Installing and Upgrading Avaya Aura™ System Manager

Release 6.0
June 2010

© 2010 Avaya Inc.

All Rights Reserved.

Notice

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

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.

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, the Avaya logo, Avaya Aura™ System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

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 Manager - installation requirements....5
- Introduction....5
- Hardware requirements....5

Chapter 2: Checklists and Worksheets....7
- System Manager installation checklist....7
- System Manager information worksheet....7

Chapter 3: Installing System Platform....9
- Preinstallation tasks for System Platform....9
  - Preinstallation checklist for System Platform....9
  - Registering the system....10
  - Registering for PLDS....11
  - Downloading software in PLDS....12
  - Verifying the downloaded ISO image....12
  - Writing the downloaded software to DVD....14
- Installing System Platform....15
  - Installation checklist for System Platform....15
  - Installation methods....18
  - Connecting your laptop to the server....18
  - Starting the installation....20
  - Selecting the type of keyboard....22
  - Verifying the System Platform image on the DVD....23
  - Configuring network settings for System Domain (Domain-0)....24
  - Configuring network settings for Console Domain....26
  - Configuring the time zone for the System Platform server....28
  - Configuring the date and time for the System Platform server....28
  - Configuring System Platform passwords....29
  - Verifying installation of System Platform....31
  - Accessing System Platform....32
- Installing a solution template....36
  - Search Local and Remote Template field descriptions....37
- Configuring the SAL gateway....39
  - SAL....39
  - Registering the system....39
  - Configuring the SAL Gateway....40
- System Platform High Availability Failover....41
  - High Availability Failover overview....41
  - Requirements for High Availability Failover....42
  - Prerequisites for configuring High Availability Failover....43
  - Configuring High Availability Failover....43
  - Configure Failover field descriptions....44

Chapter 4: Upgrading System Platform....45
- Platform upgrade....45
- Upgrading System Platform....46
- Commit and Rollback....47
- Committing an upgrade....49
- Rolling back an upgrade....49

Platform Upgrade field descriptions....49
Upgrading System Platform on High Availability Systems....51
Methods for upgrading High Availability systems....51
Stop and start of High Availability for platform upgrades....51
Stopping High Availability....51
Starting High Availability Failover....52
Upgrading System Platform on both servers....52
Upgrading System Platform on the preferred server only....53

Chapter 5: Installing System Manager....55
Downloading System Manager from PLDS....55
Installing the System Manager template....56
Default Credentials....58

Chapter 6: System Manager Upgrades....59
....0
Performing load to load upgrade....59
Performing System Manager Upgrade from Release 1.0 to 5.2....60
Performing System Manager upgrade from Release 5.2 to 6.0....61
Default credentials....62

Chapter 7: Modifying Alarm ID and Managed Element ID....63
....0
Modifying an Alarm ID....63
Modifying a Managed Element ID....64

Chapter 8: Generating Test Alarms....65
....0
Generating a test alarm....66

Chapter 9: Removing the System Manager template....67
....0

Chapter 10: High Availability support for System Manager....69
....0
Start and stop of High Availability Failover....70
Prerequisites for configuring High Availability Failover....70
Configuring High Availability Failover....71
Configure Failover field descriptions....71
Starting High Availability Failover....72
Stopping High Availability Failover....72

Index....73

Chapter 1: System Manager - installation requirements

Introduction

The Avaya Aura™ System Manager delivers a set of shared management services which you can access using the System Manager common console.

The System Manager Template is packaged and delivered in an ISO file. This template contains Red Hat Enterprise Linux 5.3 and System Manager installed on RHEL 5.3. Installing the System Manager virtual appliance requires you to perform the following steps:

1. Install System Platform.
2. Install the System Manager virtual appliance on System Platform.

Hardware requirements

Install System Manager on either an Avaya S8510 server or an Avaya S8800 server, depending on what you ordered. These servers arrive at the customer's site with all the required components and memory. Prior to installing System Manager on the server you have to install System Platform product on the hardware.

Chapter 2: Checklists and Worksheets

System Manager installation checklist

#	Action	Notes	✔
1	Download the `System Platform 6 build 11 ISO image` and applicable patch from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded ISO matches the number mentioned on the Avaya PLDS Web site.	
2	Download the System Manager template present in the `System_Manager_06_00_00.iso` file from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded template matches the number mentioned on the PLDS site.	
3	Set up a DVD or USB flash drive to perform the System Platform installation from a DVD or USB flash drive.	For more information on installing System Platform, see Chapter 3, “Installing System Platform”.	
4	Deploy the System Manager template on System Platform. For more information, see “Installing System Manager template” in Chapter 5, “Installing System Manager”.		

System Manager information worksheet

The System Manager template deployment using the System Platform Console requires you to fill in several fields. Having the information available at the time of installation expedites the System Manager deployment and ensures accuracy. Print out the following tables and work with your network administrator to fill in the appropriate value for each field displayed in the tables.

For the System Manager Virtual Appliance

Field	Value	Notes
IP address		Enter the IP address that is to be assigned to the System Manager virtual appliance on System Platform.
Short Hostname		Enter the short host name for the System Manager.
Non-root User		This is an optional field. Enter a non-root ID if you want to install using a non-root ID.
Domain Name		Enter the domain name for your setup. For example: production.mydomain.com

For the Network Configurations

Field	Value	Notes
Gateway Address		Enter the IP address of the server that has been set up as the gateway in your enterprise environment.
Network Mask		Enter the network mask value.
DNS		Enter the IP address of the Domain Name Server.
Search String		Enter the search string. The system uses this search string to resolve the domain names.

Chapter 3: Installing System Platform

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 10. **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.		
3	Download the System Platform installer ISO image file from PLDS. See Downloading software in PLDS on page 12.		
4	Download the appropriate solution template and licenses from PLDS.		

No.	Task	Notes	✔
	See Downloading software in PLDS on page 12.		
5	Verify that the downloaded ISO images match the images on the PLDS Web site. See Verifying the ISO image on a Linux-based computer on page 12 and Verifying the ISO image on a Windows-based computer on page 13.		
6	Write the ISO images to separate DVDs. See Writing the ISO image to DVD on page 14.		

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. For solution templates that include Communication Manager, the first stage of registration also provides you with the System ID (SID). 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.

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.

Installing System Platform

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. See Configuring the laptop for direct connection to the server on page 18. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Internet Explorer on page 19 or Disabling proxy servers in Firefox on page 19 .		
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.		

No.	Task	Notes	✔
	See Starting the installation from your laptop on page 20 or Starting the installation from the server console on page 21 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 20 or Starting the installation from the server console on page 21 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 20.		
7	Select the required keyboard type. See Selecting the type of keyboard on page 22.		
8	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 23.		
9	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 24.		
10	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 26.		
11	Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 28.		

No.	Task	Notes	✔
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 28.		
13	Configure the System Platform passwords. See Configuring System Platform passwords on page 29.		
14	Verify access to the System Platform Web Console. See Verifying installation of System Platform on page 31.		
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 36.	**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.	
17	Configure the SAL gateway for remote access and alarming. See SAL Gateway.		
18	If applicable, configure System Platform High Availability Failover. See Configuring High Availability Failover on page 43.		

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. This option does not apply to the S8300D. To install to the S8300D, you must use a laptop connected to the services port.

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 load System Platform ISO file. Make sure that you change the network settings on the laptop before connecting to the server.

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.

Note:

On S8510 and S8800 servers, eth1 is the services port. On S8300D server, eth0 is the services port, which is on the front of the server face plate and is marked as 'SERVICES'.

On S8800, eth1 is labelled as '2' as the IBM S8800 servers do not follow the traditional network port numbering convention.

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 22.

Related topics:

Connecting to the server through the services port on page 32

Starting the installation from the server console

Note:

This procedure does not apply to embedded servers such as S8300D.

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 22.

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 23.
- 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 24.

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 23.

  OR

- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 24

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 24.

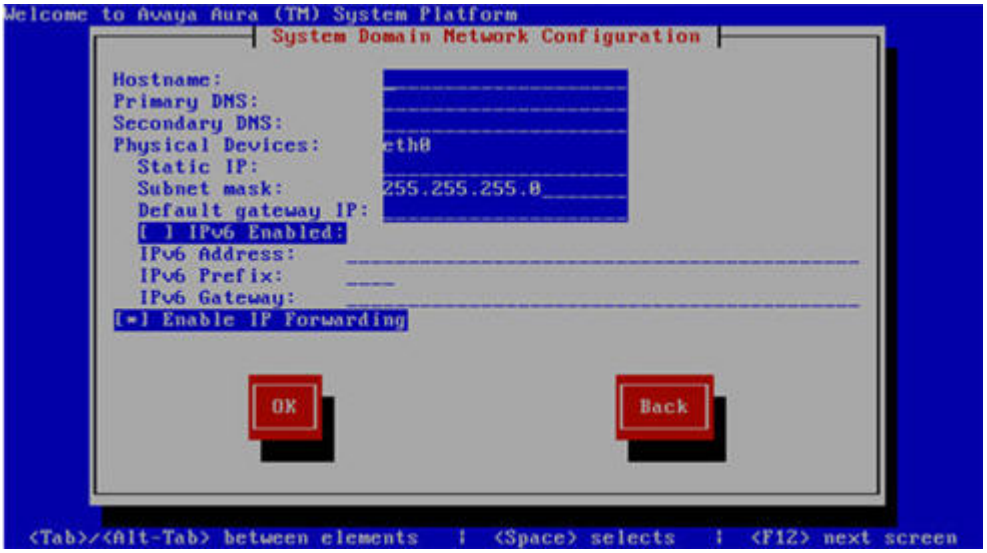
Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain.

Related topics:

Writing the ISO image to DVD on page 14

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.

   Note:
   Messaging does not support IPv6. Make sure that it is disabled.
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 26.

Related topics:

System Domain Network Configuration field descriptions on page 25

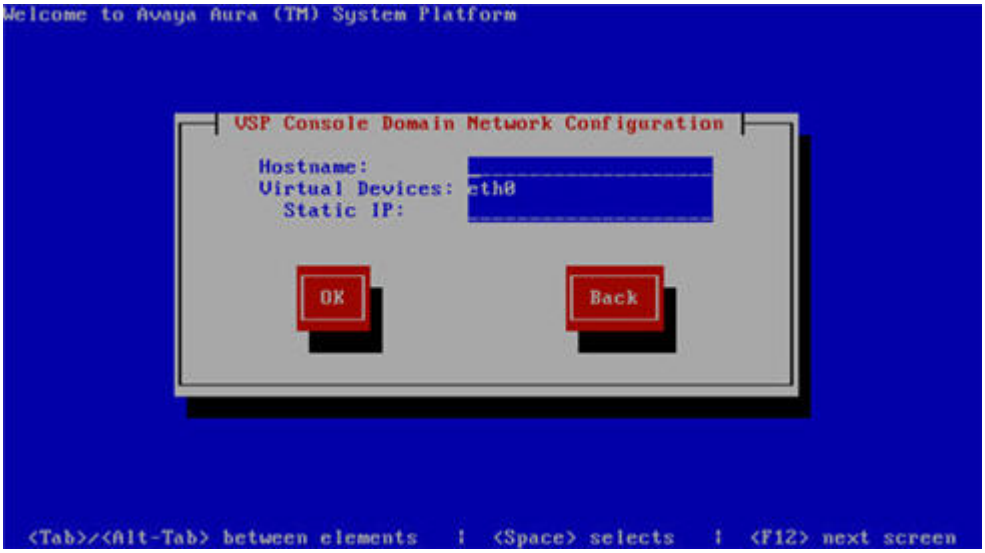
System Domain Network Configuration field descriptions

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.

Name	Description
IPv6 Enabled	The indicator whether or not the IP addresses required by System Platform needs to be IPv6-compliant. Messaging does not support IPv6. Make sure that it is disabled. Application Enablement Services 5.2.2 does not support IPv6.
IPv6 Address	The IPv6–compliant IP address of System Domain. Messaging does not support IPv6.
IPv6 Prefix	The IPv6 prefix for **IPv6 Address**. Messaging does not support IPv6.
IPv6 Gateway	The IPv6–compliant gateway IP address of System Domain. Messaging does not support IPv6.
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. IP forwarding enables access to System Platform through the services port.

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 28.

Related topics:

System Platform Console Domain Network Configuration field descriptions on page 27

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.

   Note:

   On the main server, you need to select the time zone relevant to the server location. In the case of ESS or LSP, you must set up the time zone, which is same as that of the main server. In a failover situation, the ESS or the LSP provide the correct time information to display on the phones with the help of the time zone and the translation information.

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 28.

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 29.

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
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 31.

Related topics:

Passwords field descriptions on page 30

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.

Name	Description
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 33.
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 System Platform Web Console through the services port, you must enable IP forwarding on System Domain (Dom-0) . 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:

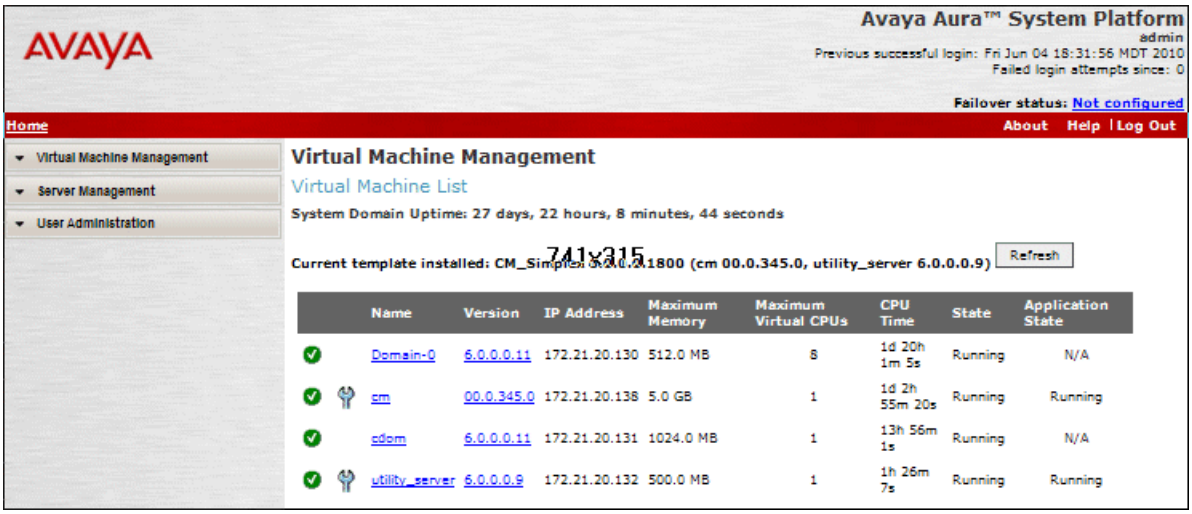
   If you use an Avaya services login that is Access Security Gateway (ASG)-protected, you must have an ASG tool to generate a response for the challenge that is generated by the login page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools 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 33

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 Console Domain.

   Tip:

   You can obtain the IP address of Console Domain by typing one of the following commands:

   - `grep cdom.vsp /etc/hosts`
   - `ping cdom.vsp`
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.

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.

   If you are installing a Communication Manager template, make sure that you remove the CD/DVD from the CD-ROM/DVD tray after the template installation completes.

   Here are the approximate installation durations for the Communication Manager templates:

   - CM_Duplex: 15 minutes
   - CM_Simplex: 25 minutes
   - CM_onlyEmbed: 50 minutes
   - CM_SurvRemote: 30 minutes
   - CM_SurvRemoteEmbed: 65 minutes

Next steps

If you are following this document as part of upgrading your Communication Manager template, refer to *Upgrading to Avaya Aura™ Communication Manager* for further instructions.

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**

Name	Description
	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.
Delete Installed Template	Deletes the currently installed template.

Configuring the SAL gateway

SAL

System Platform includes Avaya's Secure Access Link (SAL) Gateway to manage service delivery (alarming and remote access). SAL Gateway is a software application that:

- Facilitates remote access to support personnel and tools that are needed to access supported devices
- Collects and sends alarm information to a Secure Access Concentrator Core Server, on behalf of the managed devices
- Provides a user interface to configure its interfaces to managed devices, Concentrator Remote and Core Servers, and other settings

SAL requires an upload bandwidth (customer to Avaya) of at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip.)

During the installation of System Platform, you must register the system (System Platform, solution templates, and SAL Gateway) and configure SAL for the customer's network.

Important:

For Avaya to provide support, Avaya Partners or their customers must ensure that SAL is registered and configured properly. Avaya support will be delayed or not possible if SAL is not properly implemented.

Avaya Partners must provide their own B2B VPN connection (or other IP-based connectivity) to deliver remote services. SAL does not support modem connections.

You can launch the SAL Gateway management portal from within System Platform.

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. For solution templates that include Communication Manager, the first stage of registration also provides you with the System ID (SID). 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.

Configuring the SAL Gateway

To configure the SAL Gateway for the customer's network and System Platform, follow the instructions that are provided in *Administering SAL on Avaya Aura™ System Platform*. This document is available on http://support.avaya.com/css/P8/documents/100069101.

Note:

For an understanding of how to administer the customer's network to support SAL, follow the instructions provided in *Secure Access Link 1.8 SAL Gateway*

Implementation Guide. This document is available on http://www.avaya.com/support.

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 4: Upgrading System Platform

Platform upgrade

Use the **Platform Upgrade** option to upgrade Avaya Aura™ System Platform software for one or all of the following:

- System Domain (Domain-0)
- Console Domain

Note:
Before proceeding with the System Platform upgrade, check the relevant template documentation to ensure that the template is qualified for the System Platform version to which you want to upgrade. Also check for any System Platform patches that are required.

If System Platform High Availability is enabled and you are upgrading System Domain (Domain-0) and Console Domain, you must stop High Availability before performing the upgrade. Upgrade each server separately before restarting High Availability. See Methods for upgrading High Availability systems on page 51.

The platform upgrade software is distributed as an ISO file (the file type in which System Platform software is distributed for new installations) or platform upgrade files. If you are using the ISO file, you can copy it to a CD or DVD and use the **SP CD/DVD** option to upgrade. Alternately, you can decompress the ISO file and copy the decompressed contents to a USB drive. You can use the **SP USB Disk** option to upgrade.

If you are using the platform upgrade files to install, you can use any of the available options: **Avaya Downloads (PLDS)**, **HTTP**, **SP Server**, **SP CD/DVD**, or **SP USB Disk**.

Note:
On Windows, use WinZip release 12 or higher to decompress the ISO file.

Upgrading System Platform

1. Log in to System Platform Web Console.
2. Click **Server Management** > **Platform Upgrade**.
3. In the **Upgrade Platform From** field, select a location from where to download the template image files for the platform upgrade. The system searches for a template description file that has an .ovf extension. Options are:
   - **Avaya Downloads (PLDS)**
   - **HTTP**
   - **SP Server**
   - **SP CD/DVD**
   - **SP USB Device**
4. If you selected **HTTP** or **SP Server** in the **Upgrade Platform From** field, enter the platform upgrade URL.
5. Click **Search**.
6. Select the required template description file to perform the platform upgrade, and then click **Select**.
   The system displays the version and additional information for the current and the new platform (System Domain (Domain-0) or Console Domain, or both) on the Platform Upgrade Details page.
7. On the Platform Upgrade Details page, click **Upgrade**.

   Important:
   As part of the upgrade process, the System Domain (Domain-0) and Console Domain are rebooted, and as a result, all other virtual machines will be rebooted. During the platform upgrade process, all operations on the System Platform Web Console are blocked and all links (including menu items) are disabled until the system is booted up into the new platform for you to commit or rollback the upgrade.
8. In the dialog box that appears to confirm that the template has been qualified for the platform version you are about to upgrade to and that both System Platform Web Console and Console Domain will reboot on completing the upgrade, click **OK**.
   The system displays all the available template description files for the URL.
9. Click **OK** in the dialog box prompting you to confirm the upgrade.
   At this stage, the upgrade process starts and the system displays the Platform Upgrade workflow status page.

Note:

The System Domain (Domain-0) and Console Domain are rebooted at this stage. So the Platform Upgrade workflow status page does not show any updates until it reboots in the new Console Domain. After the Web Console is up, the system automatically redirects you to the login page. This can take approximately 20 minutes.

10. Log in to the System Platform Web Console.

    At this stage, you can view the time remaining for Auto Rollback of the platform upgrade on the Commit or Rollback platform upgrade page. You can also check the Web Console to make sure that the upgrade process is running alright.

11. On the Commit or Rollback platform upgrade page, do one of the following:

    - Click **Commit** to continue the upgrade process by committing to the newly upgraded platform. See Committing an upgrade on page 49

      Note:

      You are allowed a 4-hour period to log in to the System Platform Web Console. If you do not login during this period, the system will reboot using the previous release of System Platform. If a user logs in to System Platform Web Console within the 4-hour period, it is assumed that System Platform is reachable and the timer is cancelled. However, you still need to verify and commit the upgrade.

    - Click **Rollback** to cancel the upgrade process and go back to the previous version of the software. See Rolling back an upgrade on page 49.

Commit and Rollback

System Platform upgrades should be committed before performing other operations. During an upgrade, after the system boots in the new platform release, the user is required to commit or rollback the upgrade. While the system is waiting for the user to either commit or rollback, Avaya advises not to perform any of the following operations:

- Delete a template
- Install a template
- Upgrade a template
- Reboot the System Platform Web Console

Note:

Rebooting System Platform Web Console before committing will roll back the system back to the previous release.

Note:

System Platform does not prevent you from performing the above operations prior to selecting commit or rollback.

If you perform the above operations, the operations will actually take effect on the system. Thereafter, if rollback is performed, the new changes will be visible in the rolled back system. Committing an upgrade is unaffected by the changes made prior to committing the upgrade. If the template-related operations are performed and you want to recover after committing or rolling back the upgrade, you need to manually rollback the changes through System Platform Web Console. The upgrade rollback operation will not be able to roll the system back. A commit of the upgrade, on the other hand, is unaffected by the changes that you make prior to committing the System Platform upgrade.

Commit

You can execute a commit operation when you are satisfied that the new System Platform software is working without any issues. After executing a commit operation, you cannot go back to the older version of the System Platform software. If you do not log in to System Platform Web Console within 4 hours after the upgrade, the system performs an automatic rollback.

The system performs the following when you commit an upgrade:

- Disables the four hour timer that automatically performs a rollback.
- Performs a clean up operation (such as, removing state files and so on).
- Commits boot loader (grub) to boot up into the new platform from now on.
- Marks the Workflow as complete and indicates that on the Platform Upgrade Status page.

Rollback

You can execute a rollback operation if you find any errors or issues with the new System Platform software and want to go back to the older version of the software. Rollback can reboot the server.

The system performs the following when you roll back an upgrade:

- Disables the four hour timer that automatically performs a rollback.
- Commits boot loader (grub) to boot up into the old platform.
- Performs a clean up operation (such as, removing state files and so on).
- Prepares the system to notify the user of the reason for rollback after rebooting into the old platform.
- Reboots the platform to boot up into the old platform and restores access to System Platform Web Console.

Committing an upgrade

On the Commit or Rollback platform upgrade page, click **Commit** to continue the platform upgrade process.

Rolling back an upgrade

On the Commit or Rollback platform upgrade page, click **Rollback** to cancel the upgrade process and go back to the previous version of the software.

Note:

After a rollback, when you log on to the System Platform Web Console, the system displays the Rollback Acknowledge page that specifies the reason for rollback (either user initiated rollback or deadmans switch) based Auto rollback; or if the upgrade failed and the system rebooted to an older version of System Platform as part of fail-safe fallback mechanism.

Platform Upgrade field descriptions

Name	Description
Upgrade Location	Lets you specify the location from where to download or upload the template image files for the platform upgrade. Options are: • **Avaya Downloads (PLDS)** The files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. • **HTTP** The files are located on an HTTP server. You must specify the URL of the platform upgrade if you select this option.

Name	Description
	• **SP Server** The platform upgrade files are located in the `/vsp-template` directory in the System Platform Console Domain. You will need to copy the platform upgrade files in this directory using a file transfer program and change their permissions as follows: `chmod 644 <files-copied>` • **SP CD/DVD** The files are located in a CD or DVD. • **SP USB Device** The files are located in a USB flash drive.

Button descriptions

Button	Description
Search	Searches for a template description file that has an .ovf (Open Virtualization Format) extension at the location that you specify. Opens the Platform Upgrade Details page with the search results. **Note:** Open virtualization format (OVF) is an open standard for packaging and distributing software that runs on virtual machines.
Select	Selects the required template description file.
Upgrade	Upgrades the system with the template description file.
Commit	Commits an upgrade operation and upgrades the System Platform software to the latest version. **Note:** After executing a commit operation, you cannot go back to the older version of the System Platform software. If you do not execute a commit operation within 4 hours after the upgrade, the system performs an automatic rollback.
Rollback	Cancels an upgrade operation, and the system goes back to the previous version of System Platform software.
Acknowledge	Lets you confirm the reason for the rollback operation.

Upgrading System Platform on High Availability Systems

Methods for upgrading High Availability systems

You can upgrade System Platform either on both servers or on the preferred server only.

Upgrading System Platform on both servers

With this method, you must upgrade System Platform on each server. However, the benefit is that you can perform both upgrades from the System Platform Web Console. Therefore, you do not need direct access to the servers.

Upgrading System Platform on the preferred server only

With this method, you upgrade System Platform on the preferred server only. You do not upgrade the standby server. However, you must reinstall the standby server with the same version of System Platform as the preferred server was upgraded to. This task requires direct access to the standby server.

Stop and start of High Availability for platform upgrades

Stopping High Availability for platform upgrades

System Platform does not support platform upgrades while High Availability is running. If you attempt an upgrade while High Availability is running, a warning message is displayed and the system will prevent you from performing the upgrade. To proceed, first stop High Availability.

Starting High Availability after platform upgrades

Once you have finished the platform upgrade procedure on both servers, you can start High Availability from the Failover page.

This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.

Stopping High Availability

This procedure restarts the console domain and all template virtual machines.

1. Click **Server Management** > **Failover**.
2. Click **Stop 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.

3. Log in to the System Platform Web Console.
4. Click **Server Management** > **Failover** and check the status of the High Availability Failover.

Starting High Availability Failover

Prerequisites

High Availability Failover is configured on the system.

This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.

This procedure restarts the console domain and all template virtual machines.

1. Click **Server Management** > **Failover**.
2. 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.
3. Log in to the System Platform Web Console.
4. Click **Server Management** > **Failover** and check the disc synchronization progress.

Upgrading System Platform on both servers

Prerequisites

Stop High Availability.

1. Login to the System Platform Web Console on the standby node.
   The System Platform Web Console of the standby node displays the failover status in the upper right corner.
2. Go to the Platform Upgrade page and proceed with the upgrade procedure of the standby node.
3. Log in to the System Platform Web Console for the preferred node.

The System Platform Web Console of the preferred node displays the failover status in the upper right corner.

4. Go to the Platform Upgrade page and proceed with the upgrade procedure of the preferred node.
5. Once finished, start System Platform High Availability from the Failover page of the preferred node.

Note:

The order of upgrades of the servers is not really important. This is only a suggested order of the upgrades. Platform upgrade must be performed on each server separately. A difference of version between the servers will prevent System Platform High Availability from starting after the upgrade is complete.

Related topics:

Upgrading System Platform on page 46
Stopping High Availability on page 51
Starting High Availability Failover on page 52

Upgrading System Platform on the preferred server only

Prerequisites

Stop High Availability.

1. Log in to the System Platform Web Console on the preferred node.
   The System Platform Web Console displays the failover status in the right upper corner.
2. Click **Server Management** > **Failover**.
3. Click **Remove Failover** and confirm the warning.
4. Go to Platform Upgrade page and proceed with the upgrade procedure of the preferred node.
5. Reinstall the standby node with the same version of System Platform as the preferred node was upgraded to.
6. Once finished, configure and start High Availability from the Failover page of the preferred node.

Note:

Both servers must be running the same version of System Platform. A difference of version between the servers will prevent you from starting System Platform High Availability after the upgrade is complete.

Related topics:

Upgrading System Platform on page 46
Stopping High Availability on page 51
Starting High Availability Failover on page 52

Chapter 5: Installing System Manager

Downloading System Manager from PLDS

1. Type `http://plds.avaya.com` in your web browser to open the Avaya Product Licensing and Delivery System Web (PLDS) site.
2. Click **Log in with my password**.
3. Enter your login and password details.
   Your login Id is your e-mail address.
4. Click **Log In**.
5. On the Home page, expand Asset Mgmt and click **View Downloads**.
6. On the Downloads page, enter your company's name in the **%Company** field.
7. In the **Application drop down** menu, choose “System Manager”.
8. Click **Search Downloads**.
9. From the Software Downloads list, locate the `System_Manager_06_00_00.iso` file and download them.
   The ISO file contains the following files:
   a. System Manager 6.0 template (gzip file)
   b. System Manager 6.0 backup plugin script (sh file)
   c. System Manager 6.0 template descriptor (ovf file)
   d. System Manager 6.0 manifest file (mf file)

   You can also download the files that are present in the ISO file individually from the same location.
10. On the About the Download Manager page, click **Click to download your file now**.
11. If you receive an error message, click on the message, install Active X, and continue with the download.
12. When the system displays security warning, click **Install**.

When the installation is complete, Product Licensing and Delivery System (PLDS) displays the downloads again with a check mark.

Installing the System Manager template

When you install System Manager on a virtual machine using the System Manager template, the System Manager template installs Linux operating system and System Manager.

Prerequisites

Use `System Platform 6 build 11 ISO image` to install System Platform.

Note:

For more information on installing System Platform, see Chapter 3, “Installing System Platform”.

1. Perform the following sub steps in this step if you downloaded the `System_Manager_06_00_00.iso` file containing the System Manager installation files:
   a. Log in to System Platform on C-dom with root privileges using **`ssh`** .
   b. Type `mkdir /iso` at the command prompt.
   c. Copy the `System_Manager_06_00_00.iso` file in the `/tmp` folder.
   d. Type `mount -o ro,loop /tmp/System_Manager_06_00_00.iso /iso` at the command prompt.
   e. Type `cd /iso` at the command prompt to verify if the following files are present in the `iso` folder.
      a. System Manager 6.0 template (gzip file)
      b. System Manager 6.0 backup plugin script (sh file)
      c. System Manager 6.0 template descriptor (ovf file)
      d. System Manager 6.0 manifest file (mf file)
2. Enter the `https://<IPAddress>/webconsole` URL in the web browser to open the C-dom web console. Here, <IPAddress> is the IP address of C-dom.
3. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
4. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.

5. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:

   You can download the installation files from the PLDS Web site or you can extract the files from the ISO image of the installer, and store it at different locations. The locations depend on the mode of deploying the System Manager Template. For more information on Selecting a template, see the Search Local and Remote Template field descriptions section in Chapter 3, “Installing System Platform”.

6. Click **Search** to find the installation OVF file.
7. From the **Select Template** drop-down field, click the `SystemManager_06_00_Install.ovf` file and click **Select**.
8. On the Templates Details page, click **Install**.
9. Click **Save**.
10. On the Templates Details page, in the **IP address of the SMGR** field enter the IP address of the virtual machine on which you are installing System Manager.

    This IP address should be different from the IP address of the C-dom and Dom–0 virtual machines.

11. In the **SMGR short hostname** field, enter the short host name of the virtual machine.
12. In the **SMGR domain** field, enter an appropriate domain name based on your enterprise environment.

    For example, you can enter a domain name in the form of mydomain.com.

13. In the **Gateway address** field, enter the IP address of the computer configured as gateway in your enterprise environment.
14. In the **Network mask** field, enter the network mask value.
15. In the **DNS** field, enter the IP address of the domain name server.
16. In the **SearchString** field, enter a search string.
17. In the **Non-root User** field, enter the non root user name. This is an optional field.
18. Click **Install**.

    After the completion of System Manager installation, enter the `https://<IPAddress>/SMGR` URL in the web browser to access System Manager, where *<IPAddress>* is the IP address of the System Manager virtual appliance.

    Note:

    See System Manager 6.0 GA Release Notes on the Avaya Support Web site for any post install patches to be applied.

Default Credentials

Accessing System Manager Virtual Appliance

To log in to the command prompt of the System Manager virtual appliance, you need to ssh to the IP address of the virtual appliance. Use root as the login ID and root01 as password. You must change the default password when you log in for the first time.

In case of non-root installation, the password is same as the non-root User ID that you entered in the **Non-root User** field during the System Manager installation.

Accessing System Manager Common Console

To access the System Manager Common Console, enter the `https://<IPAddress>/SMGR` URL in the web browser where <IPAddress> is the IP address of the System Manager virtual appliance. The default user name and password for accessing the System Manager common console is admin and admin123. You must change the default password when you log in for the first time.

Chapter 6: System Manager Upgrades

As there is no direct path available to upgrade System Manager from Release 1.0 to Release 6.0, you have to first upgrade System Manager from Release 1.0 to Release 5.2 and then from Release 5.2 to Release 6.0.

Performing load to load upgrade

Prerequisites

- Applied all the patches provided for the System Manager release that you are upgrading from.
- Backup of the installed System Manager Template. Avaya recommends to store the backup on an external device. For more information on creating a backup of the installed System Manager data, refer System Manager GA Release Notes on the Avaya Support Web site.
- System Platform 6 build 6 installed on your computer. For more information on installing System Platform, see Chapter 3, “Installing System Platform”.
- A list containing few users and roles that exists in the current release of System Manager. After the upgrade, you require this list to verify if the upgrade has successfully imported the users and roles present in the list from the previous release to the new release.
- See System Manager 6.0 GA Release Notes on the Avaya Support Web site for any pre upgrade patches to be applied.

1. Download the latest System Manager Template files from the Avaya PLDS Web site.
2. Enter the `https://<IPAddress>/webconsole` URL in the web browser to log in to the C-dom web console, where <IPAddress> is the IP address of the C-dom web console.
3. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
4. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.

5. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:

   The files downloaded from the PLDS Web site or extracted from the ISO image of the installer in step 1 can be stored on different locations. The selection of a location depends on the mode using which you want to deploy the System Manager template. See the Search Local and Remote Template field descriptions section in Chapter 3, “Installing System Platform”.

6. Click **Upgrade**.
7. On the Select Template page, click the `SystemManager_06_00_Upgrade.ovf` file and click **Select**.
8. Click **Upgrade**.
9. Click **Save**.
10. Click **Upgrade**.
11. After the upgrade is complete, open a new browser and enter the `https://<IPAddress>/SMGR` URL to access the System Manager, where <IPAddress> is the IP address of the System Manager virtual appliance.
12. Log in to the System Manager common console and check whether the users, roles that were present in the previous release of System Manager are successfully exported in the upgraded release.
13. Click **Commit Installation** .

    If the verification as specified in step 11 and 12 failed, click **Rollback Installation**.

    Note:

    See System Manager 6.0 GA Release Notes on the Avaya Support Web site for any post install patches to be applied.

Performing System Manager Upgrade from Release 1.0 to 5.2

For more information on upgrading from System Manager 1.0 to System Manager 5.2, refer to *Installing and Upgrading Avaya Aura™ System Manager Release 5.2*. You can download this guide from the Avaya PLDS Web site.

Performing System Manager upgrade from Release 5.2 to 6.0

Prerequisites

- Applied all the patches provided for the System Manager release that you are upgrading from.
- Backup of the installed System Manager Template. Avaya recommends to store the backup on an external device. For more information on creating a backup of the installed System Manager data, refer System Manager GA Release Notes on the Avaya Support Web site.
- System Platform 6 build 11 installed on the server. For more information on installing System Platform, see Chapter 3, “Installing System Platform”.

  For information on upgrading to System Platform 6 build 11, see Chapter 4, “Upgrading System Platform”
- A list containing few users and roles that exists in the current release of System Manager. After the upgrade, you require this list to verify if the upgrade has successfully imported the users and roles present in the list from the previous release.
- See System Manager 6.0 GA Release Notes on the Avaya Support Web site for any pre upgrade patches to be applied.

1. Download the latest System Manager Template files from the Avaya PLDS Web site.
2. Enter the `https://<IPAddress>/webconsole` URL in the web browser to log in to the C-dom web console, where <IPAddress> is the IP address of the C-dom web console.
3. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
4. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.
5. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:

   The files downloaded from the PLDS Web site or extracted from the ISO image of the installer in step 1 can be stored on different locations. The selection of a location depends on the mode using which you want to deploy the System Manager template. See the Search Local and Remote Template field descriptions section in Chapter 3, “Installing System Platform”.
6. Click **Upgrade**.

7. On the Select Template page, click the `SystemManager_06_00_Upgrade.ovf` file and click **Select**.
8. Click **Upgrade**.
9. Click **Save**.
10. Click **Upgrade**.
11. After the upgrade is complete, open a new browser and enter the `https://<IPAddress>/SMGR` URL to access the System Manager, where <IPAddress> is the IP address of the System Manager virtual appliance.
12. Log in to the System Manager common console and check whether the users, roles that were present in the previous release of System Manager are successfully exported in the upgraded release.
13. Click **Commit Installation**.

    If the verification as specified in step 11 and 12 failed, click **Rollback Installation**.

    Note:

    See System Manager 6.0 GA Release Notes on the Avaya Support Web site for any post install patches to be applied.

Default credentials

Accessing System Manager Virtual Appliance

To log in to the command prompt of the System Manager virtual appliance, you need to ssh to the IP address of the virtual appliance. Use root as the login ID and root01 as password. You must change the default password when you log in for the first time.

In case of non-root installation, the password is same as the non-root User ID that you entered in the **Non-root User** field during the System Manager installation.

Note:

For root user, an upgrade resets the password to root01.

Note:

For non-root user, an upgrade resets the password to the non-root User ID that you entered in the **Non-root User** field during the System Manager installation.

Chapter 7: Modifying Alarm ID and Managed Element ID

After the new installation, the system needs to be registered using the Functional Location (FL) and product type. At that point, a Product ID will be provided for each managed element for alarm reporting.

Modifying an Alarm ID

1. Log in to the computer on which you installed System Manager.
2. At the command prompt, type `cd $SPIRIT_HOME/scripts/` and press `Enter`.
   The `$SPIRIT_HOME/scripts/` directory has SAL Agent command line utilities.
3. Type `sh spiritAgentCLI` and press `Enter` to execute the SAL Agent command line utility.
   This displays the command line options. Each option is assigned a number.
4. Type `1`.
5. Type the new alarm ID when the prompt asks you to enter the new SAL alarming ID and press `Enter`.
6. On the main menu, type `99` to save the changes and quit the SAL Agent command line utility.
   The alarm Id is modified to the required value.

Modifying a Managed Element ID

1. Log in to the computer on which you installed System Manager.
2. At the command prompt, type `cd $SPIRIT_HOME/scripts/utils` and press `Enter`.

   The `$SPIRIT_HOME/scripts/` directory has SAL Agent command line utilities.
3. Type `sh setProductID.sh` *`ProductType Element_ID`* and press `Enter`, where:

   - **`sh setProductID.sh`** is the command line utility for setting the managed element ID.
   - *ProductType* is the name of the product for which you want to modify the managed element ID. Currently, SAL Agent is configured with the following ProductType: SM and SMELEM.
   - *Element_ID* is the new managed element id for the specified product.

   For example: sh setProductID.sh SM 70000002, where SM is the name of the product and 70000002 is the new element ID that you want to assign to the product.
4. Type `sh setOverrideMeId.sh SM` to set the override managed element id to required value.
5. Type `service spiritAgent restart` to restart SAL Agent.

Chapter 8: Generating Test Alarms

You can generate a test alarm and a clear event corresponding to the generated test alarm. The severity level of the test alarm is minor. The clear event generated has no definite severity level. The clear event updates the status of the test alarms from Raised to Cleared. If Secure Access Link (SAL) Enterprise is configured to forward alarms to Avaya Data Center (ADC), the system also forwards the test alarm and the clear event for the test alarm to the ADC.

Test Alarm Event

Test Alarm property	Value
Alarm.Message	Test alarm
Alarm. Severity	Minor
Alarm.Status	Raised
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_GEN_0001

Test Clear Event

Test Clear Event property	Value
Alarm.Message	Clear event for test alarm
Alarm. Severity	Indeterminate
Alarm.Status	Cleared
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_CLR_0000

Generating a test alarm

1. Log in to the computer on which you installed System Manager.
2. Type `service spiritAgent status` at the command prompt and press `Enter` to check the status of SAL Agent.
   The system displays a message
   `SPIRIT Agent is running`
3. Type `SPIRIT Agent # service spiritAgent start` at the command prompt and press `Enter` to start SAL Agent.

   Note:
   Run this step only if on running step 2, the system displays a message
   `SPIRIT Agent is not running`
4. Type `cd $SPIRIT_HOME/scripts/utils/` at the command prompt and press the `Enter` key to go to the `/utils` directory.

   The `utils` directory contains SAL Agent command line utilities.
5. Type `sh generateTestAlarm.sh` and press the `Enter` key to generate a test alarm.

   Type `sh generateTestAlarm.sh -c` and press the `Enter` key to generate a clear alarm type.

Chapter 9: Removing the System Manager template

1. Enter the `https://<IPAddress>/webconsole` URL in the web browser to log in to the C-dom web console, where <IPAddress> is the IP address of C-dom.
2. Log in to the C-dom web console with the administrator credentials made available at the time of the System Platform installation.
3. On the System Platform console, click **Virtual Machine Management** > **Solution Template** in the left navigation pane.
4. Click **Delete Installed Template** to delete the System Manager Template.

Chapter 10: High Availability support for System Manager

System Manager leverages the failover mechanism provided by System Platform. A setup of High Availability requires two nodes that have exactly the same hardware and software configuration. One of these nodes acts as an Active node or preferred node and the other node acts as a Standby node.

The High Availability setup requires System Platform on both the nodes. But System Manager is installed on the Active node only. Note that though both the nodes are turned on but at a time virtual machines run only on the Active node. This means the System Manager is accessible on the active node only.

In the High Availability setup virtual machines have the same IP addresses on the Active and Standby nodes. Both network adapters are configured as ping paths between cluster nodes, the network switch (gateway IP address) as a public ping point - so each node has 3 ping points. Heartbeat is able to detect which node has more communication paths available and migrates resources into that node.

Each node dedicates one network adapter to data exchange related to High Availability and nodes are connected to each other by a cross over cable. All disk data is continuously replicated from the Active node to the Standby node. The system uses the network adapter dedicated to High Availability data exchange for HA pings and Distributed Replicated Block Device (DRBD) propagation between the two nodes.

The Standby node pings the Active node at regular intervals to check if the Active node is up and running. If the Primary node fails, the virtual machines and the applications installed on these virtual machines on the Standby node are automatically started and the Standby becomes Active node. The user is automatically redirected to the Standby node.

Currently, the failover process takes some time to complete and the system logs you out immediately when a failover starts. You have to log in to System Manager again to access the application.

In the High Availability configuration mode, the data between the Active and Standby nodes is synchronized at regular intervals. The synchronizing process uses a very reliable protocol that ensures that all block changes are committed and acknowledged on the Standby node before processing the next transaction.

Note:

For more information on High Availability, see Chapter 3, “Installing System Platform, section “System Platform High Availability Failover” .

Start and stop of High Availability Failover

Starting High Availability Failover

System Platform can be changed from a standard configuration to a High Availability Failover configuration during system installation or anytime later. Once you have installed a new server that has the same configuration, such as the number of processors and disk space, and installed the same version of System Platform, you are ready to proceed.

Important:

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.

When you start High Availability Failover, the console domain and all template virtual machines are restarted. When this happens, System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.

Stopping High Availability Failover

If you want to stop High Availability Failover, you should do so as soon as no disk synchronization is in progress or the disc synchronization is not paused. If you stop High Availability Failover during disk synchronization, the file system of the standby console domain could be corrupted.

When you stop High Availability Failover, the console domain and all template virtual machines are restarted. When this happens, System Platform Web Console redirects to the Reboot page and after a few minutes redirects to the Login page.

When High Availability Failover is stopped, the system does not propagate changes from the preferred node to the standby node.

When High Availability Failover is stopped, you can access the Web Console on the standby server by using its IP address (provided during configuration of High Availability Failover).

Removing the High Availability Failover configuration

If you want to permanently remove the High Availability Failover configuration, you can do so.

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.

Name	Description
Crossover network interface	Network interface connected to the standby server.

Starting High Availability Failover

Prerequisites

High Availability Failover is configured on the system.

This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.

This procedure restarts the console domain and all template virtual machines.

1. Click **Server Management** > **Failover**.
2. 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.
3. Log in to the System Platform Web Console.
4. Click **Server Management** > **Failover** and check the disc synchronization progress.

Stopping High Availability Failover

This procedure stops High Availability Failover but does not remove the High Availability Failover configuration. You can restart it at any time.

This procedure restarts the console domain and all template virtual machines.

1. Click **Server Management** > **Failover**.
2. Click **Stop 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.
3. Log in to the System Platform Web Console.
4. Click **Server Management** > **Failover** and check the status of the High Availability Failover.

Index

Numerics

1.0 to 5.2 60

A

admin password 30

C

checklist
  installation 15
  preinstallation 9
checklist, installation, ...7
command line
  accessing Console Domain 35
  accessing System Domain 35
Commit 47
Configure Failover page
  field descriptions 44, 71
console domain
  configuring network settings 26
Console Domain
  accessing command line 35
Console Domain Network Configuration screen
  configuring 26
craft password 30
cust password 30

D

date
  configuring 28
Date/Time and NTP setup screen
  configuring 28
default credentials 58, 62
downloading software 12
downloading System Manager from PLDS 55
DVD
  recommendations 14
  writing ISO image 14

F

failover
  configuring 43, 71
Firefox
  disabling proxy servers 19

G

generate test alarms 65
generating a test alarm 66

H

hardware requirements 5
High Availability
  about start and stop for upgrades 51
  stopping 51
High Availability Failover
  configuring 43, 71
  overview 41
  prerequisites for configuring 43, 70
  requirements 42
  starting 52, 72
  stop and start of 70
  stopping 72
High Availability overview 69
High Availability systems
  about platform upgrades 51
  upgrading System Platform 52, 53

I

installation
  checklist 15
  using laptop 20
  using server console 21
installation checklist 7
installing System Manager template 56
Internet Explorer
  disabling proxy servers 19
introduction 5
IP forwarding
  disabling 33
  enabling 33
IP settings
  configuring on laptop 18
ISO image
  verifying on DVD 23

verifying on Linux-based computer 12
verifying on Windows-based computer 13
writing to DVD 14

K

keyboard
selecting type 22
Keyboard Type screen 22

L

laptop
configuring to connect to server 18
connecting to server 32
using to install System Platform 20
ldap password 30
legal notice 2

M

modify Alarm ID 63
modify Managed Element ID 63
modifying a Managed Element ID 64
modifying an Alarm ID 63

N

network settings
configuring for console domain 26
configuring for system domain (domain-0) 24
NTP server
configuring in System Platform 28

P

passwords
configuring in System Platform 29
default 29
Passwords screen
configuring 29
field descriptions 30
performing load to load upgrade 59
performing System Manager upgrade 60
performing System Manager upgrade from 5.2 to 6.0 ... 61
platform upgrade 45
Platform Upgrade page
field descriptions 49
PLDS 11, 12
downloading software 12
preinstallation checklist 9
proxy servers
disabling in Firefox 19
disabling in Internet Explorer 19

R

registering 11
registration
of system 10, 39
removing the System Manager Template 67
requirements
for High Availability Failover 42
Rollback 47
root password 30

S

SAL Gateway
about 39
configuring 40
registering 10, 39
Search Local and Remote Template page
field descriptions 37
server
connecting laptop 32
server console
using to install System Platform 21
services port
accessing System Platform through 33
solution template
installing 36
registering applications 10, 39
System Domain
accessing command line 35
system domain (domain-0)
configuring network settings 24
System Domain Network Configuration screen
field descriptions 25
System Manager information worksheet 7
System Platform
registering 10, 39
System Platform Web Console
accessing 33

T

Telnet

opening session from laptop to System Platform server 20
template
installing 36
time
configuring 28
time zone
configuring 28
Time Zone Selection screen
configuring 28

U

upgrade System Manager Template 59
upgrades
about stop and start of High Availability 51
upgrading System Platform
on High Availability systems 52, 53
on preferred server 53
upgrading to System Manager 5.2 60

V

Virtual Machine Management page
field descriptions 37
VSP Console Domain Network Configuration screen
configuring 26
field descriptions 27
vspmediacheck 23

W

Web Console
accessing 33
worksheet, System Manager information 7