Installing and Configuring Avaya Aura® Session Border Controller

Release 6.0.1
November 2010

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

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

Link disclaimer

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

Warranty

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

Licenses

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

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

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third-party Components" for more information).

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those

Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

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

Trademarks

Avaya® and Avaya Aura® are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

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://support.avaya.com.

Contents

Chapter 1: Session Border Controller installation overview

Overview

Avaya Aura® Session Border Controller connects the unified communication solution through IP to other VoIP-enabled entities, either internally or externally.

Important:

Before installing Session Border Controller, you must refer the latest version of the following documents available at http://support.avaya.com:

Avaya Aura® Session Border Controller R 6.0.1 Release Notes

Avaya Aura® Session Border Controller High Availability Configuration Details application notes

Before installing Session Border Controller, obtain the following:

- System Platform installer files
- Avaya Aura® Session Border Controller license and installer files

You can obtain the System Platform installer file and the Session Border Controller license and installer files by one of the following methods:

Download the ISO images for the System Platform installer files and the Session Border Controller license and installer files from the Product Licensing Delivery System (PLDS) Web site (http:// plds.avaya.com).

Order for the System Platform CD-ROM and the Session Border Controller DVD to be shipped with the system.

Before installing Session Border Controller, you must install System Platform on the system. For detailed information about System Platform installation, see System Platform installation process on page 15.

The Session Border Controller supports two types of installation wizards:

- Session Border Controller standalone preinstallation wizard:

  The standalone preinstallation wizard supports configurations (in the form of an EPW file) to be built off-line. You can then upload the file during the installation process. The configuration pages for the standalone preinstallation wizard are the same as the configuration pages for the embedded installation wizard. The only difference is in the initial and final steps of loading and saving the file containing the Session Border Controller configuration parameters. This file is called the EPW file. The last step allows you to save the configuration in the EPW file.

- Session Border Controller embedded installation wizard:

  The embedded installation wizard has the same configuration pages as the standalone preinstallation wizard. The only difference is in the initial and final steps of loading and saving the EPW file. The embedded installation wizard does not support the loading and saving of configurations through the EPW file.

The Session Border Controller installation wizards support the following two installation types:

- Full installation wizard: Use this option to configure a basic SIP trunk for any of the supported service providers.
- Minimal installation wizard: Use this option to configure an IP address on the management interface. This enables subsequent configuration to take place manually through the Session Border Controller Web console or command line interface.

  For detailed information about the two installation types, see Installation type on page 10.

Note:

On a public interface, Session Border Controller 6.0.1 does not support VLAN tagging. If you enable any VLAN tagging functionality on the Session Border Controller, it will not work as expected.

Related topics:

Installation type on page 10

Installation type

The Avaya Aura® Session Border Controller installation wizard supports the following two installation types:

Full installation wizard:

The full installation wizard is the default installation type. Use this option to configure a basic SIP trunk for any of the supported service providers. The full installation wizard enables you to:

Configure network settings

Configure services and business partner logins

Configure VPN access for alarming and remote access as an alternative to SAL

Configure Session Border Controller data settings

Review installation summary

Finish installation

Minimal installation wizard:

Important:

The minimal installation wizard option is only intended for advanced users who prefer to configure the components of the solution manually.

Use this option to configure an IP address on the management interface. This enables subsequent configuration to take place manually through the Session Border Controller Web console or command line interface. The minimal installation wizard enables you only to:

Configure network settings

Configure services and business partner logins

Review installation summary

Finish installation

Related topics:

Selecting the installation type on page 11

Selecting the installation type

1. On the left navigation menu of the Network Settings screen, click **Configuration** > **Installation Type**.
   The system displays the Installation Type screen.
2. Select one of the following installation types:
   - **Full Installation Wizard**
   - **Minimal Installation Wizard**

   For more information about the installation types, see Installation type on page 10.

Installation checklist for Session Border Controller

Task	Notes	✔
Gather the required equipment and information relating to installation, such as IP addresses, Alarm Ids for		

Task	Notes	✔
System Platform and for Avaya Aura® Session Border Controller. See Installation prerequisite on page 173.		
Obtain the System Platform and Avaya Aura® Session Border Controller installer files by one of the following methods: Download from PLDS (Product Licensing Delivery System) Web site: a. Download the System Platform and Avaya Aura® Session Border Controller installer files from the Product Licensing Delivery System (PLDS) Web site—http:// plds.avaya.com. b. Copy the installer files to a USB flash drive or write them on to a CD (System Platform) and DVD (Session Border Controller template). Order the System Platform CD and Avaya Aura® Session Border Controller DVD: Place an order for the Avaya Aura® Session Border Controller template DVD and the System Platform CD to be shipped with the system.		
Install System Platform.For detailed information about System Platform installation, see Software installation on page 16.		
Log in to the System Platform Web console. Select the appropriate template. The type of template you select depends on whether you use the IBM S8800 1U Server ,HP ProLiant DL360 G7, orDell™ PowerEdge™ R610(SBCT.ovf) or the HP Procurve blade server (SBCT_Procurve.ovf).		
Populate the required fields in the Avaya Aura® Session Border Controller preinstallation wizard to create an Electronic Preinstallation Worksheet (EPW) file. Now install Avaya Aura® Session Border Controller.		
Apply the Avaya Aura® Session Border Controller license using the WebLM server. **Important:** WebLM licensing uses the second MAC address reported by the WebLM System Properties for licensing and does not require the Session Border Controller system information. Licensing can also be applied before installing Session Border Controller.		

Task	Notes	✔
Configure Secure Access Link (SAL) for remote access and alarming. Integrate Avaya Aura® Session Border Controllerwith Communication Manager orSession Manager. Now make a test call to check if the configuration is complete. **Note:** If you are an Avaya business partner and choose not to configure SAL for remote access and alarming, you must configure VPN access for remote access. However, SAL is the preferred mode for remote access and alarming.		

Chapter 2: System Platform installation

System Platform installation overview

System Platform installation process

Installation of System Platform consists of the following tasks:

1. Install the server hardware.
2. Connect the server to the customer network.
3. If you are using the Avaya Aura® Session Border Controller high availability failover option, connect the two servers.

   Note:

   Avaya Aura® Session Border Controller does not use the standard System Platform high availability option. The Session Border Controller high availability option is unique to Avaya Aura® Session Border Controller.

   Connect the two servers with a Gigabit-certified Ethernet cable between port 3 of each server.

   Important:

   Avaya Aura® Session Border Controller high availability failover is not supported when using the HP Procurve blade server.
4. Install the System Platform software on the servers.
5. Install the Avaya Aura® Session Border Controller solution template.
6. Configure the Secure Access Link (SAL) gateway that is included in System Platform for remote support and alarming.

   Note:

   On the Avaya Aura® Session Border Controller high availability failover systems, configure SAL gateway on both servers.
7. Configure Avaya Aura® Session Border Controller high availability failover if using the option.For detailed information about Avaya Aura® Session Border Controller

high availability failover configuration, see *Avaya Aura® Session Border Controller R 6.0.1 Release Notes* and *Avaya Aura® Session Border Controller High Availability Configuration Details* application notes.

Software installation

To install System Platform, you must obtain the installer and license files by performing one of the following actions:

- Download the System Platform installer files from the Avaya PLDS Web site (http://plds.avaya.com) and then burn the ISO image to a CD.
- Place an order for the System Platform CD to be shipped with the system.

Use one of the following methods to install System Platform:

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

Note:

On the S8800 1U Server the services port is located on the back of the server. The port is generally the physical port 2 and software Ethernet port 1.

On the HP Procurve blade server, the services port is located on the front of the blade. The port is located on the HP Extended Services zl Module, physically labelled as the management port.

If you use a laptop to install the System Platform software, you must have PuTTY SSH client on your laptop. You must change the client from the default ssh option to TELNET. Make sure that you change the network settings on the laptop before connecting to the server. See Configuring the laptop for direct connection to the server on page 27.

Use the provided worksheets and checklists during installation.

Installation requirements for System Platform

What Avaya provides

Avaya provides the following items for installing System Platform:

- One or two servers. One is for a standard configuration, and two are for High Availability Failover configuration.
- Slide rails to mount the servers in a standard 19-inch, 4-post rack that have square holes.
- System Platform installation software.
- Other hardware as ordered, such as an uninterruptible power supply (UPS). UPS is a required component.
- Product registration form. The form is available on http://support.avaya.com. Click **More Resources** > **Equipment Registration (Partners only)**. Click **Universal Install/SAL Product Registration Request Form** under **Non-Regional (Product) Specific Documentation**. For more information, see Registering the system on page 19.

Note:

Avaya provides the System Platform installation software. The customer must either purchase the System Platform CD or download the ISO image and write that image to a CD or DVD.

What customer provides

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

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

  Note:

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

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

- Gigabit-certified Ethernet cable for Session Border Controller High Availability Failover configuration.
- DVDs written with the software for installing .
- A computer that can route to the System Platform server that has Internet Explorer 7 or Firefox 2 or Firefox 3 installed on it.
- Filled-out worksheets with the system and network information needed for installation and configuration.
- Access to the customer network.
- (Optional) VPN Gateway for providing remote access to Avaya Partners.

Note:

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

Preinstallation tasks for System Platform

Preinstallation checklist for System Platform

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 19.	**Important:** Submit the registration form three weeks before the planned installation date.	
2	Gather the required information relating to installation, such as IP configuration information, DNS addresses, and address information for Network Time Protocol (NTP) servers. See Installation checklist for System Platform.		

No.	Task	Notes	✔
3	Register for PLDS if you are not already registered. See Registering for PLDS on page 20.		
4	Download the System Platform installer ISO image file from PLDS. See Downloading software in PLDS on page 21.		
5	Download the appropriate solution template and licenses from PLDS. See Downloading software in PLDS on page 21.		
6	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 22 and Verifying the ISO image on a Windows-based computer on page 22.		
7	Write the ISO images to separate DVDs. See Writing the ISO image to DVD or CD on page 23.	**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.	

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 components of System Platform and of the applications that are included in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

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

1. Access the registration form and follow the instructions. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.
2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date 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 an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices.
3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

Related topics:

SAL Gateway on page 73

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 your 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 that have been completed successfully.

Verifying the downloaded ISO image

Verifying the ISO image on a Linux-based computer

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

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. 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 or CD

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.

If you are writing to a DVD, this procedure requires a computer or server that has a DVD writer and software that is capable of writing ISO images to DVD. If you are writing to a CD, this procedure requires a computer or server that has a CD writer and software that is capable of writing ISO images to CD.

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 or CD.

Installing System Platform

Installation methods

Use one of the following methods to install System Platform:

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

Note:

You can 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 an SSH and Telnet client application such as PuTTY installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server. See Configuring the laptop for direct connection to the server on page 27.

Installation checklist for System Platform

Use this checklist to install System Platform.

Important:

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

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

No.	Task	Notes	✔
	See Configuring the laptop for direct connection to the server on page 27. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Microsoft Internet Explorer on page 27 or Disabling proxy servers in Mozilla Firefox on page 28 .		
2	If you are installing System Platform from a laptop, 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 (NIC) in your laptop, you might be able to use a straight-through cable for this connection. See the documentation for your laptop.	
3	If you are installing System Platform from the server console, connect a USB keyboard, USB mouse, and video monitor to the server.		
4	Turn on the server.		
5	Place the DVD in the DVD drive on the server. See Starting the installation from your laptop on page 29 or Starting the installation from the server console on page 30 depending on your selection of installation method.		
6	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 the server console on page 30.		
7	If using your laptop to install System Platform, establish a Telnet connection to the server. See Starting the installation from your laptop on page 29.		

No.	Task	Notes	✔
8	Select the required keyboard type. See Selecting the type of keyboard.		
9	Verify that the image on the System Platform DVD is not corrupt. See #unique_30.		
10	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 32.		
11	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 34.		
12	Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 36.		
13	Configure the date and time and specify an NTP server if using for the System Platform server. See Configuring the date and time for the System Platform server on page 36.		
14	Configure the System Platform passwords. See Configuring System Platform passwords on page 37.		
15	Verify that System Platform installed correctly. See Verifying installation of System Platform on page 39.		
16	Check for System Platform patches at http://support.avaya.com. Install any patches that are available. See *Administering Avaya Aura® System Platform* for information on installing patches.		
17	Configure the SAL gateway for remote access and alarming. See SAL Gateway on page 73.		

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 Microsoft 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.

   Caution:

   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 Microsoft Internet Explorer

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

1. Start Internet Explorer.
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.

   Tip:

   When you need to reenable the proxy server, select the **Use a proxy server for your LAN** option again.
6. Click **OK** to close each dialog box.

Disabling proxy servers in Mozilla Firefox

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

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. Start Firefox.
2. Click **Tools** > **Options**.
3. Select the **Advanced** option.
4. Click the **Network** tab.
5. Click **Settings**.
6. Select the **No proxy** option.

   Tip:

   When you need to reenable the proxy server, select the appropriate option again.
7. Click **OK** to close each dialog box.

Starting the installation

Starting the installation from your laptop

Prerequisites

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

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

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

   Note:

   Depending on the capabilities of the network interface card (NIC) 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 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 an SSH 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.

Related topics:

Connecting to the server through the services port on page 40

Starting the installation from the server console

Prerequisites

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

1. Turn on the server.
2. Insert the System Platform DVD in the server 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 on the Avaya screen, 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.

Selecting the type of keyboard

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

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

2. Use the `Tab` key to highlight **OK** and press **Enter**.

   - The system displays the CD Found screen if you are installing System Platform from a laptop, or if you are installing System Platform from the server console and entered the **`vspmediacheck`** command at the boot prompt on the Avaya screen.

     See Verifying the System Platform image on the DVD on page 31.

   - The system displays the System Domain Network Configuration screen if you are installing System Platform from the server console and did not enter the **`vspmediacheck`** command at the boot prompt on the Avaya screen. See Configuring network settings for System Domain (Domain-0) on page 32.

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 31.

  OR

- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 32

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 system displays the CD Found screen if you are installing System Platform from a laptop, or if you are installing System Platform from the server console and entered the **`vspmediacheck`** command at the boot prompt on the Avaya screen.

On the CD Found screen, perform one of the following actions:

- To test the DVD, use the `Tab` key to select **OK**.

- To skip the test and begin the installation immediately, select **Skip**.

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 displays the System Domain Network Configuration screen.

Next steps

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

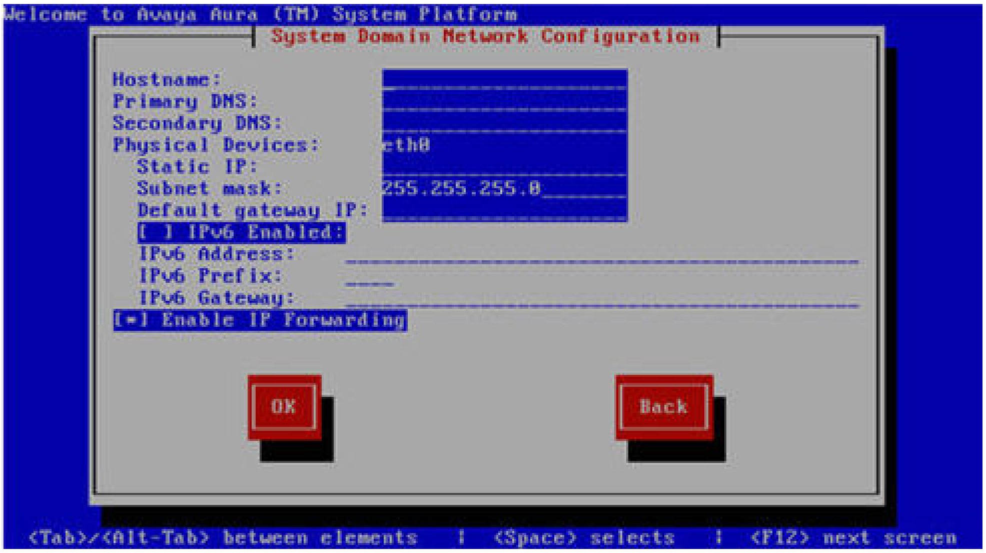
Related topics:

Writing the ISO image to DVD or CD on page 23

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**

   For descriptions of the fields on this page, see System Domain Network Configuration field descriptions on page 34.



```
Welcome to Avaya Aura (TM) System Platform
                    System Domain Network Configuration

        Hostname:
        Primary DNS:
        Secondary DNS:
        Physical Devices:      eth0
          Static IP:
          Subnet mask:         255.255.255.0
          Default gateway IP:
          [ ] IPv6 Enabled:
          IPv6 Address:
          IPv6 Prefix:
          IPv6 Gateway:
        [*] Enable IP Forwarding

                   OK                              Back

  <Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

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 **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).
5. Use the `Tab` key to highlight **OK** and press **Enter** to accept the configuration.
6. If IP forwarding is enabled, a confirmation message is displayed. Use the `Tab` key to highlight **OK** and press **Enter**.

   The system displays the System Platform Console Domain Network Configuration screen.

Next steps

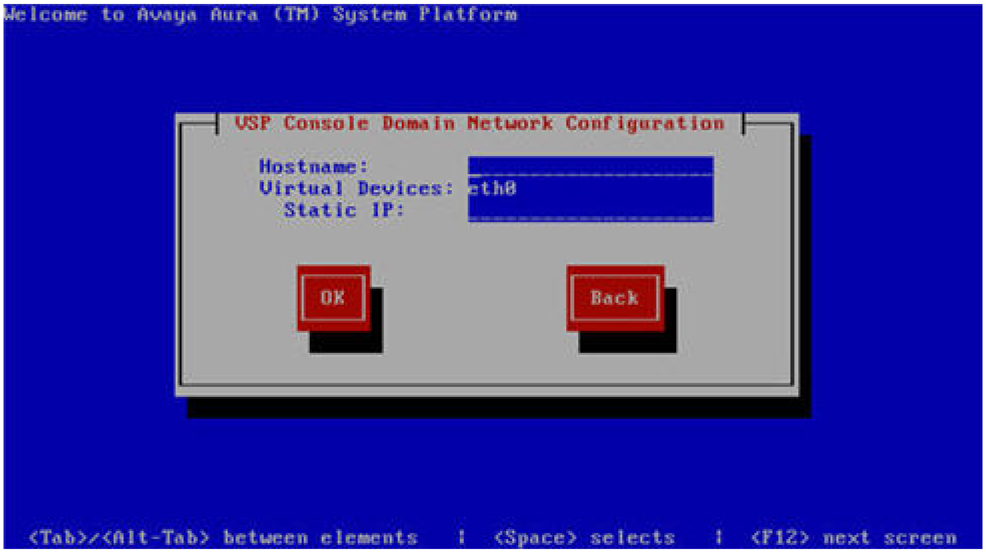
Configure network settings for Console Domain. See Configuring network settings for Console Domain on page 34.

System Domain Network Configuration field descriptions

Name	Description
Hostname	The host name for System Domain (Domain-0). This must be a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
Primary DNS	The primary Domain Name System (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.
Enable IP Forwarding	The indicator to show whether IP forwarding is enabled. An asterisk on the left of the field denotes that IP forwarding is enabled. IP forwarding enables access through the services port to virtual machines on System Platform, including System Domain and Console Domain. IP forwarding must be enabled for both SSH and Web Console access.

Configuring network settings for Console Domain

1. On the VSP Console Domain Network Configuration screen, complete the following fields to set up the Console Domain network:
   - **Hostname**. Enter an FQDN, for example, SPCdom.mydomainname.com.
   - **Static IP**



```
Welcome to Avaya Aura (TM) System Platform

VSP Console Domain Network Configuration

  Hostname:
  Virtual Devices: eth0
    Static IP:

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

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 36.

System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	The host name for the Console Domain. This must be an 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). Because System Domain acts like a bridge, the IP address that you enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).

Configuring the time zone for the System Platform server

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

Next steps

Configure date and time for the System Platform server. See Configuring the date and time for the System Platform server on page 36.

Configuring the date and time for the System Platform server

Avaya recommends that you use a Network Time Protocol (NTP) server within your network to synchronize the time of the System Platform server.

1. Set the current date and time on the Date/Time and NTP setup screen.

   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 servers.
   b. In the **NTP server** fields, enter the DNS name or the IP address of your preferred NTP servers.
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 37.

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 Lightweight Directory Access Protocol (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. Customers are responsible for managing their passwords.

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. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon 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 it manually. The system restarts the installation if the DVD is not ejected.

Caution:

Do not shut down or reboot the server during the first boot process of Console Domain. This process can take up to 20 minutes. If you shutdown or reboot the server during the first boot of Console Domain, System Platform will not function correctly and will have to be reinstalled. To determine if Console Domain has booted, attempt to access the Web Console. See Accessing the System Platform Web Console on page 41.

Next steps

Verify System Platform installation. See Verifying installation of System Platform on page 39.

Passwords field descriptions

Note:

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

Name	Description
root Password	The password for the root login.
admin Password	The password for the admin login.
cust Password	The password for the cust login.
ldap Password	The password for the ldap login.

Name	Description
	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. See Enabling IP forwarding to access System Platform through the services port on page 41.

Important:

You must wait for the first boot process to finish before you can 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 41.
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 (NIC) 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 **admin** or another valid user.
9. When you finish the session, type **`exit`** and press **Enter** to close PuTTY.

Related topics:

Configuring the laptop for direct connection to the server on page 27
Disabling proxy servers in Microsoft Internet Explorer on page 27
Disabling proxy servers in Mozilla Firefox on page 28

Enabling IP forwarding to access System Platform through the services port

To access virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0) . IP forwarding must be enabled for both SSH and Web Console access. You can set the IP forwarding status as enabled or disabled during installation of System Platform. IP forwarding is enabled by default. If you disabled 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. 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. See Enabling IP forwarding to access System Platform through the services port on page 41.

Important:

You must wait for the first boot process to finish before you can 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.

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.

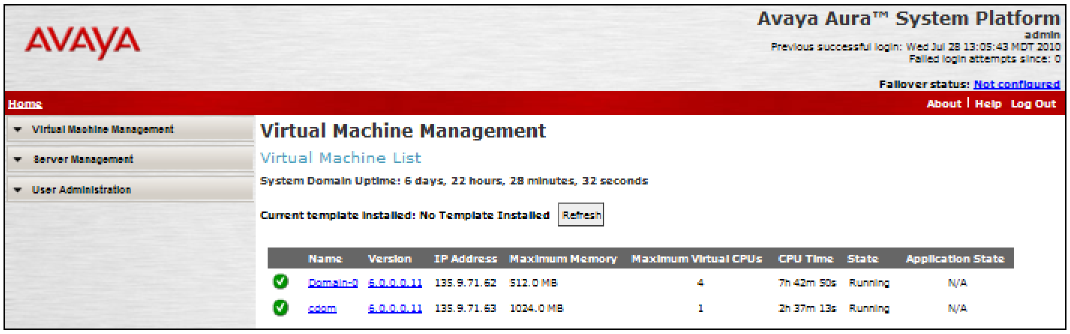
   Currently, System Platform supports Microsoft Internet Explorer 7 and Firefox 2 and 3.
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   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.
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.



Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0

Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Related topics:

Enabling IP forwarding to access System Platform through the services port on page 41

Accessing the command line for System Domain

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

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

   Tip:

   You can obtain the IP address of System Domain (Domain-0) from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su — root`
6. Enter the password for the *root* user.

   Tip:

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

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

Accessing the command line for Console Domain

Important:

You must wait for the first boot process to finish before you can 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.

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

   ⊕ **Tip:**

   The IP address of Console Domain (cdom) is the same as the IP address of the System Platform Web Console.
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.

Server management

Server Management overview

Use the options under Server Management to perform various administrative activities for the System Platform server. Some of the administrative activities that you can perform include:

- Configuring various settings for the server
- Viewing log files
- Upgrading to a latest release of the software
- Backing up and restoring current version of the software

Managing patches

Patch management

You can install, download, and manage the regular updates and patches for System Platform and the various templates provided by Avaya. Go to http://support.avaya.com and see the latest Release Notes for information about the latest patches.

You can install or download the patches from the Avaya Product Licensing and Delivery System (PLDS) Web site at http://plds.avaya.com.

Downloading patches

1. Click **Server Management** > **Patch Management** .
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, choose a location to search for a patch. Options are:
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP** or **SP Server**, specify the **Patch URL**.
5. If you selected **HTTP**, click **Configure Proxy** to specify a proxy server if required.
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Related topics:

Configuring a proxy on page 46

Search Local and Remote Patch field descriptions on page 47

Configuring a proxy

If the patches are located in a different server (for example, Avaya PLDS or HTTP), you may need to configure a proxy depending on your network.

1. Click **Server Management** > **Patch Management**.
2. Click **Upload/Download**.
3. On the Search Local and Remote Patch page, click **Configure Proxy**.
4. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
5. Specify the proxy address.
6. Specify the proxy port.
7. Select the appropriate keyboard layout.
8. Enable or disable statistics collection.
9. Click **Save** to save the settings and configure the proxy.

Related topics:

Search Local and Remote Patch field descriptions on page 47
System configuration field descriptions on page 59

Installing patches

Prerequisites

If installing a service pack as part of an installation, make sure that all applications (virtual machines) are fully installed and running.

Use this task to install all service packs and other patches (that is, System Platform and solution template patches) through System Platform Web Console. Make sure that you do not use the patch installers provided by your solution templates.

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Related topics:

Patch List field descriptions on page 49

Patch Detail field descriptions on page 49

Removing patches

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
3. On the Patch List page, click on a patch that you want to remove.
4. On the Patch Detail page, click **Deactivate**, if you are removing a template patch.
5. Click **Remove**.

   ⊕ **Tip:**

   You can clean up the hard disk of your system by removing a patch installation file that is not installed. To do so, in the last step, click **Remove Patch File**.

Related topics:

Patch List field descriptions on page 49

Patch Detail field descriptions on page 49

Search Local and Remote Patch field descriptions

Use the Search Local and Remote Patch page to search for available patches and to upload or download a patch.

Name	Description
Supported Patch File Extensions	The patch that you are installing should match the extensions in this list. For example, *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.patch.
Choose Media	Displays the available location options for searching a patch. Options are: • **Avaya Downloads (PLDS)**: The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter

Name	Description
	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**: Files are located in a different server. You must specify the Patch URL for the server. • **SP Server**: Files are located in the vsp-template file system in the System Platform server. You must specify the Patch URL for the server. **Tip:** When you want to move files from your laptop to the System Platform Server, you may encounter some errors, as System Domain (Domain-0) and Console Domain support only SCP, but most laptops do not come with SCP support. You can download the following two programs to enable SCP (Search the Internet for detailed procedures to download them): - Pscp.exe - WinSCP • **SP CD/DVD**: Files are located in a System Platform CD or DVD. • **SP USB Disk**: Files are located in a USB flash drive. • **Local File System**: Files are located in a local computer.
Patch URL	Active only when you select **HTTP** or **SP Server** as the media location. URL of the server where the patch files are located.

Button descriptions

Button	Description
Search	Searches for the available patches in the media location you specify.
Configure Proxy	Active only when you select **HTTP** as the media location option. Opens the System Configuration page and lets you configure a proxy based on your specifications. If the patches are located in a different server, you may be required to configure a proxy depending on your network.
Add	Appears when **Local File System** is selected and adds a patch file to the local file system.
Upload	Appears when **Local File System** is selected and uploads a patch file from the local file system.
Download	Downloads a patch file.

Related topics:

Downloading patches on page 45

Configuring a proxy on page 46

Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installing or removing. Use this page to view the details of patch file by clicking on the file name.

Name	Description
System Platform	Lists the patches available for System Platform under this heading.
Solution Template	Lists the patches available for the respective solution templates under respective solution template headings.
Patch ID	File name of a patch.
Description	Information of a patch, for example, if the patch is available for System Platform the description is shown as SP patch.
Status	Shows the status of a patch. Possible values of **Status** are **Installed**, **Not Installed**, **Active**, and **Not Activated**.
Service Effecting	Shows if installing the patch causes the respective virtual machine to reboot.

Button descriptions

Button	Description
Refresh	Refreshes the patch list.

Related topics:

Installing patches on page 46

Removing patches on page 47

Patch Detail field descriptions

The Patch Detail page provides detailed information about a patch. Use this page to view details of a patch or to install, commit, roll back, or remove a patch.

Name	Description
ID	File name of the patch file.
Version	Version of the patch file.
Product ID	Name of the virtual machine.
Description	Virtual machine name for which the patch is applicable.

Name	Description
Detail	Virtual machine name for which the patch is applicable. For example, Console Domain (cdom patch).
Dependency	Shows if the patch file has any dependency on any other file.
Applicable for	Shows the software load for which the patch is applicable.
Service effecting when	Shows the action (if any) that causes the selected patch to restart the System Platform Web Console.
Restart this console when	Shows the conditions or circumstances when the System Platform Web Console must be restarted.
Disable sanity when	Shows at what stage the sanity is set to disable.
Status	Shows if the patch is available for installing or already installed.
Patch File	Shows the URL for the patch file.
Publication Date	Shows the publication date of the patch file.
License Required	Shows whether installation and use of the patch file requires the Avaya Aura customer to obtain a software license from the Avaya corporation.
Rollbackable	Shows whether you can roll back the patch after installation.

Button descriptions

Button	Description
Refresh	Refreshes the Patch Details page.
Patch List	Opens the Patch List page, that displays the list of patches.
Install	Installs the respective patch.
Commit	Commits the installed patch.
Activate	Activates the installed patch of a solution template.
Deactivate	Deactivates the installed patch of a solution template.
Rollback	Rolls back the installed patch if the **Rollbackable** field value is `Yes`.
Remove	Removes the respective patch.
Remove Patch File	Removes the respective patch file. The button appears only if the patch file is still present in the system. On removing the patch file, the button does not appear.

Related topics:

Installing patches on page 46

Removing patches on page 47

Viewing System Platform logs

Log viewer

You can use the Log Viewer page to view the following log files that System Platform generates:

- System logs: These logs contain the messages that the System Platform operating system generates.
- Event logs: These logs contain the messages that the System Platform generates.
- Audit logs: These logs contain the messages that the System Platform generates as a record of user interaction such as the action performed, the time when the action was performed, the user who performed the action, and so on.

To view a log, you should provide the following specifications:

- Select one of the following logs to view:
    - System logs
    - Event logs
    - Audit logs
- Select one of the log levels relevant to the selected logs. The log level denotes the type of incident that might have occurred such as an alert, an error condition, a warning, or a notice.
- Specify a time duration within which an incident of the selected log level might have occurred.
- Enter some text that you want to search in the selected logs. This is optional.

Viewing log files

1. Click **Server Management** > **Log Viewer**.
2. On the Log Viewer page, do one of the following to view log files:
    - Select a message area and a log level area from the list of options.
    - Enter text to find a log.
3. Click **Search**.

Related topics:

Log Viewer field descriptions on page 52

Log Viewer field descriptions

Use the Log Viewer page to view various log messages that the system has generated.

Name	Description
Messages	Select the type of log messages that you want to view. Options are: • **System Logs** are log messages generated by the System Platform operating system (syslog). • **Event Logs** are log messages generated by the System Platform software. These logs are related to processes and commands that have run on System Platform. • **Audit Logs** are a history of commands that users have run on the platform.
Log Levels	Select the severity of log messages that you want to view: Options are: • **Alert** • **Critical/Fatal** • **Error** • **Warning** • **Notice** • **Informational** • **Debug/Fine** If you select **Audit Logs** for **Messages**, you have only **Informational** as an option.
Timestamp From	The timestamp of the last message in the type of log messages selected. This timestamp is greater than or equal to the value entered for **Timestamp From**.
To	The timestamp of the first message in the type of log messages selected. This timestamp is less than or equal to the value entered for **To**.
Find	Lets you search for particular log messages or log levels.

Button descriptions

Button	Description
Search	Searches for the log messages based on your selection of message category and log levels.

Related topics:

Viewing log files on page 51

Log severity levels on page 56

Configuring date and time

Configuring System Platform to synchronize with an NTP server

Configuring the date and time are optional and you can skip these steps. However, you must set up the correct time zone for System Platform.

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.

2. Specify a time server and click **Add** to add the time server to the configuration file.

3. Click **Ping** to check whether the specified time server, that is, the specified host, is reachable across the network.

4. Click **Start ntpd** to synchronize the System Platform time with the Network Time Protocol (NTP) server.

   If you want to stop the synchronization, click the same button, which the system now displays as **Stop ntpd**.

5. Select a time zone and click **Set Time Zone** to set the time zone in System Platform.
   The system sets the selected time zone on the System Platform virtual machines (System Domain (Dom-0) and Console Domain). The system also updates the time zone on the other virtual machines.

6. Click **Query State** to check the NTP (Network Time Protocol) status.

Related topics:

NTP daemon on page 54

Date Time Configuration field descriptions on page 55

Configuring date and time

Use this procedure to configure the date and time if you are not synchronizing the System Platform server with an NTP server.

Configuring the date and time are optional and you can skip these steps. However, you must set up the correct time zone for System Platform.

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page with default configuration settings.
2. Click the calendar icon located next to the **Save Date and Time** button.

   The system displays the Set Date and Time page.

   Note:

   If the **Save Date and Time** button is not enabled, you must stop the NTP server that is currently being used.
3. Select a date in the calendar to change the default date and set the required date.
4. Do the following to set the time:
   1. Click the time field at the bottom of the calendar.
      The system displays a box showing time information.
   2. Use the up and down arrow keys beside the hour to change the hour, and up and down arrows beside the minutes field to set the minutes.
   3. Click **OK** to accept your time changes.
5. Click **Apply** to save your changes.
6. Click **Save Date and Time**.
   The system displays a warning message stating that this action will cause a full system reboot.
7. Click **OK** to accept the message and set the updated date and time in the system.

Related topics:

Date Time Configuration field descriptions on page 55

NTP daemon

The NTP daemon reads its configuration from a file named ntp.conf. The ntp.conf file contains at least one or more lines starting with the keyword *server*. Each of those lines specify one reference time source, that is, time server, which can be either another computer on the network, or a clock connected to the local computer.

Reference time sources are specified using IP addresses, or host names which can be resolved by a name server. NTP uses the pseudo IP address 127.127.1.0 to access its own system clock, also known as the local clock. You must not mix this IP address with 127.0.0.1, which is the IP address of the local host, that is the computer's loopback interface. The local clock will be used as a fallback resource if no other time source is available. That is why the system does not allow you to remove the local clock.

Related topics:

Configuring System Platform to synchronize with an NTP server on page 53

Date Time Configuration field descriptions on page 55

Removing a time server

1. Click **Server Management** > **Date/Time Configuration**.

   The system displays the Date/Time Configuration page.

2. Select a time server from the list of added servers and click **Remove Time Server** to remove the selected time server.

   Note:

   The changes will be effective after you restart NTP.

Related topics:

Date Time Configuration field descriptions on page 55

Date Time Configuration field descriptions

Use the Date/Time Configuration page to view or change the current date, time, time zone, or the status of NTP daemon on the System Platform server.

Name	Description
Date/Time Configuration	Shows the local time and the UTC time. Also shows the status of the NTP daemon, if it is started or stopped.
Save Date and Time	Lets you edit the date and time set during System Platform installation.
Manage Time Servers	Lets you ping a time server and see its status and manage the existing time servers.

Button descriptions

Button	Description
Start ntpd	Starts the Network Time Protocol (NTP) daemon on System Platform to synchronize the server time with an NTP server. If the NTP daemon (ntpd) is started, this button changes to **Stop ntpd**. Click this button to stop the NTP daemon.
Set Date and Time	Edits the date and time that are configured for System Platform. The button is disabled if ntpd is running.
Set Time Zone	Edits the time zone that is configured for System Platform . System Platform updates the time zone on System Domain (Domain-0), Console Domain, and the virtual machines running on System Platform.
Ping	Checks whether the specified time server, that is, the specified host, is reachable across the network.
Add	Adds the time server that you specify to the list of time servers with which System Platform can synchronize.
Remove Time Server	Removes the selected time server.
Query State	Checks the status of the NTP daemon on System Platform.

Related topics:

Configuring System Platform to synchronize with an NTP server on page 53
Configuring date and time on page 54
NTP daemon on page 54
Removing a time server on page 55

Configuring Logging

Log severity levels

Different log messages in System Platform have different severity levels. The severity levels are:

- Fine
- Informational
- Warning
- Error
- Fatal

You can select how detailed the log output of System Platform will be. Log messages of the severity you select and of all higher severities are logged. For example, if you select

Information, log messages of severity levels Information, Warning, Error, and Fatal are logged. Log messages of severity level Fine are not logged.

Log retention

To control the size and number of historical log files that System Platform retains, you configure a maximum size for log files and a maximum number of log files.

When a log file reaches the maximum size, it rolls over. When rollover occurs, .1 is appended to the file name of the current log file and a new, empty log file is created with the original name. For example, `vsp-all.log` is renamed `vsp-all.log.1`, and a new, empty `vsp-all.log` file is created. The number that is appended to older log files is increased by one. For example, the previous `vsp-all.log.1` is renamed `vsp-all.log.2`, `vsp-all.log.2` is renamed `vsp-all.log.3`, and so on. When the maximum number of backup (old) log files is reached, the oldest log file is deleted.

Configuring log levels and retention parameters

1. Click **Server Management** > **Logging Configuration**.
2. Edit the default values, if required.
3. Click **Save** to save the settings.

Related topics:

Log severity levels on page 56
Log retention on page 57
Logging Configuration field descriptions on page 57

Logging Configuration field descriptions

Use the Logging Configuration page to configure the severity of log messages that you want logged, a maximum size for log files, and the number of backup files that you want retained.

⚠ **Caution:**

Change the default values only for troubleshooting purposes. If you change the logger level to **FINE**, the system writes many log files. There are chances of potential performance issues when using this logging level. So, Avaya recommends you to switch to **FINE** only to debug a serious issue.

Name	Description
SP Logger	SP Logger is used for the System Platform Web Console logs, which are generated by the System Platform code base (for example, com.avaya.vsp).
3rd Party Logger	Third Party Logger is the root logger, which can include logs from other third party components included in the System Platform Web Console (for example, com.* or com.apache.*).
vsp-all.log	Contains all logs generated bySystem Platform Web Console, regardless of whether they include event codes.
vsp-event.log	Contains all event logs generated by System Platform Web Console. The logs in vsp-event are available in Avaya common logging format.
vsp-rsyslog.log	Contains syslog messages.
Max Backups	Maximum number of historical files to keep for the specified log file.
Max FileSize	Maximum file size (for example, for a file vsp-all.log. Once the maximum file size is reached it, the log file will roll over (be renamed) to vsp-all.log.1.

Related topics:

Log severity levels on page 56
Log retention on page 57
Configuring log levels and retention parameters on page 57

Configuring the system

Configuring system settings for System Platform

1. Click **Server Management** > **System Configuration**.
2. On the System Configuration page, modify the fields as appropriate. If the default settings are satisfactory, no changes are necessary.
3. Click **Save**.

Related topics:

System configuration field descriptions on page 59

System configuration field descriptions

Use the System Configuration page to configure proxy settings, change the current keyboard layout, or enable or disable statistics collection.

Note:

If an administrator modifies WebLM parameters in the System Configuration page — for example, to configure an alternate WebLM Server – the web console halts the local instance of WebLM. If the administrator clicks the License Manager menu option, the web console goes to the alternate instance of WebLM. If the administrator blanks out WebLM host and port values, the Web console recovers WebLM default values, resaves them, and then restarts the local instance of WebLM.

Refer to the Release Notes for more information about any known issues relating to WebLM behaviour.

Name	Description
Proxy Configuration Area:	
Status	Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Address	The address for the proxy server.
Port	The port address for the proxy server.
WebLM Configuration Area:	
SSL	Specifies whether the Secure Sockets Layer (SSL) protocol will be used to invoke the WebLM server. Select **Yes** if the alternate WebLM application has an HTTPS web address. Otherwise, select **No** if the alternate WebLM application has an HTTP web address. Default value = **Yes**.
Host	The IP address or hostname extracted from the web address of the WebLM application. Default value = **<cdom_IP_address>**.
Port	The logical port number extracted from the web address of the WebLM application, for example, **4533**. Default value = **52233**
Other System Configuration Area:	
Syslog IP Address	IP address of the Syslog server, which collects log messages generated by the System Platform operating system.

Name	Description
Keyboard Layout	Determines the specified keyboard layout for the keyboard attached to the System Platform server.
Statistics Collection	If you disable this option, the system stops collecting the statistics data. **Note:** If you stop collecting statistics, the system-generated alarms will be disabled automatically.

Related topics:

Configuring system settings for System Platform on page 58

Configuring an alternate WebLM server on page 72

Configuring network settings

Configuring System Platform network settings

Important:

The System Platform network settings are independent of the network settings of the virtual machines running on it. This means that the System Platform network settings will not affect the network settings of the virtual machines.

Make sure that the IP addresses for the *avprivate* bridge do not conflict with any other IP addresses in your network.

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

The avprivate bridge is an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any connection to your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration page. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is not connected to your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly.

Important:

Avaya recommends that you change all the IP addresses (wherever required) in a single instance to minimize the service disruption.

1. Click **Server Management** > **Network Configuration**.
2. On the Network Configuration page enter values to configure the network settings.
3. Click **Save**.

Related topics:

Network Configuration field descriptions on page 61

Network Configuration field descriptions

Use the **Network Configuration** page to configure network settings for System Platform. The first time that you view this page, it displays the network settings that you configured during installation of System Platform.

After you install a template, the Network Configuration page displays additional fields based on the specific template installed. Examples of template-specific fields include bridges, dedicated NICs, or IP configuration for each of the guest domains created for the template.

The bonding interface fields explained below are applicable only to certain templates such as Duplex Survivable Core.

General Network Settings field descriptions

Name	Description
Default Gateway	The default gateway.
Primary DNS	The primary Domain Name System (DNS) server address.
Secondary DNS	(Optional) The secondary DNS server address.
Domain Search List	The search list, which is normally determined from the local domain name. By default, it contains only the local domain name. This may be changed by listing the desired domain search path following the *search* keyword with spaces or tabs separating the names.
Udom hostname	The host name for the Console Domain. This must be an FQDN, for example, SPCdom.mydomainname.com.
Dom0 hostname	The host name for System Domain (Domain-0). This must be a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com.
Physical Network Interface	The physical network interface details for eth0 and eth1 (and eth2 in case of High Availability Failover is enabled).
Domain Dedicated NIC	Applications with high network traffic or time-sensitive traffic may be allocated a dedicated NIC. This means the virtual machine connects

Name	Description
	directly to a physical Ethernet port and may require a separate cable connection to the customer network. See respective template installation topics for more information.
Bridge	The bridge details for the following: • **avprivate**: This is called a private bridge because it does not use any Ethernet interface, so it is strictly internal to the server. The System Platform installer attempts to assign IP addresses that are not in use. • **avpublic**: This bridge uses the Ethernet interface associated with the default route, which is usually eth0, but can vary based on the type of the server. This bridge generally provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0) and Console Domain have on this bridge. • **template bridge**: These bridges are created during the template installation and are specific to the virtual machines installed.
Domain Network Interface	The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
Global Template Network Configuration	The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.

Bonding Interface field descriptions

Name	Description
Name	Is a valid bond name. It should match regular expression in the form of “bond[0-9]+”.
Mode	Is a list of available bonding modes that are supported by Linux. The available modes are: • Round Robin • Active/Backup • XOR Policy • Broadcast • IEEE 802.3ad • Adaptive Transmit Load Balancing • Adaptive Load Balance

Name	Description
	For more information about bonding modes, refer to http://www.linuxhorizon.ro/bonding.html. **Note:** The default mode of new bonding interface is Active/Backup. **Important:** System Platform doesn't allow to configure any advance parameters not listed in this page. If you want to configure an advanced feature, log in to System Platform Web Console and make the required changes.
Slave 1/ Primary	Is the first NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the primary NIC.
Slave 2/ Secondary	Is the second NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the secondary NIC.

Bonding Interface link descriptions

Name	Description
Add Bond	Adds new bonding interface.
Delete	Deletes a bonding interface.

Related topics:

Configuring System Platform network settings on page 60

Adding a bonding interface

While you are configuring network settings in the Network Configuration page, use this procedure to add a bonding interface.

1. Scroll down to make the Bonding Interface frame visible.
2. Click **Add Bond** link.
3. Enter the following fields:
    a. **Name**
    b. **Mode**
    c. **Slave 1/Primary**
    d. **Slave 2/Primary**

Deleting a bonding interface

While you are configuring network settings in the Network Configuration page, use this procedure to delete a bonding interface.

1. Scroll down to make the Bonding Interface frame visible.
2. Click **Delete** link against the bonding interface you want to delete.

Configuring static routes

Adding a static route

Use this procedure to add a static route to System Platform. Static routes can be used to route packets through a VPN to an Avaya Partner that is providing remote service.

1. Click **Server Management** > **Static Route Configuration**.
2. On the Static Route Configuration page, select the required interface.
3. Enter the network address.
4. Enter the network mask address.
5. Enter the gateway address.
6. Click **Add Route**.

Related topics:

Static route configuration field descriptions on page 65

Deleting a static route

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Delete** next to the static route that you want to delete.

Related topics:

[Static route configuration field descriptions](#) on page 65

Modifying a static route

1. Click **Server Management** > **Static Route Configuration**.
2. Click **Edit** next to the static route that you want to modify.
3. Modify the settings as appropriate.
4. Click **Apply** to save the settings.

Related topics:

Static route configuration field descriptions on page 65

Static route configuration field descriptions

Use the Static Route Configuration page to add static routes to System Domain (Dom-0), view details of existing static routes, or modify or delete existing static routes.

Field Names	Descriptions
Interface	The bridge through which the route is enabled.
Network Address	The destination network for the static route.
Network Mask	The network mask for the destination network.
Gateway	The gateway or the router through which the route functions.

Related topics:

Adding a static route on page 64
Deleting a static route on page 64
Modifying a static route on page 65

Configuring Ethernet settings

Configuring Ethernet interface settings

1. Click **Server Management** > **Ethernet Configuration**.

   The Ethernet Configuration page displays the values for all Ethernet interfaces on the server, for example, eth0, eth1, eth2, and so on.

2. Modify the values for eth0 and eth1 as appropriate.
3. Click **Save** to save your settings.

Related topics:

Ethernet configuration field descriptions on page 66

Ethernet configuration field descriptions

Use the Ethernet Configuration page to configure settings for the Ethernet interfaces on System Platform.

Name	Description
Speed	Sets the speed in MB per second for the interface. Options are: • 10 Mb/s half duplex • 10 Mb/s full duplex • 100 Mb/s half duplex • 100 Mb/s full duplex • 1000 Mb/s full duplex Auto-Negotiation must be disabled to configure this field.
Port	Lists the available Ethernet ports. Auto-Negotiation must be disabled to configure this field.
Auto-Negotiation	Enables or disables auto-negotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Button descriptions

Button	Description
Apply	Saves and applies the settings for the Ethernet device.
Refresh	Refreshes the Ethernet Configuration page.

Related topics:

Configuring Ethernet interface settings on page 66

Configuring alarms

Alarm descriptions

System Platform generates the following alarms:

Alarm	Description
High CPU	Average CPU Usage of VM
Disk Usage (Logical Volume)	Percentage of logical volume used (/, /template-env, /dev/shm, /vspdata, vsp-template)
Disk (Volume Group)	Percentage of volume group used (VolGroup00)
Disk reads	Disk read rate (sda)
Disk Writes	Disk write rate (sda)
Load Average	Load average on each virtual machine
Network I/O received	Network receive rate for all guests (excluding dedicated NICs)
Network I/O Transmit	Network transmit rate for all guests (excluding dedicated NICs)
Webconsole heap	Percentage of webconsole (tomcat) heap memory in use
Webconsole open files	Number of file descriptors that webconsole has open
Webconsole permgen	Percentage of webconsole (tomcat) permgen heap used
SAL Agent heap SAL Agent permgen	Percentage of SAL heap memory in use
SAL Agent permgen	Percentage of SAL permgen heap used

Alarm	Description
Domain-0 Memory (Committed_AS)	Memory for System Domain (Dom-0)
udom Memory (Committed_AS)	Memory for Console Domain

Note:

A virtual machine other than System Domain and Console Domain may support configuring alarms relevant to its operations. Please check the administration document of the virtual machine to know whether any alarms are present for the virtual machine and how to configure them.

Configuring alarm settings

1. Click **Server Management** > **Alarm Configuration**.
2. On the Alarm Configuration page, modify the settings as appropriate.
3. Select **Enabled** to enable an alarm.
4. In the **Limit Value** field, enter the threshold value for the alarm.
5. Specify the number of consecutive samples that must exceed the threshold value for the system to generate an alarm.
6. Specify the **Suppression Period** for an alarm after the system generates the previous alarm.
7. Click **Save** to save the settings.

Related topics:

Alarm descriptions on page 67
Alarm configuration field descriptions on page 68

Alarm configuration field descriptions

Use the **Alarm Configuration** page to configure alarms generated from the data collected by the Performance Statistics feature.

Field Names	Descriptions
Alarm	Name of the alarm.
Limit Values	The threshold value above which the value is potentially in an alarming state.

Field Names	Descriptions
For	The period for which the value must be above the threshold to generate an alarm.
Suppression Period	The period for which the same alarm is not repeated after generating the alarm for the first time.
Enable	Enables the selected alarm.

Related topics:

Alarm descriptions on page 67
Configuring alarm settings on page 68

Managing Certificates

Certificate management

The certificate management feature allows a user with the right administrative privileges to replace the default System Platform Web Console certificate and private key. It also allows the user to upload and replace the enterprise LDAP certificate, if the option of transport layer security (TLS) was enabled in the Enterprise LDAP page.

The user can replace the default System Platform Web Console certificate and private key by selecting a new certificate file and a new private key on the local machine and uploading them. The default System Platform Web Console certificate is generated during System Platform installation with the CN value same as the Console Domain hostname. During platform upgrade, the certificate is first backed up and then restored after the upgrade completes.

Similarly, the user can upload and replace the enterprise LDAP certificate by selecting new certificate file on the local machine, and uploading it. The Certificate Management page shows the following data for the current System Platform Web Console and Enterprise LDAP certificate:

- Type
- Version
- Expiry date
- Issuer

Here are the things to note relating to a certificate:

- The only acceptable extension of a new certificate file is `.crt`.
- The only acceptable extension of a new private key file is `.key`.

- The option to upload the key is only for the System Platform Web Console certificate.
- An uploaded certificate is valid if its start date is not after the current date and its end date is not before the current date. An uploaded private key is valid if it matches the uploaded certificate.

Related topics:

Enterprise LDAP field descriptions

Selecting System Platform certificate

1. Click **Server Management** > **Certificate Management**.
2. Click **Select New Certificate** in the System Platform Certificate area.

Selecting enterprise LDAP certificate

This task is enabled only if **TLS** was clicked in the Enterprise LDAP page.

1. Click **Server Management** > **Certificate Management**.
2. Click **Select New Certificate** in the Enterprise LDAP Certificate area.

Certificate Management field descriptions

Use the Certificate Management page to get new certificate issued from your certification authority for System Platform Web Console or Enterprise LDAP. In the case of System Platform Web Console, you also get the private key.

Field descriptions

Name	Description
Type	Is the type of the certificate issued.
Version	Is the version number of the certificate.
Expiry Date	Is the expiry date of the certificate.
Issuer	Is the issuing agency of the certificate.

Button descriptions

Name	Description
Select New Certificate	Selects new System Platform Web Console certificate and private key or Enterprise LDAP certificate depending on the area where the button is located.

Managing System Platform licenses

License management

System Platform includes Avaya's Web License Manager (WebLM) to manage its licenses. WebLM is a Web-based software application that facilitates easy tracking of licenses. You can launch the WebLM application from within System Platform.

Launching WebLM

System Platform uses Web License Manager (WebLM) to manage its licenses. Use this procedure to launch WebLM from System Platform.

1. Click **Server Management** > **License Management**.
2. On the License Management page, click **Launch WebLM License Manager** .
3. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.
4. Manage the licenses as appropriate.

   For more information on managing licenses in Avaya WebLM, see *Installing and Configuring Avaya WebLM Server* at http://support.avaya.com.

Related topics:

License management on page 71
License Management launch page field descriptions on page 72

Configuring an alternate WebLM server

Prerequisites

Obtain the Web address of the alternate WebLM application. It should be in either HTTP or HTTPS format, including either the hostname or host IP, plus a logical port number, for example, any of the following:

- **http://111.125.34.56:4533/WebLM/LicenseServer**
- **http://avayahost-a:4533/WebLM/LicenseServer**
- **https://111.125.34.56:4533/WebLM/LicenseServer**
- **https://avayahost-a:4533/WebLM/LicenseServer**

Extract information from the web address to enter as WebLM configuration values during the following procedure.

Perform this task when you need to designate an alternate server to host a different (non-default) instance of the WebLM application.

1. Click **Server Management** > **System Configuration**.
2. On the System Configuration page, modify the following fields according to information obtained through the prerequisites:
   - **SSL** – Select **Yes** if the alternate WebLM application has an HTTPS web address. Otherwise, select **No** if the alternate WebLM application has an HTTP web address.
   - **Address** – Enter the hostname (for example, `avayahost-a`) or host IP address extracted from the web address of the alternate WebLM application.
   - **Port** – Enter the logical port number (for example, `4533`) extracted from the web address of the alternate WebLM application
3. Click **Save**.

Related topics:
System configuration field descriptions on page 59

License Management launch page field descriptions

Use the **License Management** page to launch the Web License Manager (WebLM) application and manage System Platform licenses.

Button descriptions

Name	Description
Launch WebLM License Manager	Launches the WebLM application.

Related topics:

[License management](#) on page 71
[Launching WebLM](#) on page 71

Configuring the SAL Gateway

SAL Gateway

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

Remote Serviceability

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

Note:

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

Stand-alone SAL Gateway

You can choose to use a stand-alone SAL Gateway instead of the SAL Gateway that is embedded in System Platform. You might prefer a stand-alone gateway if you have a large network with many Avaya devices. The stand-alone gateway makes it possible to consolidate alarms from many Avaya devices and send those alarms from one SAL Gateway rather than multiple SAL Gateways sending alarms. See **Secure Access Link** on http://support.avaya.com for more information on stand-alone SAL Gateway.

If you use a stand-alone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 102. You can also disable the SAL Gateway that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See Disabling SAL Gateway on page 76.

SAL Gateway configuration

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

To configure SAL, perform these high-level steps:

1. Register the system.

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

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

2. Configure the SAL Gateway.

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

Related topics:

Registering the system on page 19
Launching the SAL Gateway management portal on page 75
Launching the SAL Gateway management portal on page 75
Configuring the SAL Gateway on page 75
Configuring the SAL Gateway on page 75
SAL Gateway Management field descriptions on page 76
SAL Gateway Management field descriptions on page 76

Launching the SAL Gateway management portal

Use this procedure to launch the SAL Gateway management portal from within System Platform.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
3. When the portal displays its Log On page, enter your user name and password for Console Domain.
4. Configure the SAL Gateway as appropriate.

Related topics:

SAL Gateway on page 73
SAL Gateway on page 73
Configuring the SAL Gateway on page 75
Configuring the SAL Gateway on page 75
SAL Gateway Management field descriptions on page 76
SAL Gateway Management field descriptions on page 76

Configuring the SAL Gateway

To configure the SAL Gateway for the customer's network and System Platform, follow the instructions that are provided in *Installing and Configuring Avaya Aura^{TM} System Platform*. This document is available on http://support.avaya.com.

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.

Disabling SAL Gateway

Use this procedure to disable the SAL Gateway that is embedded in System Platform. Disable the embedded SAL Gateway if you are using a stand-alone SAL Gateway to send alarms to Avaya.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Disable SAL Gateway**.

Enabling SAL Gateway

Use this procedure to enable the SAL Gateway that is embedded in System Platform. The embedded SAL Gateway is enabled by default and only needs to be enabled if you have previously disabled it.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Enable SAL Gateway**.

SAL Gateway Management field descriptions

Button	Description
Launch SAL Gateway Management Portal	Launches the SAL Gateway management portal in a new Web browser window. You must provide valid certificate details to access the portal.
Disable SAL Gateway	Disables the SAL Gateway that is embedded in System Platform. If you are sending alarms to a stand-alone SAL Gateway, disable the embedded SAL Gateway.
Enable SAL Gateway	Enables the SAL Gateway that is embedded in System Platform.

Related topics:

SAL Gateway on page 73
SAL Gateway on page 73
Launching the SAL Gateway management portal on page 75
Launching the SAL Gateway management portal on page 75
Configuring the SAL Gateway on page 75
Configuring the SAL Gateway on page 75

Viewing System Platform statistics

Performance statistics

System Platform collects data on operational parameters such as CPU usage, free and used heap and permgen memory, number of open files on System Platform Web Console, and disk input and output operations to name a few. System Platform collects this data at one minute interval and stores it in an RDD database. System Platform presents this data as graphs using an open source data logging and graphing tool called RRDtool. The following sections should help you understand the System Platform performance statistics capability:

Data retention and consolidation

System Platform stores data for 24 hours and then consolidates it into one hour average and maximum, which is kept for a week. After a week, System Platform consolidates the one hour average and maximum data into 4 hour average and maximum, and stores it for six months.

Monitored parameters

System Platform collects data on the following parameters every minute:

Variable	Domain	Description	Source
CPU usage	All domains	Average CPU usage. Is calculated from cpuSeconds	`xm list -long`
System Platform Web Console memory	cdom	Free and used heap and permgen memory.	JVM
System Platform Web Console open files	cdom	Number of open file handles.	`proc <pid>/fd`
Spirit agent memory	cdom	Free and used heap and permgen memory.	JVM (through JMX)

Variable	Domain	Description	Source
Memory usage	Domain-0, cdom	Committed_AS and kernel.	`/proc/meminfo`
Disk space (logical info)	Domain-0, cdom	Mounted at: /, /template-env, /dev/shm, /vspdata, vsp-template	`df`
Disk space (volume group)	Domain-0	VolGroup00	`vgs`
Disk I/O	Domain-0	Disk read and write rate for sda.	`iostat`
Network I/O	All domains	Network receive/transmit rate for all guests (excluding dedicated NICs.)	`xentop`
Load average	Domain-0, cdom	average load.	`/proc/loadavg`

Graphs

Click **Server Management** > **Performance Statistics** to generate graphs for all or selected parameters and for a specified duration. You can also obtain the comma separated value (CSV) file of the graphed data.

Alarms

System Platform can raise alarms for parameters whose values and frequencies exceed the configured threshold limits.

Related topics:

Log severity levels on page 56
Exporting collected data on page 79
Performance statistics field descriptions on page 79

Viewing performance statistics

1. Click **Server Management** > **Performance Statistics**.
2. On the Server Management page, perform one of the following steps:
    - Select **All Statistics** to generate a graph for all recorded statistics.
    - Clear **All Statistics**, and select the type of graph from the **Type** drop down menu. Then select the required domain from the list in the **Domains** box.
3. Specify the date and time for the period that you want the report to cover.
4. Click **Generate** to generate the performance graph for the system.

Related topics:

[Exporting collected data](#) on page 79
[Performance statistics field descriptions](#) on page 79

Exporting collected data

Use this procedure to export to a CSV file the data points that were used to generate a graph.

1. Click **Server Management** > **Performance Statistics**.
2. On the Performance Statistics page, select the required details and generate a graph.
3. Click **Download CSV File** for the data you want to export.
4. Click **Save** and specify the location to download the data.

Related topics:

[Log severity levels](#) on page 56
[Performance statistics](#) on page 77
[Performance statistics field descriptions](#) on page 79

Performance statistics field descriptions

Use the **Performance Statistics** page to view the health and usage of the system. The Performance Statistics page displays the performance statistics for System Platform and the hosted virtual machines.

Field Names	Descriptions
All Statistics	If you select this option, the system displays a graph for all the recorded statistics.
Type	Appears only if the **All Statistics** check box is cleared. Lets you specify the type of statistics you want to display from a list of options.
Domains	Appears only if the **All Statistics** check box is cleared. Lets you select the virtual machines for which you want to generate the statistics, for example, System Domain (Dom-0) and Console Domain.
Date and Time	Lets you specify the date and time for generating performance statistics from three options as follows: **Predefined Values**: Lets you specify the range of days. **Last**: Lets you specify the day or time.

Field Names	Descriptions
	Between: Lets you specify the date range.
Generate	Generates the performance statistics of the system based on your specifications.

Related topics:

Viewing performance statistics on page 78

Exporting collected data on page 79

Ejecting the CD or DVD

Use the Eject CD/DVD page to force open the DVD drive of the System Platform server. The CD or DVD used for installing System Platform and virtual machines ejects automatically after successfully completing the installation or an upgrade . However, if any problem occurs during installation or upgrade, the CD or DVD remains locked in the drive. You can use the **Eject CD/DVD** page to force open the drive and remove the CD or DVD.

The data on the CD or DVD receives no damage because of force opening the drive.

1. Click **Server Management** > **Eject CD/DVD**.
2. Click **Eject** on the Eject CD/DVD page to eject the CD or DVD.

Deleting old, unused files

Use the File Management page to delete old versions of the solution template files and platform upgrade images. However, you cannot delete the files for the currently installed solution templates. System Platform stores solution template files and platform upgrade images in a folder on the system.

1. Click **Server Management** > **File Manager**.
2. Select the folder file that you want to delete.
3. Click **Delete**.

Configuring security

Security configuration

Most JITC features are built into the System Platform image and are available after installing System Platform. However, there are some features which need more user input and can be configured from the Security Configuration page. This page allows an advanced administrator user to do the following tasks:

- Remove network debugging tools, namely wireshark from System Platform
- Enable JITC Audit
- Set certain security parameters on the system

Important:

Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain.

The **Remove network debugging tools (wireshark)** check box is not enabled once the tools are removed from the system. However, a platform upgrade makes the tools available again and the **Remove network debugging tools (wireshark)** check box is also enabled.

Important:

Enabling audit is also irreversible. The **Enable Audit** check box is not available again after you save the changed security configuration.

Configuring security

Use this procedure to change one or more security features such as enabling audit, resetting the Grub password, changing host access list, and so on.

1. Click **Server Management** > **Security Configuration**.
2. Enter one or more required fields in the Security Configuration page.
3. Click **Save**.

Security Configuration field descriptions

Field descriptions

Name	Description
Remove network debugging tools (wireshark)	Indicates whether or not to remove the network debugging tools. **Important:** Removing the network debugging tools is irreversible. The tools are removed from System Platform Web Console and the Console Domain. A platform upgrade makes the tools available again and the **Remove network debugging tools (wireshark)** check box is also enabled.
Enable Audit	Indicates whether or not the audit is to be enabled. **Important:** Enabling audit is irreversible.
Reset Grub Password	Is the new System Platform Web Console Grub password.
Retype Grub Password	Is the new System Platform Web Console Grub password being retyped for verification.
Verify Dom0 Reset Password	Is the System Platform Web Console root password to reset the System Platform Web Console Grub password.
Cdom Hosts Allow List	Is the list of hosts that can access the Console Domain. **Note:** The list of hosts is maintained in the `hosts.allow` file at `/etc` on the Console Domain.
Cdom Hosts Deny List	Is the list of hosts that cannot access the Console Domain. **Note:** The list of hosts is maintained in the `hosts.deny` file at `/etc` on the Console Domain. **Important:** When JITC is enabled, all that `hosts.deny` has is the entry `ALL:ALL`.
Dom0 Hosts Allow List	Is the list of hosts that can access the System Platform Web Console. **Note:** The list of hosts is maintained in the `hosts.allow` file at `/etc` on the System Platform Web Console.

Name	Description
Dom0 Hosts Deny List	Is the list of hosts that cannot access the System Platform Web Console. **Note:** The list of hosts is maintained in the `hosts.deny` file at `/etc` on the System Platform Web Console. **Important:** When JITC is enabled, all that `hosts.deny` has is the entry `ALL:ALL`.
Login Banner Header	Is the header shown for the login banner.
Login Banner Text	Is the text shown for the login banner.

Button descriptions

Name	Description
Save	Saves the security configuration.

Backing up System Platform

System Platform backup

You can back up configuration information for System Platform and the solution template (all virtual machines). Sets of data are backed up and combined into a larger backup archive. Backup sets are related data items that need to be backed up. When you perform a back up, the system executes all the backup sets. All the backup sets must succeed to produce a backup archive. If any of the backup sets fail, then the system removes the backup archive. The amount of data backed up is dependent on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, so that you can restore the data, if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. You can also send the backup data to an external e-mail address if the file size is not larger than 10 MB.

If a backup fails, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

Note:

It is not the aim of the backup feature to provide a mechanism to re-enable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions in this document on how to re-enable failed High Availability Failover node back to High Availability Failover configuration.

Related topics:

Re-enabling failed standby node to High Availability Failover

Re-enabling failed preferred node to High Availability Failover

Backing up the system

Use this procedure to back up configuration information for System Platform and the solution template (all virtual machines). Use the System Platform Web Console to back up the files.

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

   Important:

   The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.
4. Select where to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
5. Enter other information as appropriate.
6. Click **Backup Now**.

Related topics:

Backup field descriptions on page 86

Scheduling a backup

Use this procedure to back up System Platform and the solution template on a regular basis. Backups are not scheduled by default on System Platform.

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Schedule Backup**.
4. Specify the following:
   - **Frequency**
   - **Start Time**
   - **Archives kept on server**.
   - **Backup Method**

     Use this field to copy the backup archive file to a remote server or to send the file to an e-mail address. The file is also stored on the on theSystem Platform server.
5. Click **Schedule Backup**.

Related topics:
Backup field descriptions on page 86

Transferring the Backup Archives to a remote destination

You can send the backup archive to a mail address or to a remote server by SFTP with using the **Backup Method** option.

1. To send the archive by email:
   a. Select the **Email** option as the **Backup Method**.
   b. Specify the **Email Address** and the **Mail Server**.
2. To send the archive to a remote server by SFTP:
   a. Select **SFTP** option as the **Backup Method**.
   b. Specify the **SFTP Hostname** (or IP Address), Directory to which the archive will be sent and the username and password to log in the server.

Viewing backup history

Use this procedure to view the last 10 backups executed and their status. If the last backup failed, the system automatically redirects you to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup is successful.

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select **Backup History**.
   The system displays the last 10 backups executed with their dates and the status.

Backup field descriptions

Use the Backup page to back up configuration information for System Platform and the solution template (all virtual machines).

Backup Now fields

The following table describes the fields that are displayed if you select **Backup Now** at the top of the Backup page.

Field Names	Descriptions
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Backup Now	Starts the backup operation.

Schedule Backup fields

The following table describes the fields that are displayed if you select **Schedule Backup** at the top of the Backup page.

Field Names	Descriptions
Frequency	Select one of the following options: • Daily • Weekly • Monthly
Start Time	The start time for the backup.
Archives kept on the server	The number of backup archives to store on the System Platform server. The default is 10.
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server. Enter the e-mail address and the server address of the recipient.
Schedule Backup	Schedules the backup process.
Cancel Schedule	Cancels an existing backup schedule.

Related topics:

Backing up the system on page 84
Scheduling a backup on page 85

Restoring System Platform

Restoring backed up configuration information

Use this procedure to restore backed up configuration information for System Platform and the Solution Template (all virtual machines).

Note:

The restore operation does not restore the High Availability Failover configuration from the backup file. It is not the aim of the restore feature to re-enable the failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how to re-enable the failed High Availability Failover node back to High Availability Failover configuration. Avaya recommends that you restore the backup configuration before configuring and starting High Availability Failover.

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
   The Restore page displays a list of previously backed up archives on the System Platform system.
3. Select an archive file from the list, and then click **Restore** to restore from the selected archive.

   Restoring an archive requires the System Platform Web Console to restart, so you must log in again when the restore operation is completed.

Related topics:

System Platform backup on page 83
Restore field descriptions on page 88

Restore field descriptions

Field Names	Descriptions
Restore from	Select the location of the backup archive file from which you want to restore configuration information. • **Local**: Restores from a file on System Platform. If you select this option, the Restore page displays a list of previously backed up archives on the System Platform system. • **SFTP**: Restores from a file on a remote server. If you select this option, enter the hostname or IP address of the remote server, directory where the archive file is located, and user name and password for the SFTP server. • **Upload**: Restores from a file on your computer.
Archive Filename	Filenames of the backup archive files at the location you specify.
Archive Date	Date that the file was created.
Selection	Select this check box to restore from the archive file.
Restore History	Displays the restore history for the last ten restores. If an error occurred during the last restore, the system directs you to this page after login and continues to display an error message until a restore is successful.

Button descriptions

Button	Description
Search	Displayed if you select **SFTP**. Searches for archive files in the specified directory of the remote server.
Clear Search Result	Clears the list of archive files found on a remote server after an SFTP search.

Related topics:

Restoring backed up configuration information on page 87

Viewing restore history

Use this procedure to view the last 10 restores executed and their status. If the last restore failed, the system automatically redirects you to the Restore page after login and displays the following message: `Last Restore Failed`. The system continues to display the message until a restore is successful

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the Restore page, select the **Restore History** option.

Rebooting or shutting down the System Platform server

Rebooting the System Platform Server

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. When this happens, a service disruption may occur.

Note:

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

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Reboot**.

Related topics:

Server Reboot Shutdown field descriptions on page 90

Shutting down the System Platform Server

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. When this happens, a service disruption may occur.

Note:

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

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Related topics:

Server Reboot Shutdown field descriptions on page 90

Server Reboot Shutdown field descriptions

Use the Server Reboot/Shutdown page to reboot or shutdown the System Platform server and all the virtual machines running on it.

Name	Description
Name	Name of the application being shutdown. This is always System Domain (Domain-0).
MAC Address	Machine address of the virtual machine.
IP Address	IP address of the System Platform server.
OS Type	Operating system of the System Platform server, for example, Linux.
State	Current status of the virtual machine.

Name	Description
	Possible values are as follows: • **Running**: Virtual machine is running normally. • **Starting**: Virtual machine is currently booting and should enter a running state when complete. • **Stopping**: Virtual machine is in the process of being shutdown and should enter stopped state when complete. • **Stopped**: Virtual machine has been shutdown. • **Rebooting**: Virtual machine is in the process of a reboot and should return to running when complete. • **No State**: The virtual machine is not running or the application watchdog is not being used.
Application State	Current status of the application (respective virtual machine). Possible values are as follows: • **Starting**: Application is currently booting and should enter a running state when complete. • **Running**: Application is running normally. • **Stopped**: Application has been shutdown. • **Stopping**: Application is in the process of being shutdown and should enter stopped state when complete. • **Partial**: Some elements of the application are running, but not all elements. • **Timeout**: Application has missed a heartbeat, signifying a problem and may result in the Console Domain rebooting the virtual machine to clear the problem. • **Error**: Application's sanity mechanism provided some kind of error message. • **Unknown**: Application's sanity mechanism failed.
Used Memory	The amount of memory currently used by the virtual machine.
Maximum Memory	This is a display only field. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.
CPU Time	The amount of CPU time the virtual machine has had since boot. This is not the same as uptime.
Virtual CPUs	The maximum number of virtual CPUs that can run on System Platform server.
Domain UUID	Unique ID of the virtual machine.
Auto Start	Status of auto start - shows if the System Platform server starts automatically after a shut down operation.

Name	Description
	Available status are **True** (if auto start is set), and **False** (if auto start is not set).

Button descriptions

Button	Description
Reboot	Reboots the System Platform server and all the virtual machines running on it.
Reboot HA System	Reboots the whole High Availability Failover system that includes the primary and the secondary servers and all the virtual machines running on the primary server.
Shutdown Server	Shuts down the System Platform server and all the virtual machines running on it.
Shutdown HA System	Shuts down the whole High Availability Failover system that includes the primary and the secondary servers and all the virtual machines running on the primary server.

Related topics:

Rebooting the System Platform Server on page 89

Shutting down the System Platform Server on page 90

Configuring SAL Gateway on System Platform

SAL Gateway

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

Remote Serviceability

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

Note:

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

Stand-alone SAL Gateway

You can choose to use a stand-alone SAL Gateway instead of the SAL Gateway that is embedded in System Platform. You might prefer a stand-alone gateway if you have a large network with many Avaya devices. The stand-alone gateway makes it possible to consolidate alarms from many Avaya devices and send those alarms from one SAL Gateway rather than multiple SAL Gateways sending alarms. See **Secure Access Link** on http://support.avaya.com for more information on stand-alone SAL Gateway.

If you use a stand-alone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 102. You can also disable the SAL Gateway that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See Disabling SAL Gateway on page 76.

SAL Gateway configuration

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

To configure SAL, perform these high-level steps:

1. Register the system.

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

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

2. Configure the SAL Gateway.

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

Related topics:

Registering the system on page 19
Launching the SAL Gateway management portal on page 75
Launching the SAL Gateway management portal on page 75
Configuring the SAL Gateway on page 75
Configuring the SAL Gateway on page 75
SAL Gateway Management field descriptions on page 76
SAL Gateway Management field descriptions on page 76

Configuration prerequisites

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

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

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

Note:

Submit the registration form three weeks before the planned installation date.

Related topics:

Registering the system on page 19

Changing the Product ID for System Platform

Prerequisites

You must have registered the system and obtained a Product ID for System Platform from Avaya. The Product ID is included in alarms that System Platform sends to alarm receivers. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

When you install System Platform, a default Product ID of 100111999 is set. You must change this default ID to the unique Product ID that Avaya provides.

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, delete the ID that is displayed in the **Product ID** field and enter the unique Product ID for System Platform Console Domain.

   Note:

   VSPU is the model name for Console Domain.
3. Click **Save**.

System and browser requirements for accessing the SAL Gateway user interface

Browser requirements for SAL Gateway:

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

System requirements:

A computer with access to the System Platform network.

Starting the SAL Gateway user interface

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

   To configure SAL Gateway, you must log in as `admin` or another user that has an advanced administrator role. Users that have an administrator role can only view configuration of the SAL Gateway.

When you are successfully logged in, the Managed Element page of the SAL Gateway user interface is displayed. If the SAL Gateway is up and running, the system displays two messages at the top of the page:

- `SAL Agent is running`
- `Remote Access Agent is running`

Configuring the SAL Gateway

Use this procedure to configure the identity of the SAL Gateway. This information is required for the SAL Gateway to communicate with the Secure Access Concentrator Core Server (SACCS) and Secure Access Concentrator Remote Server (SACRS) at Avaya.

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

   For field descriptions, see Gateway Configuration field descriptions on page 103.
4. (Optional) Complete the following fields if the template supports inventory collection:
   - **Inventory Collection**
   - **Inventory collection schedule**
5. Click **Apply**.

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

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

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

Next steps

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

Related topics:

Applying configuration changes on page 101
Gateway Configuration field descriptions on page 103

Configuring a proxy server

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

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

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

Next steps

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

Related topics:

Applying configuration changes on page 101

Proxy server field descriptions on page 104

Configuring SAL Gateway communication with a Secure Access Concentrator Core Server

Use the SAL Enterprise page to review settings for communication between SAL Gateway and a Secure Access Concentrator Core Server (SACCS) at Avaya Data Center. The SACCS handles alarming and inventory. Do not change the default settings unless you are explicitly instructed to do so.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **SAL Enterprise**.
   The SAL Enterprise page is displayed.
2. Do not change the default settings on this page.

   See the *Secure Access Link Gateway 1.8 Implementation Guide* for more information. This document is available at http://support.avaya.com.
3. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Core Servers.

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

Next steps

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

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

Related topics:

Applying configuration changes on page 101
SAL Enterprise field descriptions on page 104

Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server

Use the Remote Access page to review settings for communication between SAL Gateway and a Secure Access Concentrator Remote Server (SACRS) at Avaya Data Center. The

SACRS handles remote access, and updates models and configuration. Do not change the default settings unless you are explicitly instructed to do so.

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Remote Access**.
   The Remote Access page is displayed.
2. Do not change the default settings on this page unless you are explicitly instructed to do so.
3. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Remote Servers.

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

Next steps

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

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

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

Related topics:

Applying configuration changes on page 101
Remote Access field descriptions on page 105

Configuring NMS

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

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **NMS**.
2. On the Network Management Systems page, complete the following fields:
   - **NMS Host Name/ IP Address**

- **Trap port**
- **Community**

3. Click **Apply**.
4. (Optional) Use the **Add** button to add multiple NMSs.

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

Next steps

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

Related topics:

Applying configuration changes on page 101

Network Management Systems field descriptions on page 106

Managing service control

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

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

   The system displays the Gateway Service Control page. The page lists the following services:

   - **Inventory**
   - **Alarming**
   - **Remote Access**
   - **Health Monitor**

   The Gateway Service Control page also displays the status of each service as:

   - **Stopped**
   - **Running**
2. Click one of the following buttons:

   - **Stop** to stop a service.

- **Start** to start a service that is stopped.
- **Test** to send a test alarm to the Secure Access Concentrator Core Server.

Important:

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

Applying configuration changes

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Apply Configuration**.
   The system displays the Apply Configuration Changes page.
2. Click the **Apply** next to **Configuration Changes**.

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

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

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

Adding a managed element

Prerequisites

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

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

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

4. Click **Add**.
5. Click **Apply** to apply the changes.

Next steps

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

Related topics:

Applying configuration changes on page 101

Managed Element field descriptions on page 106

Using a stand-alone SAL Gateway

Adding an SNMP trap receiver

Use this procedure to add an SNMP trap receiver for System Platform. If you are using a stand-alone SAL Gateway, you must add it as an SNMP trap receiver.

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, complete the following fields:
    - **IP Address**
    - **Port**
    - **Community**
3. Click **Add SNMP Trap Receiver**.

Disabling SAL Gateway

Use this procedure to disable the SAL Gateway that is embedded in System Platform. Disable the embedded SAL Gateway if you are using a stand-alone SAL Gateway to send alarms to Avaya.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Disable SAL Gateway**.

Field descriptions

Gateway Configuration field descriptions

Name	Description
Gateway Hostname	A host name for the SAL Gateway. ⚠ **Warning:** Do not edit this field as the SAL Gateway inherits the same hostname as the CentOS operating system that hosts both the System Platform Web Console and the SAL Gateway.
Gateway IP Address	The IP address of the SAL Gateway. This IP address is the same as that of cdom (also called VSPU).
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. Format is `(000)123-4567`. If you have not obtained Solution Element IDs for the system, start the registration process as described in Registering the system on page 19. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.
Gateway Alarm ID	The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits. The system uses the value in the **Gateway Alarm ID** field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.
Alarm Enabled	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
Inventory Collection	Enables inventory collection for the SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel who are working on tickets and want to review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8*

Name	Description
	Implementation Guide. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which you want inventory collected.

Related topics:

Configuring the SAL Gateway on page 96

Proxy server field descriptions

Name	Description
Use Proxy	Check box to enable use of a proxy server.
Proxy Type	Type of proxy server that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy server.
Port	The port number of the Proxy server.
Login	Login if authentication is required. ❗ **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.
Password	Password for login if authentication is required. ❗ **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.

Related topics:

Configuring a proxy server on page 97

SAL Enterprise field descriptions

Name	Description
Passphrase	Default passphrase is `Enterprise-production`. Do not change the default unless you are explicitly instructed to do so. This passphrase

Name	Description
	is used to establish a channel for communication between the SAL Gateway and the Secure Access Concentrator Core Server.
Primary Enterprise	IP Address or the host name of the primary Secure Access Concentrator Core Server. The default value is `secure.alarming.avaya.com`.
Port	Port number of the primary Secure Access Concentrator Core Server. The default value is `443`.
Secondary Enterprise	This value must match the value in the **Primary Enterprise** field.
Port	This value must match the value in the **Port** field for the primary server.

Related topics:

Configuring SAL Gateway communication with a Secure Access Concentrator Core Server on page 98

Remote Access field descriptions

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

Related topics:

Configuring SAL Gateway communication with a Secure Access Concentrator Remote Server on page 98

Network Management Systems field descriptions

Name	Description
NMS Host Name/ IP Address	The IP address or host name of the NMS server.
Trap port	The port number of the NMS server.
Community	The community string of the NMS server. Use `public` as the **Community**, as SAL agents support only public as community at present.

Related topics:

Configuring NMS on page 99

Managed Element field descriptions

Name	Description
Host Name	Host name for the managed device. This must match the host name on the Network Configuration page of the System Platform Web Console (**Server Management** > **Network Configuration** in the navigation pane).
IP Address	IP address of the managed device.
NIU	Not applicable for applications that are installed on System Platform. Leave this field clear (not selected).
Model	The model that is applicable for the managed device.
Solution Element ID	The Solution Element ID (SE ID) of the device. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
Product ID	The Product ID (also called Alarm ID). The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.
Provide Remote Access to this device	Check box to allow remote connectivity to the managed device.
Transport alarms from this device	(Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server.
Collect Inventory for this device	Check box to enable inventory collection for the managed device.

Name	Description
	When this check box is selected, SAL Gateway collects inventory information about the managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel who are working on tickets and want to review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which you want inventory collected from the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
Generate Health Status missed alarm every	Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device. You must restart the SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart and generates alarms if it does not receive a heartbeat within the configured interval.
Suspend health monitoring for this device	Check box to suspend health monitoring for the managed device.
Suspend for	Number of minutes for which you want health monitoring suspended for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Related topics:

Adding a managed element on page 101

Chapter 3: Session Border Controller installation

Licensing Session Border Controller

Session Border Controller licenses and installer files

Obtain the Avaya Aura® Session Border Controller license and installer files by one of the following two procedures:

- Download the ISO image of the Session Border Controller license and installer files from the Product Licensing Delivery System (PLDS) Web site.
- Place an order for the Session Border Controller template DVD to be shipped with the system.

Related topics:

Registering for PLDS on page 20

Session Border Controller licenses and installer files from DVD on page 112

Session Border Controller licensing from PLDS

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 your 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 that have been completed successfully.

Verifying the ISO image on a Linux-based computer

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

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.

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 or CD

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.

If you are writing to a DVD, this procedure requires a computer or server that has a DVD writer and software that is capable of writing ISO images to DVD. If you are writing to a CD, this procedure requires a computer or server that has a CD writer and software that is capable of writing ISO images to CD.

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 or CD.

Session Border Controller licensing from DVD

Session Border Controller licenses and installer files from DVD

Place an order for the Session Border Controller: Avaya Aura® Session Border Controller template DVD to be shipped with the system.

The Session Border Controller template DVD contains the license and installer files.

Related topics:

Session Border Controller licenses and installer files on page 109

Installing a template

Installing a template

Prerequisites

After installing System Platform, install the Session Border Controller template. For information on installing System Platform, see System Platform installation process on page 15.

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

   The system displays the Search Local and Remote Template page. Use this page to select the Session Border Controller template (SBCT.ovf) that you want to run on System Platform.

   ⚠ **Caution:**

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

   Before installing the template, validate that the IP addresses on the Network Configuration page of the System Platform Management console do not conflict with the IP addresses of your network. To do so, on the System Platform Management console, click **Server Management** > **Network Configuration** and validate the IP addresses listed for the bridge **avprivate** with the IP addresses of your network.
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, such as Avaya PLDS or HTTP, you may have 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 on one of the following templates as applicable for your hardware:
   - SBCT.ovf: For the Avaya supplied servers, such as S8800 1U Server or HP ProLiant DL360 G7 server.
   - SBCT_Procurve.ovf : For HP Procurve hardware.
6. Click **Select**.
   The system displays the page from where you can either upload the Electronic Preinstallation Worksheet (EPW) file, or continue with the installation without the EPW file. Perform one of the following actions:
   - If you have an EPW file that you generated using the Avaya Aura® Session Border Controller standalone preinstallation wizard:

     Click **Browse EPW File**.

     Navigate to the EPW file location and select the EPW file.

     Click **Upload EPW File**.
   - If you do not have an EPW file, click **Continue without EPW file**. The system displays the template properties.
7. To continue installation, click **Install** .

   The template installation progresses and the system displays the installation workflow status.

   The installation process continues and the system launches the Network Settings screen on a separate browser window.

   Important:
   Make sure that your browser settings enable pop-up windows.

Search Local and Remote Template field descriptions

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

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

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

Search Local and Remote Template button descriptions

Name	Description
Install	Installs the solution template. This button is displayed only if no template is currently installed on System Platform.
Configure Proxy	Active only when you select the HTTP option to search for a solution template. Lets you configure a proxy for the HTTP address. A proxy may also be required for Secure Access Link (SAL) and alarming to access the internet.
Upgrade	Upgrades the installed solution template from the selected template location option. This button is displayed only if a template is installed on System Platform.
Delete Installed Template	Deletes the currently installed and active template. This button is displayed only if a template is installed on System Platform.

Session Border Controller standalone preinstallation wizard

System and browser requirements for installation

Ensure that you have one of the following browsers installed on your system for running the installation wizards for Avaya Aura® Session Border Controller:

- Internet Explorer 6.x or 7.x or 8.x
- Firefox 2.x or 3.x

If you wish to install and use the Session Border Controller standalone installation wizard, ensure that the following requirements are also met:

- Java SE 5.0 or later installed on the system from where you are going to run the installation wizard
- Windows XP or later installed on your computer or laptop
- Free TCP Port 31005. This port is used by the standalone preinstallation wizard by default.

Note:

If the TCP port 31005 is in use, select a free port and configure it by editing the installer. properties file at `C:\Program Files\Avaya\SP Pre-installation Wizard`. Restart the wizard to use the new port.

Launching the standalone preinstallation wizard

Prerequisites

You must have the zip file for the stand-alone installation wizard downloaded from PLDS and installed on your computer.

1. Unzip the stand-alone installation wizard file and extract the file to a location on your computer.
2. Locate the `SP_Pre-Installation_Wizard_<`*`version number`*`>.exe` file and click on it to start the setup.
3. Click through the Setup screens to complete the installation.

The installation creates a shortcut link within the **Start** > **Programs** menu.

4. To launch the stand-alone installation wizard, select **Start** > **Programs** > ***PreinstallWizardname*** > `Run`***PreinstallWizardname***, where *PreinstallWizardname* is the name of the stand-alone installation wizard for the template, for example, SP Pre-installation Wizard.

   The stand-alone installation wizard opens in your default browser.

Session Border Controller installation using the standalone preinstallation wizard

The Session Border Controller standalone preinstallation wizard is a Windows executable file. You can use this file to create or modify a configuration file for use during the installation. The standalone preinstallation wizard starts in your default Web browser and creates the same configuration pages as the embedded installation wizard. The only difference is in the initial and final steps of loading and saving the file containing the Session Border Controller configuration parameters. This file is called the EPW file. The last step allows you to save the configuration in the EPW file. The system loads this file during installation. You can save both partial and complete configurations. If you did not enter a mandatory field, you must enter the value when using the embedded wizard before the installation completes at the site.

An EPW file

An Electronic Pre-installation Worksheet (EPW) file plays an important role in installing a template. It helps you set up and save those parameters required during the template installation ahead of time. When installing the template, you upload the EPW file and let the installation happen with minimal intervention. For example, obtain the required IP addresses before the installation and enter those IP addresses when you create the EPW file. Then when you upload the EPW file at the customer site, the IP addresses are automatically populated in the installation wizard.

If you need to reinstall a template, you can reuse the original EPW with all the correct specifications.

To create the EPW file, you use a stand-alone version of the installation wizard that you install on a Windows PC. The stand-alone installation wizard displays the same configuration pages that appear in the installation wizard. The configuration pages that the stand-alone installation wizard displays depend on which template is being installed.

Creating an EPW file

Prerequisites

You must have the zip file for the stand-alone installation wizard downloaded from PLDS and installed on your computer.

To create the EPW file, you use a stand-alone installation wizard. The stand-alone installation wizard is the same as the installation wizard that launches as part of the template installation. By downloading, installing, and filling out the fields in the stand-alone installation wizard file ahead of time, you save time during the template installation. The stand-alone installation wizard installs only on a Windows PC.

1. Unzip the stand-alone installation wizard file and extract the file to a location on your computer.
2. Locate the setup_wizard.exe file and click it to start the setup.
3. Click through the Setup screens to complete the installation.

   The installation creates a shortcut link within the **Start** > **Programs** menu.
4. To launch the stand-alone installation wizard, select **Start** > **Programs** > ***PreinstallWizardname*** > `Run`***PreinstallWizardname***, where *PreinstallWizardname* is the name of the stand-alone installation wizard for the template, for example, SP Pre-installation Wizard.

   The stand-alone installation wizard opens in your default browser.
5. On the Load Files page, select the appropriate template, and then click **Next Step**.
6. Complete the fields on the rest of the screens. Click **Next Step** to move from screen to screen.
7. On the Save page, read the warning text, and then click **Accept**.
8. Click **Save EPW file**, and save the file to a location on your computer.

   Give the file a unique name that identifies the template.

Loading existing EPW file

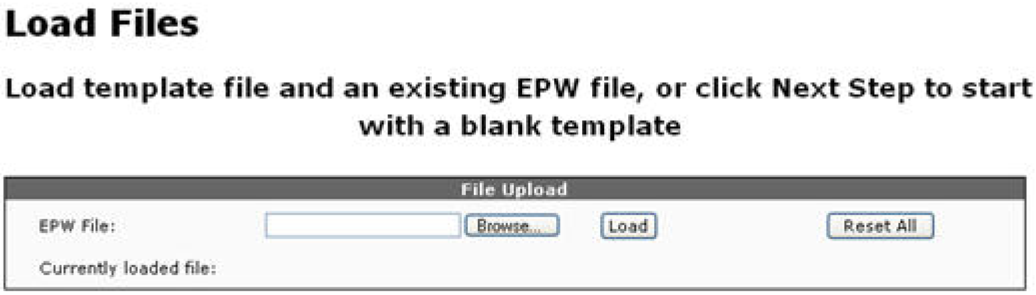
Perform one of the following tasks:

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

Note:

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

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



Load Files

Load template file and an existing EPW file, or click Next Step to start with a blank template

Next steps

Configure network settings.

Load Files field descriptions

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

Network settings configuration

The Network Settings page allows configuration of the virtual machine IP addresses and host names and other IP addresses used by the system, such as DNS and proxy settings. You must configure the IP addresses for System Domain (Dom-0) and Session Border Controller on the same network.

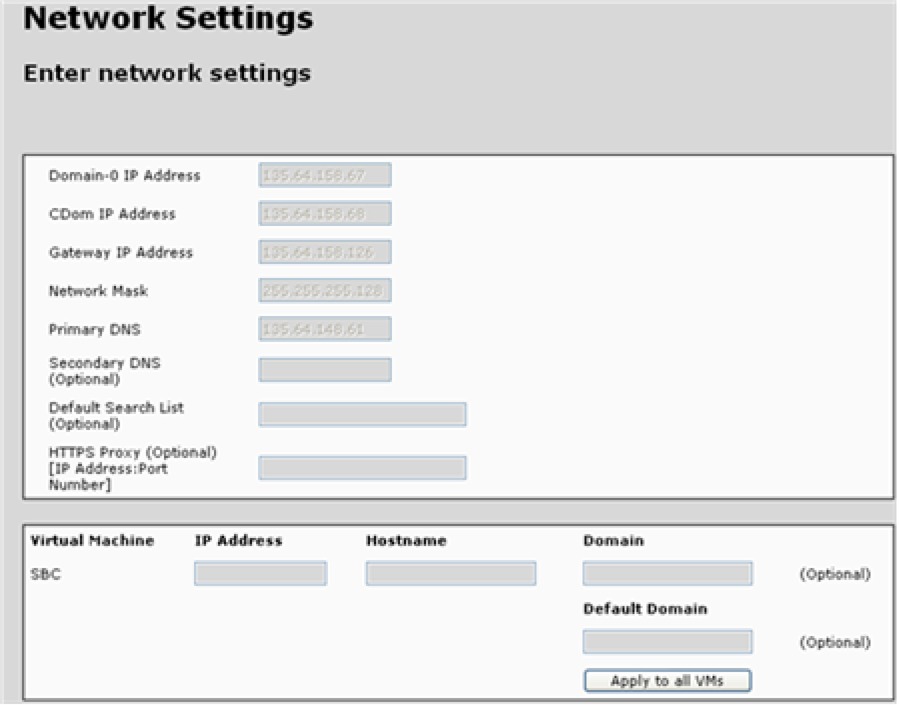
Note:

If any of the fields available on the Network Settings page are already configured during the System Platform installation, those configurations appear on the Network Settings page and are available as read-only fields.

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

Configuring network settings

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



Network Settings

Enter network settings

Domain-0 IP Address	135.64.158.67
CDom IP Address	135.64.158.68
Gateway IP Address	135.64.158.126
Network Mask	255.255.255.128
Primary DNS	135.64.148.61
Secondary DNS (Optional)	
Default Search List (Optional)	
HTTPS Proxy (Optional) [IP Address:Port Number]	

Virtual Machine	IP Address	Hostname	Domain	
SBC				(Optional)
			Default Domain	
				(Optional)

Note:

If any of the fields available on the Network Settings page are already configured during the System Platform installation, those configurations appear on the Network Settings page and are available as read-only fields.

Network Settings field descriptions

Name	Description
Domain-0 IP Address	The IP address of the System Domain (Dom-0). The system compares this to the IP address used when you install System Platform. This ensures that the correct EPW file is being used during installation.

Name	Description
CDom IP Address	This system compares this address to the IP address used when you install System Platform. This ensures that the correct EPW file is being used during installation.
Gateway IP Address	The gateway IP address.
Network Mask	The network mask address.
Primary DNS	The primary DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center. ❗ **Important:** If you configure either the DNS or HTTPS proxy data on System Platform, and when the pre-installation wizard runs, then the system displays that the data is read-only. If you do not configure the DNS or HTTPS proxy data on System Platform, then you can edit these fields. The data will be read from the EPW file, if present.
Secondary DNS (Optional)	The secondary DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center.
HTTPS Proxy (Optional)	The proxy server address, if the network to which the Session Border Controller is connected requires a proxy server to route its Internet traffic. ❗ **Important:** If you configure either the DNS or HTTPS proxy data on System Platform, and when the pre-installation wizard runs, then the system displays that the data is read-only. If you do not configure the DNS or HTTPS proxy data on System Platform, then you can edit these fields. The data will be read from the EPW file, if present.
Virtual Machine	The IP address and host name for Session Border Controller.

Login account configuration

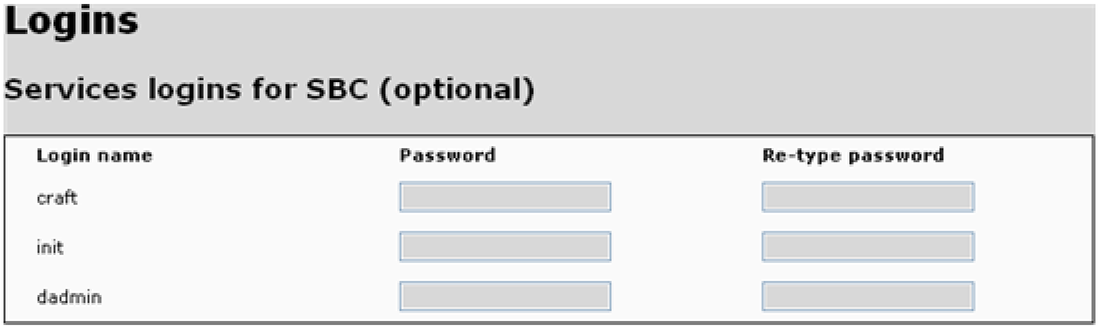
The Logins page is an optional configuration page that enables you to configure the following login accounts:

craft: Avaya services login account

init: Avaya services login account

dadmin: Avaya business partner login account

You can choose to configure all, any, or none of the login accounts.



Logins

Services logins for SBC (optional)

Login name	Password	Re-type password
craft		
init		
dadmin		

You must enter a password for a given login name for that login account to be active. If you do not enter the corresponding password for a login name, the installation wizard does not configure the login account.

If you configure a login account, you must change the default password. For detailed information about the procedure to change password, see Session Border Controller default password change.

Related topics:

Configuring a login account on page 122

Logins field descriptions on page 122

Configuring a login account

1. On the **Password** and **Re-type password** boxes, enter the password that corresponds to the login name.
2. Click **Next Step**.

Logins field descriptions

Name	Description
Login name	The name of the Avaya services or business partner login account. • **craft**: Avaya services login. • **init**: Avaya services login. • **dadmin**: Avaya business partner login.
Password	Enter the password that corresponds to the login name.

Name	Description
	Note: Use default passwords to configure a login account. You can obtain the default password from the Avaya Call Prompter.
Re-type password	Enter the password that corresponds to the login account.

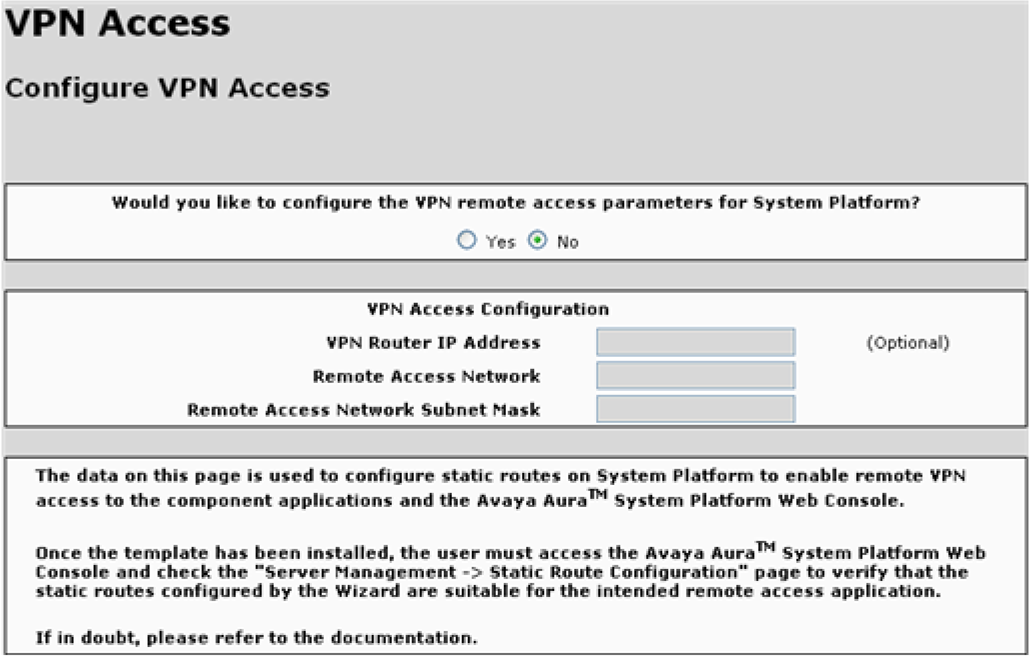
VPN access

You only need to configure this page if your VPN gateway is on the same network as the management interface of Session Border Controller. If the VPN gateway is on a different network, you may need to speak to the customer IT department to ensure that the VPN traffic is routed correctly.

Configuring VPN access

Use the VPN Access page to configure the routing required on the applications to support remote access through a VPN. If you plan to gain access to the system through a VPN gateway local to the Session Border Controller system, you should enter the required details on this page. These values are used to add static routes into the system to route traffic down the VPN tunnel to the remote network.

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



VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

○ Yes ● No

VPN Access Configuration

VPN Router IP Address (Optional)

Remote Access Network

Remote Access Network Subnet Mask

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

2. Complete the fields to configure Session Border Controller to allow VPN access.

Next steps

Configure Session Border Controller parameters.

VPN Access configuration field descriptions

Name	Description
Would you like to configure the VPN remote access parameters for System Platform?	If you want to configure VPN remote access for System Platform, select **Yes**. If you do not want to configure VPN remote access for System Platform, select **No**.
VPN Router IP Address	The IP address of the external VPN gateway device.
Remote Access Network	The IP address of the network, that is, the Avaya business partner home network, from which Session Border Controller will be accessed.

Name	Description
Remote Access Network Subnet Mask	The subnet mask associated with the network, that is, the Avaya business partner home network, from which Session Border Controller will be accessed.

Configuring Session Border Controller Parameters

Log in to the Session Border Controller, the SBC page is displayed. Navigate to **Configuration** > **Installation** > **Network Settings** to configure the Session Border Controller data such as SBC network data and the Enterprise SIP server data on this page.

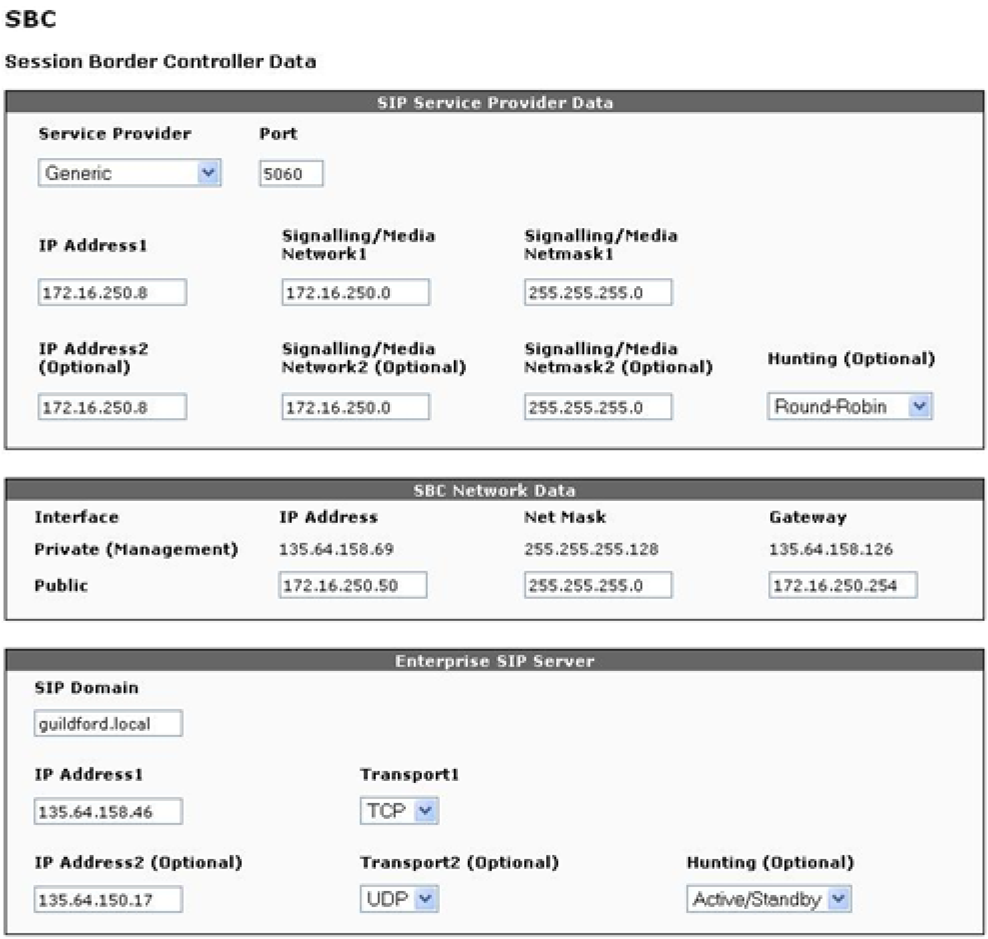
Select the required service provider from the drop-down list and provide any additional information such as far-end domain and IP addresses that is required in order to establish the SIP trunk connection.

Note:

If the Service Provider is not included in the drop-down list yet, do one of the following:

- Load an appropriate approved Avaya AA-SBC configuration ("Upload config file" option).
- If your service provider is not available on the **Service Provider** drop-down window, you must select the option **Generic**.

1. On the SBC page, select the service provider from the **Service Provider** drop-down list.



SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider	Port		
Generic	5060		
IP Address1	Signalling/Media Network1	Signalling/Media Netmask1	
172.16.250.8	172.16.250.0	255.255.255.0	
IP Address2 (Optional)	Signalling/Media Network2 (Optional)	Signalling/Media Netmask2 (Optional)	Hunting (Optional)
172.16.250.8	172.16.250.0	255.255.255.0	Round-Robin

SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	135.64.158.69	255.255.255.128	135.64.158.126
Public	172.16.250.50	255.255.255.0	172.16.250.254

Enterprise SIP Server

SIP Domain		
guildford.local		
IP Address1	Transport1	
135.64.158.46	TCP	
IP Address2 (Optional)	Transport2 (Optional)	Hunting (Optional)
135.64.150.17	UDP	Active/Standby

2. Complete the Session Border Controller service provider, network data, and enterprise SIP server sections to configure the Session Border Controller network parameters. For more information on Session Border Controller network parameters, seeConfiguring Session Border Controller parameters field descriptions on page 126.

Configuring Session Border Controller parameters field descriptions

SIP Service Provider Data

Field	Description
Service Provider	Choice of service provider configuration templates that configure Avaya Aura® Session Border Controller with the most appropriate settings for

Field	Description
	the selected service provider. The service providers supported in this release, through the wizard, include: • AT & T • Broadvox • BT Germany • BT Spain • Nectar • Skype • T-Systems • Verizon • Generic **Note:** On selecting **Skype** as the service provider: • you must enter the Skype user ID and password when the system prompts you to do so. • instead of displaying the IP address, the SBC page automatically displays the fully qualified domain name (FQDN) of the Skype server. The FQDN that appears is **sip.skype.com**. FQDN1 and FQDN2 (Optional) are specific for Skype. These fields use an FQDN as supplied by Skype instead of IP addresses. • the default gateway is set on the public interface rather than on the private interface. As such, component on the internal interface that are on a different network requires a static route to be defined to enable routing to an from Session Border Controller. • As a security measure, the Session Border Controller installation wizard configures source IP address filtering for all service providers except Skype. Source IP address filtering blocks traffic from all IP addresses other than the Post Office Protocol (POP) of the service provider to avoid potential denial of service or other similar attacks. The Skype POPs are addressed using a fully qualified domain name which prevents the wizard from configuring such a filter. As such, if you configure Skype as the service provider, you must use other security measures for protection. For detailed information about other security measures, refer appropriate Acme documentation. For the chosen service provider, select the service provider configuration template that configures the provider Session Border Controller with the most appropriate settings. If your service provided is not available on the **Service Provider** drop-down window, you must select the option **Generic**.
Port	The SIP signalling traffic port for the service provider. This applies to both the primary connection and the optional secondary connection.
IP Address 1	The IP address in dot-decimal notation for the Service Provider's SIP signalling traffic primary connection.

Field	Description
Signalling/ Media Network1	The IP network address in dot-decimal notation for the Service Provider's SIP signalling or media primary network.
Signalling/ Media Netmask1	The Netmask in dot-decimal notation for the Service Provider's SIP signalling or media primary network.
IP Address 2 (Optional)	The IP address in dot-decimal notation for the Service Provider's SIP signalling traffic secondary connection.
Signalling/ Media Network2 (Optional)	The IP network address in dot-decimal notation for the Service Provider's SIP signalling or media secondary network.
Signalling/ Media Netmask2 (Optional)	The Netmask in dot-decimal notation for the Service Provider's SIP signalling or media secondary network.
Hunting (Optional)	If dual connections are defined, this field specifies the connection behavior as one of the following: • **Active/Standby** • **Round Robin** **Hunting (Optional)** determines the algorithm used to select the outgoing connection. If you select **Active/Standby**, the traffic uses connection 1 when it is in service. If connection 1 is not in service, the traffic switches to connection 2. If you select **Round Robin** and both connection 1 and connection 2 are in service, the traffic is evenly balanced across both the connections. If one connection fails, traffic switches to the connection in service.

SBC Network Data — Private (Management)

Field	Description
IP Address	The IP address in dot-decimal notation of the Avaya Aura® Session Border Controller Private Interface. This IP address is shared with the Avaya Aura® Session Border Controller Management Interface.
Net Mask	The Netmask in dot-decimal notation of the Avaya Aura® Session Border Controller Private Interface. This IP address is shared with the Avaya Aura® Session Border Controller Management Interface.
Gateway	The gateway in dot-decimal notation used by the Avaya Aura® Session Border Controller Management and Private Interfaces.

Field	Description
	By default this is set to the Default Gateway defined on System Platform.

SBC Network Data — Public

Field	Description
IP Address	The IP address in dot-decimal notation of Avaya Aura® Session Border Controller Public Interface.
Net Mask	The Netmask in dot-decimal notation of the Avaya Aura® Session Border Controller Public Interface.
Gateway	The gateway in dot-decimal notation for the Avaya Aura® Session Border Controller Public Interface.

Enterprise SIP Server

Field	Description
SIP Domain	The SIP Domain Name to be used by Avaya Aura® Session Border Controller.
IP Address 1	The IP address in dot-decimal notation of the primary SIP connection of the enterprise.
Transport1	The SIP Transport Protocol to be used for communication with the primary SIP connection of the enterprise. Valid values are UDP, TCP or TLS.
IP Address 2 (Optional)	The IP Address in dot-decimal notation of the secondary enterprise SIP server.
Transport2 (Optional)	The SIP Transport Protocol to be used for communication with the secondary SIP connection of the enterprise. Valid values are UDP, TCP or TLS.
Hunting (Optional)	If dual connections are defined, this field specifies the connection behavior as one of the following: • **Active/Standby** • **Round Robin** **Hunting (Optional)** determines the algorithm used to select the outgoing connection. If you select **Active/Standby**, the traffic uses connection 1 when it is in service. If connection 1 is not in service, the traffic switches to connection 2. If you select **Round Robin** and both connection 1 and connection 2 are in service, the traffic is evenly balanced across both the connections. If one connection fails, traffic switches to the connection in service.

Review installation summary

Click **Summary** on the left pane to view the Summary page which provides an overview of the configuration data already gathered by the wizard. This page displays the values you have not yet set in red.

Next steps

Confirm installation.

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

Confirming Installation

1. Click **Finish** on the left pane to view the Confirm Installation page and click **Accept** to accept the settings.

   The system enables the **Install** option.
2. Click **Install** to start installing the template.

Result

After the configuration, the installation wizard downloads, starts, and configures the virtual machines. You can see the progress on each section. This process takes approximately 30 minutes depending on the system size. The system does not require any extra input during this process.

Note:

Do not attempt to configure the virtual machines during the post-installation process. All the applications are configured at this stage. Attempting to configure the system too early may result in your changes being lost or the wizard being blocked from completing its tasks.

If there is any error during the post-installation process, the system displays the error in bold letters together with a warning symbol in the extreme right column. Investigate such errors immediately. Some errors might be minor and might not affect the success of the installation. Other errors may require corrective action including reinstallation.

You can test the installation after the system loads the machines and configures them.

Next steps

If the installation fails, perform the troubleshooting steps. For more information on troubleshooting, see the Troubleshooting System Platform and Session Border Controller installation chapters.

Changing Session Border Controller Parameters

If you are not familiar with the native SBC web console or command line interface, major configuration changes such as change of service provider or addition of a back-up trunk can be implemented by reinstalling the template.

Note:

Reinstalling the template will result in loss of all existing configuration data.

1. Make a note of all pertinent configuration data such as IP addresses, network masks, and gateway addresses.
2. Back-up the existing configuration that you can revert to, in the event of any problem.
3. Delete the existing template.
4. Run the pre-installation wizard and reinstall the template. For information on reinstalling a template, see Installing a template on page 113.
5. Configure parameters with new values.

   To change parameters manually, see *Avaya Aura™ SBC Session Services Configuration Guide*.

Session Border Controller embedded installation wizard

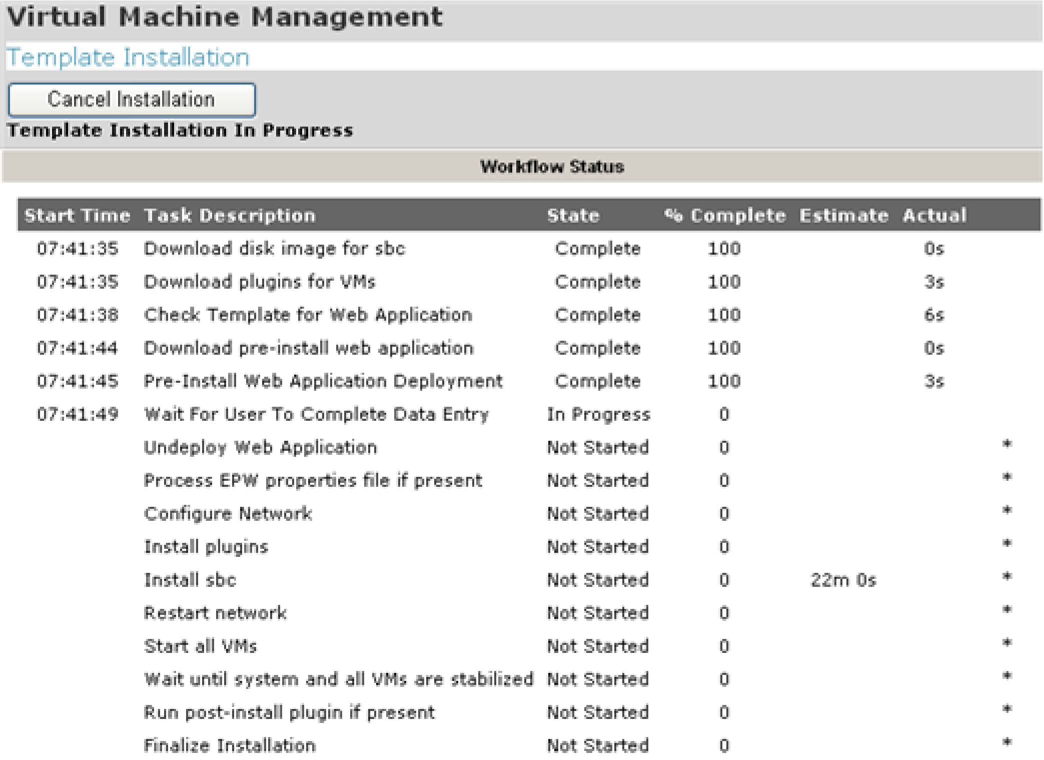
Installing the virtual machine template

1. Log in to the System Platform Web Console.
2. On the left navigation menu, click **Virtual Machine Management** > **Solution Template**.
   The system displays the Virtual Machine Management screen.
3. Select the source for the template and click **Search**.
   The system displays the template directory listing.
4. Select the template to install and click **Select**.
   The system prompts for the EPW file.

   For detailed information about EPW file, see An EPW file on page 117
5. If you have the EPW file, perform the following:
   a. Click **Browse EPW File**.
   b. Navigate to the EPW file location on your system and select the EPW file.
   c. Click **Upload EPW File**.
      The system displays the template properties.
6. If you do not have the EPW file, click **Continue without EPW file**.
   The system displays the template properties.
7. To continue installation, click **Install**.

Initial Configuration of the virtual machine template

The template installation progresses and the system displays the installation workflow status:



Virtual Machine Management

Template Installation

Template Installation In Progress

Workflow Status

Start Time	Task Description	State	% Complete	Estimate	Actual	
07:41:35	Download disk image for sbc	Complete	100		0s	
07:41:35	Download plugins for VMs	Complete	100		3s	
07:41:38	Check Template for Web Application	Complete	100		6s	
07:41:44	Download pre-install web application	Complete	100		0s	
07:41:45	Pre-Install Web Application Deployment	Complete	100		3s	
07:41:49	Wait For User To Complete Data Entry	In Progress	0			
	Undeploy Web Application	Not Started	0			*
	Process EPW properties file if present	Not Started	0			*
	Configure Network	Not Started	0			*
	Install plugins	Not Started	0			*
	Install sbc	Not Started	0	22m 0s		*
	Restart network	Not Started	0			*
	Start all VMs	Not Started	0			*
	Wait until system and all VMs are stabilized	Not Started	0			*
	Run post-install plugin if present	Not Started	0			*
	Finalize Installation	Not Started	0			*

The system launches the Network Settings page on a separate browser window.

Important:

Make sure that your browser settings enable pop-up windows.

Configuring Session Border Controller using the embedded installation wizard

1. Select **Manage Template** from the System Platform Management Console.
2. Select the media location for the Session Border Controller image.
3. If you configured this system beforehand using the standalone preinstallation wizard, upload that file in the system.
4. If you did not use the standalone preinstallation wizard, select the option to continue without the EPW file.

System Platform downloads the files and launches the embedded installation wizard.

Note:
You must enable pop-ups in your Web browser.

Network settings configuration

The Network Settings page allows configuration of the virtual machine IP addresses and host names and other IP addresses used by the system, such as DNS and proxy settings. You must configure the IP addresses for System Domain (Dom-0) and Session Border Controller on the same network.

Note:
If any of the fields available on the Network Settings page are already configured during the System Platform installation, those configurations appear on the Network Settings page and are available as read-only fields.

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

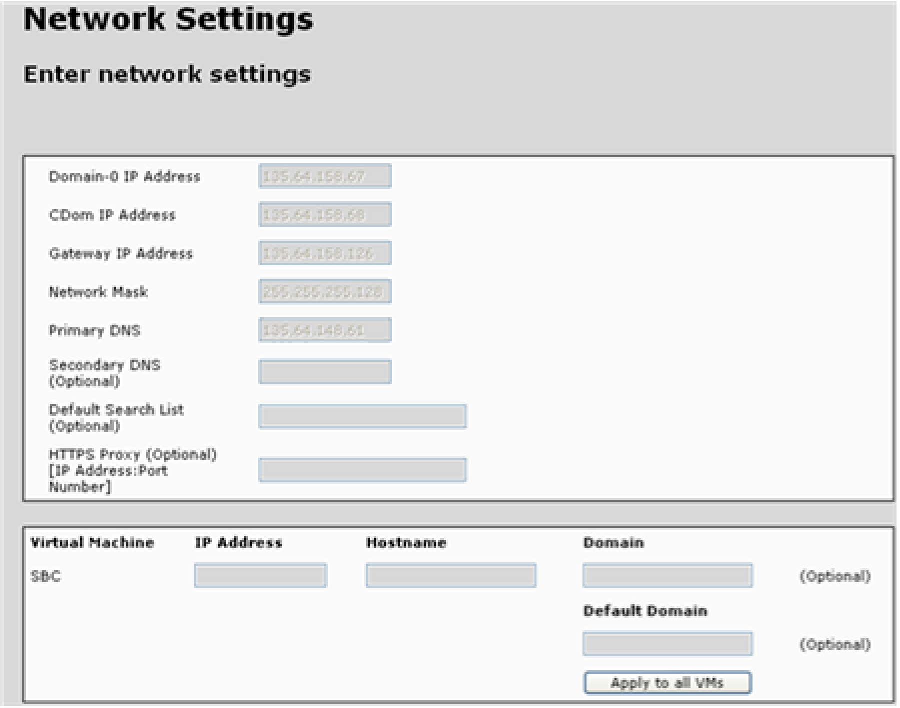
Network Settings field descriptions

Name	Description
Domain-0 IP Address	The IP address of the System Domain (Dom-0). The system compares this to the IP address used when you install System Platform. This ensures that the correct EPW file is being used during installation.
CDom IP Address	This system compares this address to the IP address used when you install System Platform. This ensures that the correct EPW file is being used during installation.
Gateway IP Address	The gateway IP address.
Network Mask	The network mask address.
Primary DNS	The primary DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center.

Name	Description
	Important: If you configure either the DNS or HTTPS proxy data on System Platform, and when the pre-installation wizard runs, then the system displays that the data is read-only. If you do not configure the DNS or HTTPS proxy data on System Platform, then you can edit these fields. The data will be read from the EPW file, if present.
Secondary DNS (Optional)	The secondary DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center.
HTTPS Proxy (Optional)	The proxy server address, if the network to which the Session Border Controller is connected requires a proxy server to route its Internet traffic. **Important:** If you configure either the DNS or HTTPS proxy data on System Platform, and when the pre-installation wizard runs, then the system displays that the data is read-only. If you do not configure the DNS or HTTPS proxy data on System Platform, then you can edit these fields. The data will be read from the EPW file, if present.
Virtual Machine	The IP address and host name for Session Border Controller.

Configuring network settings

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



Network Settings

Enter network settings

Domain-0 IP Address	135.64.158.67
CDom IP Address	135.64.158.68
Gateway IP Address	135.64.158.126
Network Mask	255.255.255.128
Primary DNS	135.64.148.61
Secondary DNS (Optional)	
Default Search List (Optional)	
HTTPS Proxy (Optional) [IP Address:Port Number]	

Virtual Machine	IP Address	Hostname	Domain	
SBC				(Optional)
			Default Domain	
				(Optional)

Note:

If any of the fields available on the Network Settings page are already configured during the System Platform installation, those configurations appear on the Network Settings page and are available as read-only fields.

Login account configuration

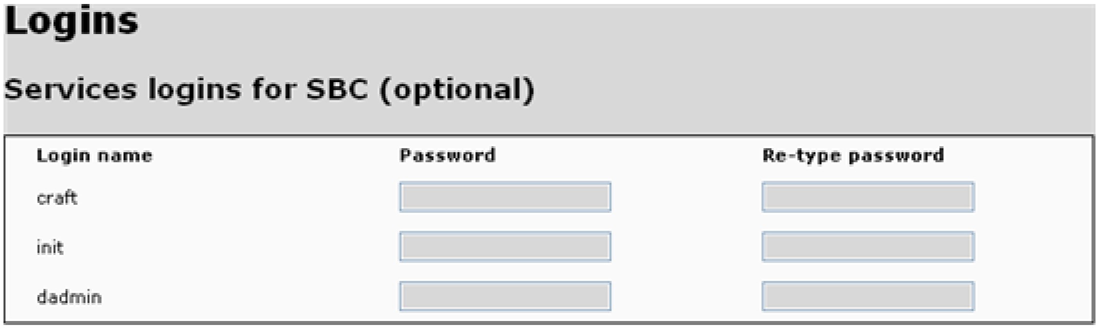
The Logins page is an optional configuration page that enables you to configure the following login accounts:

craft: Avaya services login account

init: Avaya services login account

dadmin: Avaya business partner login account

You can choose to configure all, any, or none of the login accounts.



Logins

Services logins for SBC (optional)

Login name	Password	Re-type password
craft		
init		
dadmin		

You must enter a password for a given login name for that login account to be active. If you do not enter the corresponding password for a login name, the installation wizard does not configure the login account.

If you configure a login account, you must change the default password. For detailed information about the procedure to change password, see Session Border Controller default password change.

Related topics:

Configuring a login account on page 122
Logins field descriptions on page 122

Configuring a login account

1. On the **Password** and **Re-type password** boxes, enter the password that corresponds to the login name.
2. Click **Next Step**.

Logins field descriptions

Name	Description
Login name	The name of the Avaya services or business partner login account. • **craft**: Avaya services login. • **init**: Avaya services login. • **dadmin**: Avaya business partner login.
Password	Enter the password that corresponds to the login name.

Name	Description
	Note: Use default passwords to configure a login account. You can obtain the default password from the Avaya Call Prompter.
Re-type password	Enter the password that corresponds to the login account.

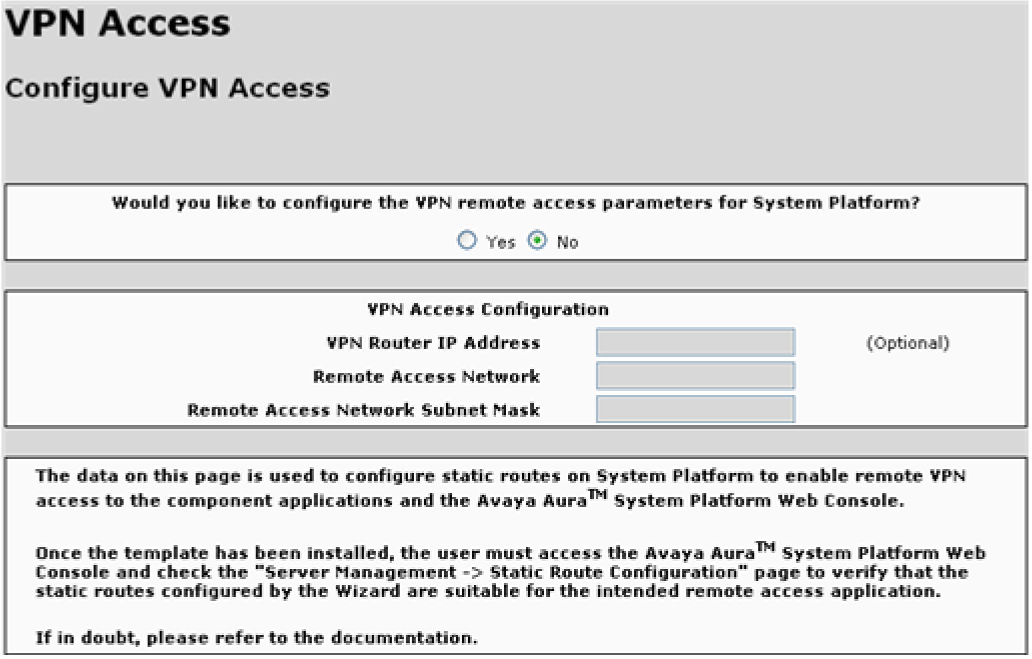
VPN access

You only need to configure this page if your VPN gateway is on the same network as the management interface of Session Border Controller. If the VPN gateway is on a different network, you may need to speak to the customer IT department to ensure that the VPN traffic is routed correctly.

Configuring VPN access

Use the VPN Access page to configure the routing required on the applications to support remote access through a VPN. If you plan to gain access to the system through a VPN gateway local to the Session Border Controller system, you should enter the required details on this page. These values are used to add static routes into the system to route traffic down the VPN tunnel to the remote network.

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



VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

○ Yes ● No

VPN Access Configuration

VPN Router IP Address		(Optional)
Remote Access Network		
Remote Access Network Subnet Mask		

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

2. Complete the fields to configure Session Border Controller to allow VPN access.

Next steps

Configure Session Border Controller parameters.

VPN Access configuration field descriptions

Name	Description
Would you like to configure the VPN remote access parameters for System Platform?	If you want to configure VPN remote access for System Platform, select **Yes**. If you do not want to configure VPN remote access for System Platform, select **No**.
VPN Router IP Address	The IP address of the external VPN gateway device.
Remote Access Network	The IP address of the network, that is, the Avaya business partner home network, from which Session Border Controller will be accessed.

Name	Description
Remote Access Network Subnet Mask	The subnet mask associated with the network, that is, the Avaya business partner home network, from which Session Border Controller will be accessed.

Configuring Session Border Controller Parameters

Log in to the Session Border Controller, the SBC page is displayed. Navigate to **Configuration** > **Installation** > **Network Settings** to configure the Session Border Controller data such as SBC network data and the Enterprise SIP server data on this page.

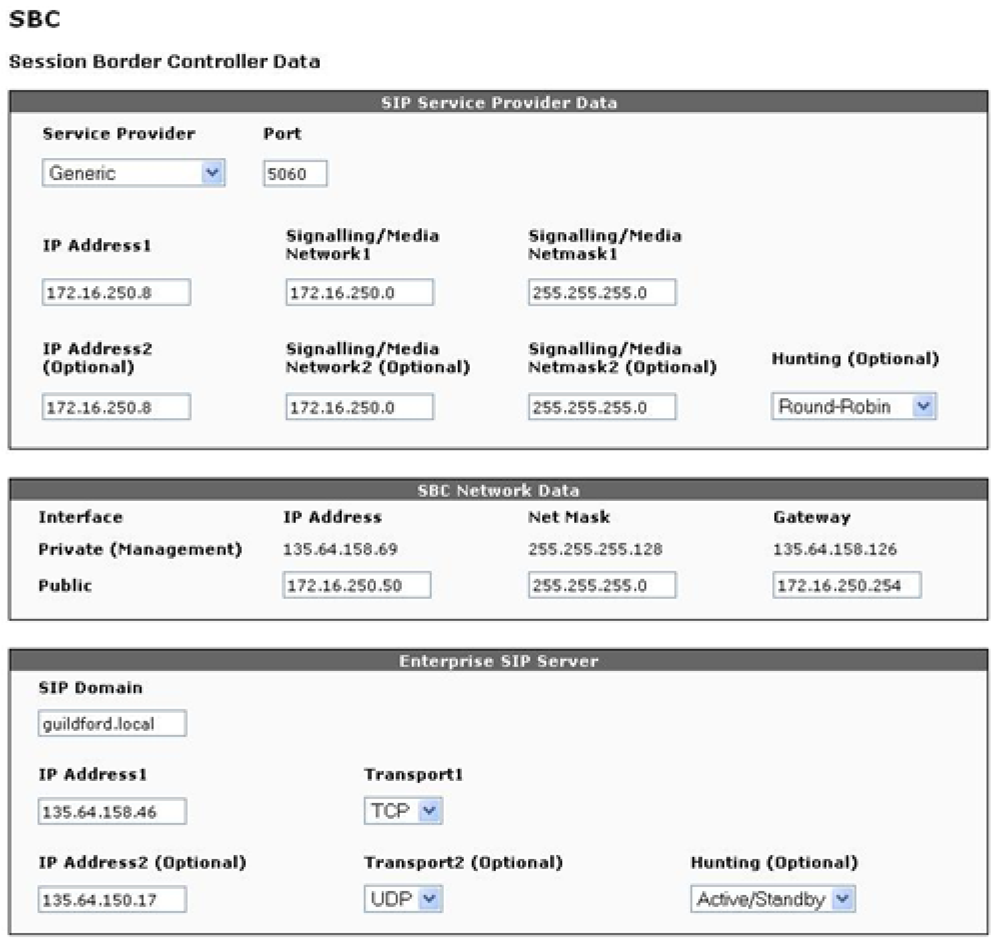
Select the required service provider from the drop-down list and provide any additional information such as far-end domain and IP addresses that is required in order to establish the SIP trunk connection.

Note:

If the Service Provider is not included in the drop-down list yet, do one of the following:

- Load an appropriate approved Avaya AA-SBC configuration ("Upload config file" option).
- If your service provider is not available on the **Service Provider** drop-down window, you must select the option **Generic**.

1. On the SBC page, select the service provider from the **Service Provider** drop-down list.



SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider: Generic

Port: 5060

IP Address1: 172.16.250.8

Signalling/Media Network1: 172.16.250.0

Signalling/Media Netmask1: 255.255.255.0

IP Address2 (Optional): 172.16.250.8

Signalling/Media Network2 (Optional): 172.16.250.0

Signalling/Media Netmask2 (Optional): 255.255.255.0

Hunting (Optional): Round-Robin

SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	135.64.158.69	255.255.255.128	135.64.158.126
Public	172.16.250.50	255.255.255.0	172.16.250.254

Enterprise SIP Server

SIP Domain: guildford.local

IP Address1: 135.64.158.46

Transport1: TCP

IP Address2 (Optional): 135.64.150.17

Transport2 (Optional): UDP

Hunting (Optional): Active/Standby

2. Complete the Session Border Controller service provider, network data, and enterprise SIP server sections to configure the Session Border Controller network parameters. For more information on Session Border Controller network parameters, seeConfiguring Session Border Controller parameters field descriptions on page 126.

Configuring Session Border Controller parameters field descriptions

SIP Service Provider Data

Field	Description
Service Provider	Choice of service provider configuration templates that configure Avaya Aura® Session Border Controller with the most appropriate settings for

Field	Description
	the selected service provider. The service providers supported in this release, through the wizard, include: • AT & T • Broadvox • BT Germany • BT Spain • Nectar • Skype • T-Systems • Verizon • Generic **Note:** On selecting **Skype** as the service provider: • you must enter the Skype user ID and password when the system prompts you to do so. • instead of displaying the IP address, the SBC page automatically displays the fully qualified domain name (FQDN) of the Skype server. The FQDN that appears is **sip.skype.com**. FQDN1 and FQDN2 (Optional) are specific for Skype. These fields use an FQDN as supplied by Skype instead of IP addresses. • the default gateway is set on the public interface rather than on the private interface. As such, component on the internal interface that are on a different network requires a static route to be defined to enable routing to an from Session Border Controller. • As a security measure, the Session Border Controller installation wizard configures source IP address filtering for all service providers except Skype. Source IP address filtering blocks traffic from all IP addresses other than the Post Office Protocol (POP) of the service provider to avoid potential denial of service or other similar attacks. The Skype POPs are addressed using a fully qualified domain name which prevents the wizard from configuring such a filter. As such, if you configure Skype as the service provider, you must use other security measures for protection. For detailed information about other security measures, refer appropriate Acme documentation. For the chosen service provider, select the service provider configuration template that configures the provider Session Border Controller with the most appropriate settings. If your service provided is not available on the **Service Provider** drop-down window, you must select the option **Generic**.
Port	The SIP signalling traffic port for the service provider. This applies to both the primary connection and the optional secondary connection.
IP Address 1	The IP address in dot-decimal notation for the Service Provider’s SIP signalling traffic primary connection.

Field	Description
Signalling/ Media Network1	The IP network address in dot-decimal notation for the Service Provider's SIP signalling or media primary network.
Signalling/ Media Netmask1	The Netmask in dot-decimal notation for the Service Provider's SIP signalling or media primary network.
IP Address 2 (Optional)	The IP address in dot-decimal notation for the Service Provider's SIP signalling traffic secondary connection.
Signalling/ Media Network2 (Optional)	The IP network address in dot-decimal notation for the Service Provider's SIP signalling or media secondary network.
Signalling/ Media Netmask2 (Optional)	The Netmask in dot-decimal notation for the Service Provider's SIP signalling or media secondary network.
Hunting (Optional)	If dual connections are defined, this field specifies the connection behavior as one of the following: • **Active/Standby** • **Round Robin** **Hunting (Optional)** determines the algorithm used to select the outgoing connection. If you select **Active/Standby**, the traffic uses connection 1 when it is in service. If connection 1 is not in service, the traffic switches to connection 2. If you select **Round Robin** and both connection 1 and connection 2 are in service, the traffic is evenly balanced across both the connections. If one connection fails, traffic switches to the connection in service.

SBC Network Data — Private (Management)

Field	Description
IP Address	The IP address in dot-decimal notation of the Avaya Aura® Session Border Controller Private Interface. This IP address is shared with the Avaya Aura® Session Border Controller Management Interface.
Net Mask	The Netmask in dot-decimal notation of the Avaya Aura® Session Border Controller Private Interface. This IP address is shared with the Avaya Aura® Session Border Controller Management Interface.
Gateway	The gateway in dot-decimal notation used by the Avaya Aura® Session Border Controller Management and Private Interfaces.

Field	Description
	By default this is set to the Default Gateway defined on System Platform.

SBC Network Data — Public

Field	Description
IP Address	The IP address in dot-decimal notation of Avaya Aura® Session Border Controller Public Interface.
Net Mask	The Netmask in dot-decimal notation of the Avaya Aura® Session Border Controller Public Interface.
Gateway	The gateway in dot-decimal notation for the Avaya Aura® Session Border Controller Public Interface.

Enterprise SIP Server

Field	Description
SIP Domain	The SIP Domain Name to be used by Avaya Aura® Session Border Controller.
IP Address 1	The IP address in dot-decimal notation of the primary SIP connection of the enterprise.
Transport1	The SIP Transport Protocol to be used for communication with the primary SIP connection of the enterprise. Valid values are UDP, TCP or TLS.
IP Address 2 (Optional)	The IP Address in dot-decimal notation of the secondary enterprise SIP server.
Transport2 (Optional)	The SIP Transport Protocol to be used for communication with the secondary SIP connection of the enterprise. Valid values are UDP, TCP or TLS.
Hunting (Optional)	If dual connections are defined, this field specifies the connection behavior as one of the following: • **Active/Standby** • **Round Robin** **Hunting (Optional)** determines the algorithm used to select the outgoing connection. If you select **Active/Standby**, the traffic uses connection 1 when it is in service. If connection 1 is not in service, the traffic switches to connection 2. If you select **Round Robin** and both connection 1 and connection 2 are in service, the traffic is evenly balanced across both the connections. If one connection fails, traffic switches to the connection in service.

Review installation summary

Click **Summary** on the left pane to view the Summary page which provides an overview of the configuration data already gathered by the wizard. This page displays the values you have not yet set in red.

Next steps

Confirm installation.

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

Confirming Installation

1. Click **Finish** on the left pane to view the Confirm Installation page and click **Accept** to accept the settings.

   The system enables the **Install** option.
2. Click **Install** to start installing the template.

Result

After the configuration, the installation wizard downloads, starts, and configures the virtual machines. You can see the progress on each section. This process takes approximately 30 minutes depending on the system size. The system does not require any extra input during this process.

> **Note:**
> Do not attempt to configure the virtual machines during the post-installation process. All the applications are configured at this stage. Attempting to configure the system too early may result in your changes being lost or the wizard being blocked from completing its tasks.

If there is any error during the post-installation process, the system displays the error in bold letters together with a warning symbol in the extreme right column. Investigate such errors immediately. Some errors might be minor and might not affect the success of the installation. Other errors may require corrective action including reinstallation.

You can test the installation after the system loads the machines and configures them.

Next steps

If the installation fails, perform the troubleshooting steps. For more information on troubleshooting, see the Troubleshooting System Platform and Session Border Controller installation chapters.

Installing Session Border Controller with minimal configuration

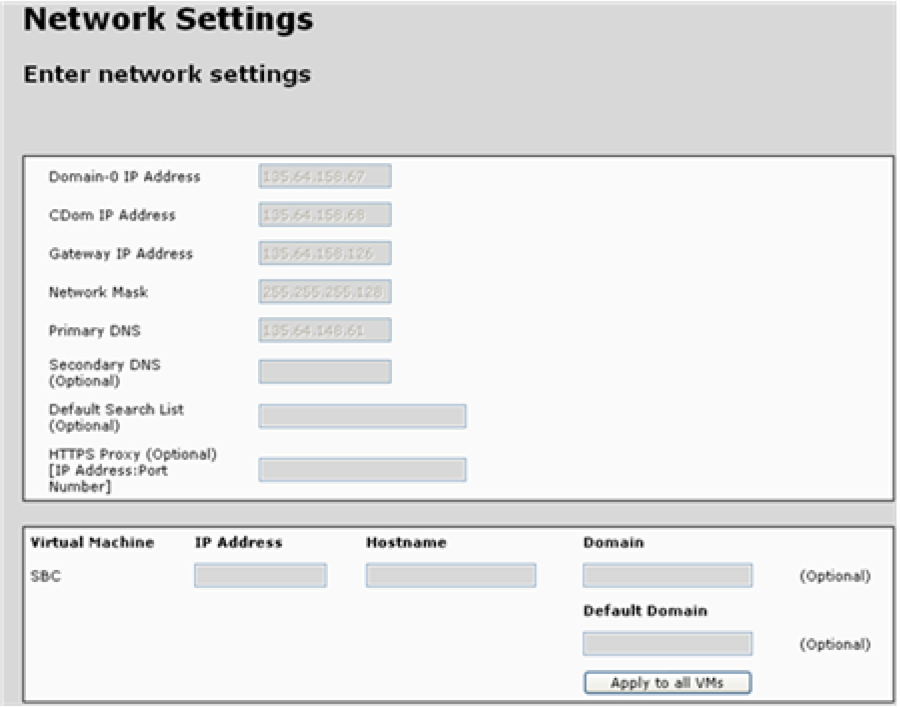
Installing minimally configured Session Border Controller

If you are an advanced user, you can administer the system through other means, such as provision, or by restoring a previously saved Session Border Controller file. In this case, you must select the **Configuration** > **Minimal Installation Wizard** option in the navigation pane of the wizard. When you select this, many of the installation wizard sections disappear and you can no longer configure these parameters through the wizard. The minimal Session Border Configuration installation comprises three steps:

1. Configuring network settings
2. Configuring services and business partner logins
3. Reviewing installation summary
4. Finishing installation

Configuring network settings

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



Network Settings

Enter network settings

Domain-0 IP Address	135.64.158.67
CDom IP Address	135.64.158.68
Gateway IP Address	135.64.158.126
Network Mask	255.255.255.128
Primary DNS	135.64.148.61
Secondary DNS (Optional)	
Default Search List (Optional)	
HTTPS Proxy (Optional) [IP Address:Port Number]	

Virtual Machine	IP Address	Hostname	Domain	
SBC				(Optional)
			Default Domain	
				(Optional)

Note:

If any of the fields available on the Network Settings page are already configured during the System Platform installation, those configurations appear on the Network Settings page and are available as read-only fields.

Network Settings field descriptions

Name	Description
Domain-0 IP Address	The IP address of the System Domain (Dom-0). The system compares this to the IP address used when you install System Platform. This ensures that the correct EPW file is being used during installation.
CDom IP Address	This system compares this address to the IP address used when you install System Platform. This ensures that the correct EPW file is being used during installation.
Gateway IP Address	The gateway IP address.
Network Mask	The network mask address.

Name	Description
Primary DNS	The primary DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center. **Important:** If you configure either the DNS or HTTPS proxy data on System Platform, and when the pre-installation wizard runs, then the system displays that the data is read-only. If you do not configure the DNS or HTTPS proxy data on System Platform, then you can edit these fields. The data will be read from the EPW file, if present.
Secondary DNS (Optional)	The secondary DNS Server address. The system requires the DNS server to resolve the host names for alarming and remote access name associated with the Avaya Service Center.
HTTPS Proxy (Optional)	The proxy server address, if the network to which the Session Border Controller is connected requires a proxy server to route its Internet traffic. **Important:** If you configure either the DNS or HTTPS proxy data on System Platform, and when the pre-installation wizard runs, then the system displays that the data is read-only. If you do not configure the DNS or HTTPS proxy data on System Platform, then you can edit these fields. The data will be read from the EPW file, if present.
Virtual Machine	The IP address and host name for Session Border Controller.

Login account configuration

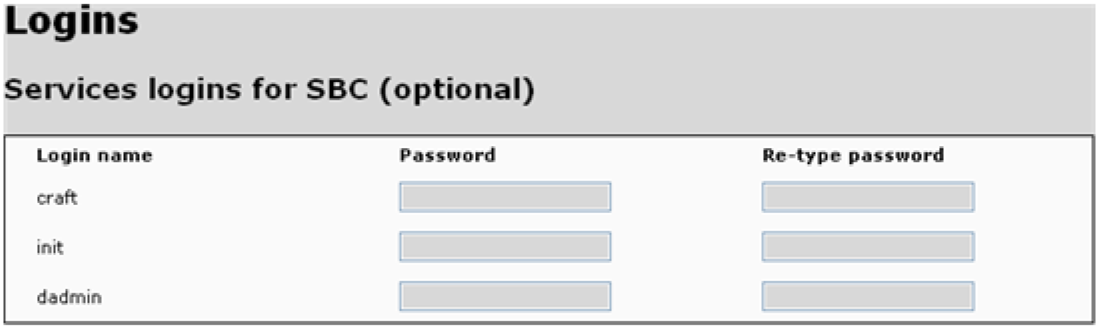
The Logins page is an optional configuration page that enables you to configure the following login accounts:

craft: Avaya services login account

init: Avaya services login account

dadmin: Avaya business partner login account

You can choose to configure all, any, or none of the login accounts.



Logins

Services logins for SBC (optional)

Login name	Password	Re-type password
craft		
init		
dadmin		

You must enter a password for a given login name for that login account to be active. If you do not enter the corresponding password for a login name, the installation wizard does not configure the login account.

If you configure a login account, you must change the default password. For detailed information about the procedure to change password, see Session Border Controller default password change.

Related topics:

Configuring a login account on page 122

Logins field descriptions on page 122

Configuring a login account

1. On the **Password** and **Re-type password** boxes, enter the password that corresponds to the login name.
2. Click **Next Step**.

Logins field descriptions

Name	Description
Login name	The name of the Avaya services or business partner login account. • **craft**: Avaya services login. • **init**: Avaya services login. • **dadmin**: Avaya business partner login.
Password	Enter the password that corresponds to the login name.

Name	Description
	Note: Use default passwords to configure a login account. You can obtain the default password from the Avaya Call Prompter.
Re-type password	Enter the password that corresponds to the login account.

Review installation summary

Click **Summary** on the left pane to view the Summary page which provides an overview of the configuration data already gathered by the wizard. This page displays the values you have not yet set in red.

Next steps

Confirm installation.

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

Confirming Installation

1. Click **Finish** on the left pane to view the Confirm Installation page and click **Accept** to accept the settings.

   The system enables the **Install** option.
2. Click **Install** to start installing the template.

Result

After the configuration, the installation wizard downloads, starts, and configures the virtual machines. You can see the progress on each section. This process takes approximately 30 minutes depending on the system size. The system does not require any extra input during this process.

Note:

Do not attempt to configure the virtual machines during the post-installation process. All the applications are configured at this stage. Attempting to configure the system too early may result in your changes being lost or the wizard being blocked from completing its tasks.

If there is any error during the post-installation process, the system displays the error in bold letters together with a warning symbol in the extreme right column. Investigate such errors immediately. Some errors might be minor and might not affect the success of the installation. Other errors may require corrective action including reinstallation.

You can test the installation after the system loads the machines and configures them.

Next steps

If the installation fails, perform the troubleshooting steps. For more information on troubleshooting, see the Troubleshooting System Platform and Session Border Controller installation chapters.

Session Border Controller license management

License management

Avaya Aura® Session Border Controller includes Avaya's Web License Manager (WebLM) to manage its licenses. WebLM is a Web-based software application that facilitates easy tracking of licenses. You can launch the WebLM application from within Session Border Controller.

Launching WebLM

Avaya Aura® Session Border Controller uses Web License Manager (WebLM) to manage its licenses. Use this procedure to launch WebLM from System Platform.

1. Click **Server Management** > **License Management**.
2. On the License Management page, click **Launch WebLM License Manager** .
3. When WebLM displays its Logon page, enter the user name and password for WebLM. For initial login to WebLM, the user name is `admin`, and the password is `weblmadmin`. However, you must change the password the first time that you log in to WebLM.
4. Manage the licenses as appropriate.

For more information on managing licenses in Avaya WebLM, see *Installing and Configuring Avaya WebLM Server* at http://www.avaya.com/css/P8/documents/100069577.

License Management field descriptions

Use the **License Management** page to launch the Web License Manager (WebLM) application and manage Avaya Aura® Session Border Controller licenses.

Button descriptions

Name	Description
Launch WebLM License Manager	Launches the WebLM application.

Configuring the SAL Gateway

SAL Gateway

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

Remote Serviceability

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

Note:

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

Stand-alone SAL Gateway

You can choose to use a stand-alone SAL Gateway instead of the SAL Gateway that is embedded in System Platform. You might prefer a stand-alone gateway if you have a large network with many Avaya devices. The stand-alone gateway makes it possible to consolidate alarms from many Avaya devices and send those alarms from one SAL Gateway rather than multiple SAL Gateways sending alarms. See **Secure Access Link** on http://support.avaya.com for more information on stand-alone SAL Gateway.

If you use a stand-alone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 102. You can also disable the SAL Gateway that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See Disabling SAL Gateway on page 76.

SAL Gateway configuration

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

To configure SAL, perform these high-level steps:

1. Register the system.

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

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

2. Configure the SAL Gateway.

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

Related topics:

Registering the system on page 19

Launching the SAL Gateway management portal on page 75

Launching the SAL Gateway management portal on page 75

Configuring the SAL Gateway on page 75

Configuring the SAL Gateway on page 75
SAL Gateway Management field descriptions on page 76
SAL Gateway Management field descriptions on page 76

Launching the SAL Gateway management portal

Use this procedure to launch the SAL Gateway management portal from within System Platform.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
3. When the portal displays its Log On page, enter your user name and password for Console Domain.
4. Configure the SAL Gateway as appropriate.

Related topics:
SAL Gateway on page 73
SAL Gateway on page 73
Configuring the SAL Gateway on page 75
Configuring the SAL Gateway on page 75
SAL Gateway Management field descriptions on page 76
SAL Gateway Management field descriptions on page 76

Configuring the SAL Gateway

To configure the SAL Gateway for the customer's network and System Platform, follow the instructions that are provided in *Installing and Configuring Avaya Aura^{TM} System Platform*. This document is available on http://support.avaya.com.

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.

Disabling SAL Gateway

Use this procedure to disable the SAL Gateway that is embedded in System Platform. Disable the embedded SAL Gateway if you are using a stand-alone SAL Gateway to send alarms to Avaya.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Disable SAL Gateway**.

Enabling SAL Gateway

Use this procedure to enable the SAL Gateway that is embedded in System Platform. The embedded SAL Gateway is enabled by default and only needs to be enabled if you have previously disabled it.

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Enable SAL Gateway**.

SAL Gateway Management field descriptions

Button	Description
Launch SAL Gateway Management Portal	Launches the SAL Gateway management portal in a new Web browser window. You must provide valid certificate details to access the portal.
Disable SAL Gateway	Disables the SAL Gateway that is embedded in System Platform. If you are sending alarms to a stand-alone SAL Gateway, disable the embedded SAL Gateway.
Enable SAL Gateway	Enables the SAL Gateway that is embedded in System Platform.

Related topics:

SAL Gateway on page 73
SAL Gateway on page 73
Launching the SAL Gateway management portal on page 75
Launching the SAL Gateway management portal on page 75
Configuring the SAL Gateway on page 75
Configuring the SAL Gateway on page 75

Session Border Controller password management

Session Border Controller default passwords

❗ **Important:**

After you complete the installation of a new Session Border Controller system, you must change the default password for all logins.

Make a careful note of the new passwords that you set for all logins. Customers are responsible for managing their passwords.

There are no password rules for entering a new password. Customers are responsible for selecting secured passwords.

A newly installed Avaya Aura® Session Border Controller system has the following default customer logins and passwords:

Login	Default password	Capability
root	sips	Advanced administrator. Use this login ID and password to access the Session Border Controller command line interface (CLI).
admin	admin01	Advanced administrator. Use this login ID and password to access the Session Border CLI and Session Border Controller GUI.
cust	cust01	Normal administrator. Use this login ID and password to access the Session Border CLI and Session Border Controller GUI with read-only permission.

Changing the admin and cust passwords for Avaya Aura® Session Border Controller

Important:

Avaya highly recommends that, for security reasons, you change the admin and cust passwords for Avaya Aura® Session Border Controller.

Make a careful note of the new passwords that you set for all logins. Customers are responsible for managing their passwords.

There are no password rules for entering a new password. Customers are responsible for selecting secured passwords.

1. Access the Avaya Aura® Session Border Controller Web interface by typing `https://<ip address>` in your Internet browser, where *<ip address>* is the IP address of Avaya Aura® Session Border Controller.

   Tip:

   You can also access the Avaya Aura® Session Border Controller Web interface from the System Platform Web Console. On the Virtual Machine Management page (**Virtual Machine Management** > **Manage**), click the wrench icon next to **sbc**.
2. Log in as `admin`.

   The default password is `admin01`.
3. Click the **Access** tab.
4. In the navigation pane, click **users** > **user admin**.
5. Clear the ***password** field, and enter a new password.
6. Retype the new password in the **confirm** field.
7. Click **Set**.
8. In the navigation pane, click **users** > **user cust**.
9. Clear the ***password** field, and enter a new password.
10. Retype the new password in the **confirm** field.
11. Click **Set**.
12. In the navigation pane, click **Configuration** > **Update and save configuration**.
13. Click **OK** when prompted.

Changing the root password for Avaya Aura® Session Border Controller

Important:

Avaya highly recommends that, for security reasons, you change the root password for Avaya Aura® Session Border Controller.

Make a careful note of the new passwords that you set for all logins. Customers are responsible for managing their passwords.

There are no password rules for entering a new password. Customers are responsible for selecting secured passwords.

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of Avaya Aura® Session Border Controller.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. Log in as `root`.

   The default password is `sips`.
5. At the `username` prompt, log in as `admin`.

   The default password is `admin01`.
6. Enter the following command: **`secret root`**
7. When prompted, enter a new password, and then reenter to confirm the new password.
   The root password is changed. Make a note of the new root password. Next time you log in to Avaya Aura® Session Border Controller as `root`, use the new password.
8. Type **`exit`** to exit the SSH session.

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 components of System Platform and of the applications that are included in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

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

1. Access the registration form and follow the instructions. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.
2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date 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 an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices.
3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

Related topics:

SAL Gateway on page 73

Chapter 4: Session Border Controller high availability

Session Border Controller high availability overview

Important:

Before configuring the Session Border Controller high availability failover option, refer the latest version of the following documents available at http://support.avaya.com:

- *Avaya Aura® Session Border Controller R 6.0.1 Release Notes*
- *Avaya Aura® Session Border Controller High Availability Configuration Details* application notes

Avaya Aura® Session Border Controller supports high availability failover as an optional feature. The Session Border Controller high availability failover feature is not interoperable with the System Platform high availability failover feature. If you want to configure the Session Border Controller high availability failover and System Platform high availability failover is already configured on your system, you must first disable System Platform high availability failover and then configure Session Border Controller high availability failover. For detailed information about disabling System Platform high availability failover, see *Administering Avaya Aura® System Platform* available at http://support.avaya.com.

The Session Border Controller high availability failover option monitors the following failover scenarios and ensures continuation of service in the event of an outage:

- Connectivity of the crossover cable with heartbeat monitoring between servers.
- Health of the server hardware and software processes.

To set up the high availability failover option, you must operate an active and a standby S8800 1U Server or HP ProLiant DL360 G7 Server with exactly the same configuration and with the same version of Avaya Aura® Session Border Controller installed on both the servers.

Important:

Avaya Aura® Session Border Controller high availability failover is not supported in the HP Procurve blade server.

Prerequisites

The prerequisites for configuring Avaya Aura® Session Border Controller high availability failover are as follows:

- Two S8800 1U Servers or two HP ProLiant DL360 G7 servers with exactly the same configuration.

  Note:

  The HP Procurve Server does not support the high availability failover feature.

- Both the servers must have a spare Gigabit network interface to be used as a crossover connection which is dedicated exclusively to high availability failover services [heartbeat health checks and DRBD (Distributed Replicated Block Device) synchronization propagation].
- Both the servers must reside in the same subnet.
- The same version of Session Border Controller must be installed on both the active and standby nodes.
- Both the servers must be connected with a gigabit-crossover cable on the ports detected as eth2 on operating system (physical Ethernet port 3).
- The primary server and the standby server must have the same memory, number of processors, and total free disk space.

Limitations

The Avaya Aura® Session Border Controller high availability failover option has the following limitations:

- Unplugging of the Ethernet cable is not supported as a high availability failover scenario.
- On a Session Border Controller high availability system, you can change the IP addresses of the Session Border Controller interfaces through System Platform to ensure that there are no IP addresses conflict. However, changes to the IP addresses of the Session Border Controller interfaces are only valid when updating the Cluster Master. That is, you must not attempt to change the other server using this method.

For detailed information about configuring Session Border Controller high availability failover option, see the following documents available at http://support.avaya.com:

- *Avaya Aura® Session Border Controller R 6.0.1 Release Notes*
- *Avaya Aura® Session Border Controller High Availability Configuration Details* application notes

Chapter 5: Session Border Controller template upgrade

Template upgrade

You can upgrade the Session Border Controller template from System Platform Console Domain.

If you have enabled the template high availability failover option and want to upgrade a template, you must first stop failover before running the upgrade operation. Then upgrade each node separately before restarting failover again.

Important:

To minimize service disruption, Avaya recommends that you perform platform upgrades during a planned maintenance window. The upgrade procedure is service affecting and includes a reboot of the entire system.

Related topics:

Stopping High Availability operation on page 163

Upgrading a template on page 164

Stopping High Availability operation

Prerequisites

Important:

Stopping High Availability operations during disk synchronization could corrupt the file system of the standby console domain. To check synchronization status indicators, see the messages in the Disk Status (FRHA, MPHA) and CPU Memory Status (MPHA) areas of the High Availability page in the Web Console.

This procedure stops High Availability operation but does not remove the High Availability feature configuration.

You can restart High Availability operations at any time.

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

1. Click **Server Management** > **High Availability**.
2. Click **Stop HA** and confirm the displayed warning.

   The 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** > **High Availability** and recheck the virtual machine disk and (if MPHA is configured) the virtual machine CPU memory status on the High Availability page in the Web Console.

Upgrading a template

The template upgrade sources are located at PLDS, Web server, SP server, template CD or DVD, or USB device. The system searches for the template upgrade files at the location you specify. If the system cannot find the file that has an `.ovf` extension, it does not continue to search for the template upgrade files.

1. Log in to the Avaya Aura® System Platform Web Console.
2. On the left navigation menu, click **Server Management** > **Solution Template**.
   The system displays the list of sources to upgrade the template.
3. Select the location from where to download the template image files for the upgrade.
   The system looks for the template description file that has an `.ovf` extension.

   Note:

   If you select the location as Web server or System Platform server, you must enter the template upgrade URL.
4. Click **Search**.
   The system displays the available upgrade templates and the version numbers.
5. Select the upgrade template and click **Upgrade**.
   The system displays a pop-up window confirming that the template is qualified for upgrade and informing that both the System Domain (Dom–0) and Console Domain will reboot when the upgrade completes.

   Important:

   As part of the upgrade process, System Domain (Dom–0) and Console Domain reboot, which in turn reboots all the other virtual machines. During the platform upgrade process, operations on the System Platform Management Console are blocked and all the links (including menu items) are disabled until you commit or rollback the upgrade.

6. Click **OK**.
   The system displays all the available template descriptor files.
7. Click **OK** to confirm the upgrade.
   The upgrade process starts and the system displays the Platform Upgrade workflow status page.

   As System Domain (Dom–0) and Console Domain reboot, the Platform Upgrade workflow status page does not show any updates until Console Domain becomes active. After the System Platform Management Console is up, the system automatically redirects you to the login page. This can take approximately 20 minutes.
8. Log in to the System Platform Management Console.
9. On the Commit or Rollback platform upgrade page, perform one of the following:
   - To continue the template upgrade process, click **Commit**.

     If you do not execute a commit operation within 4 hours after the upgrade, the system performs an automatic rollback.

     Important:
     If you click **Commit**, you cannot go back to the earlier version of the template.
   - To cancel the template upgrade process and go back to the previous version of the software, click **Rollback**.

     Important:
     If you click **Rollback**, the server reboots.

Template upgrade on high availability systems

On a high availability system, you can upgrade the template in the following methods:

- Upgrade the template on both the systems:

  This method requires execution of template upgrade on both the machines separately. However, the benefit is that you can upgrade the template for both the systems from the System Platform Management Console without directly accessing the machines.
- Upgrade the template only on the preferred system:

This method does not require execution of platform upgrade on both machines. However, you must reinstall the standby machine and need direct access to the standby system.

Related topics:

Upgrading the template on both the systems on page 166
Upgrading the template on the preferred system on page 166

Upgrading the template on both the systems

1. Log in to the System Platform Web Console.
2. On the left navigation menu, click **Server Management** > **Failover**.
3. Click **Stop Failover** and confirm the warning.
   System Platform Management Console reboots the page. After a few minutes, System Platform Management Console redirects to the login page.
4. Login to the System Platform Management Console on standby node.
   The System Platform Management Console of the standby node displays the failover status as **Failover status: (Standby node), Configured, Stopped**.
5. On the left navigation menu, click **Server Management** > **Solution Template** and proceed with the standby node upgrade procedure.

   For more information, see Template upgrade on page 163.
6. Log in to the System Platform Management Console for the preferred node.
   The System Platform Management Console of the preferred node displays the failover status as **Failover status: (Preferred node), Configured, Stopped**.
7. On the left navigation menu, click **Server Management** > **Solution Template** and proceed with the preferred node upgrade procedure.

   For more information, see Template upgrade on page 163.

Upgrading the template on the preferred system

1. Log in to the System Platform Web Console.
2. On the left navigation menu, click **Server Management** > **Failover**.
3. Click **Stop Failover** and confirm the warning.

System Platform Management Console reboots the page. After a few minutes,System Platform Management Console redirects to the login page.

4. Login to the System Platform Management Console on preferred node.
   The System Platform Console of the preferred node displays the failover status as **Failover status: (Preferred node), Configured, Stopped**.
5. On the left navigation menu, click **Server Management** > **Failover**.
6. Click **Remove Failover** and confirm the warning.
7. On the left navigation menu, click **Server Management** > **Solution Template** and proceed with the preferred node upgrade procedure.

   Fore more information, see Template upgrade on page 163.
8. Reinstall the standby node with the same template version as the preferred node was upgraded to.
9. After reinstalling is complete, configure and start the template high availability failover mode from the **Failover** page of the preferred node.

Chapter 6: Troubleshooting System Platform and Session Border Controller installations

Troubleshooting System Platform installation

Template DVD does not mount

The template DVD does not mount automatically.

Troubleshooting steps

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

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

Cannot ping Console Domain or access the Web Console

Troubleshooting steps

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

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

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

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

   Note:

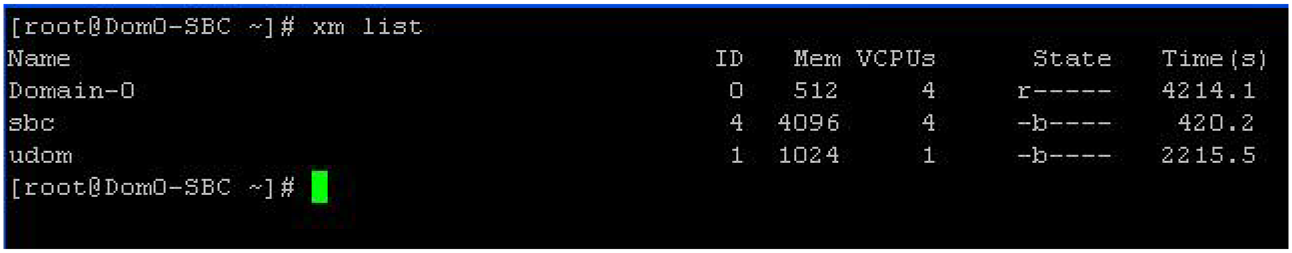
   The blocked state does not mean that there is a problem with the virtual machine. It only means that the virtual machine is currently not using any CPU time.

   Other possible virtual machine states are:

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

   For more information on the information displayed, see the Linux manual page for the **`xm`** command.
4. On the Linux screen, type **`exit`** to log off as root. Type `exit` again to log off from System Domain (Domain-0).

Example



```
[root@Dom0-SBC ~]# xm list
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0   512     4     r-----    4214.1
sbc                                          4  4096     4     -b----     420.2
udom                                         1  1024     1     -b----    2215.5
[root@Dom0-SBC ~]#
```

SAL does not work

Troubleshooting steps

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

Example

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

You should get an output similar to the following:

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

Multiple reinstallations can result in an out of memory error

If an installation wizard is used to install a template and you reinstall the template by deleting and installing it multiple times, an out of permanent generation memory space (PermGen) error can occur.

Troubleshooting steps

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

1. Delete the template.
2. Restart Tomcat by performing the following steps:
   a. Log in to Console Domain as admin.
   b. Type `su`
   c. Type `/sbin/service tomcat restart`

3. Start the pre-installation Web application.
4. Install the template.

Troubleshooting Session Border Controller installation

Session Border Controller installation wizard does not start

When you run the installation wizard from the **Start** menu, a network error appears in the Internet explorer.

Troubleshooting steps

1. Launch Internet Explorer.
2. Click **Tools** > **Internet options** > **Connections** > **LAN settings**.
3. Clear the **Use a proxy server for your LAN** checkbox.
4. Click **OK**.

Appendix A: Installation Pre-requisite for Session Border Controller - worksheets

Installation prerequisite

Requirement	Description	✔
Bootable CD reader or USB flash drive	Contains the System Platform installer files provided by Avaya or downloaded from the PLDS Web site, http://plds.avaya.com.	
Bootable DVD reader or USB flash drive	Contains the Session Border Controller installer files provided by Avaya or downloaded from the PLDS Web site, http://plds.avaya.com.	
CAT5 Ethernet crossover cable for Session Border Controller high availability failover option.	For detailed information, see the Server installation and connectivity chapter on *Installing and Configuring Avaya Aura® System Platform*.	
Verify the following: • For a simplex configuration: You must have one S8800 1U Server, or HP Procurve blade server, or the HP-Avaya common server with System Platform installed. • For a Session Border Controller high availability failover configuration: You must have two S8800 1U Server with System Platform installed and other required configuration.	For detailed information , see *Avaya Aura® Session Border Controller R 6.0.1 Release Notes* and application notes for *Avaya Aura® Session Border Controller High Availability Configuration Details* application notes available at http://support.avaya.com.	

Network Configuration worksheet

Requirement / component / machine name	**Notes**	**Value / Requirement**
You need to know the network configuration to be applied to Avaya Aura® Avaya Aura® Session Border Controller in terms of: • Avaya Aura®Avaya Aura® Session Border Controller Management and Private Interface. (These interfaces share the same network configuration). • Avaya Aura®Avaya Aura® Session Border Controller Public Interface • Service Provider IP Address and Port for signalling and Media Network • Enterprise IP Address, SIP transport method, and SIP domain name		
System Platform Domain (Dom–0) IP address		
System Platform Console Domain (C-Dom) IP address		
System Platform Gateway IP address	This also applies to the Session Border Controller Management / Private Interface.	
System Platform Primary DNS IP address	The system requires the DNS server to resolve the host names for alarming and for remote access names associated with the Avaya Service Centre. This also applies to the Session Border Controller Management / Private Interface.	
System Platform Secondary DNS IP address		

Requirement / component / machine name	Notes	Value / Requirement
HTTPS Proxy IP address	The proxy server address, if the network to which the Session Border Controller is connected, requires a proxy server to route its Internet traffic.	
Session Border Controller Management / Private Interface IP address	Must be within the same network as System Platform.	
Session Border Controller Public Interface IP address		
Session Border Controller Public Interface netmask		
Session Border Controller Public Interface Gateway		
SIP Service Provider signaling IP address		
SIP Service Provider signaling port	Example: 5060	
SIP Service Provider media network address		
SIP Service Provider media network netmask		
Enterprise SIP Server IP address		
Enterprise SIP Server transport method	Example: UDP, TCP	
Enterprise SIP Server domain name		

Index