Installing and Configuring Avaya Aura™ Session Manager

03-603473
Release 6.0
Issue 2
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.

For full hardware support, please see the document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759 on the Avaya support web site, http://www.avaya.com/support.

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Concurrent User License

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.

Copyright

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

Third-party components

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

Preventing toll fraud

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

Avaya fraud intervention

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

Trademarks

Avaya Aura™ is a registered trademark of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: Installation overview

This guide contains the installation and initial administration information for Avaya Aura™ Session Manager Release 6.0. It also contains the information needed to install, configure, and administer a survivable remote server.

Avaya Aura™ System Manager Release 6.0 manages up to six Session Manager instances. You can set up and administer the Session Managers concurrently.

The Session Manager application is installed on the Avaya S8800 server. The server is shipped with all of the required components and software applications installed. The server connects to the customer's network and the System Manager server using CAT5 Ethernet cables provided by the customer. Remote access is through the network only; modem access is not supported.

Starting with Release 6.0, the PCI hardware version of the SM100 security module was converted to a software module running on the Session Manager server. The SM100 PCI hardware version is no longer used. The software version of the Security Module uses the Eth2 network interface for SIP traffic.

Note:

Customers must have the Linux Operating System Kickstart DVD and the Session Manager Software CD on-site for advanced installation issues and/or catastrophic failure. The software is available for download from PLDS.

System Manager must be installed and on the customer's network prior to starting Session Manager installation.

Remote access

The Secure Access Link (SAL) uses the customer's existing Internet connectivity for remote support and alarming. All communication is outbound from the customer's environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS). The SAL requires upload bandwidth (customer to Avaya/Partner) of at least 90 KB/s (720 KB/s) with latency no greater than 150 ms (round trip).

Business Partners without a SAL Concentrator must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

Direct SSH access to Session Managers is available from all servers.

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 SMnetSetup, the customer access login defaults to *cust*. It is the customer's responsibility to ensure the security of this login account. The customer login has permission 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 installation of the Security Module software. 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.

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. This document also contains the information for adding memory to the S8510 and S8800 servers for upgrading to Release 6.0 and later.

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

Note:

System Manager must be upgraded prior to starting the installation process on the Session Manager(s).

Related documents

Session Manager comes with a complete set of documents. The following list provides the title, document number, and a brief description of all of the documents in the documentation set.

- *Avaya Aura™ Session Manager Overview* (03–603323) — Provides descriptions of Session Manager and its components.
- *Installing and Configuring Avaya Aura™ Session Manager* (03–603473) — Describes how to install Session Manager and the initial administration required.
- *Administering Avaya Aura™ Session Manager* (03–603324) — Describes how to administer Session Manager through System Manager.
- *Administering Avaya Aura™ Communication Manager Server Options* (03–603479) — Describes how to administer Communication Manager as a feature server, evolution server, or trunk gateway and the associated Session Manager administration.
- *Maintaining and Troubleshooting Avaya Aura™ Session Manager* (03–603325) — Provides information on maintaining and troubleshooting Session Manager, including logging and alarming.
- *Security Design for Avaya Aura™ Session Manager* — Provides information on making Session Manager secure on the network.

Chapter 2: Session Manager Preinstallation

Before installing Session Manager

The following prerequisites must be met before Session Manager can be installed:

- The System Manager template must be installed and operating. To install the System Manager template, see *Installing and Upgrading Avaya Aura™ System Manager* on the Avaya support web site, http://www.avaya.com/support
- License activation code — You should have a license activation code (LAC) before you install Session Manager. The LAC email recipients are identified during the order placement process.
- Network ports — The document *Avaya Aura™ Session Manager: Port Matrix* identifies which network ports must be open in firewalls. This document is available to Avaya customers, associates, and business partners using the InSite Knowledge Management Database at http://www.avaya.com/support
- Access to the PLDS web site — If you do not have access to the Product License Delivery System (PLDS) web site, see Registering for PLDS on page 11
- Make sure you have a reachable DNS server. Otherwise, you will not be able to complete the installation. Currently, System Manager and Session Manager only support DNS suffixes of up to 6 characters.

Registering for PLDS

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site (https://plds.avaya.com).
   You will be redirected to the Single sign-on (SSO) Web site.
2. Log in to SSO using SSO ID and Password.
   You will be redirected to the PLDS registration page.
3. If you are registering:

- as an Avaya Partner, enter the Partner Link ID. If you do not know your Link ID, send an e-mail to prmadmin@avaya.com.
- as a customer, enter one of the following:
  - Company Sold-To
  - Ship-To number
  - License Authorization Code (LAC)

4. Click **Submit**.
   Avaya will send you the PLDS access confirmation within one business day.

Chapter 3: Installing Session Manager

The high-level installation steps are:

- Obtain and enter the networking and related information on the worksheets - see Worksheets on page 45
- Install the Session Manager server
- Administer the Session Manager
- Test the installation

The Session Manager application is installed on the Avaya S8800 server. The server is shipped with all of the required components and software applications.

Session Manager installation checklist

You need a copy of this checklist for each Session Manager that will be installed.

The customer must have the Linux Operating System Kickstart DVD and the Session Manager Software CD on-site for advanced installation issues and/or catastrophic failures. The software is available for download from PLDS.

#	Installation Action	Link to installation description	✔
1	Complete the Session Manager configuration information worksheet and verify that the information is correct.	Session Manager configuration information worksheet on page 45	
2	Complete the Session Manager Entity information worksheet and verify that the information is correct.	Session Manager Entity information worksheet on page 46	
3	Configure the laptop for direct connection to the server.	Configuring the laptop for direct connection to the server on page 14	
4	Disable proxy servers.	• If using Internet Explorer, see Disabling proxy servers in Microsoft Internet Explorer on page 15 • If using Firefox, see Disabling proxy servers in Mozilla Firefox on page 16	

#	Installation Action	Link to installation description	✔
5	Connect the laptop to the server.	Connecting a laptop to the server on page 16	
6	Ping System Manager from the customer's LAN to ensure it is up and on the network prior to starting the Session Manager software installation.		
7	Install the Session Manager server.	• If you are installing an Avaya S8800 server, see *Installing the Avaya S8800 Server for Avaya Aura ™ Communication Manager (03–602918)* • If you are installing an Avaya S8510 server, see *Installing the Avaya S8510 Server Family and Its Components (03–602918)*	
8	Install the Session Manager license file on System Manager.	Activating entitlements on page 17	
9	Log into the System Manager associated with the Session Manager.		
10	Establish the Session Manager enrollment password on System Manager.	Enrolling a password on page 18	
11	Configure Session Manager using the **`SMnetSetup`** command.	Configuring Session Manager with SMnetSetup on page 19	
12	Administer the Session Manager.	Session Manager administration checklist on page 23	
13	Use the setproductID command to complete alarming configuration.	setProductID on page 20	

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 connecting the laptop to the server.

Note:

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

1. On your laptop, right-click **My Network Places**, then click on **Properties**.
2. In the **Local Area Connection Status** dialog box, under the **General** tab, click **Properties**.
3. In the **Local Area Connection Properties** dialog box, under the **General** tab, click **Properties**.
4. Click on **Internet Protocol (TCP/IP)** from the list of items.
5. Click **Properties**.
6. In the Internet Protocol (TCP/IP) Properties dialog box, under the **General** tab, select **Use the following IP address**.

   Warning:

   Do not click the **Alternate Configuration** tab.
7. In the **IP address** field, enter `192.11.13.5`.
8. In the **Subnet mask** field, enter `255.255.255.252`.
9. In the **Default gateway** field, enter `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.

Connecting a laptop to the server

Prerequisites

- Make sure that you have an SSH application such as PuTTY installed on your laptop.
- Configure the IP settings of the laptop for direct connection to the server.
- Disable use of proxy servers.

1. Connect the laptop to the services port (Eth1) with a standard or crossover Ethernet cable.

   If you do not have a crossover cable, you can use an IP hub.
2. Start an SSH client application (i.e., PuTTY) session.
3. In the **Host Name (or IP Address)** field, enter `192.11.13.6`.

   The system assigned the IP address 192.11.13.6 to the services port.
4. Verify that the protocol is **SSH**.
5. Verify that the **Port** is `22`
6. Click on **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. Login using **craft** (Session Manager) or **admin** (System Platform/System Manager).
9. When you are finished with the session, enter `exit` to close PuTTY.

Activating entitlements

When entitlements are successfully activated, PLDS sends an Activation Record to the customer registered with the entitlements by an e-mail. 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

You must have License Activation Codes (LACs) and the Host ID of the WebLM server (i.e., System Manager Server) on which you want to install the licenses.

1. Enter http://plds.avaya.com in the 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. Enter the License activation code (LAC) that you have received through an e-mail in the **LAC(s)** field in the Quick Activation section.
4. Enter the host information.

5. Click **Next** to validate the registration detail.
6. Enter the System Manager or other WebLM 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. Send a confirmation e-mail:
   a. Enter any additional certificate recipient e-mail addresses in the **E-mail to:** field.
   b. Enter Comments (optional).
   c. Click **Finish**.
10. Click **View Activation Record** and verify the information.

Enrolling a password

Enrolling a password allows the establishment of “trust” between the System Manager and Session Manager servers. The Trust Management Enrollment Password is required for installing and configuring the Session Manager software.

1. On the System Manager console, select **Security** > **Certificates** > **Enrollment Password**.
2. If a password already exists and the **Time Remaining** is not 0, click **Done** and skip the remaining steps. The enrollment password is already valid. Make note of the password displayed on the screen for future reference.
3. In the **Password expires in** box, select a value from the drop-down menu for the time when the password should expire.
4. If a password already exists, copy it to the **Password** box.
5. If a password does not exist, do one of the following:
   - Click **Generate** if you wish to use a randomly generated string as a password , or
   - Enter a password in the **Password** field and click **Done**.

Note:

The system 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.

Configuring Session Manager with SMnetSetup

Session Manager has the following configuration as shipped from the factory:

- System Name — avaya-asm
- Eth0 — 192.168.0.2/24
- Eth1 — 192.11.13.6/30
- DNS Domain — localdomain
- DNS Server — 127.0.0.1

1. Cable the Ethernet Ports to the customer's Local Area Network:
   a. GB1 = Eth0 (Management interface)
   b. GB3 = Eth2 (Security Module)
2. Install the cables to access the Session Manager server using a laptop or USB keyboard, mouse, and monitor.
3. Log into the Linux console of the Session Manager server using **craft** or **sroot**.
4. Enter the command **`./SMnetSetup`**
5. Refer to the Session Manager configuration information worksheet on page 45 for the information required by SMnetSetup:
   a. Enter the Session Manager server hostname.
   b. Enter the Session Manager IP address (Mgmt).
   c. Enter the Netmask.
   d. Enter the Gateway IP address.
   e. Enter the Network Domain.
   f. Enter the Primary DNS server.
   g. Enter the Secondary DNS (if applicable).
   h. Enter the Tertiary DNS (if applicable).
   i. When prompted, press Enter.
   j. Configure the local time zone.
   k. Enter **y** to continue.

l. When prompted for **Disable NTP?**, enter **no**.
m. Enter the NTP server.
n. Enter the Secondary NTP server (if applicable).
o. Enter the Tertiary NTP server (if applicable).
p. When prompted, create a customer account with a password.
q. Enter the System Manager IP Address.
r. Enter the System Manager FQDN.
s. Verify your settings.
t. Enter the enrollment password.

6. At this point, the system configures itself. The configuration takes approximately 25 minutes to complete.
7. When prompted to reboot, enter `y` and press Enter. The reboot takes about 10 minutes to complete.
8. Wait until the login screen appears, then continue with the next step in the Session Manager installation checklist.

Product ID commands

At installation time, the new system needs to be registered using the Functional Location (FL) and product type. During installation, 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 must be run as either sroot, root, or craft.

The **`setProductID`** and **`getProductID`** commands run on Session Manager and the System Manager virtual machine which is running on System Platform. The commands will not run on the System Platform virtual machines (DOM–0/CDOM).

setProductID

Use **`setProductID`** to set the Product ID for reporting alarms for managed elements. The parameter to this command starts with the number **8**. The Product ID is the 10–digit unique customer Product ID.

Syntax

```
setProductID ASM | SM | SMELEM 8xxxxxxxxxx
```

ASM *8xxxxxxxxxx* Sets the Session Manager Product ID as specified by *8xxxxxxxxxx* (Session Manager only)

SM *8xxxxxxxxxx* Sets the System Manager Product ID as specified by *8xxxxxxxxxx* (System Manager only)

SMELEM *8xxxxxxxxxx* Sets the Session Manager Element Manager Product ID to the value specified by *8xxxxxxxxxx* (System Manager only)

Example

setProductID ASM 89876543216

getProductID

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

Syntax

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

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

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

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

spiritAgentCLI

Use **`spiritAgentCLI`** to set and view the Product ID in order to report alarms for a managed element. The parameter to this command starts with the number **5**. The Product ID is displayed when the command is entered with no parameters.

Syntax

```
spiritAgentCLI [ alarmId 5xxxxxxxxxx ]
```

alarmId *5xxxxxxxxxx* Sets the SAL Agent Product ID to the value specified by *5xxxxxxxxxx*.

Example

spiritAgentCLI

spritAgentCLI alarmId 59876543215

Chapter 4: Session Manager Administration

Introduction

After Session Manager installation, perform the following basic administrative steps at customer site:

1. Add SIP Domains
2. Add Session Manager as SIP entities
3. Administer Session Manager instance(s)

For details on the following, refer to *Administrating Avaya Aura™ Session Manager*, 03–603324:

1. Routing settings
2. Security default settings
3. User account setup

For configuring various SIP entities to work with Session Manager, refer to the topic SIP Entities and references on page 47 for details.

Session Manager administration checklist

Use the following checklist for the initial administration of a newly-installed Session Manager.

#	Administration action	Link to administration action	✔
1	Log into the System Manager associated with this Session Manager.		
2	Add Domain Names.	Adding Domain Names for Session Manager on page 24	
3	Add the installed Session Manager as a SIP Entity.	Adding Session Manager as a SIP Entity on page 24	

#	Administration action	Link to administration action	✔
4	Administer the Session Manager.	Administering Session Manager on page 25	
5	Check the installation.	Checking the Session Manager installation on page 26	
6	Test the installation.	Testing the Session Manager installation on page 26	
7	Verify System Manager Data Replication to the Session Manager.	Verifying Data Replication to Session Manager on page 26	

Adding Domain Names for Session Manager

1. On the System Manager console, select **Routing** > **Domains**
2. Click on **New**
3. In the **Name** field, enter the Network Domain Name of the Session Manager.
4. The **Type** should be **SIP**.
5. Enter a description in the **Notes** field (optional).
6. Click on **Commit**
7. Select **New** again.
8. In the **Name** field, enter `na`
9. In the **Notes** field, enter `na`
10. Click on **Commit**

Adding Session Manager as a SIP Entity

1. On the System Manager console, select **Routing** > **SIP Entities**
2. Select **New**

3. In the **Name** field, enter the name of the Session Manager.
4. In the **FQDN or IP Address** field, enter the IP address of the Session Manager Security Module. Note: This is *not* the management IP address.
5. Under the **Port** section of the screen, select a **Default Domain** from the drop-down menu.
6. Click on **Commit**

Administering Session Manager

Entity Links can be monitored (or not) based on the setting on the entity form of the far-end entity. On a survivable remote server, regardless of administration, the link to the Communication Manager feature server on the LSP will always be monitored (1 second interval). In the case of two entities (Communication Manager configured as a combination feature server/trunk gateway), the trunk gateway link will use whatever monitoring status is administered on the core Communication Manager that is being subtended.

1. On the System Manager console, select **Elements** > **Session Manager** > **Session Manager Administration**
2. Select **New**
3. In the **SIP Entity Name** field, enter the name of the Session Manager.
4. in the **Description** field, enter a description for the Session Manager (optional).
5. In the **Network Mask** field, enter the network mask of the Session Manager Security Module.
6. In the **Default Gateway** field, enter the default gateway of the Session Manager Security Module.
7. The **Enable Monitoring?** field should be `Yes` by default.
8. Click on **Commit**

Checking the Session Manager installation

1. Log in to the System Manager using the **admin** login.
2. Select **Elements** > **Session Manager**
3. The service state for the new Session Manager should be **Accept New Service**. If you see a RED error box for the installed Session Manager, refer to Unable to access Management State on page 41 for troubleshooting information.

Testing the Session Manager installation

1. On the System Manager console, select **Elements** > **Session Manager** > **System Tools** > **Maintenance Tests**
2. Select the appropriate Session Manager instance from the drop-down list in the **Select Target** box.
3. Click on **Execute all Tests**
4. Verify that the result of each test is **Success**.

   If any of the tests fail, refer to *Maintaining and Troubleshooting Avaya Aura™ Session Manager, 03–603325*.

Verifying Data Replication to Session Manager

1. On the System Manager console, select **System Manager Data** > **Replication**
2. Verify that the status for the Session Manager is **Synchronized**

Chapter 5: Session Manager Redundancy

System Manager supports up to six Session Manager instances in an enterprise.

Session Manager uses the active-active approach where two instances are simultaneously active; any request routes to either instance, and a failure of one of the Session Manager instances does not interrupt service. Active-active redundancy requires that the Session Manager instances be interconnected over an IP network with sufficient bandwidth and low enough latency to synchronize runtime data.

Configuring Session Manager redundancy

In the following configuration example, **SM-1** is one Session Manager instance, and **SM-2** is the active backup.

Route-through failover relies on Communication Manager look-ahead routing to choose a secondary route. The route pattern form will need to add the secondary/failover trunk group administration.

If you are using load balancing, you should not need additional administration if you reuse the same Port IDs and IP addresses (CLANs or procr) for the added SM-2 trunk group(s).

1. Add SM-2 as the backup Session Manager server.
2. On SM-2, create the entity links that exist on SM-1 (VP-1, etc.)
3. For route-through failover, add an entity link SM-1 to SM-2.
4. Add the trunk setup on your device (CM, VP, etc.) For example, if you have a CM signaling group to SM-1, you need to add a CM signaling group to SM-2.
5. All other administration is accessible to SM-2 automatically. Additional dial plan administration is not necessary.

Chapter 6: Branch Session Manager

This section describes how to install, configure, and administer a survivable remote Communication Manager server with Branch Session Manager.

Assumptions

It is assumed that:

- System Manager and Session Manager are installed, administered, and operational in a system.
- The main Communication Manager server is installed, administered, and running Release 6.0.
- The main Communication Manager has been administered as a SIP entity on Session Manager.

About Branch Session Manager

The Branch Session Manager provides a SIP-enabled branch survivability solution. It allows a customer who has SIP phones in a branch to receive LSP-style survivability. When the core Session Manager is unreachable, the SIP phones receive their Communication Manager features from the LSP. The Branch Session Manager provides service when the branch losses WAN connectivity. An active Branch Session Manager domain is very similar to a core Session Manager.

Note:

The Branch Session Manager is designed to support a total WAN outage in the branch when all of the devices in the branch network have lost connectivity to all of the devices in the core network.

When a Branch Session Manager is installed as inactive, the Survivable Branch functions as a traditional LSP. There is no SIP routing. The Branch Session Manager can be activated if the customer decides to add SIP at a later time.

The Branch Session Manager is installed and configured through System Platform.

Branch Session Manager Installation

The high-level installation/administration steps are:

- Administer the Branch Session Manager on the main Communication Manager server.
- Install the survivable S8300D or S8800 server.
- Administer the S8300D or S8800 server using System Manager.
- Install and configure the Communication Manager survivability template on the survivable server.
- Administer Branch Session Manager using System Manager.

Important:

The Branch Session Manager will not initialize properly if there are no SIP users administered for the branch. Furthermore, it is *VERY* important to not mix users on different Communication Manager servers.

For example, if a Branch Session Manager subtends CM1, an administrator *MUST NOT* administer a user for this Branch Session Manager that application sequences to CM2. The administrator must

ensure that CM1 is always the Communication Manager that is sequenced to for any user using that Branch Session Manager as its survivability server.

Branch Session Manager Installation checklist

Branch Session Manager installation and administration requires using more than one document. The following table contains the procedure for installing, configuring, administering, and testing Branch Session Manager and which document to use for that step.

The following are assumed to have already been completed on the core Communication Manager and Session Manager servers and are not part of the checklist:

- The main Communication Manager is installed, licensed, configured either as a feature server or evolution server, and is operational.
- The main Communication Manager is administered as a SIP entity on Session Manager.

#	Task	Book/Link to use	Notes	✔
1	Administer survivability options on the main Communication Manager server.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558		
2	Administer the Survivable Communication Manager using System Manager.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558		
3	Administer the Branch Session Manager server on the main Communication Manager server.	Branch Session Manager SAT administration checklist on page 32		
4	If an Avaya S8800 server will be used as the Branch Session Manager, install the S8800 server.	*Installing the Avaya S8800 Server for Avaya Aura™ Communication Manager*, 03-603444		
5	If an Avaya S8510 server will be used as the Branch Session Manager, install or upgrade the S8510 server.	*Upgrading to Avaya Aura™ Communication Manager,* 03–603560	The S8510 server must be upgraded first if it does not have 8GB of memory. The S8510 server requires a Communication	

#	Task	Book/Link to use	Notes	✔
			Manager Migration kit.	
6	If an Avaya S8300D server will be used as the Branch Session Manager, install the server in the gateway.	• *Quick Start for Hardware Installation: Avaya G250 Media Gateway*, 03-300433 • *Quick Start for Hardware Installation: Avaya G350 Media Gateway*, 03-300148 • *Quick Start for Hardware Installation: Avaya G430 Media Gateway*, 03-603236 • *Quick Start for Hardware Installation: Avaya G450 Media Gateway*, 03-602053 • *Quick Start for Hardware Installation: Avaya G700 Media Gateway*, 555-233-150	Refer to the book for your particular Gxxx media gateway.	
7	Install System Platform on the server.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558		
8	Install license and authentication files	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558		
9	Install the appropriate Communication Manager template using the System Platform Web Console.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558		
10	Administer the Branch Session Manager Security Module IP address for System Platform > Server Management > Network Configuration.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	Administer the **SIP Entity IP Address** under the bsm section See “Confirming template network configuration”.	

#	Task	Book/Link to use	Notes	✔
11	Administer Branch Session Manager using System Manager.	Branch Session Manager administration checklist on page 35		
12	Verify registration.	Verifying survivable server registration		
13	Make test calls.	Testing calls on page 39		

Branch Session Manager SAT administration checklist

The following SAT commands are executed on the main Communication Manager.

Prerequisites:

- The Processor Ethernet IP for the main Communication Manager has been configured via the **add ip-interface procr** SAT command or via the Communication Manager web interface.
- If applicable, the media gateway has been added using the **add media-gateway x** SAT command.
- If applicable, media gateways have had their mgc lists updated with the IP addresses of both the main Communication Manager server Processor Ethernet IP address (1st) and the Survivable Remote Processor Ethernet IP address (2nd).
- System Manager and Session Manager are already active in an existing SIP routing deployment.

#	Administration	Link	✔
1	Log in to the Communication Manager server.		
2	Add the appropriate IP address to node-name mappings.	Adding a node name for Branch Session Manager on page 33	
3	Administer the survivable processor configuration information	Administering a Survivable Remote Server on page 33	
4	If a media gateway is part of the enterprise, verify the Minimum time of network stability.	Validating Minimum time of network stability on page 34	
5	If a media gateway is part of the enterprise, validate the Recovery Rule.	Validating media gateway recovery rule on page 34	

Adding a node name for Branch Session Manager

Define a node name for the IP address of the Branch Session Manager Security Module.

procr is the main Communication Manager server Processor Ethernet IP address.

For the Branch Session Manager administration:

- Make sure the LSP address is added as the second entry in the mgc list of the media gateway.
- Make sure at least one SIP signaling group to a Session Manager uses **procr** as its near-end node name. In addition to the SIP signaling group to core Session Manager using CLANS at the near-end, you need at least one signaling group with Communication Manager Processor Ethernet at the near-end. This is so the main server's Processor Ethernet can be changed to the LSP's Processor Ethernet in the case of a network failure.

1. On the SAT, enter **change node-names ip**
2. In the **Name** field, enter the name associated with the IP address of the Branch Session Manager Security Module (i.e., BSM1HostName).
3. In the **IP Address** field, enter the IP address of the Branch Session Manager Security Module.
4. Add any other IP address to node-name mappings such as the Survivable Remote Processor Ethernet IP address and Media Gateway IP address.
5. Submit the screen.

Administering a Survivable Remote Server

1. On the SAT, enter **add survivable-processor *node-name*** where *node-name* is the name of the remote server (for example, lsp6) that was added on the **change node-name ip** form.
2. The **Type** field should be **lsp**.
3. The **Cluster ID/MID** matches the MID number used in the web interface of the Survivable Remote server under **Server Maintenance** > **Server Configuration** > **Server Role**
4. Submit the form.

Validating Minimum time of network stability

Validate that the Minimum time of network stability is set to 3 minutes. This will allow the media gateway to failback to the main Communication Manager feature/evolution server when it becomes available.

1. On the SAT, enter **change system-parameters mg-recovery-rule 1**
2. In the **Minimum time of network stability** field, verify that the value is **3**.
3. If the value of the **Minimum time of network stability** field is not **3**, change the value to **3**.
4. Submit the form.

Validating media gateway recovery rule

Validate that the correct Recovery Rule number is specified for each mediate gateway under the Recovery Rule field.

1. On the SAT, enter **change media-gateway *x*** where *x* is the number of the media gateway. In this example, use **1**
2. In the **Type** field, enter the type of media gateway that is being used (i.e., g350).
3. In the **Name** field, enter the name associated with the media gateway (i.e., cm6mg).
4. In the **Serial No** field, enter the serial number of the media gateway.
5. In the **Network Region** field, enter the Network Region associated with this media gateway.
6. In the **Location** field, enter the Location number associated with this media gateway.
7. In the **Recovery Rule** field, enter the number of the recovery rule associated with this media gateway. For this example, enter **1**.
8. Submit the form.

Branch Session Manager administration checklist

The following table contains the steps to administer a Branch Session Manager using System Manager.

#	Administration	Link	✔
1	Log in to the System Manager web console.		
2	Add the Branch Manager server as a SIP Entity.	Adding a Branch Session Manager as a SIP Entity on page 35	
3	Create Entity Links between the Branch Session Manager and Communication Manager.	Creating Entity Links on page 36	
4	Verify the connections between Communication Manager and Branch Session Manager.	Checking the connections on page 36	
5	Administer Branch Session Manager.	Administering Branch Session Manager on page 37	
6	Verify the information in the /etc/hosts file.	Verifying Branch Session Manager information on page 38	
7	Test the survivable remote Communication Manager with Branch Session Manager.	Testing calls on page 39	

Adding a Branch Session Manager as a SIP Entity

1. Using the System Manager web interface, select **Routing** > **SIP Entities**
2. Select **New**
3. In the **FQDN or IP Address** field, enter the IP address of the security module of the Branch Session Manager.
4. In the **Type** field, select **Session Manager** from the drop-down menu.
5. Click **Commit**

Creating Entity Links

Create entity links between the Branch Session Manager and the main Communication Manager.

If separate entities and entity links have been configured in the core for the feature server (feature server/IMS) link and the trunk gateway (trunk gateway/non-IMS) link, then an entity link should be configured from the Branch Session Manager to each of those entities for a total of 2 entity links on the Branch Session Manager. If only one entity/entity link is being used (as in an evolution server configuration), then only one link will be administered on the Branch Session Manager.

The protocol(s) and transport(s) used should be exactly the same as those used between the primary Session Manager and the core Communication Manager entity (or entities).

1. On the System Manager console, select **Routing** > **Entity Links**
2. Click on **New**
3. In the **Name** field, enter a descriptive Entity Link name (for example, BSM1 to CM-FS1).
4. In the **SIP Entity 1** field, select the name of the Branch Session Manager from the drop-down menu that the Communication Manager Server should be linked to.
5. The **Protocol** should be `tls`.
6. The **Port** should be `5061`.
7. In the **SIP Entity 2** field, select the name of the Communication Manager server from the drop-down menu that the Branch Session Manager should be linked to.
8. The **Port** should be `5061`.
9. The **Trusted** box *must* be checked.
10. The **Notes** field is optional.
11. Click on **Commit**.

Checking the connections

1. On Communication Manager:
   a. Enter the command **list history**
   b. Verify that Session Manager has logged in.

c. Verify that initial data synchronization has begun.

2. Check the Communication Manager SIP Entity Link status:
   a. On System Manager, select **Elements** > **Session Manager** > **System Status** > **SIP Entity Monitoring**
   b. Select the Communication Manager server name from the list of **All Monitored SIP Entities**
   c. Verify that the **Link Status** is `Up` for the Communication Manager server.
3. Check the Session Manager Dashboard:
   a. On System Manager, select **Elements** > **Session Manager** > **Dashboard**
   b. Verify that the Session Manager is active.

Administering Branch Session Manager

Prerequisites

Before starting this procedure, make sure that the SIP entity that you want to add was created. For a Session Manager SIP entity, the listen ports must be administered on the SIP entity form. These listen ports are used by endpoints to connect to Branch Session Manager and can be used to map different ports to different domains.

1. Using the System Manager web interface, select **Elements** > **Session Manager** > **Session Manager Administration**.
2. Click **New** under the Branch Session Manager Instances section.
3. Under the **General** section:
   a. Select the Branch Session Manager SIP Entity from the **SIP Entity Name** drop-down list.
   b. In the **Description** field, add a comment if desired.
   c. In the **Management Access Point Host Name/IP** field, add the IP address of the host on which the management agent is running. This is *not* the Security Module IP address.
   d. Select the Communication Manager Server from the **Main CM for LSP** drop-down menu.
   e. Select **Enable** for **Direct Routing to Endpoints** from the drop-down list if it is not enabled already.
   f. If applicable, select the **Adaptation for Trunk Gateway** from the drop-down menu.

      By default, the adaptation used for the trunk gateway entity that is being subtended by this Branch Session Manager will be used. If a different

adaptation is desired, it can be specified here and will override the default. If two entities are administered, one for a feature server and one for a trunk gateway, then the adaptation will only be applied to the trunk gateway entity. If a single entity is used, it will be applied to both application sequenced and trunk gateway routed calls.

4. Under the **Security Module** section:
   a. The **SIP Entity IP Address** field is automatically populated as per the IP address of the SIP entity.
   b. In the **Network Mask** field, enter the value for the network mask.
   c. In the **Default Gateway** field, enter the applicable IP address.
5. Click **Commit**

Verifying Branch Session Manager information

Verify the Branch Session Manager administration.

1. Log in as **root** to the System Manager CLI using SSH PuTTY.
2. Verify the Branch Session Manager information in the **/etc/hosts** file:
   a. Open the /etc/hosts file with your favorite editor.
   b. Verify the Branch Session Manager Management IP Address is entered and correct. Add the information if it is missing.
   c. Verify the FQDN is entered and correct. Add the information if it is missing.
   d. Verify the hostname is entered and correct. Add the information if it is missing.
   e. Verify that there is an entry for **avaya-lsp** with the correct IP address.
   f. Save and exit the file.
3. Verify the IP address of the Branch Session Manager Security Module:
   a. Open the /ecs.conf file with your favorite editor.
   b. Verify that an entry exists for **SIPEntityIpAddress** with the correct address.
   c. Save and exit the file.
4. If the Branch Session Manager is monitored:
   a. Navigate to the Dashboard screen.
   b. Click on the **Entity Monitoring** column for the Branch Session Manager entry.

c. Verify that there is an Entity with the name **avaya-lsp-fs** and that it has the proper port and transport protocol displayed.

Testing calls

Test Branch Session Manager and Survivable Remote Communication Manager calls.

1. Place a phone call from one SIP extension to another and keep it up.
2. To test the Branch Session Manager functionality, disconnect the Session Manager and main Communication Manager from the network.
3. Validate that the connections failback.
4. Reestablish the network connections to Session Manager and the main Communication Manager server.

Chapter 7: Troubleshooting

The following sections describe problems that may occur during the installation or administration of Session Manager or Branch Session Manager and the troubleshooting steps to resolve the problem.

The server has no power

1. Make sure the power cord is plugged into the back of the server and into a non-switched outlet or UPS
2. If the server has a single power supply, make sure the power supply is installed in power supply bay 1 and is seated securely.
3. Make sure the UPS is plugged into a non-switched outlet.
4. Make sure the outlet has power.
5. Check the power supply LEDs on the back of the server. During normal operation, the AC LED and the DC LED are both lit.

Unable to access Management State

1. Check the cabling. GB1 = (Eth 0) Management Interface and GB3 = (Eth2) Security Module.
2. Create an SSH session to the System Manager IP address (not the Dom0 or Cdom) using the **root** login.
3. Create an SSH session to the Session Manager (Management Interface IP address) using the **craft** login, then super-user to sroot with the command **su - sroot**
4. In both SSH sessions, enter the command **cat /etc/hosts**

   The files should look EXACTLY like the following, except for the `GMI` and `Avaya` names:

```
**********************************System Manager*******************
127.0.0.1    localhost.localdomain localhost (DO NOT CHANGE THIS LINE)
```

```
135.9.123.456    GMI-SM1.global2.avaya.com GMI-SM1
135.9.123.987    GMI-SP4-SMGR.global2.avaya.com GMI-SP4-SMGR
::1           localhost6.localdomain6 localhost6 (DO NOT CHANGE THIS LINE)

*******************************Session Manager*********************
::1           localhost6.localdomain6 localhost6 (DO NOT CHANGE THIS LINE)
127.0.0.1    localhost localhost.localdomain (DO NOT CHANGE THIS LINE)
135.9.123.456    GMI-SM1.global2.avaya.com GMI-SM1
                   (This is a blank line)
135.9.123.987    gmi-sp4-smgr.global2.avaya.com gmi-sp4-smgr AsmSysMgr
```

BSM fails to completely install

When Branch Session Manager is installed within the Survivable Remote template and after the initialization has been given 20 additional minutes to run, the Virtual Machine Manage page on the System Platform Web console should list the bsm state as Running. If not, follow these troubleshooting steps.

Troubleshooting steps

1. Log into the System Manager Web interface.
2. Under **Data Replication** > **Synchronization**, check to see what state BSM is in.
3. If the state is Queued for Repair, then
   a. Log into the System Manager on the command line.
   b. Verify that the /etc/hosts file has the IP address and hostnames of itself, all the Session Managers, and all the Branch Session Managers.
   c. Log into the Branch Session Manager on the command line.
   d. Verify that the /etc/hosts file has the IP address and hostnames of itself and the System Manager
   e. Enter **`initDRS`**. The command should complete within 5 minutes. If not, go to the next step.
   f. Enter **`initTM`**. The command should complete within 5 minutes. If not, go to the next step.
   g. Enter SMnetSetup.

h. Verify all the information and retype the Enrollment password.

4. On System Manager under **Data Replication** > **Synchronization**, recheck to see if BSM is now synchronized.

Survivable server fails to sync with main server

Troubleshooting steps

1. Within the survivable remote server:
   a. Access the Communication Manager System Management Interface.
   b. In the navigation pane, click **Server Configuration** > **Server Role**.
   c. Verify that the **This Server is** field is set to a local survivable processor (LSP) and the other fields are filled out correctly.
2. Within the main server:
   a. Start a SAT session.
   b. Enter **`list survivable-processor`**.
   c. Verify that the following fields are set correctly:
      - Reg: **y**. If set to **n**, then the survivable remote server has not registered with the main server. You must reregister the survivable server.
      - Act: **n**
      - Translation Updated: Shows a timestamp.

Appendix A: Worksheets

The following worksheets contain the information that you will need for administering Session Manager and Session Manager-related entities using System Manager.

Important:
Do NOT use underscores in any of the ***Name*** *fields.* Linux does not like them.

Session Manager configuration information worksheet

Make a copy of this worksheet for each Session Manager that is being installed.

Field	Information to enter
Session Manager server hostname	
Session Manager IP address (Mgmt) - Eth 0 IP address (management interface for Session Manager on the customer network)	
Netmask (Network Mask Eth0)	
Gateway IP address (for Eth0)	
Network Domain (i.e., MyCompany.com)	
Primary DNS server	
Secondary DNS (if applicable)	
Tertiary DNS (if applicable)	
DNS Search Domains (separated with a space)	
System Manager server hostname	
System Manager IP address	
Local time zone	
NTP server	
Secondary NTP server (if applicable)	
Tertiary NTP server (if applicable)	
Optional Customer Linux Login (default is cust)	

Field	Information to enter
Session Manager Product Alarm ID	
Session Manager SAL Alarm ID	

Session Manager Entity information worksheet

The following information is required for each Session Manager or Communication Manager SIP entity to be administered using System Manager.

Use this information to administer SIP Entities and Entity Links. See SIP Entities and references on page 47 for a list of possible SIP Entities and application note references.

Field	Information to Enter
Entity Name	
Entity Type (Session Manager, Communication Manager, etc.)	
Location Name	
Management IP Address (i.e., SAT)	
FQDN	
Port (5060, 5061, etc.)	
Transport (UDP, TCP, or TLS)	
Session Manager Security Module IP Address	
Session Manager Security Module Network Mask	
Session Manager Security Module Default Gateway	

CLAN/PROCR Node Name	CLAN/PROCR IP Address	Signaling Group #	Tunk Group #

SIP Entities and references

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

SIP Entity	Release	Application Notes
Communication Manager	6.1	Configuring Avaya Aura™ Communication Manager to Work with Avaya Aura™ Session Manager
Communication Manager Feature Server	6.1	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	7.5	
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	5.2	
Voice Portal	5.1	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

Special Characters

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

W