Deploying Avaya Aura® Branch Session Manager

Release 6.3
Issue 3
August 2014

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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 you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

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 or an Instance of the Software.

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United

States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura® are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides information on the deployment and initial administration of Avaya Aura® Branch Session Manager Release 6.3.

For information about deploying a core Session Manager, see *Deploying Avaya Aura® Session Manager* on the Avaya support website at http://support.avaya.com.

For information about deploying a Session Manager in a virtualized environment, see *Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment* .

Intended audience

The primary audience for this document is anyone who wants to install and configure a Branch Session Manager.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Replaced the **Supported hardware** section with the **Supported servers** section.

Related resources

Documentation

You can download documents from the Avaya Support website at http://support.avaya.com. For the latest information, see the Release Notes.

The following table lists all the documents relating to Session Manager:

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management
Implementation		
Deploying Avaya Aura® Session Manager	Describes how to install and configure a Session Manager instance.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager.	Services and support personnel
Deploying Avaya Aura® Communication Manager on System Platform	Describes how to install the appropriate Communication Manager template, including Branch Session Manager, on the server.	Services and support personnel
Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment	Describes how to deploy the Session Manager virtual application in a VMware environment.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade a Session Manager to the latest software release.	Services and support personnel
Installing Service Packs for Avaya Aura® Session Manager	Describes the procedures to install service packs on Session Manager.	Services and support personnel
Installing Patches for Avaya Aura® Session Manager	Describes the procedures to install patches on Session Manager.	Services and support personnel
Installing the Avaya S8800 Server for Avaya Aura® Communication Manager	Describes the installation procedures for the S8800 Server.	Services and support personnel
Installing the Avaya S8510 Server Family and Its Components	Describes the installation procedures for the S8510 Server.	Services and support personnel
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620sServer.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Maintaining		
Maintaining and Troubleshooting Avaya Aura® Session Manager	Describes the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel
Administration		

Title	Description	Audience
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides case studies about common administration scenarios.	System administrators

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go** .

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Session Manager and System Manager Implementation
5U00050E	Knowledge Access: Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Session Manager 6.2 Delta Overview
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
ATC01840OEN	Survivable Remote Session Manager Administration
3U00100O	Designing Avaya Aura 6.2 Part 1
3U00101O	Designing Avaya Aura 6.2 Part 2

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Warranty

Avaya provides a 90-day limited warranty on Session Manager. See the sales agreement or other applicable documentation for more information about the terms of the limited warranty. In addition, see the standard warranty and details about Session Manager support during the warranty period on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Maintenance and Warranty Information**. See also **Help & Policies > Policies & Legal > License Terms**.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Avaya Aura® Branch Session Manager overview

With the Branch Session Manager, you can enable survivable remote server-style survival capabilities for a customer with SIP phones in a branch. The Branch Session Manager, also known as a Survivable Remote Session Manager, supports a total WAN outage in the branch when all devices in the branch network have lost connectivity to all devices in the core network.

Survivable remote sites include an Avaya Aura® Session Manager and an Avaya Aura® Communication Manager. You configure the Communication Manager as either a feature server or an evolution server. SIP phones simultaneously register to the primary Session Manager, secondary Session Manager, and the Survivable Remote Session Manager. During a WAN outage, SIP phones failover to the Survivable Remote Session Manager, and the Survivable Remote Communication Manager provides feature functionality.

When the Survivable Remote Session Manager is active in survivability mode, any administrative changes made in System Manager take effect only if the Survivable Remote Session Manager has network connectivity to the System Manager.

There is no SIP routing when a Survivable Remote Session Manager is installed. The server functions as a traditional Survivable Remote Server. You can activate the Survivable Remote Session Manager if the customer decides to add SIP at a later time.

You install and configure Survivable Remote Session Manager on Avaya Aura® System Platform using Communication Manager Survivable Remote templates.

Chapter 3: Deployment process

The following are the high-level tasks for installing and configuring an Avaya Aura® Branch Session Manager:

1. Complete the Survivable Remote configuration information checklist.
2. Complete the site preparation activities.
3. Install and configure the System Manager, Session Manager, and Communication Manager servers.
4. Administer the Branch Session Manager server on the main Communication Manager server.
5. Install the necessary hardware and equipment for the Branch Session Manager server.
6. Deploy the Communication Manager Survivable Remote template on the Branch Session Manager server.
7. Administer the Branch Session Manager.
8. Perform post-installation verification procedures.

Chapter 4: Planning and configuration

Communication Manager Survivable Remote templates

The Communication Manager Survivable Remote templates include the following applications:

- Avaya Aura® Communication Manager
- Avaya Aura® Branch Session Manager
- Avaya Aura® Utility Services

You can install the Survivable Remote (CM_SurvRemote) template on the following servers:

- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- Avaya S8800 (upgrade only)
- Avaya S8510 server with 8 GB memory (upgrade only)

You can install the Survivable Remote Embedded (CM_SurvRemoteEmbed) template on an Avaya S8300D server in a G250, G350, G430, G450, or G700 Gateway.

Supported servers

Session Manager Release 6.3 supports:

- S8510 and S8800 servers for upgrades only.
- S8300D server for Survivable Remote.

Session Manager supports the following servers:

Release	Servers
6.3 6.3.2	Dell R610, HP DL360 G7
6.3.4	Dell R610, Dell R620, HP DL360 G7, HP DL360 G8

6.3.8 6.3.9	

HP and Dell will discontinue HP DL360 G7 and Dell R610 servers in the near future. For more information, see the respective vendor websites.

Avaya has issued End of Sale notices for the S8800 and S8510 servers. Avaya supports these servers for existing installations only. For information about the effective dates, see the Avaya support website at http://support.avaya.com/.

Session Manager Port Matrix

Avaya Aura® Session Manager Port Matrix documents contain information about the ports and protocols that Session Manager uses. See the Port Matrix documents at https://support.avaya.com/security.

Accessing the Compatibility Matrix

The Compatibility Matrix provides compatibility information of the Avaya products that are supported with the various releases of Session Manager.

Note:

The screen refreshes each time you make a selection.

Procedure

1. Access the Avaya support website at http://support.avaya.com.
2. At the lower left of the screen, under **Tools**, click **Product Compatibility Matrix**.
3. Scroll down the **Tools** screen and click on the **Click here to access the Compatibility Matrix** link.
4. At the bottom of the screen, select **Avaya Aura® Session Manager** from the **Product** drop-down menu.
5. Select the appropriate release from the **Release** drop-down menu.
6. Select **Compatible Avaya Components** from the **Components and Products** drop-down menu.
7. Click the red **(View All)** link under the **Primary Components** title.

Chapter 5: Initial setup and pre-deployment

Pre-deployment checklist

Verify information with the customer and complete the steps in this checklist.

#	Action	Notes/Link	✔
1	Complete the Survivable Remote configuration information worksheet and verify the information is correct.	Survivable Remote configuration information worksheet on page 14.	
2	Verify the Site Preparation steps are completed.	Site preparation on page 16.	
3	Install and administer the System Manager server.	See *Deploying Avaya Aura® System Manager on System Platform*.	
4	Install and administer the core Session Manager server.	See *Deploying Avaya Aura® Session Manager*.	
5	Install and administer the main Communication Manager server.	See *Deploying Avaya Aura® Communication Manager on System Platform*.	
6	Verify the main Communication Manager is administered as a SIP entity.	Verifying Communication Manager is administered as a SIP Entity on page 16.	
7	Administer the Survivable Remote server on the main Communication Manager.	Continue with the Checklist for Survivable Remote Processor administration on Communication Manager on page 17.	

Survivable Remote configuration information worksheet

Make one copy of the Survivable Remote configuration information worksheet for each Survivable Remote server that you install.

Important:

Do not use underscores in any of the ***Name*** *fields.* Names can only contain letters, numbers, and hyphens. System host names cannot contain underscore characters according to Internet Standards RFC 952.

Field	Information to enter
Communication Manager IP address	
Communication Manager Hostname	
Cluster ID/MID (Module ID) value on the main Communication Manager **Survivable Processor** form.	
Utility Server IP address	
Utility Server Hostname	
Branch Session Manager IP Address (Admin IP)	
Branch Session Manager Hostname/FQDN	
Customer Login	
Customer Login Password	
DHCP parameters (optional): • DHCP Network Address • DHCP Subnet Mask • DHCP Router IP address • DHCP Pool IP address range • DHCP DNS Server IP address • DHCP WINS Server IP address	
DNS search string	
Primary System Manager IP Address	
Primary System Manager FQDN	
Secondary System Manager IP Address (optional)	
Secondary System Manager FQDN (optional)	
Trust Management Password: You set the password in the Security section of System Manager. **Note:** Verify the password is active.	
Branch Session Manager SIP Entity IP Address	

You set the product IDs on the SAL Gateway for a Branch Session Manager managed element.

Note:

You will need additional configuration data when you install System Platform. For more information, see the *System Platform* documentation on the Avaya Support website.

Site preparation

#	Action	Notes	✔
1	VPN access is available.		
2	All of the prerequisites as per the planning sheet have been completed.		
3	All required hardware has been purchased and delivered on site.		
4	All required licenses have been purchased and are accessible.		
5	Staging and verification activities have been planned and resources assigned.		

Verifying Communication Manager is administered as a SIP entity

Procedure

1. On the System Manager web console home page, under **Elements**, select **Routing** > **SIP Entities**.
2. Verify the main Communication Manager appears in the **SIP Entities** table.

Chapter 6: Survivable Remote Processor Administration on Communication Manger

Checklist for Survivable Remote Processor administration on Communication Manager

Before you begin

Verify the following requirements are complete before proceeding with the checklist.

- Configure the Processor Ethernet IP address (procr) for the main Communication Manager using the **add ip-interface procr** SAT command or using the Communication Manager web interface.
- If applicable, add the gateway using the **add media-gateway x** SAT command.
- If applicable, update the mgc lists of the gateways with the IP addresses of both the main Communication Manager server Processor Ethernet IP address (the first entry) and the Survivable Remote Processor Ethernet IP address (the second entry).
- Ensure that System Manager and Session Manager are already active in an existing SIP routing deployment.
- Ensure that at least one SIP signaling group and one SIP trunk group exist between the main Communication Manager and Session Manager.

#	Action	Link	✔
1	Log in to the Communication Manager server.		
2	Administer the survivable processor configuration information on Communication Manager.	Adding a Survivable Remote Processor on Communication Manager on page 18.	
3	If a gateway is part of the enterprise and branch, validate the Recovery Rule.	Validating the Gateway recovery rule on page 18.	
4	If a gateway is part of the enterprise and branch, verify the minimum time of network stability.	Validating the minimum time of network stability on page 18.	

#	Action	Link	✔
5	Install the Branch Session Manager.	Continue with Branch Session Manager server installation checklist on page 20.	

Adding a Survivable Remote Processor on Communication Manager

Procedure

1. On the Communication Manager SAT, enter **add survivable-processor *node-name*** where *node-name* is the name of the remote server.

   For example, `add survivable-processor lsp6`

2. Verify the **Type** field is **lsp** for the Survivable Remote server.
3. Enter the **Cluster ID/MID** from the configuration data worksheet.
4. Submit the form.

Validating the Gateway recovery rule

Procedure

1. On the Communication Manager SAT interface, enter **change media-gateway *x*** where *x* is the number of the Gateway.
2. In the **Recovery Rule** field, either:
   - Enter the **Recovery Rule** number of the Gateway, or
   - Enter **(none)** to disable the recovery rule. A value of **(none)** indicates the system does not accept any automatic fallback registrations.

   You can apply a single rule to all Gateways, or each Gateway can have a separate rule, and any permutation in-between. You administer the recovery rules on the **system-parameters mg-recovery-rule** form. The **system-parameters mg-recovery-rule** displays the assigned **Recovery Rule** numbers.
3. Submit the form to save the changes.

Validating the minimum time of network stability

Verify the **Minimum time of network stability** is set to 3 minutes. When the timer is set to 3 minutes, the gateway can failback to the main Communication Manager feature server or evolution server when the server becomes available. The 3-minute timer also prevents unnecessary failback and failover when the network is unreliable.

Procedure

1. On the Communication Manager SAT interface, enter **change system-parameters mg-recovery-rule n**, where *n* is the rule number.
2. In the **Minimum time of network stability** field, verify 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.

Chapter 7: Branch Session Manager server installation

Branch Session Manager server installation checklist

Survivable remote installation and administration requires using more than one document. The following table contains the procedures for installing, configuring, administering, and testing the survivable remote server and the documents to use for different procedures.

Important:

Verify the date and time are consistent between the System Platform that is supporting the branch and the associated System Manager. A clock shift can cause certificate and DRS replication problems.

#	Action	Document or link	Notes	✔
1	Install the Branch Session Manager server. See the installation documentation for the particular server on the Avaya support website at http://support.avaya.com.	If you are installing an Avaya S8510 server, see *Upgrading to Avaya Aura® Communication Manager Release 6.3*.	Ensure that the S8510 server has at least 8 GB of memory and a Communication Manager migration kit.	
		If you are installing an Avaya S8300D server, see • *Quick Start for Hardware Installation: Avaya G250 Gateway* • *Quick Start for Hardware Installation: Avaya G350 Gateway* • *Quick Start for Hardware Installation: Avaya G430 Gateway* • *Quick Start for Hardware Installation: Avaya G450 Gateway*	See the documentation for your particular Gxxx Gateway.	

#	Action	Document or link	Notes	✔
		• *Quick Start for Hardware Installation: Avaya G700 Gateway*		
2	Install System Platform on the server.	See *Installing and configuring Avaya Aura® System Platform*.	See the note above regarding the date and time.	
3	Install the most recent Communication Manager template using the System Platform web console.	See *Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394.	When you perform this step, you install Communication Manager, Branch Session Manager, and the Utility Server.	
4	Upgrade Communication Manager to the latest release.	See: • *Upgrading to Avaya Aura® Communication Manager Release 6.3* • PCN1599S		
5	Upgrade Branch Session Manager to the latest release.	See Upgrades to Branch Session Manager on page 37.		
6	Upgrade the Utility server.	See *Accessing and Managing Avaya Aura® Utility Services*.		
7	Configure Communication Manager.	*Deploying Avaya Aura® Communication Manager on System Platform*, 18-604394	Configure Server Role and Network Configuration.	
8	Administer, verify, and test the Branch Session Manager using System Manager.	Continue with the Branch Session Manager administration checklist on page 22.		

Chapter 8: Branch Session Manager Administration

Branch Session Manager administration checklist

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

#	Action	Link	✔
1	Log in to the System Manager web console.		
2	Add the Branch Session Manager server as a SIP Entity.	Adding a survivable remote server as a SIP entity on page 23.	
3	Verify the Branch Session Manager entry is added to the customer DNS. Otherwise, you will see Trust Management and DRS synchronization issues.		
4	Administer the Branch Session Manager server on System Manager.	Administering a Branch Session Manager using System Manager on page 23.	
5	Create Entity Links between the Branch Session Manager server and the core Communication Manager.	Creating entity links on page 24.	
6	Create Entity Links between the Branch Session Manager server and the Session Manager.	Creating entity links on page 24.	
7	Verify the connections between Communication Manager and the Branch Session Manager server.	Checking the connections on page 25.	
8	Configure alarming.	Continue with the Alarming configuration checklist on page 26.	

Adding a survivable remote server as a SIP entity

Procedure

1. On the System Manager Web Console home page, under **Elements**, click **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, enter the name of the Branch Session Manager.
4. In the **FQDN or IP Address** field, enter the IP address of the Branch Session Manager Security Module. This IP address is *not* the management IP address.
5. In the **Type** field, select **Session Manager** from the drop-down menu.
6. In the **Port** section, click **Add**.
7. Add the port, protocol, and default domain entries for each port and protocol on which the Branch Session Manager listens for SIP traffic. Add failover ports if the SIP entity is a failover group member. Fpr information about Failover Groups, see *Administering Avaya Aura® Session Manager*.
8. Click **Commit**.

Administering a Branch Session Manager using System Manager

Before you begin

Verify that you created the SIP entity that you want to add. For a Session Manager SIP entity, ensure that the listen ports are administered on the SIP entity form. Endpoints use these listen ports to connect to the survivable remote server and to map different ports to different domains. For details regarding administration of listen ports, see *Administering Avaya Aura® Session Manager*.

Procedure

1. On the System Manager web console home page, under **Elements**, select **Session Manager** > **Session Manager Administration**.
2. Click **New** in the **Branch Session Manager Instances** section.
3. In the **General** section:
   a. Select the survivable remote SIP entity from the **SIP Entity Name** drop-down list.
   b. (Optional) In the **Description** field, add a comment.
   c. In the **Management Access Point Host Name/IP** field, enter the IP address of the host on which the management agent is running. This IP address 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 **Adaptation for Trunk Gateway** from the drop-down menu.

You can use the default adaptation, which is the adaptation used for the trunk gateway entity that this survivable remote server subtends. You can also specify a different adaptation. When you specify a different adaptation, the system overrides the default adaptation. If you administer two entities, one for a feature server and one for a trunk gateway, then the adaptation applies only to the trunk gateway entity. If you use a single entity, then the adaptation applies to application-sequenced and trunk-gateway routed calls.

4. In the **Security Module** section:

a. The **SIP Entity IP Address** field is automatically populated with 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.

d. For the **Speed & Duplex** field, select **Auto** from the drop-down menu.

For details about other fields, see *Administering Avaya Aura® Session Manager*.

5. Click **Commit**.

Creating entity links

About this task

When applicable, create the entity links between:

- Each Session Manager server and the Communication Manager feature server or evolution server.
- The Branch Session Manager server and the Communication Manager feature server or evolution server.

If you use separate entities and entity links, such as for a feature server and trunk gateway configuration, you must administer two entity links for each entity on the Survivable Remote server. However, if you use only one entity and entity link, such as for an evolution server configuration, you must administer only one entity link on the Survivable Remote server.

Procedure

1. Log on to System Manager Web Console.
2. Click **Elements** > **Routing**.
3. In the navigation pane, click **Routing** > **Entity Links**.
4. Click **New**.
5. In the **Name** field, type a name for the entity link.
6. In the **SIP Entity 1** field, select the Branch Session Manager server.

For administering Communication Manager as a feature server and trunk gateway, select the Session Manager entity.

7. In the **Protocol** field, select **tls**.
8. In the **Port** field, type the port number.
9. In the **SIP Entity 2** field, select the Communication Manager server.
10. In the **Port** field, type the port number.
11. In the **Connection policy** list box, select **Trusted**.
12. **(Optional)** In the **Notes** field, type a description for the entity link.
13. Click **Commit**.

Checking the connections

Procedure

1. Check the Branch Session Manager SIP Entity Link status:
   a. On System Manager Web console, in **Elements**, select **Session Manager** > **System Status** > **SIP Entity Monitoring**.
   b. Select the Branch Session Manager name from the list in the table *SIP Entities Status for All Monitoring Session Manager Instances*.
   c. Verify that the **Link Status** is `Up` for the Survivable Remote Session Manager.
2. Check the Session Manager Dashboard:
   a. On System Manager Web console, under **Elements** , select **Session Manager** .
   b. On the Session Manager Dashboard page, click the **Entity Monitoring** column. For Branch Session Manager, the status is (---).

      The Session Manager Entity Link Connection Status page opens.
   c. Verify the entity monitoring status of Branch Session Manager.

Chapter 9: Alarm configuration

Alarming configuration checklist

#	Action	Notes	✔
1	Configure the Serviceability Agent for Session Manager.	See the chapter for *SNMP support for Session Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.	
2	Add the Session Manager to the SAL Gateway.	Adding a Session Manager to the SAL Gateway on page 26.	
3	Generate a test alarm.	Generating a test alarm on page 27.	
4	Test the installation.	Continue with the Post-installation verification checklist on page 29.	

Adding a Session Manager to the SAL Gateway

Configure alarming and remote access for a Session Manager instance.

Before you begin

The Secure Access Link (SAL) Gateway must already be set up for System Manager Release 6.3.

Procedure

1. Log in to the System Platform Web console.
2. Click **Server Management** > **SAL Gateway Management**.
3. On the **SAL Gateway Management** page, click **Launch SAL Gateway Management Portal**.
4. When the SAL Gateway login page appears, enter the same user ID and password that you used when you logged in to the System Platform Web Console.
5. In the navigation pane of the SAL Gateway user interface, select **Secure Access Link Gateway** > **Managed Element**.

6. On the **Managed Element** page, click **Add new**.
7. Enter information in the following fields:
   - **Host Name**: Host Name of the Session Manager.
   - **IP Address**: IP Address of the Session Manager.
   - In the **Model** field, select **SessionMgr_x.x.x.x** from the drop-down menu.

     The **Product** field is filled in automatically after you select Session Manager.
   - **Solution element ID**: The Solution Element ID (SE ID) of Session Manager. The format of the ID is (NNN)NNN-NNNN where N is any digit from 0 to 9.
   - **Product ID**: The Product ID of Session Manager.
   - Select the **Provide remote access to this device** check box.
   - Select the **Transport alarms from this device** check box.

     Important:

     The SAL Gateway forwards alarms for this Session Manager only after you select the **Provide remote access to this device** and **Transport alarms from this device** check boxes.
8. Click **Add**.
9. Click **Apply** to apply the changes.
10. Restart the SAL Gateway for the configuration changes to take effect:
    a. In the navigation pane of the SAL Gateway user interface, select **Administration** > **Apply Configuration Changes**.
    b. Click **Apply** next to **Configuration Changes**.

       The system restarts the SAL Gateway and updates the SAL Gateway with the new configuration values.

Generating a test alarm

Generate a test alarm to the targets assigned to the serviceability agent. These targets may include:

- A SAL Gateway (the alarm is forwarded to ADC)
- System Manager Trap Listener
- Third-party NMS
- Avaya SIG server

You can either run the **generateTestAlarmSM.sh** script using the Session Manager CLI, or you can use the **Generate Test Alarm** button on the **Serviceability Agents** screen.

Procedure

1. If using the Session Manager CLI:
   a. Login to the Session Manager server.
   b. Enter Session Manager CLI command **generateTestAlarmSM.sh**.
2. If using the **Generate Test Alarm** button on the **Serviceability Agents** screen:
   a. On the System Manager web console, under **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
   b. Select a Hostname from the list and click **Generate Test Alarm**.
3. Verify the System Manager received the test alarm message:
   a. On the System Manager Web Console, under **Services**, select **Events** > **Alarms**.
   b. Verify the message **Test alarm for testing only, no recovery action necessary** displays under the **Description** column.
4. If the serviceability agent is configured with other targets, verify the other targets also received the test alarm.

Chapter 10: Post-installation verification procedures

Post-installation verification checklist

#	Action	Link	✔
1	Verify the Branch Session Manager host name exists in System Platform.	Verifying survivable remote information on page 29.	
2	Verify the `avaya-lsp-fs` information.	Verifying avaya-lsp-fs administration on page 30 .	
3	Verify the Communication Manager Survivable Remote Processor is registered to the main Communication Manager.	Verifying Survivable Server registration on Communication Manager on page 30.	
4	Test the System Manager and Branch Session Manager installation.	Testing System Manager and Branch Session Manager on page 31.	
5	Change the state of the Branch Session Manager server to **Accept New Service**.	Accepting new service on page 32.	
6	Test Communication Manager with the Branch Session Manager server.	Testing calls on page 32.	

Verifying survivable remote information

Procedure

1. Log in to the System Platform Web console.
2. Select **Server Management** > **Network Configuration**.
3. Verify the following information:
   - Default Gateway
   - Subnet Mask located in the Netmask column and **avpublic** row in the **Domain-0** area of the form.
   - Hostnames: Ensure that Branch Session Manager Hostname is in FQDN format.
   - IP Addresses

4. Log out of the System Platform Web console.

Verifying avaya-lsp-fs administration

About this task

This topic is related to verification of the **avaya-lsp-fs** value. If the **avaya-lsp-fs** entry is missing, the Branch Session Manager will not initialize properly. The cause might be an administration error.

Procedure

1. On the System Manager Web console, click **Elements** > **Session Manager** .
2. Locate the appropriate Branch Session Manager instance in the table.
3. On the Session Manager Dashboard page, in the **Entity Monitoring** column, click the associated entry of the server .
4. On the **Session Manager Entity Link Connection Status** screen:
   a. Verify that there is a SIP Entity with the name **avaya-lsp-fs**.
   b. Verify that the port and transport protocol information is correct.

      The state is *deny* for this **avaya-lsp-fs** link when the Branch Session Manager is *inactive*. This link is the same for Communication Manager Evolution Servers as well as Communication Manager Feature Servers.
5. If the **avaya-lsp-fs** entry is missing, Branch Session Manager did not initialize properly.
   a. On the System Manager Web console, verify the following:
      - one or two entity links from the Branch Session Manager to the core Communication Manager are administered correctly.
      - entity links from the Branch Session Manager to the core Session Managers, that are controllers for the users on the branch, are administered correctly.
   b. Verify that the same port and transport are used as administered between the primary Session Manager and the core Communication Manager.
   c. Verify that all users that are administered with this survivability server have application sequencing to a Communication Manager entity. This Communication Manager entity represents the main Communication Manager that is administered on the Branch Session Manager page.

Verifying Survivable Server registration on Communication Manager

Verify the Survivable Core or Survivable Remote template is registered with the main server.

Note:

This procedure can take several minutes to complete.

Procedure

1. Log in to a Communication Manager SAT session.
2. Enter `list survivable-processor` to display the **Survivable Processor** screen.
3. Verify the **Reg** field is set to **y**, indicating that the survivable server has registered with the main server.
4. Verify the **Translations Updated** field displays the current time and date, indicating that the translations have been updated on the survivable server.

Testing the System Manager and Branch Session Manager installation

About this task

Perform the following steps to verify the System Manager and Branch Session Manager are installed and configured properly, and that the servers and applications are communicating.

Procedure

1. On the System Manager Web Console home page, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests** .
2. Select **System Manager** from the **Select Target** drop-down menu.
3. Click **Execute All Tests**.
4. Verify all tests display **Success**.
5. On the System Manager Web Console home page, under **Elements**, select **Session Manager** > **System Status** > **Security Module Status**.
6. Verify the status is **Up** for the Branch Session Manager.
7. Verify the IP address is correct.
8. If the status is **Down**, reset the security module:
    a. Select the appropriate Branch Session Manager from the table.
    b. Click **Reset**.
9. On the System Manager Web Console, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.
10. Select the appropriate Branch Session Manager instance from the drop-down menu.
11. Select **Execute All Tests**.
12. Verify all tests ran successfully.

13. Check the replication status of the Branch Session Manager:
    a. On the System Manager Web Console, under **Services**, select **Replication**.

       The **Synchronization Status** for the Branch Session Manager should be green and the status should be **Synchronized**.

    b. If the status is not **Synchronized**, select the check box next to the Branch Session Manager replica group name and click **View Replica Nodes** to determine which host is not synchronized with System Manager.
14. For Geographic Redundant systems, verify the following:
    - Ping the vFQDN of the System Managers to make sure connectivity is working properly.
    - Using the System Manager Data Replication Service, verify theBranch Session Manager is in the DRS node list and is synchronized.
    - Using the System Manager Inventory, verify the managed elements in the **managed by** column show the correct value of the managing System Manager.

Accepting new service

Note:

Even though the Security Module displays the status as **Up**, the security module might take 5 to 10 minutes before the security module can begin routing calls.

Procedure

1. On the System Manager web console home page, under **Elements**, click **Session Manager**.
2. On the **Session Manager Dashboard** page, select the appropriate Session Manager in the **Session Manager Instances** table.
3. Click **Service State**.
4. Select **Accept New Service** from the drop-down menu.
5. Click **Confirm**.

Testing calls

Make test calls between the Branch Session Manager server and the main Communication Manager server.

Procedure

1. Place a phone call from one SIP extension to another and stay online.
2. To test the survivable remote functionality, disconnect the Session Manager and main Communication Manager from the network.
3. Verify you can make calls between SIP stations.

4. Re-establish the network connections to the Session Manager and the main Communication Manager server.
5. Verify you can make calls between SIP stations.

Chapter 11: Troubleshooting

The following sections describe troubleshooting steps for errors that may occur during installation or administration of the Branch Session Manager server.

Related Links

Server has no power on page 34
Unable to access Service State on page 36

Server has no power

Procedure

1. Verify the power cord to the server is plugged into a non-switched outlet or uninterrupted power supply (UPS).
2. If using a UPS, verify the UPS is plugged into a non-switched outlet.
3. If the server has a single power supply, verify the power supply bay is installed and is seated securely.
4. Verify the outlet has power.
5. Check the LEDs of the server and verify the AC LED and the DC LED are both lit during normal operation.

Related Links

Troubleshooting on page 34

Issues with replica group state

Troubleshooting steps

About this task

Perform the following troubleshooting steps if the replica group state is not **Synchronized**, **Queued for Repair**, or **Repairing**, or if the replica group is stuck in the **Starting** state.

Procedure

1. Log in to the System Manager Web interface.
2. Under **Services**, click **Replication**.
3. Select the appropriate **Replica Group** for the Session Manager server.
4. Click **View Replica Nodes**.
5. Verify information in the `/etc/hosts` file of the System Manager:
   a. Log in to the CLI of the System Manager.
   b. Verify the `/etc/hosts` file has the IP address, FQDN, and hostnames of itself and all of the associated Session Managers (applicable only if DNS is not used for host resolution of an IP address).

      Note:

      Hostname is case sensitive.
6. Enter the **`smconfig`** command and verify the basic data entry values of Session Manager.
7. Enter **`initTM`**. The command should complete within 10 minutes. If it does not complete within that time, continue with the next step.
8. Verify that the system date and time on the Session Manager server is the same as the system date and time on the System Manager virtual machine. Trust certificate initialization can fail if the clocks differ by more than a few seconds.
9. Verify the information on the Network Configuration page on the System Platform Web Console (**Server Management** > **Network Configuration**).
10. On System Manager, verify the Session Manager is synchronized.

Related Links

Troubleshooting on page 34

Survivable server fails to sync with main server

Branch Session Manager fails to completely install

CM_SurvRemote and CM_SurvRemoteEmbed templates include Branch Session Manager. After the template installation is finished, allow 20 additional minutes for the Branch Session Manager virtual machine to install and initialize. The Virtual Machine Management page on the System Platform Web console should list the Branch Session Manager's application state as *Running*. If not, follow these troubleshooting steps.

Troubleshooting steps

Procedure

1. On the survivable remote server:
   a. Access the Communication Manager System Management Interface.
   b. In the navigation pane, click **Server Configuration** > **Server Role**.
   c. Verify the **This Server is** field is set to a local survivable processor (LSP) and the other fields are filled out correctly.

      Note:

      If you change any of the configuration settings, click **Change**, then click **Restart now** for the changes to take effect.
2. On the main server:
   a. Start a SAT session.
   b. Enter `list survivable-processor`.
   c. Verify the following fields contain the specified values:
      - Reg: **y**. If set to **n**, then the survivable remote server has not registered with the main server.
      - Act: **n**
      - Translation Updated: Displays the time stamp when translations were last updated.

Unable to access Service State

Procedure

1. On the Session Manager Dashboard page, check the **Service State** of the Branch Session Manager.
2. If the **Service State** displays an unknown value:
   a. Check the cable for Eth0 and Eth2.
   b. Create a SSH session to the System Manager IP address (not the Dom0 or Cdom) using the customer account specified during the template install.
   c. Create a SSH session to the Session Manager with the Management Interface IP address using the **craft** or **customer** login.
   d. Enter the command `SMnetSetup` and verify the settings.

Related Links

Troubleshooting on page 34

Chapter 12: Maintenance procedures

Upgrades to Branch Session Manager

Branch Session Manager upgrade involves upgrading of the Communication Manager Survivable Remote templates as outlined in the document *Upgrading Avaya Aura® Communication Manager*.

To install service packs for Branch Session Manager, see *Installing Service Packs for Avaya Aura® Session Manager* on the Avaya support Web site at http://www.avaya.com/support.

To install patches for Branch Session Manager, see *Installing Patches for Avaya Aura® Session Manager* on the Avaya support Web site at http://www.avaya.com/support.

Note:

Upgrade System Manager before starting the upgrade process on Session Managers.

Remote access

Secure Access Link (SAL) uses the existing Internet connectivity of the customer for remote support and alarming. All communication from the customer environment is sent by Secure Hypertext Transfer Protocol Secure (HTTPS). SAL requires upload bandwidth, for example, from customer to Avaya or Avaya Partner, of at least 90 Kbs with round trip latency no greater than 150 ms.

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

Appendix A: Certificate management

Session Manager uses five unique certificates: WebSphere, SAL Agent, Management, SIP, and HTTPS. SIP and HTTPS are the most important because these certificates communicate with outside entities such as Communication Manager and endpoints.

Any changes to these interfaces can cause major service interruptions. *Be very careful when changing these certificates.* The near end and far end use the certificates to trust each other. Each side presents its identity certificate during TLS negotiation. If one side does not trust the identity certificate of the other side, the connect fails. For an entity to trust another certificate, the entity must contain the root CA certificate from the CA that issued the identity certificate. Some example CAs are VeriSign, Symantec, System Manager, and Avaya's SIP Product CA.

The root CA certificate must be stored in the entity's trusted list, also known as a trust store. To change the SIP or HTTPS identity certificate of a Session Manager, each far end entity must first contain the new root CA certificate in its trusted list. *You must add the new root CA certificate to the trusted list of the far end before changing the identity certificates.*

There are two options for handling certificates for a new installation:

- Use the new System Manager issued ID certificates (default behavior). See Using the System Manager CA on page 41.
- Use third party ID certificates. See Using a Third Party CA on page 44.

Related Links

SIP Identity Certificate on page 38
HTTPS Identity Certificate on page 39
Viewing the TLS version on page 40

SIP Identity Certificate

Generate the Session Manager SIP Identity Certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required?
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	Optional

Attribute	Value	Required?
Authority Key Identifier	*hash*	Required[1]
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path}	Optional
	URI:ldap://{crl-server}{:crl-port}{/crl-dn}[2]	Optional
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.2.1	Required
	id-kp-clientAuth = 1.3.6.1.5.5.7.3.2.2	Optional[3]
	id-kp-sipDomain = 1.3.6.1.5.5.7.3.20	Contraindicated [4]
Key Usage	digitalSignature	All values are Optional. [5]
	nonRepudiation	
	keyEncipherment	
	dataEncipherment	
Subject	CN={fqdn}	Required
Subject Alternative Name	IP:{ip}	Optional
	URI:sip:{domain}	Required [6]
	DNS:{domain}	Required [7]
	DNS:{fqdn}	Required
Subject Key Identifier	*hash*	Recommended
Validity	*validity period*	Required

Related Links

Certificate management on page 38

HTTPS Identity Certificate

Generate the Session Manager HTTPS Identity Certificate with the following X509v3 extensions and attributes.

[1] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[2] URLS and DNs that identify the location of CRLs in LDAP directories can be complex. Entities must be able to handle characters as defined by the LDAP URI specification in RFC 4516.
[3] Required if the same Identity Certificate is used when the server is acting as a client.
[4] Validation of the presence of the `id-kp-sipDomain` extended key usage as described in RFC 5924 is discouraged, as it limits use of the certificate to SIP only and forces certificate proliferation.
[5] Values may vary as specified in RFC 5280 and RFC 3279.
[6] The SIP domain may not be known at install time, so the `URI:sip:{domain}` Subject Alternative Name value suggested by RFC 5922 is not likely to be present.
[7] See Footnote 6. Also, the 96xx endpoints require the SIP domain to be present in the **CN** or as a `DNS:{domain}` entry in the Subject Alternative Name field.

Attribute	Value	Required?
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	Optional
Authority Key Identifier	*hash*	Required[8]
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path} URI:ldap://{crl-server}{:crl-port}{/crl-dn}[9]	Optional Optional
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.2.1 id-kp-clientAuth = 1.3.6.1.5.5.7.3.2.2	Required Optional[10]
Key Usage	digitalSignature nonRepudiation keyEncipherment dataEncipherment	All values are Optional. [11]
Subject	CN={fqdn}	Required
Subject Alternative Name	IP:{ip} DNS:{fqdn}	Optional [12] Required
Subject Key Identifier	*hash*	Recommended
Validity	*validity period*	Required

Related Links

Certificate management on page 38

Viewing the TLS version

Determine if you are using a demo identity certificate.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select the **securitymodule**.

[8] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[9] URLS and DNs that identify the location of CRLs in LDAP directories can be complex. Entities must be able to handle characters as defined by the LDAP URI specification in RFC 4516.
[10] Required if the same Identity Certificate is used when the server is acting as a client.
[11] Values may vary as specified in RFC 5280 and RFC 3279.
[12] For the 96xx endpoints, PPM is defined as an IP address so PPM certificates must contain the `IP:{ip}` Subject Alternative Name entry when these endpoints are part of the solution.

5. Check the **Issuer Name**.

   If the **Issuer Name** field contains **CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US**, you have a demo identity certificate.

Related Links

Certificate management on page 38

Using the System Manager CA

System Manager can act as a certificate authority similar to VeriSign and Symantec. Many adopters, such as Communication Manager, Session Manager, and Presence, already use certificates issued by System Manager.

For fresh installations, all Identity Certificates, including SIP and HTTPS, are issued by the System Manager CA. You must install the System Manager's trusted root certificates on endpoints that communicate with Session Manager over TLS for the endpoints to trust the Session Manager's identity certificate.

Use this checklist for using the System Manager issued Identity Certificates.

#	Action	Link	✔
1	Export the System Manager CA.	Exporting the System Manager CA on page 42.	
2	Add the System Manager's Root Certificate to Communication Manager.	Adding the System Manager CA to Communication Manager on page 42.	
3	Add System Manager's Root Certificate to 96xx phones.	Adding the System Manager Root Certificate to 96XX phones on page 43.	
4	Add the System Manager's Root Certificate to any other SIP connections, such as CS1K and Radvision.		
5	Replace the Session Manager SIP and HTTP Identity Certificates. **Note:** This step needs to be performed for all Session Managers and Branch Session Managers.	Installing Enhanced Validation Certificates on Session Manager on page 43.	
6	Remove the SIP CA Root Certificate from all trust lists, such as Communication Manager and phones.	Other Session Managers administered under the same System Manager will already trust the new Identity Certificate.	

Exporting the System Manager CA

Procedure

1. On the home page of the System Manager web console, under **Services**, select **Security** > **Certificates** > **Authority**.
2. On the main page, click **Download pem file**.
3. Save the file.

Note:

To avoid HTTP download issues, save the file with the **.txt** extension.

Adding System Manager CA to Communication Manager

When you configure the Session Manager's SIP Identity Certificate to use System Manager as the CA, links to Communication Manager will go down because the Communication Manager will not trust the System Manager CA. Use this procedure to make Communication Manager trust the System Manager CA certificate.

Procedure

1. Verify you can access the System Manager CA certificate.
2. Log in to the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.
4. In the left menu, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server**.
6. Click **Browse**.
7. Select the System Manager CA certificate you want to download and click **Open**.
8. Click **Download**.
9. In the left menu, under **Security**, click **Trusted Certificates**.
10. Click **Add**.
11. Enter the name of the downloaded System Manager CA certificate.

Note:

You only need to enter the name of the file.

12. Click **Open**.
13. Select the Communication Manager check box.
14. Click **Add**.

15. Restart Communication Manager.

    Warning:

    Select **Delayed Shutdown** and **Restart server after shutdown**. Restarting the Communication Manager server stops the SMI server you are currently using. You will be unable to access the Web pages until the server restarts.

Adding System Manager's Root Certificate to 96xx Phones

This procedure describes how to make phones trust the System Manager CA certificate.

Important:

To avoid a service outage, run this procedure before switching Session Manager to certificates issued by System Manager.

Procedure

1. Copy the file to the file server that the 96xx phones are using.
2. On the file server, edit the file **46xxsettings.txt**.
3. In the file, set the **TRUSTCERTS** option to include the System Manager CA certificate. For example:

   ```
   SET TRUSTCERTS "smgr.txt, av_sipca_pem_2027.txt"
   ```

4. Reboot all of the phones.

   After rebooting, the phones download the System Manager root CA and are ready to the replacing of the Session Manager's SIP identity certificate.

Installing Enhanced Validation Certificates for Session Manager

By default, 96xx phones perform enhanced validation of certificates. To make use of these certificates, you need to populate the **Common Name** and **Subject Alternate Name** of the certificate. You need to perform this procedure for all Session Managers and Branch Session Managers.

Important:

The 96xx phones need to trust the System Manager Root Certificate before you replace an SIP or HTTP certificates. Failure to do so results in the loss of communication with the phones.

Procedure

1. On the System Manager web console home page, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the appropriate Session Manager from the list and click **More Actions**.

3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the **Identity Certificates** page, select **Security Module SIP**, or the name associated with **Common Name** securitymodule.
5. Click **Replace**.
6. On the **Replace Identity Certificate** page, select **Replace this Certificate with Internal CA Signed Certificate**.
7. Select the **Common Name (CN)** checkbox and enter the host name or IP address of the Security Module. The address is the same as the SIP Entity address.
8. Select **RSA** for the **Key Algorithm**.
9. Select **2048** or **4096** as the **Key Size**.
10. Select the **DNS Name** checkbox and enter the SIP domain (for example, avaya.com). You can enter multiple SIP domains using commas (no spaces), such as `avaya.com,company.com,xyz.com`.
11. Click **Commit**.
12. On the **Identity Certificates** page, select **Security Module HTTP**.
13. Click **Replace**.
14. On the **Replace Identity Certificate** page, select **Replace this Certificate with Internal CA Signed Certificate**.
15. Select the **Common Name (CN)** check box and enter the host name or IP address of the Security Module. The address is the same as the SIP Entity address.
16. Select **RSA** for the **Key Algorithm**.
17. Select **2048** or **4096** as the **Key Size**.
18. Select the **DNS Name** checkbox and enter the SIP domain (for example, company.com). You can enter multiple SIP domains using commas (no spaces), such as `abc.com,company.com,xyz.com`.
19. Click **Commit**.
20. Restart all phones.

    After rebooting, the phones download the System Manager Root CA and will be able to communicate with the Session Manager.

Using a third party CA

The use of third party certificates is optional. Third party certificates are not required.

A third party CA can be a commercial vendor such as VeriSign and Symantec, or an enterprise-run CA that is maintained by the customer's IT department. You can create third party certificates using openssl or open source tools such as EJBCA (http://www.ejbca.org).

Use this checklist for using third party Identity Certificates.

#	Action	Link	✔
1	Add the third party Root Certificate to Communication Manager. Repeat this step for each Communication Manager that is connected to the Session Manager.	Adding a third party Root Certificate to Communication Manager on page 45.	
2	Add the third party Root Certificate CA to 96xx phones.	Adding a third party root certificate CA to 96xx phones on page 46.	
3	Add the third party Root Certificate CA to the trusted list for any other adjunct device that uses TLS to connect to Session Manager through SIP. .	For example, Avaya Voice Portal and Meeting Exchange.	
4	Replace the Session Manager SIP and HTTP Identity Certificates.	Installing third party certificates on Session Manager on page 47.	
5	Add the third party certificate to the trusted list.	Adding trusted certificates on page 48.	

Adding a third party CA to Communication Manager

Configure Communication Manager to trust a third party root CA.

When you replace the SIP CA with the third party certificate, all Communication Manager TLS connections will go down.

Perform this procedure for each Communication Manager that is connected to the Session Manager.

Procedure

1. Verify you can access the third party root CA certificate.
2. Log in to the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.
4. In the left menu, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server**.
6. Click **Browse**.
7. Select the third party CA certificate you want to download and click **Open**.

8. Click **Download**.
9. In the left menu, under **Security**, click **Trusted Certificates**.
10. Click **Add**.
11. Enter the name of the downloaded third party CA certificate.

    Note:

    You only need to enter the name of the file.
12. Click **Open**.
13. Select the Communication Manager check box.
14. Click **Add**.
15. Restart Communication Manager.

    Warning:

    Select **Delayed Shutdown** and **Restart server after shutdown**. Restarting the Communication Manager server stops the SMI server you are currently using. You will be unable to access the Web pages until the server restarts.
16. Repeat this procedure for each Communication Manager connected to the Session Manager.

Adding a third party Root Certificate to 96xx Phones

This procedure describes how to make phones trust a third party Root Certificate CA.

Important:

To avoid a service outage, perform this procedure before switching the Session Manager to certificates issued by System Manager.

Procedure

1. Copy the third party root certificate file to the file server that the 96xx phones are using.
2. On the file server, edit the file **46xxsettings.txt**.
3. In the file, set the **TRUSTCERTS** option to include the third party CA certificate. For example:

   ```
   SET TRUSTCERTS "Third_Party_CA.txt, av_sipca_pem_2027.txt"
   ```
4. Reboot all the phones.

   After rebooting, the phones download the System Manager root CA and are ready to the replacing of the Session Manager's SIP identity certificate.

Installing third party certificates on Session Manager

This procedure describes how to install a third party certificate for SIP and HTTP on Session Manager.

When the certificate changes to the third party certificate, each SIP Entity must trust the third party CA.

Procedure

1. On the System Manager web console home page, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the appropriate Session Manager from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. Install the SIP third party certificate:
    a. On the **Identity Certificates** page, select **Security Module SIP**, or the name associated with **Common Name** securitymodule.
    b. Click **Replace**.
    c. On the **Replace Identity Certificate** page, select **Import third party PKCS#12 file**.
    d. When prompted for **Please select a file**, browse for the third party signed certificate.
    e. Enter the password in the **Password** field.
    f. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
    g. Click **Commit**.
5. On the System Manager web console home page, under **Services**, click **Inventory** > **Manage Elements**.
6. Select the appropriate Session Manager from the list and click **More Actions**.
7. Select **Configure Identity Certificates** from the drop-down menu.
8. Install the HTTP third party certificate:
    a. On the **Identity Certificates** page, select **Security Module HTTP**.
    b. Click **Replace**.
    c. On the **Replace Identity Certificate** page, select **Import third party PKCS#12 file**.
    d. When prompted for **Please select a file**, browse for the third party signed certificate.
    e. Enter the password in the **Password** field.
    f. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
    g. Click **Commit**.

Adding trusted certificates

You can import a trusted certificate:

- from a file.
- by copying the contents of a PEM file.
- from a list of an existing certificates.
- from a remote location using a TLS connection.

Procedure

1. On the System Manager web console home page, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
   a. Select **Import from file**.
   b. Click **Browse** and locate the file.
   c. Click **Retrieve Certificate**.
   d. Click **Commit**.
6. To import a certificate in the PEM format:
   a. Select **Import as PEM Certificate**.
   b. Locate the PEM certificate.
   c. Open the certificate using Notepad.
   d. Copy the entire contents of the file. You can include the start and end tags: -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.
   e. Paste the contents of the file where indicated.
   f. Click **Commit**.
7. To import certificates from existing certificates:
   a. Select **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.
8. To import certificates using TLS:
   a. Select **Import using TLS**.
   b. Enter the IP Address of the location in the **IP Address** field.

c. Enter the port of the location in the **Port** field.

d. Click **Retrieve Certificate**.

e. Click **Commit**.

Demo certificates

Previously, Session Manager was shipped with demo certificates issued by the SIP CA to simplify TLS connection setup. Demo certificates are non-unique identity certificates issued by the Avaya SIP Product Certificate Authority. Demo certificates are very insecure and do not meet current NIST standards (SHA256 and 2048 bit keys).

Starting with Session Manager 6.3.8, Session Manager no longer uses or supports default demo certificates for new installations. Fresh installations of Session Manager result in SIP and HTTP certificates signed by System Manager. In most cases, existing TLS connections will break until the System Manager CA is installed on the far end. You can reinstall the demo certificates to quickly restore a previously working environment.

For upgrades, Session Manager preserves the previous certificates. If a demo certificate was in use in the previous release, the certificate is preserved through the upgrade.

Appendix B: OS-level logins for Session Manager

The following is a list of logins that are created during the Session Manager software installation:

- **craft**: An Avaya services login to gain access to the system remotely for troubleshooting purposes.
- **sroot**: An Avaya services root permission login to gain access to the system remotely for troubleshooting purposes. You cannot gain access to the sroot login directly from a login prompt except on the server console.
- **customer**: A login that the **SMnetSetup** script creates. The default name of the *customer* login is **cust**. The customer must ensure the security of this login account. The *customer* login can run software tools which do not require root access on the Session Manager servers.
- **CDR_User**: A restricted shell login for the Call Detail Recording (CDR) feature. CDR collects call data from the Session Manager server. This login is restricted to sftp access only.
- **asset**: A login created during the installation of the Security Module software. By default, access to the system using this login is disabled.
- **spirit**: A login created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **postgres**: A login created by the installation of the Session Manager software PostgresSQL database system. Access to the system using this login is disabled.
- **init** : An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **inads**: An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **rasaccess**: An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **jboss**: A login created for running the management jboss and is not a login account.
- **wsuser**: A login created for running WebSphere and is not a login account.

Warning:

As of Session Manager Release 6.2, the Access Security Gateway secures the following logins and prevents unauthorized access to the Session Manager servers by non-Avaya services personnel:

- **sroot**
- **inads**
- **rasaccess**
- **init**
- **craft**

Using the customer login account, you can run most of the maintenance and troubleshooting commands. You do not need root access for standard maintenance and support purposes. For more information, see PSN (PSN003925U).

Appendix C: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Related Links

Viewing PCNs and PSNs on page 52
Registering for product notifications on page 53

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

   Note:

   You can select multiple filters to search for different types of documents at one time.
7. Click **Enter**.

Related Links

Product notifications on page 52

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **HI, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
   a. Click **Add More Products**.
   b. Select the appropriate product.
7. In the Product box that appears on your screen:
   a. Select the appropriate release or releases for which you want to receive notifications.
   b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
   c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

Related Links

Product notifications on page 52

Index

N

P

R

S

T

U

V

W