Installing Avaya Aura™ Session Manager

03-603473, Issue 1.4
Release 5.2
September 2010

Notices

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

For full support, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03–600758.

For full support, please see the complete document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://www.avaya.com/support

Copyright

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

Contact Avaya Support

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

Contents

Chapter 1: Installation overview

This document contains the procedures for installing and upgrading Avaya Aura™ Session Manager.

Avaya Aura™ System Manager manages up to three Session Manager instances. The servers running Session Manager are in different locations and likely in different geographical regions. You can set up and administer the three Session Managers concurrently.

System Manager must be installed first before installing Session Manager. Installing System Manager is described in *Implementing Avaya Aura™ System Manager*

The high-level steps for installing Session Manager are:

- device registration
- connection validation
- PLDS registration, software, and licensing
- equipment inventory
- data collection
- install and configure System Manager
- install and configure Session Manager #1
- install and configure Session Manager #2
- Network Configuration Center administration
- testing and validation

Avaya-provided equipment

For Session Manager installation, Avaya provides the following:

- Avaya S8800 server and associated hardware
- SM100 security module installed on the server
- Operating System
- Session Manager software

System Manager Server requirements

Server

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

Remote access

VPN connectivity to the System Manager and Session Manager server(s) via SSG, SAC-LIT, SAL, or SIG is a requirement for remote implementation.

PLDS software and licensing

The System Manager software and licensing need to be obtained from the Avaya PLDS website at http://plds.avaya.com. PLDS access and registration require an Avaya SSO login.

Customer-provided equipment

The customer must provide the following equipment:

- Standard 19–inch 4–post equipment rack that is properly installed and solidly secured. The rack must meet the following standards:
  - American National Standards Institute (ANSI) and Electronic Industries Association (EIA) standard ANSI/EIA-310–D-92.
  - International Electrotechnical Commission (IEC) 297
  - Deutsche Industrie Norm (DIN) 41494
- Screws that come with the racks for installing the rails
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor must be available on-site for advanced installation or troubleshooting.
- Power from a nonswitched electrical outlet
- Access to the network

Customer responsibilities

It is the customer's responsibility to download and burn the software to a bootable DVD. This is needed for advanced installation and/or troubleshooting. The DVD should contain the following:

- Session Manager Kick Start RHEL
- Session Manager software
- System Manager template
- System Platform software

Technician installation responsibilities

At the customer site, field technicians will:

1. Validate connectivity
2. Ensure the customer has downloaded and burned a DVD containing the required software
3. Ensure System Manager is set up and on the customer's network:
    - ping System Manager from the customer's network
    - login to System Manager to retrieve the trusted password (this password is needed during Session Manager setup)
4. Install the S8800 server (rack, stack and cable out)
5. Configure the basic Session Manager
6. Handoff to the Network Integration Center for routing and user configurations
7. Test and validate the system

Session Manager Operating System

The Session Manager software installs on top of the Red Had Enterprise Linux Version 5.3 operating system. This software includes additional RPMs that may or may not be part of the base Red Hat Linux OS. Session Manager may require newer versions of these packages.

The following table contains a list of the additional RPM packages which are installed by the Session Manager installer:

Package Description	RPM Name
Java 1.6 Sun Compatibility Libraries	java-1.6.0–sun-compat
PostgreSQL Database System ver 8.2.6	postgresql postgresql-docs postgresql-libs postgresql-contrib postgresql-server
Java Development Kit & Runtime 1.6.0_11	jdk-1.6.0_11fcs
Security Module-100 Hardware Drivers & Software	asset-gefanuc
Core Services Watchdog (Process/Service Management)	cs_watchd
XML to C/C++ language binding for web services	gsoap
rssh	Restricted Shell supporting scp/sftp for use with OpenSSH
snfw-i386	Session Manager Network Firewall
aspell **php** **php-common** **php-soap** **php-cli** **php-mbstring** **php-xml**	PHP support for PPM
aesvcs-sms	SMS support

Session Manager software also contains the JBOSS Application Server and the Avaya SIP Application Server. Most of this software is installed in /opt/Avaya.

The *Avaya Aura Session Manager: Port Matrix* document identifies which network ports must be open in firewalls. This document is available to Avaya customers, associates, and business partners via SSO and the InSite Knowledge Management Database by logging in to http://www.avaya.com/support

Installed OS-level logins for Session Manager

For security purposes, the **root** login has been disabled on the Session Manager. The following is a list of logins which are created during the Session Manager software installation:

- **craft** — This is an Avaya services login which accesses the system remotely for troubleshooting purposes. The Avaya Password Change System changes the password associated with this login to a random value every 82 days.
- **sroot** — This is an Avaya services root permission login which accesses the system remotely for troubleshooting purposes. The sroot login cannot be accessed directly from a login prompt except at the server console. The Avaya Password Change System changes the password associated with this login to a random value every 82 days.
- **customer** — The customer login is created by the SMnetSetup script. During execution of the SMnetSetup script, the customer access login defaults to cust. It is your responsibility to ensure the security of this login account. The customer login has permissions to run tools on the Session Manager server which do not require root access
- **CDR_User** — This login is a restricted shell login for the Call Detail Recording (CDR) feature which collects call data from the Session Manager server. This login is restricted to sftp access only.
- **asset** — This login is created during the SM100 Security Module software installation. Access to the system using this login is disabled by default.
- **spirit** — This login is created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **postgres** — This login is created by the installation of the Session Manager software's PostgresSQL database system. Access to the system using this login is disabled.

Product ID commands

At installation time, the new system needs to be registered using the Functional Location (FL) and product type. At that time, a Product ID will be provided for each managed element for alarm reporting. Product IDs (or Alarm IDs) are assigned to the various managed elements and are used in identifying the source of an alarm for each installed server.

The CLI commands **`setProductID`** and **`getProductID`** set and read the Product ID for the managed elements. The CLI command **`spiritAgentCLI`** assigns the resident Secure Access Link (SAL) Product ID. All of these commands require root permission.

setProductID

Use **setProductID** to set the Product ID for reporting alarms for managed elements. The Product ID is a 10–digit number which starts with the number **8**.

Syntax

```
setProductID ASM | SM | SMELEM productid
```

ASM *productid* Sets the Session Manager Product ID to *productid* (Session Manager only)

SM *productid* Sets the System Manager Product ID to *productid* (System Manager only)

SMELEM *productid* Sets the Session Manager Element Manager Product ID to *productid* (System Manager only)

getProductID

Use **getProductID** to view the Product ID for reporting alarms for managed elements.

Syntax

```
getProductID ASM | SM | SMELEM
```

ASM Gets the Session Manager Product ID (Session Manager only)

SM Gets the System Manager Product ID (System Manager only)

SMELEM Gets the Session Manager Element Manager Product ID (System Manager only)

spiritAgentCLI

Use **spiritAgentCLI** to set and view the Product ID for reporting alarms for a managed element. The Product ID is a 10–digit number which starts with the number **5**. The Product ID is displayed when the command is entered with no parameters.

Syntax

```
spiritAgentCLI  [alarmId  productid ]
```

alarmId *productid* Sets the SAL Agent Product ID to *productid*.

Chapter 2: Installing Session Manager

The following checklist contains the steps for installing Session Manager and who is responsible for the implementation of that procedure. The checklist is a guide and is subject to change.

Session Manager installation checklist

Task Description	Role	✔
Complete Installation and Administration worksheet .	Customer	
Confirm VPN access is available (SAL or SSG)	Customer	
Preconfigure SAL or SSG with Session Manager and System Manager IP addresses	Avaya	
Configure System Manager server and OS • Provide monitor, keyboard, and mouse • Configure IP address for System Manager • Modify /etc/host file on server	Customer	
Configure Avaya Services logins	Avaya	
Validate SAL or SSG Connectivity	Avaya	
Register with PLDS • Obtain LAC for download of licenses • Obtain license file using PLDS and activate license entitlements • Download System Manager file and burn to DVD or upload to WebLM on System Manager	Customer	
Install System Manager software	Avaya	
Install WebLM license file	Avaya	
Use the setproductID command to complete alarming configuration	Avaya	

Task Description	Role	✔
Enable trust management • Enrollment password • Trusted certificate operation • Identity certificate operation	Avaya	
Confirm System Manager installation is complete	Avaya	
Avnet Session Manager server staging completed • Complete load of RHEL 5.3 and base configuration • Installation and configuration of SM100 TLS accelerator card	Avaya	
Install Session Manager single server • Connect eth0 to customer network • Connect SM100 port 1 to customer network	Avaya	
Install and run the ASM install script • Configure the IP and Host Name • Configure DNS (only if being used) • Configure NTP addresses • Confirm latest Session Manager software and Service Pack installed	Avaya	
Test Remote Access via SAL or SSG	Avaya	
Use the setproductID command to complete alarming configuration	Avaya	
Configure any additional Session Managers	Avaya	
System Manager Configuration • Add Session Manager instances and SIP entities • Configure SIP entities on the Session Manager servers • Configure the various SIP entities to work with Session Manager • Confirm synchronizing configuration changes work • Administer the Session Manager Dial Plans and Adaptations • Complete the Network Routing Policy administration tasks	Avaya	
Build customer login/administration of additional users	Avaya	
Verify security default settings and change as necessary • Security Administration • Network firewall • SIP firewall (rules, blacklist, whitelist, rule precedence, etc.)	Avaya	

Task Description	Role	✔
Test alarms	Avaya	
Configure the Welcome Packet	Avaya	
Acceptance of Avaya deliverables	Customer	

Session Manager configuration information worksheet

This information is used for entering data during the SMnetSetup step.

Make a copy of this worksheet for each Session Manager instance.

Field	Information to enter
Eth 0 IP address (management interface for Session Manager on the customer network)	
Network Mask Eth0	
Default Gateway IP for Eth0	
Primary DNS	
Secondary DNS (if applicable)	
Tertiary DNS (if applicable)	
System Manager server hostname	
Session Manager IP address	
DNS Search Domains (space-separated for multi-entry)	
Local time zone	
NTP server	
Secondary NTP server (if applicable)	
Tertiary NTP server (if applicable)	
Optional Customer Linux Login (default is cust)	
IP address of the System Manager server	

Verifying installation information

Verify that you have the correct Session Manager licenses.

1. Verify that you have the required information on the installation worksheets for configuring and administering Session Manager.
2. Obtain the Product ID of each managed element for alarming purposes.
3. Verify that you have the license key or the License Entitlement Code for the Session Manager.

Setting up a Trust Management enrollment password

Enrolling a password

1. Log on to the System Manager Common Console.
2. Click **Security** > **Trust Management** > **Enrollment Password**.

   If a password has already been generated, copy it from the **Existing Password** box if the **Time Remaining** field is not set to zero.
3. If an existing password is not present or the time or count are set to zero, select the expiration of password in days in the **Password expires in** field.
4. In the **Certificate allowed** field, select the number of certificates.

   Note:

   Select at least ten certificates per Session Manager instance.
5. Click **Generate** if you wish to use a randomly generated string as a password.

   If you click **Generate**, the password field displays the generated password. If you do not wish to use a randomly generated string, enter a password.
6. Click **Done**.

   Note:

   When you click **Done**, the system updates the number of certificates with the number of certificates selected in the **Certificate allowed** field. The system also

updates the time displayed next to the **Time remaining** label with the value selected in the **Password expires in** field.

You *must* remember this password. You need to provide it as input at the time of installing Session Manager.

Installing the S8800 server

See Installing the S8800 Server on page 25 for installing the S8800 server.

Configuring Session Manager

Session Manager has the following configuration information:

- System Name — avaya-asm
- Eth0 — 192.168.0.2/24
- Eth1 — 192.11.13.6/30
- Eth2 and Eth3 are unused
- DNS Domain — localdomain
- DNS Server — 127.0.0.1

1. Install the cables to access the Session Manager server using a laptop or USB keyboard, mouse, and monitor.
2. Log into the Session Manager server with user name **craft** and the password.
3. Enter the command `./SMnetSetup`
4. Refer to the information on the Session Manager information worksheet Session Manager configuration information worksheet on page 13 for the information required by `SMnetSetup`
5. If the question **Previous install has been detected — continue?** appears, enter `y`.
6. When prompted, enter the trust management password as administered in System Manager in the previous section.
7. At this point, the system configures itself. The configuration takes approximately 15 minutes to complete.

8. When prompted to reboot, enter `y` and press Enter. The reboot takes about 10 minutes to complete.
9. Wait until the login screen appears.

Testing the installation

1. On the System Manager console, select **Session Manager** > **System Tools** > **Maintenance Tests** in the left navigation pane.
2. Select the System Manager server in the drop-down list.
3. Click **Select all Tests.**
4. Verify that all tests show **Success**. If any of the tests fail, refer to *Maintaining and Troubleshooting Avaya Aura™ Session Manager, 03–603325*
5. Select **Session Manager** > **System Status** > **Security Module Status** to display the SM100 security module status.
6. Verify that **Security Module Deployment** is UP for all Session Managers.
7. Select **Session Manager** > **System Status** > **System State Administration** in the left navigation pane.
8. Verify that the installed software versions of all Session Managers are the same version and that all Session Manager servers are in the **Management Enabled** state.
9. Select **Session Manager** > **System Tools** > **Maintenance Tests**
10. Select the Session Manager instance to test.
11. Click **Execute all Tests**
12. Verify that all tests show **Success**.

    Note:
    For information about troubleshooting the tests, refer to *Maintaining and Troubleshooting Avaya Aura™ Session Manager, 03–603325*.
13. Select **Session Manager** > **System Status** > **System State Administration** in the left navigation pane.
14. Select the appropriate Session Manager.
15. Change the service state to **Accept New Service**.

Chapter 3: Upgrades to Session Manager

Upgrading to a new software release for Session Manager is described in *Upgrading Avaya Aura™ Session Manager* on the Avaya support web site, http://www.avaya.com/support

Installing service packs for Session Manager is described in *Installing Service Packs on Avaya Aura™ Session Manager* on the Avaya support web site, http://www.avaya.com/support

Chapter 4: PLDS Licensing

Overview

Downloading product software and licenses

The Avaya Product Licensing and Delivery System Avaya PLDS provides customers, BusinessPartners, distributors, and Avaya Associates with easy-to-use tools for managing asset entitlements and electronic delivery of software and related licenses. Using PLDS, you can perform activities such as license activation, license de-activation, license re-host, and software downloads.

Installation software applications for different products are available as ISO files on PLDS. After activating the license entitlements, installation administrators must download the ISO images to a PC, and choose to either burn a DVD for installation or transfer the ISO file to the target server for installation.

Always review the PLDS to determine if a later service pack or release is available. If updates do exist, you should refer to the appropriate upgrade procedures, contact Avaya, or contact the Avaya BusinessPartner Service representative.

Obtaining licenses

You should have a license code with you before you install a product. Using PLDS, you can activate the license entitlements and download the products.

After you buy a product, an Avaya BusinessPartner or an Avaya Associate who has permissions in PLDS for your site or sales order can access PLDS and generate license entitlements for you. You must provide the MAC address of the WebLM server to generate license entitlements in the form of License Activation Codes (LACs). The LAC will help you identify the product among other Avaya products you hold licenses for, keep track of the number of downloads, and automatically download patches and upgrades - all the while keeping the required groups and coordinators informed, through e-mail messages. The LAC e-mail recipients must be identified during the order placement process by providing their e-mail addresses.

With the LACs in hand, you can use the Quick Activation screen to activate the LACs and download the product.

Activating entitlements

Use this functionality to activate one or more entitlements for a product using the license activation code. You may choose to activate all the licenses or specify the number of licenses that you want to activate from the total number of licenses associated with the entitlements. On successful activation of the entitlements, PLDS sends an Activation Record to the customer registered with the entitlements by an e-mail. The Activation Record provides details of the number of activated licenses, the Host ID of the computer on which licenses are activated, and the complete link of the product download. The e-mail also contains the license file. You need to install the license on the License Host (WebLM server) to use the licenses.

Prerequisites

To activate a license entitlement, you must have License Activation Codes (LACs) and the Host ID of the computer on which you want to install the licenses.

1. Type http://plds.avaya.com in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Enter the License activation code (LAC) that you have received through an e-mail in the **LAC(s)** field in the Quick Activation section.

   Note:

   If you do not have an e-mail with your LAC ID, follow the steps in the Searching for Entitlements section and make a note of the appropriate LAC ID from the LAC column. The Quick Activation automatically assumes you want to activate all entitlements on LAC, and gives the option to remove line items, and enter amount of each license to activate (full or partial amount).
4. Enter the host information.
5. Click **Next** to validate the registration detail.
6. Enter WebLM Host Server Information.

   The Host ID is the MAC address from the machine hosting the WebLM server. Click on the **Help** link and follow the instructions on how to obtain the MAC address.
7. Enter the number of licenses you want to Activate.
8. Read and accept the Avaya Legal Agreement.
9. Perform the following steps, to send a confirmation e-mail:
   a. Enter any additional certificate recipients e-mail addresses in the **E-mail to:** field.
   b. Enter Comments.

c. Click **Finish**.

10. Click **View Activation Record**.
    - The **Overview** tab displays a record of the key activation information.
    - The **Ownership** tab confirms the registration information.
    - The **License/Key** tab displays the actual license files which allow x number of users to use the software. A single license file will be generated for each product line. From **License/Key** tab, you can select options to view activation details, and installation instructions.

Searching for entitlements

Use this functionality to search for an entitlement by using any one or all of the following search criteria:

- Company name
- Group name
- Group ID
- License activation code

1. Type http://plds.avaya.com in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Enter the company name in the **%Company: field**. If you would like to see a complete list of possible companies before searching for their corresponding entitlements, do the following:
   a. Click **Search**.
   b. Enter the name or several characters of the name and a wildcard (%) character.
      Company names are case sensitive. Search using both upper and lower case characters to ensure that you have visibility into all possible records.
   c. Click **Search Companies**.

Tip:

You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter `Av%`, the system searches for all the company names starting with the letter Av. You can enter a wildcard character (%) at any position in the search criteria except at the beginning. If you enter %av as the search criteria, the page displays an error.

4. Enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

   Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the group you are searching for. For example, if you enter `Gr%`, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character (%) at any position in the search criteria except at the beginning. If you enter %av as the search criteria, the page displays an error.

5. Enter the specific license activation code (LAC) ID in the **%LAC:** field.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the group you are searching for. For example, if you enter `AS0%`, the system searches for all the LACs starting with AS0. You can enter a wildcard character (%) at any position in the search criteria except at the beginning. If you enter %AS0 as the search criteria, the page displays an error.

   You will receive LAC IDs in an e-mail if you have supplied the e-mail address to your sales order. If you do not have this code, you will need to search using one of the other search criteria.

6. Select the application, product, license type and status from the drop-down field.
7. Click **Search Entitlements**.

Result

All corresponding entitlement records appear at the bottom of the page.

Regenerating a license file

Use this functionality to regenerate the License/Key on a selected License Host. During the regenerate process, you are able to change the activation details, except for the Host ID.

1. Type http://plds.avaya.com in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Click **Activation** > **Regeneration** from the Home page.
4. Search License Activations to Regenerate.

You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail and click **Next**.
7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.
9. Perform the following steps, to send a confirmation e-mail:
   a. Enter any additional certificate recipients e-mail addresses in the **E-mail to:** field.
   b. Enter Comments.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a record of the key activation information.
    - The **Ownership** tab confirms the registration information.
    - The **License/Key** tab displays the actual license files which allow x number of users to use the software. A single license file will be generated for each product line. From **License/Key** tab, you can select options to view activation details, and installation instructions.

Downloading software in PLDS

1. Type http://plds.avaya.com in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Select **Assets** from the Home page and select **View Downloads**.
4. Search for the downloads available using one of the following methods:
   - By Actual Download name
   - By selecting an Application type from the drop-down list
   - By Download type
   - By clicking **Search Downloads**
5. Click the download icon from the appropriate download.

6. When the confirmation box displays, select **Click to download your file now**.
7. If you receive an error message, click on the message, install Active X, and continue with the download.
8. When the security warning displays, click **Install**.

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

Appendix A: Installing the S8800 Server

The S8800 Server supports several Avaya software applications. The server is available as a 1U model or 2U model with various hardware components. The server model and specific hardware components in your server depend on the requirements of the software application which runs on the server. For Session Manager Release 5.2, the 1U model is used.

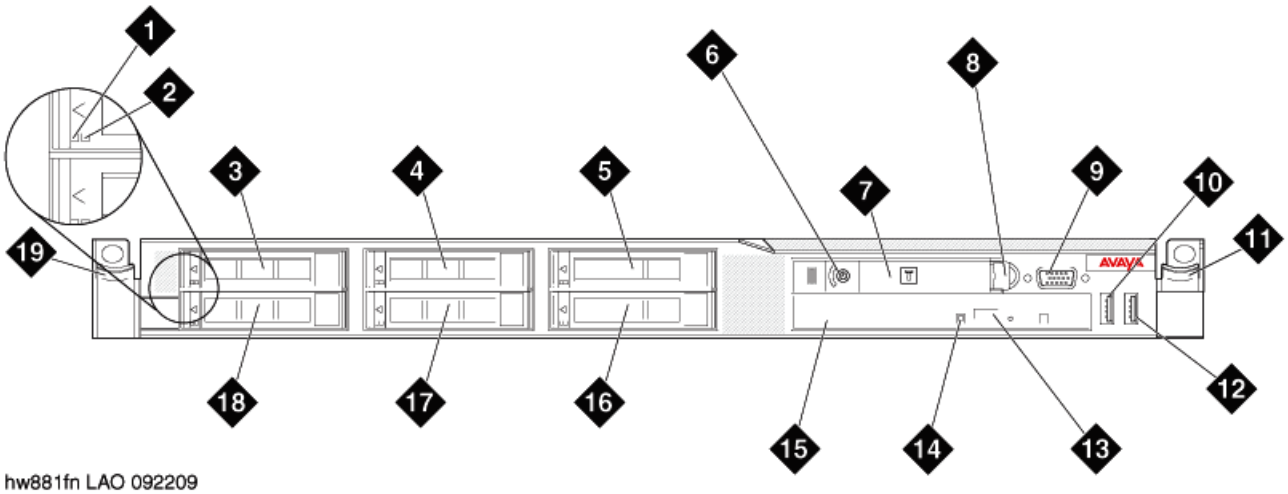
The high-level steps for installing the S8800 server are:

- Attaching the rails to the rack
- Installing the server in the rack
- Installing the cable management arm
- Powering up the server

Follow the steps in the Server installation checklist on page 32 for installing the S8800 server.

Note:
The PCIe card is the SM100 Security Module for Session Manager.

Front of server

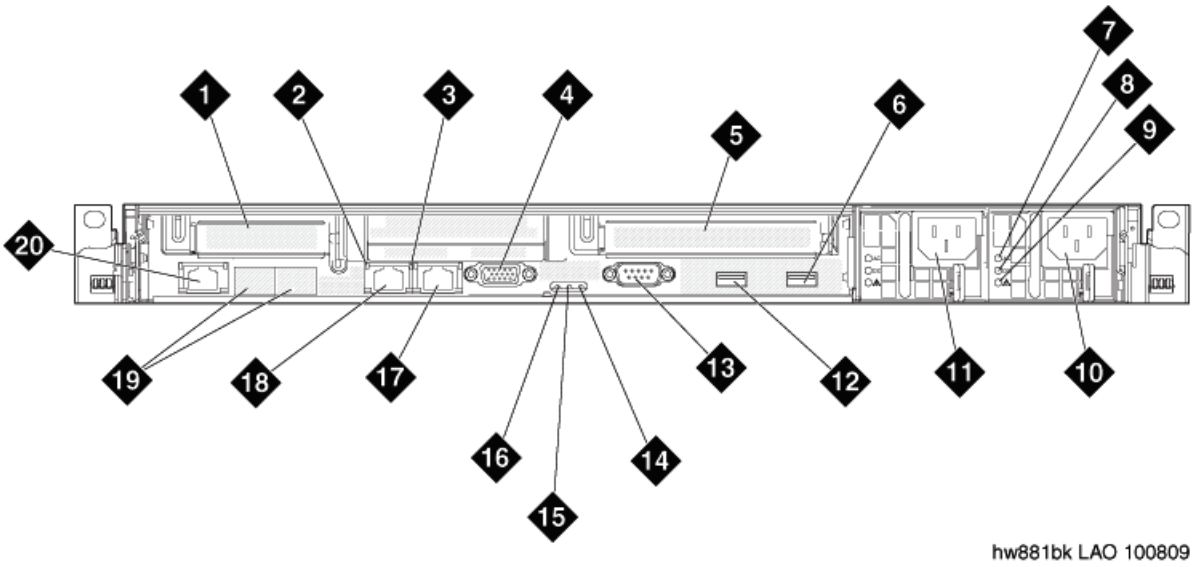


hw881fn LAO 092209

1	Hard disk drive activity LED (green)
2	Hard disk drive status LED (amber)

3	Drive bay 0
4	Drive bay 2
5	Drive bay 4
6	Power control button and LED
7	Operator information panel
8	Operator information panel release latch
9	Video connector
10	USB connector 1
11	Rack release latch
12	USB connector 2
13	DVD eject button
14	DVD drive activity LED
15	DVD drive
16	Drive bay 5
17	Drive bay 3
18	Drive bay 1
19	Rack release latch

Back of server



1	PCIe slot 1 (used for optional Ethernet connectors 5 and 6)
2	Ethernet activity LED
3	Ethernet link LED
4	Video connector
5	PCIe slot 2
6	USB connector 4
7	AC power LED (green)
8	DC power LED (green)
9	Power supply error LED (amber)
10	Power supply 2 (redundant power supply)
11	Power supply 1 (primary power supply)
12	USB connector 3
13	Serial connector
14	System error LED (amber)
15	System locator LED (blue)
16	Power LED (green)
17	Ethernet connector 2

18	Ethernet connector 1
19	Ethernet connectors 3 and 4 (with optional 2–port Ethernet daughter card)
20	System management Ethernet connector (IMM)

Server components

Component	Minimum specification	Upgrade options based on product requirements
Microprocessor	One Intel E5520 quad core, 2.26 GHZ processor	• One additional E5520 processor for a total of two processors • Higher speed E5570 processor that runs at 2.93 Ghz.
Memory	4 GB of 1333 Mhz, fully-buffered DDR-3 RDIMMs (Two 2GB DIMMs): • ECC registered • Slots: 16 dual inline	Up to 32 GB with specified 2GB DIMMs (16 GB per processor)
Media drive	DVD-R/W SATA slimline	No additional options
Hard disk drive expansion bays	Six 2.5-inch hot-swap SAS hard disk drive bays	No additional options
Hard disk drive	Two 146 GB SAS 2.5" 10K RPM hard drives	• Additional 146 GB 10K RPM drives • High performance 146 GB 15K drives
RAID controllers	ServeRAID-MR10i RAID SAS adapter that provides RAID levels 1 or 5. Includes 256 MB cache module and battery for write cache	ServeRAID-BR10i SAS RAID adapter that provides RAID level 1 (used for AES)
PCI expansion slots	Two PCI Express x16 Gen 2 slots: • Slot 1 supports half-height, half-length cards • Slot 2 supports full-height, half-length cards	No additional options

Component	Minimum specification	Upgrade options based on product requirements
Hot-swap fans	Six	No additional options
Power supply	One 675W, 12V AC power supply	Redundant 675W, 12V AC power supply
Video controller	Integrated Matrox G200 (two analog ports: one front and one rear that can be connected at the same time) The maximum video resolution is 1280 x 1024 at 75 Hz. • SVGA compatible video controller • DDR2 250 MHz SDRAM video memory controller • Avocent Digital Video Compression • Video memory is not expandable	No additional options

Environmental requirements

Server status	Air temperature	Maximum Altitude	Relative humidity
Server on	10 to 35º C (50 to 95º F) at altitude of up to 914.4 m (3,000 feet)	2,133 m (7,000 feet)	8% to 80%
	10 to 32º C (50 to 90º F) at altitude of 914.4 m to 2,133 m (3,000 to 7,000 feet)		
Server off	10°C to 43°C (50.0°F to 109.4°F)	2,133 m (7,000 feet)	8% to 80%

Safety instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system and working environment from potential damage.

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, *component* refers to any system as well as to various peripherals or supporting hardware.

Danger:

- Before installing systems in a rack, install front and side stabilizers on stand-alone racks or the front stabilizer on racks that are joined to other racks. Failure to install stabilizers before installing systems in a rack could cause the rack to tip over, potentially resulting in bodily injury.
- After installing components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

Note:

- Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements.
- System rack kits are intended to be installed in a rack by trained service technicians.

Important:

- Two or more people are required to install components that are 2U or larger in a rack cabinet.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack:
  - Do not block any air vents; usually 15 cm (6 in.) of space provides proper airflow.
  - Install the server only in a rack cabinet with perforated doors.
  - Do not leave open spaces above or below an installed server in your rack cabinet. To help prevent damage to server components, always install a blank filler panel to cover the open space and to help ensure proper air circulation.

- Do not step on or stand on any component when servicing other components in a rack.
- Do not place any object on top of rack-mounted components.

Caution:

Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

Avaya-provided equipment

Avaya provides the following equipment:

- Server and power cord
- Slide rails
- Cable management arm assembly
- Cable management arm stop bracket
- Cable management arm mounting bracket
- Cable management support arm
- Two 10–32 screws
- Four M6 screws
- Five small cable ties
- One large cable tie
- Compact flash reader, USB cable, and flashcard (for backing up files. Included when required by the product ordered.)
- Modem and USB or serial cable (for remote maintenance. Included when required by the product ordered.)
- Other hardware as ordered, such as uninterruptible power source (UPS).

Customer-provided equipment

The customer must provide the following equipment:

- Standard 19–inch 4–post equipment rack that is properly installed and solidly secured. The rack must meet the following standards:
  - American National Standards Institute (ANSI) and Electronic Industries Association (EIA) standard ANSI/EIA-310–D-92.

- International Electrotechnical Commission (IEC) 297
- Deutsche Industrie Norm (DIN) 41494

- Screws that come with the racks for installing the rails
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor must be available on-site for advanced installation or troubleshooting.
- Power from a nonswitched electrical outlet
- Access to the network

Clearance requirements

Install the server in a rack that meets the following requirements:

- Minimum depth of 70 mm (2.76 in.) between the front mounting flange and inside of the front door if the server is installed in a cabinet.
- Minimum depth of 157 mm (6.18 in.) between the rear mounting flange and inside of the rear door if the server is installed in a cabinet.
- Minimum depth of 718 mm (28.27 in.) and maximum depth of 762 mm (30 in.) between the front and rear mounting flanges to support the use of the cable-management arm.

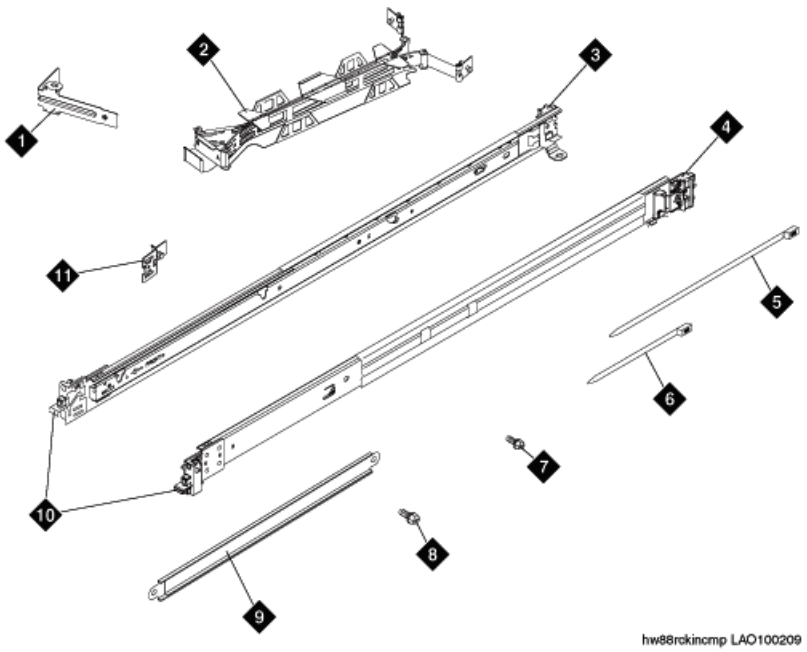
Server installation checklist

#	Task	Notes	✔
1	Verify that all equipment is on site.	Compare the list of items that were ordered to the contents of the boxes. Use the inventory list provided by your project manager. Do not rely on the packing slips inside the boxes for the correct information.	
2	Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws.		
3	Verify that the rack is grounded in accordance with local electrical code.	See *Approved Grounds* (555–245–772), available at http://support.avaya.com.	

#	Task	Notes	✔
4	Remove the cabinet doors, if necessary.	See the cabinet manufacturer's documentation.	
7	Attaching rails to the rack on page 34		
8	Installing the server in the rack on page 36		
	Installing the cable management arm on page 38 (optional)		
9	Replace the cabinet doors, if necessary.	See the cabinet manufacturer's documentation.	
10	Turn on the server.		
11	Troubleshoot the installation.		

Rack installation components

The following figure shows the items that you need to install the server in the rack cabinet.



1	Cable-management arm stop bracket (1)

2	Cable-management arm assembly
3	Slide rail (left)
4	Slide rail (right)
5	Large cable tie (1)
6	Cable ties (5)
7	M6 screws (4)
8	10–32 screws (2)
9	Cable-management support arm
10	Front of rails
11	Cable-management arm mounting bracket (1)

Attaching rails to the rack

Prerequisites

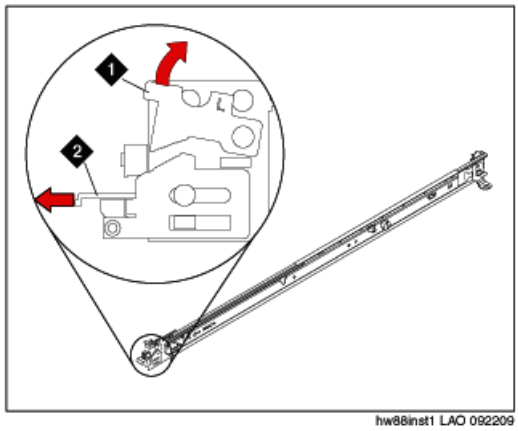
If the slide rails in your rack installation kit came with thumbscrews installed, remove them before you begin the following installation procedure.

Each slide rail is marked with either an R (right) or an L (left).

Important:

The slide rails that come with the server are compatible with racks that have square holes. If you are installing the server in a rack that has round holes, Avaya recommends that you use the appropriate rails or shelf to ensure proper fit. The customer must provide the appropriate rails or shelf.

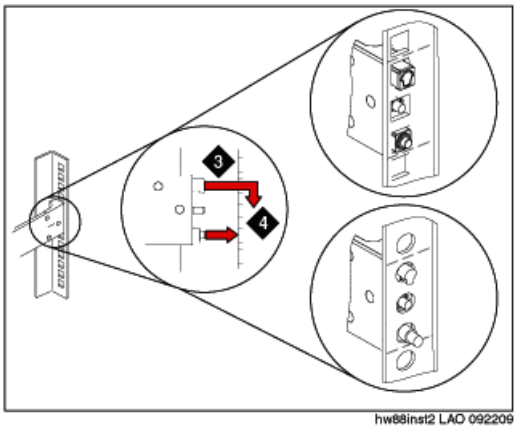
1. Select one of the slide rails and push up on the front moveable tab (1). See the following figure.



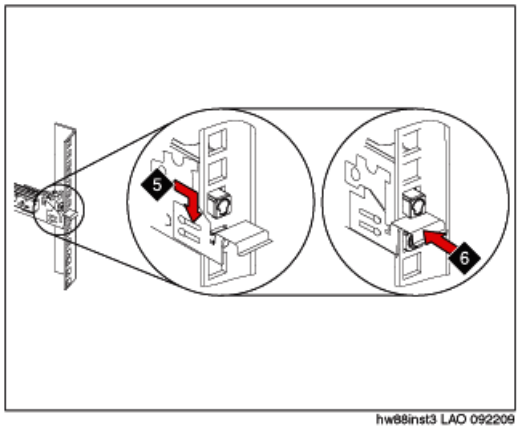
2. Pull out the front latch (2) to slide out the front side rail. See the preceding figure.
3. From the front of the rack, line up the three pins on the rear of the slide rail with the three holes in the selected U on the rear of the rack. Push the rails so that the pins go into the holes (3). See the following figure.

Important:

When you install a 2U server, be sure to install the slide rails in the bottom U of the 2U area in the rack.



4. Drop the slide rail down (4) until it latches into place. See the preceding figure.
5. Pull the slide rail forward, and insert the two pins (5) on the front of the rail into the two lower holes in the U on the front of the rack. See the following figure. Drop the rail into place until it clicks.



6. Push the front latch (6) in all the way. See the preceding figure.
7. Repeat this procedure to install the other rail onto the rack.
8. Make sure that each front latch is fully engaged.

Next steps

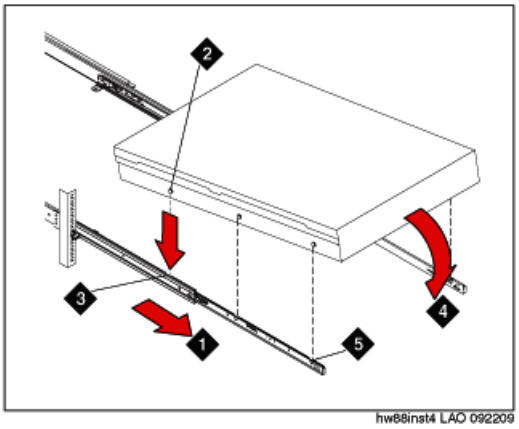
Install the server in the rack.

Installing the server in the rack

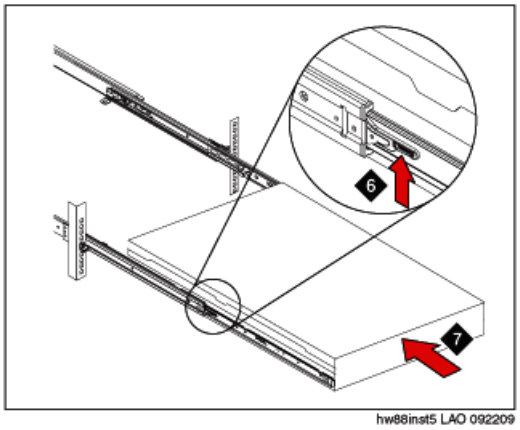
Prerequisites

Attach rails to the rack.

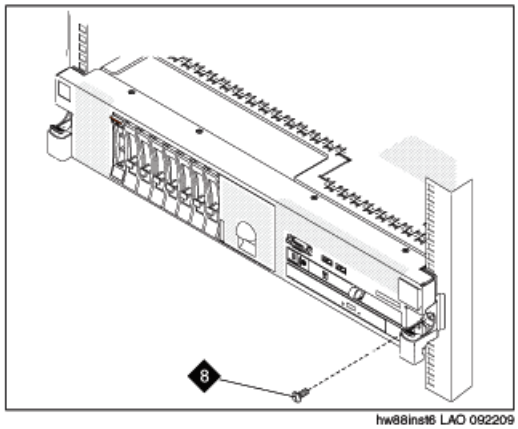
1. Pull the slide rails forward (1) until they click, two times, into place. See the following figure.



2. Carefully lift the server and tilt it into position over the slide rails so that the rear nail heads (2) on the server line up with the rear slots (3) on the slide rails. See the preceding figure.
3. Slide the server down until the rear nail heads slip into the two rear slots.
4. Slowly lower the front of the server (4) until the other nail heads slip into the other slots on the slide rails. See the preceding figure.
5. Make sure that the front latch (5) slides over the nail heads. See the preceding figure.
6. Lift the locking levers (6) on the slide rails. See the following figure.



7. Push the server (7) all the way into the rack until it clicks into place. See the preceding figure.
8. Insert the optional M6 screws (8) in the front of the server when you move the rack cabinet or if you install the rack cabinet in a vibration-prone area. See the following figure.



Next steps

Install the cable management arm if desired.

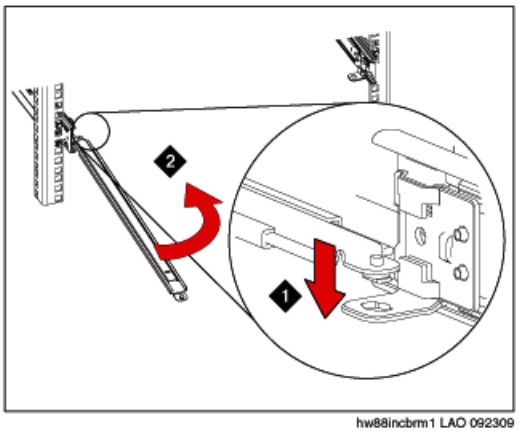
Installing the cable management arm

Prerequisites

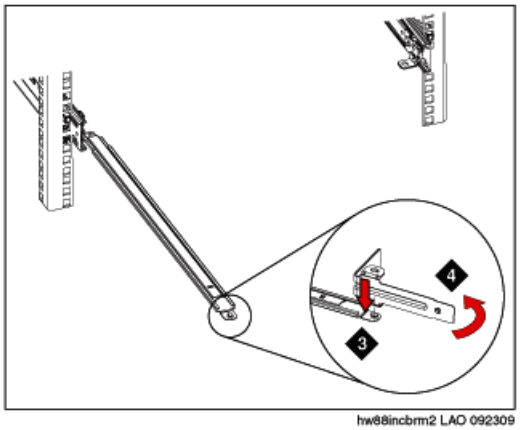
Attach rails to the rack and install the server in the rack.

The cable-management arm can be installed on either side of the server. This procedure shows it being installed on the left side. To install the cable-management arm on the right side, follow the instructions and install the hardware on the opposite side.

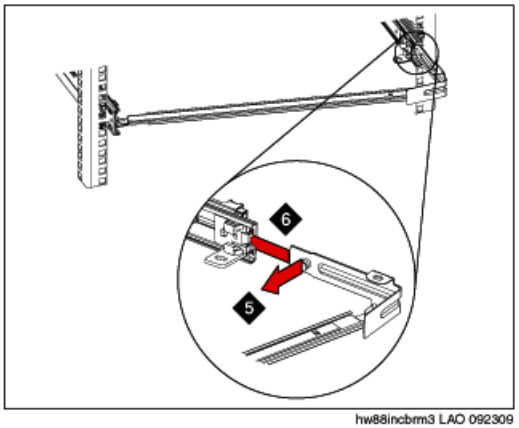
1. Connect one end of the support arm (1) to the same slide rail to which you plan to attach the cable-management arm so that you can swing the other end of the support arm (2) toward the rack. See the following figure.



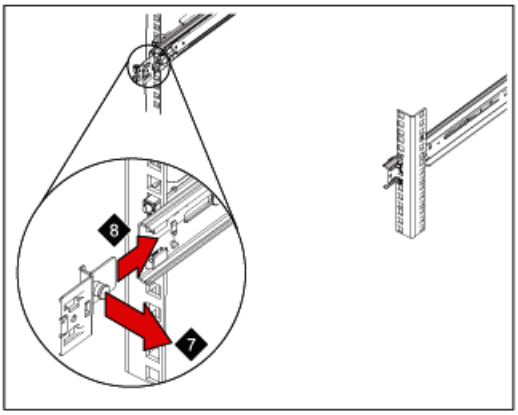
2. Install the L-shaped cable-management stop bracket (3) on the unattached end of the support arm. See the following figure



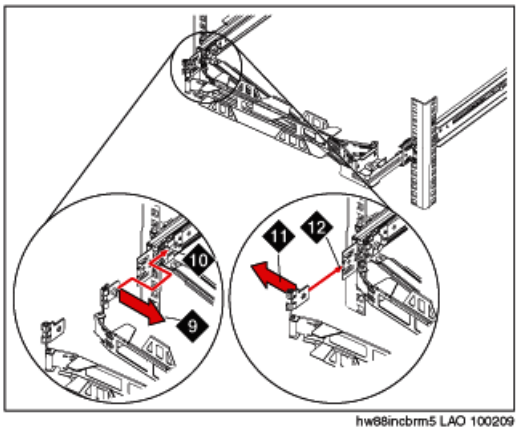
3. Turn the bracket (4) to secure it to the support arm. See the preceding figure.
4. To attach the other side of the support arm to the backside of the slide rail, pull the pin out (5), and then slide the bracket (6) into the slide rail. See the following figure.



5. Pull out the mounting bracket pin (7) and slide the mounting bracket (8) into the slide rail onto which you are installing the cable-management arm. See the following figure.



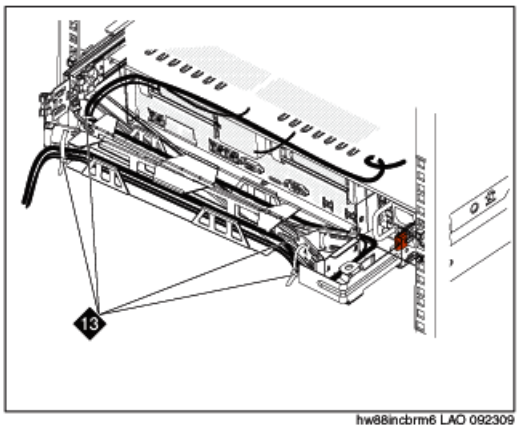
6. Push the bracket into the slide rail until the spring-loaded pin snaps into place.
7. Place the cable-management arm on the support arm.
8. Pull out the cable-management arm pin (9), and then slide the cable-management arm tab (10) into the slot on the inside of the slide rail. See the following figure.



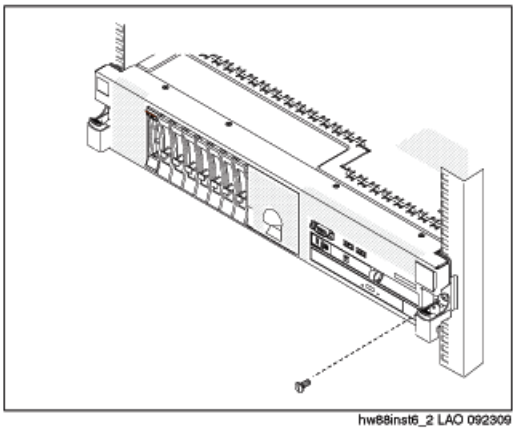
9. Push the tab until it snaps into place.
10. Pull out the other cable-management arm pin (11), and then slide that cable management arm tab into the slot (12) on the outside of the slide rail. See the preceding figure.
11. Push the tab until it snaps into place.
12. Attach the power cords and other cables to the rear of the server (including keyboard, monitor, and mouse cables, if required).
13. Route the cables and power cords on the cable-management arm (13) and secure them with cable ties or hook-and-loop fasteners. See the following figure.

Note:

Allow slack in all cables to avoid tension in the cables as the cable-management arm moves.



14. Slide the server into the rack until it snaps into place.
15. Insert the optional M6 screws in the front of the server when you move the rack cabinet or if you install the rack cabinet in a vibration-prone area. See the following figure.



Turning on the server

1. Plug one end of the power cord into the back of the power supply and the other end into a UPS or non-switched outlet. Approximately 5 seconds after the server is

connected to power, one or more fans may start running and the power-on LED will blink quickly (three flashes per second).

2. Wait until the power-on LED blinks slowly (one flash per second). This will happen approximately 3 minutes after the server has been connected to power.
3. Within 30 seconds of when the LED starts to blink slowly, press the power button on the front of the server. The power-on LED will stop blinking and stay lit.

   Important:

   You *must wait* for the power-on LED to blink slowly before pressing the power button. If you press the power button while the power-on LED is blinking quickly, the server will not turn on.
4. Wait until the server has initialized. This takes approximately 5 minutes to complete.
5. If there are no installation problems, continue with Configuring Session Manager on page 15

Troubleshooting the installation

1. If the server has no power:.
   a. Make sure the power cord is plugged into the back of the server and into a non-switched outlet or UPS
   b. If the server has a single power supply, it must be installed in power supply bay 1.
   c. Make sure the UPS is plugged into a non-switched outlet.
   d. Make sure the outlet has power.
   e. Check the power supply LEDs on the back of the server. During normal operation, the AC LED and the DC LED are both lit.
2. If the SM100 is not working: Some Ethernet Rj45 cables have trouble locking into place when connected to an SM100. If this problem is encountered, attempt to find a different working cable or provide additional security of the cable to the server to reduce the possibility of an accidental disconnection.
3. All other problems: contact your project manager.

Appendix B: Worksheets

Collecting key information prior to administering Session Manager can expedite the process. You can use the following worksheets to collect some of the information ahead of time that you need to administer Session Manager-related entities using System Manager.

The worksheet information does not represent all of the information needed, but it does represent the information that may take some lead time to collect.

Session Manager Entity information worksheet

You need the following information for each Session Manager or Communication Manager SIP entity to be administered using System Manager. This information is used to administer NRP SIP Entities and NRP Entity Links. See SIP Entities and references on page 44 for a list of several SIP Entities with application note references.

Field	Information to enter
Entity Name	
Entity Type (Session Manager, Communication Manager, etc.)	
Location Name	
IP Address	
FQDN	
Port (5061)	
Transport (TCP or TLS)	
SM100 IP Address (Session Manager)	
SM100 Network Mask (Session Manager)	
SM100 Default Gateway (Session Manager)	
CLAN/PROCR Node Name (Communication Manager)	
CLAN/PROCR IP address (Communication Manager)	
Signaling Group (Communication Manager)	
Trunk Group (Communication Manager)	

SIP Entities and references

SIP Entities must be configured to work with Session Manager. The following table provides a list of several SIP Entities with reference to application notes which provide configuration procedures. These application notes are available on the Avaya website within the Avaya Resource Library.

SIP Entity	Release	Application Notes
Communication Manager	5.1 5.2	Configuring Avaya Aura™ Communication Manager to Work with Avaya Aura™ Session Manager
Communication Manager as a Feature Server	5.2.1 Communication Manager software	Configuring Avaya Aura™ Communication Manager to Work with Avaya Aura™ Session Manager
Cicso CallManager	7.x	Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco Unified Communications Manager
Nortel CS1000	4.5	
AT&T (IP FlexReach)	NA	SIP Trunking to AT&T with Session Manager 5.2 through Acme Packet Session Director
Verizon	NA	
Avaya G860 Trunk Gateway	2.0	Voice Portal First Solution: Configuring Avaya Aura™ Session Manager with Avaya G860 High Density Trunk Gateway, Avaya Aura™ Communication Manager, and Avaya Voice Portal
Modular Messaging	5.1	
Voice Portal	4.1 5.0	Voice Portal First Solution: Configuring Avaya Aura™ Session Manager with Avaya G860 High Density Trunk Gateway, Avaya Aura™ Communication Manager, and Avaya Voice Portal
Meeting Exchange	5.1	
Extended Meet-Me Conference	1.0.7	Avaya Aura™ Session Manager and Expanded Meet Me Conference (EMMC)

Index

R

S

T

V

W