom 0)
Primary DNS		
Secondary DNS		Optional
Static IP		The static IP address for the Ethernet interface that connects to the customer network.
Subnet mask	255.255.255.0 (default)	
Default gateway IP		This will be the default gateway for all the virtual machines, if you do not configure gateways for them.
VLAN		Is required only if an S8300D server is used for installing System Platform.

VSP Console Domain Network Configuration

Field	Value/requirement	Notes
Hostname		This is the hostname for Console Domain.
Static IP		The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System Domain (Domain-0). As System Domain acts like a bridge, the IP address that you enter here must

Field	Value/requirement	Notes
		be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).

Date/Time and NTP setup

Field	Value/requirement	Notes
NTP Server 1		Use of NTP server is optional. However, Avaya recommends its use.
NTP Server 2		Optional
NTP Server 3		Optional

Passwords

Default passwords are provided. You should change these default passwords.

Field	Value/requirement	Notes
root		
admin		
cust		
ldap		

Appendix B: Managed element worksheet for SAL Gateway

Use this worksheet to record the information that you will need to add managed devices to SAL Gateway.

Managed device (virtual machine)	IP Address	SE ID	Product ID	Model	Notes
System Domain (Dom 0)				VSP_2.0.0.0	System Domain (Dom 0) does not have alarming enabled; however, it has its own Product ID (Alarm ID). Console Domain (cdom or udom) has alarming enabled. System Domain sends all syslog (system logs) to Console Domain, which then triggers alarms on behalf of System Domain. **Important:** For High Availability Failover configurations, you must have two different solution element IDs (SEIDs) for System Domain (Dom 0): one for the active System Domain and one for the standby System Domain. You must administer both SEIDs in the SAL Gateway user interface.
Console Domain (cdom or udom)				VSPU_2.1.1.2	

Index

M

N

P

R

S

T

V

W