Avaya Aura® System Manager Overview and Specification

Release 6.3
Issue 4
June 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.

License type

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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.

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.

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

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

All 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 7
Purpose 7
Intended audience 7
Document changes since last issue 7
Related resources 8
Documentation 8
Training 9
Viewing Avaya Mentor videos 10
Support 11
Warranty 11
Chapter 2: System Manager overview 13
System Manager overview 13
Feature description 13
Overview 13
Common console 13
Geographic Redundancy 14
Data Replication Service 14
Manage users, public contacts, and shared address 15
Fault management 15
Logging service 16
Log Harvester 16
Scheduler 16
Bulk import and export 16
Bulk import and export using the Excel file 17
Multi Tenancy 19
User provisioning rule 19
Virtualized Environment footprint flexibility 20
Configuration management 20
Element management 20
Group management 20
License management 21
System Manager Communication Manager capabilities overview 21
Granular role-based access control 22
Support for Communication Manager 6.3 features 23
What's new in System Manager 24
Common console enhancements 24
Bulk import and export enhancements 25
Directory synchronization enhancements 25
Scheduler enhancements 25
Security enhancements 26
VMware enhancements 26
WebLM enhancements 26
Reports 27
Discover survivable servers 27

Software Management 27
Avaya Multimedia Messaging element 29
NRP sync feature 29
Simplified Communication Manager upgrades 29
Communication Manager templates 30
Supported servers 31
Software Management infrastructure enhancements 31
Chapter 3: Interoperability 33
Product compatibility 33
Chapter 4: Security 35
Security specification 35
Trust Management 35
External authentication 36
SAML authentication 36
Role Based Access Control 36
Port utilization 37
Chapter 5: Performance specifications 39
Capability and scalability specification 39
Redundancy and high availability 40
Chapter 6: Licensing requirements 41
Licensing requirements 41
Glossary 43
Index 45

Chapter 1: Introduction

Purpose

This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of the product features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Document changes since last issue

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

- Added common console enhancements.
- Added support for System Manager deployment on VMware Release ESXi 5.5 in Virtualized Environment.
- Simplified and automated Communication Manager upgrades by using System Manager Release 6.3.8 Software Management:
    - Upgrades from Communication Manager Release 5.2.1 to Release 6.3.6, a non-System Platform to a System Platform-based upgrade.
    - Upgrades from Communication Manager Release 6.0, 6.1, or 6.2 to Release 6.3.6, a System Platform-based to a System Platform-based upgrade.
    - Preupgrade check to verify if the hardware is supported by the new release, the RAID battery is sufficient, the bandwidth is sufficient, and required files have been downloaded.
    - Automatic upgrade rollback when a System Platform error occurs during the upgrade process. The manual rollback and commit options are available for the

Communication Manager template upgrade. The rollback and commit apply to Communication Manager Release 6.x upgrades.

- Added discovery enhancements that are required for software management.
- Added bulk import and export enhancements by using the Excel file.
- Added the capability to repair the serviceability agent when the alarming functionality of an element fails.
- Added capacity enhancements to increase the scale of SIP users and devices.

Related resources

Documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Implementation		
Installing the Dell™ PowerEdge™ R620 Server	Describes the procedures to install the Dell™ PowerEdge™ R620 Server.	Implementation Engineers and Support personnel
Installing the HP ProLiant DL360p G8 Server	Describes the procedures to install the HP ProLiant DL360p G8 Server.	Implementation Engineers and Support personnel
Installing and Configuring Avaya Aura® System Platform	Describes the procedures to install and troubleshoot System Platform.	Implementation Engineers and Support personnel
Implementing Avaya Aura® System Manager on VMware.	Describes the procedures to install Avaya Aura® System Manager virtual application on VMware in Virtualized Environment. This document includes installation, configuration, initial administration, and basic maintenance procedures.	Implementation Engineers and Support personnel

Title	Description	Audience
Implementing Avaya Aura® System Manager on System Platform	Describes the procedures to install System Manager on System Platform and troubleshoot.	Implementation Engineers and Support personnel
Administration		
Administering Avaya Aura® System Manager	Describes the procedures to configure System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel
Maintenance and Troubleshooting		
Upgrading Avaya Aura® System Manager on VMware	Describes the procedures to upgrade System Manager from the previous releases to Release 6.3.8 on VMware.	Implementation Engineers and Support personnel
Upgrading Avaya Aura® System Manager on System Platform	Describes the procedures to upgrade System Manager from the previous releases to Release 6.3.8 on System Platform.	Implementation Engineers and Support personnel
Troubleshooting Avaya Aura® System Manager	Describes the procedures to troubleshoot the problems during the installation and administration of System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel
Maintaining and Troubleshooting the Dell™ PowerEdge™ R620 Server	Describes the procedures to maintain and troubleshoot the Dell™ PowerEdge™ R620 Server.	Implementation Engineers and Support personnel
Maintaining and Troubleshooting the HP ProLiant DL360p G8 Server	Describes the procedures to maintain and troubleshoot the HP ProLiant DL360p G8 Server.	Implementation Engineers and Support personnel

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title	Type
1A00234 E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236 E	Knowledge Access: Avaya Aura® Session Manager and System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106 W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040 E	Knowledge Access: Avaya Aura®Session Manager and System Manager Implementation	ALE License
5U00050 E	Knowledge Access: Avaya Aura®Session Manager and System Manager Support	ALE License
5U00095 V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura®Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103 W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

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 web site, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://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 site.

✱ **Note:**

Videos are not available for all products.

Support

Visit 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.

Warranty

Avaya provides a 90-day limited warranty on the System Manager software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Additionally, for the standard warranty description of Avaya and the details of support, see **Help & Policies** > **Policies & Legal** > **Maintenance and Warranty Information** on the Avaya Support website at http://support.avaya.com. For additional information, see **Help & Policies** > **Policies & Legal** > **License Terms**.

For more details on the hardware maintenance for supported products, see http://portal.avaya.com/ptlWeb/services/SV0452.

Chapter 2: System Manager overview

System Manager overview

System Manager is a central management system that delivers a set of shared management services and provides a common console for Avaya Aura® applications and systems. You can download System Manager from the Avaya Support website at http:// support.avaya.com or order the System Manager software DVD.

Feature description

Overview

The following sections provide a brief description of the functionality of the feature that System Manager provides in support for various Avaya products. For detailed information on the services available for a specific Avaya product, see the interoperability table in the *System Manager 6.3 Product Offer Definition* on the Avaya Support website at http://support.avaya.com.

Common console

The common console is a common management interface for managing various applications in System Manager. The common console is primarily a framework for the aggregation of management presentation views. The common console framework supports dynamic extendibility and contraction as you add or remove management applications. You can use the Web management console in a variety of scenarios ranging from product-specific management to suite management. The different scenarios can leverage the common look-and-feel, common components, and the behavior.

Geographic Redundancy

The System Manager Geographic Redundancy service replicates the Avaya Aura® element support for two geographically distant System Manager sites with separate subnetworks and across a WAN so that the System Manager management services can change from one site to another when one of the sites or servers fails. The System Manager Geographic Redundancy sites are set up in pairs with each site in a System Manager standalone or System Manager HA configuration. You can designate one server from the pair as the primary System Manager server and the other as the secondary System Manager server.

In normal operation also called sunny-day scenario, the primary System Manager provides all element administration and automatically replicates the administrative changes made on the primary System Manager server to the secondary System Manager server on a batch transaction basis. The secondary System Manager functions in the warm standby mode or the read-only mode and provides a subset of System Manager services, such as the System Manager Geographic Redundancy status or statistics, Inventory, and Authentication and Authorization.

In the event of catastrophic failure or split network, also called rainy-day scenario, you can activate the System Manager server that you designated as secondary to assume full management of all supported Avaya Aura® elements. The elements that support the Active-Standby mode include Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Geographic Redundancy-unaware elements might require manual intervention to gain services from the secondary System Manager server that is active.

The primary and the secondary System Manager servers can be in active mode in the split network scenarios.

After deactivation of the secondary System Manager server, the system administrator selects the database of the primary or the secondary System Manager server as the master database. The System Manager feature provides tools to select the database. After the database recovery and replication, the System Manager Geographic Redundancy servers revert to the normal operation mode, Active-Standby.

Data Replication Service

Data Replication Service (DRS) replicates the data stored on the System Manager server to other element nodes or the slave nodes. DRS uses and extends SymmetricDS, an asynchronous data replication software, for data replication. SymmetricDS supports multiple subscribers and bi-directional synchronization.

SymmetricDS uses Web and database technologies to replicate tables between relational databases in near real time. The system provides several filters while recording the data, extracting the data that must be replicated to a slave node, and loading the data on the slave node.

DRS provides a mechanism wherein elements can specify the data requirements in an XML document. Based on the XML document, DRS creates database triggers on the specified application tables and captures the database events for delivery to the other element nodes. The client nodes then fetch the database events.

Manage users, public contacts, and shared address

Manage users

User Management (UPM) is a shared service that supports a logically centralized data store. Applications can gain access to the data store using System Manager Web Console and obtain the user information that applications need. Administrators or end users do not need to provide user information for each application.

UPM uses data synchronization to achieve a single-point user administration. UPM synchronizes a user data event that is generated at the application level with the central user space and other connected applications. If an enterprise directory is connected, then UPM maintains synchronization at the enterprise level. UPM adapts to the changes that occur in the enterprise directory, specifically additions, deletions, and modifications.

Manage public contacts

As an administrator, you can define public contacts of users in System Manager for an enterprise. You can share the public contacts with all the users in System Manager.

Manage shared address

You can manage the shared address of the users in the enterprise. All users in the enterprise share the common addresses. As an administrator, you can create a new shared address, modify, and delete an existing shared address.

Fault management

The Fault management service presents the status of alarms, traps, and notifications received by System Manager and System Manager components, and the other elements that are integrated with the System Manager SAL agent. The Fault management service maps events to alarms and tracks the state of alarms. Using the Fault Management service, you can acknowledge and clear alarms.

The Alarm management service provides a central point for receiving alarms that System Manager and other components generate. The Alarm management service supports alarm monitoring, acknowledgement, configuration, clearing, and retiring. You can also browse System Manager for historical alarm events.

Logging service

The Logging service provides configuration capabilities and overall management of logs. The Logging service receives and stores log events and harvests file-based logs or local database logs. The log viewer is integrated with the common console to provide consistent presentation of log messages for System Manager and the adopters.

The log viewer displays a list of logs where you can view the details of each log, search for logs, and filter specific logs. The log details include information about the event that generates the log, the severity level of the log. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

Log Harvester

The Log Harvester service manages the retrieval, archival, and analysis of harvested log files stored in hosts or elements on which Serviceability Agent is enabled. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging service through HTTPS. The logging service identifies a successful harvest request related to a harvest profile, accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same computer or on different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface and the status of each archive is available in the user interface table.

Scheduler

The Scheduler service provides a generic job scheduling service for System Manager and the adopting products. The Scheduler service provides an interface to execute a task on demand or on a periodic basis. You can schedule a job to generate an output immediately or set the frequency of the task execution to run on a periodic basis. You can modify the frequency for a periodic job schedule any time. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled jobs can be of three types: system scheduled, admin scheduled, and on-demand.

Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. To import data in bulk, you must provide an XML file or an Excel file as input file. While exporting data in bulk, the system can export the data to an XML file and an Excel file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity Data
- Communication Profile Set
- Handles
- Communication profiles

  The supported communication profiles are CM Endpoint, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, and Presence, and Collaboration Environment.

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

❗ **Important:**

System Manager does not support the bulk import and export of roles.

Bulk import and export using the Excel file

In System Manager, you can import and export user profiles in bulk by using an Excel file and an XML file. To import data in bulk, provide an XML file or an Excel file as input that System Manager supports. When you export the data from System Manager Web Console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the .xlsx format. You can download the Excel file from the User Management page.

Import and export in bulk using the Excel template provides the following features:

- Supports the following types of user information:
  - Basic. The identity attributes of the user that include user provisioning rule name for the user, the tenant, and organization hierarchy details
  - Profile Set. Entries for all communication profile sets for all users

    The Profile Set sheet contains an entry for each communication profile set for a user. The user must set only one communication profile set as true for a user in the **Is Default** column. The value true indicates that the communication profile set of the user is default.
  - Handle. The communication address of the user
  - Session Manager profile

    - Collaboration Environment profile
    - CM Endpoint profile with all attributes of the station communication profile.

      System Manager supports import and export of the CM Agent profile data associated with the user using XML only. You cannot import or export the CM Agent profile data by using Excel. Therefore, with the Excel file bulk import functionality, you cannot create a user with the CM Agent profile. If you export a user with the CM Agent profile, the system exports the user without the agent profile data in the Excel file.
    - Messaging profile
    - CallPilot profile
    - IP Office Endpoint profile
    - CS 1000 Endpoint profile
    - Presence profile
    - Conferencing profile
- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user using the same Excel file. However, you can perform one operation at a time.
- For updation, supports only the partial merge operation.

  Bulk import and export by using Excel does not support complete or partial replace of the user for imports in bulk.

Bulk import and export by using Excel supports a subset of user attributes that XML supports. For example, Excel does not support user contacts, address, and roles.

The Excel file

The sample Excel file contains the sample data of some key attributes of the user. The Excel file provides a description of header fields. When you download the Excel template from the **User Management** page, the values remain blank. To use the Excel file, export some users for reference in an Excel file.

The Excel file provides the login name in the **Basic** worksheet as the key attribute that you use to link the user records in other worksheets.

The login name of the user and the profile set name in the **Profile Set** worksheet are used as key to link to the user records in other worksheets for that user profile.

- Although you can edit the header fields in the Excel template, do not change any details of any headers in the worksheets. The import or export might fail if you change the details of the header.
- Do not change the column position in the Excel file or change the structure of the Excel template.
- Do not sort the data in worksheets.

CM Endpoint communication profile

The Excel file contains all attributes for the CM station endpoint profile. The Excel file provides the station endpoint attributes in more than one worksheets. The parent sheet provides a link to the same user profile record in the child worksheet. The link points to the first record in the child sheet if the user profile contains multiple records in the child worksheet.

Multi Tenancy

Using the Multi Tenancy feature, customers, also known as tenants, can share the same instance of the application, while allowing the tenants to manage users to fit the customer needs as if the application runs on a dedicated environment.

You can manage Multi Tenancy from System Manager web console. System Manager supports the following capabilities:

- View, create, edit, copy, and delete the tenant.
- View, create, edit, and delete tenant administrators for a tenant.
- View, create, edit, and delete the organization hierarchy of the tenant.
- View the tenant hierarchy on the Tenant Management page and User Management page.
- View the tenant associated with a user.
- Create and edit the user associated with a tenant from the User Management page.

System Manager provides a tenant administration dashboard that requires administrator credentials.

By default, the Multi Tenancy feature is disabled. You have to manually enable the Multi Tenancy feature. After enabling the Multi Tenancy feature, you cannot disable the feature.

System Manager supports a maximum of 250 tenant partitions as part of System Manager Multi Tenant Management.

User provisioning rule

The administrator can create rules called user provisioning rules. When the administrator creates a user by using the user provisioning rule, the system displays the default values, the communication addresses, and the communication profiles that are defined in the rule. The administrator need to provide minimal user information.

The administrator can provision the user by using the user provisioning rules from the System Manager web console, Web services, directory synchronization, and bulk import services. You can assign only one user provisioning rule to a user.

System Manager supports creating, editing, duplicating, and deleting the user provisioning rule. You can use the User Management link on the System Manager web console to associate the user provisioning rule with users while creating and editing users.

Virtualized Environment footprint flexibility

Virtualized Environment applications provide a fixed profile based on the maximum capacity requirements. Based on the number of supported users, System Manager offers a flexible footprint profile for customers who do not require the maximum capacity.

The customer can configure VMware CPU and RAM of the System Manager virtual machine based on the following capacity size categories:

- Profile 1 is the default profile that supports 35000 to 250,000 users.
- Profile 2 supports up to 35000 users.

The System Manager Multi Tenancy feature does not support Profile 2.

Configuration management

Configuration management provides a configuration repository for System Manager services. Configuration management is responsible for storing configuration data, also called as profiles, for System Manager services and notifying the services of configuration changes.

You can view and edit a profile of a service using Configuration management.

Element management

Inventory maintains a repository that records elements deployed on System Manager, including their runtime relationships. An element in the Inventory refers to a single or clustered instance of a managed element. Inventory provides a mechanism for creating, modifying, searching, and deleting elements and the access point information from the repository. Inventory retrieves information about elements that are added or deleted from the repository.

Inventory integrates the adopting products with the common console of System Manager. Through Inventory, element type can provide a link that can redirect to the Web page of the element manager. System Manager Web Console displays the links for only specific element types.

Inventory supports the creation and updation of application systems by importing data from an XML file. You can import elements only through the Web console.

Group management

Group and Lookup Service (GLS) in System Manager is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, modifying, searching, and deleting groups and group memberships. Using GLS, you can group resources any way that works best for the business, such as organizing resources by location, organization, and function.

Using GLS, you can create a set of permissions and assign the permissions to different users based on the designations of users. You can distribute different roles to the administrators and restrict the administrators to perform limited tasks on System Manager Web Console. For example, a user with the role of an auditor can only audit limited functionality of the system. An auditor cannot perform any administrative changes on System Manager Web Console.

GLS supports group administration for common resources shared across elements, such as roles and users, and unshared element-specific resources.

As a shared service, GLS reduces the time and effort involved by defining reusable groups of managed resources that more than one application or service require.

License management

System Manager provides Web-based license manager (WebLM) to centrally manage licenses for one or more Avaya software products for your organization. All Avaya applications that use WebLM for license management use WebLM that System Manager provides instead of WebLM on System Platform.

System Manager WebLM supports the Centralized licensing feature for Avaya Aura® Communication Manager.

To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

System Manager Communication Manager capabilities overview

System Manager provides a common, central administration of some of the existing IP Telephony products. Using central administration feature, you can consolidate the key capabilities of the current suite of Integrated Management administration products with other Avaya Management tools on a common software platform. System Manager helps you administer Avaya Aura® Communication Manager, Communication Manager Messaging, Avaya Aura® Messaging, and Modular Messaging. Some features of System Manager include the following:

Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. Using System Manager, you can add, edit, view, or delete the objects through **Communication Manager**.

Endpoint management

Using endpoint management you can create and manage endpoint objects and add, change, remove, and view endpoint data.

Template management

Using Templates, you can specify specific parameters of an endpoint or a subscriber once and reuse the template for subsequent tasks of adding endpoints or subscribers. You can use default templates or add your own custom templates.

The two categories of templates are: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates at any time.

Subscriber management

Using Subscriber Management, you can manage, add, change, remove, and view subscriber data. Subscriber management supports Avaya Aura® Messaging, Communication Manager Messaging, and Modular Messaging objects.

Discovery Management

You can discover specific devices within the network using the Discovery Management capability of System Manager. You can also manage the Simple Network Management Protocol (SNMP) access parameters used for the discovery process. Device discovery discovers your network, including subnets and nodes.

Element Cut Through

Using the Element Cut-Through link, you can gain access to the Communication Manager cut through the Element Cut-Through page. As an administrator, you have permission to gain access to the Communication Manager cut through.

Granular role-based access control

With the Granular role-based access control feature, you can restrict access to Communication Manager resources, such as gateways and servers, and objects on resources, such as Agent Login ID.

Based on the role that a user has, System Manager supports range permissions along with the operation permissions assigned to the user. You can assign permissions or a combination of permissions to users. The permissions include adding, editing, deleting, and duplicating objects. For example, if you assign a range of 1000:4000 and define permissions for Add, Edit, and Delete operations, the user can create, edit, and delete extensions within the range of 1000:4000.

The default value in the specific **Range** field is asterisk (*). If you retain this value, the user has access to the entire defined range.

You can define range-level granular permissions for the following Communication Manager objects:

- Endpoints
- Agent Login ID
- Announcement
- Audio Group
- Best Service Routing Pickup Group
- Holiday Table
- Variables
- Vector
- Vector Directory Number (VDN)
- Vector Routing Table
- Service Hours Table
- Coverage Answer Group
- Coverage Path
- Coverage Remote
- Coverage Time-of-Day
- Group-Page
- Hunt-Group
- Intercom Group
- Pickup Group
- Terminating Extension Group
- Route-Pattern
- Class of Restriction (COR)

Support for Communication Manager 6.3 features

System Manager supports the following features of Communication Manager 6.3:

- System-level limit for the number of concurrent SAT sessions increased to 22. This limit is for login profiles 18 to 69 and for system logins. This limit is applicable to Communication Manager servers with large and extra-large memory. System Manager prevents you from initiating a new session if you exceed the maximum number of concurrent sessions. The system displays an error message if the maximum number of logins is reached.
- Coverage Answer Groups increased to 1500.
- Coverage Answer Group members increased from 8 to 100.
- Locations for endpoints increased to 2000 .

- Route Patterns increased to 2000.
- IP network regions increased to 2000.
- Location qualifier increased to 2000 in AAR and ARS Analysis.
- AAR and ARS Analysis entries increased to 16000.
- ARS Digit Conversion entries increased to 12000.

What's new in System Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® System Manager in Release 6.3.8.

Related topics:

Common console enhancements on page 24
Bulk import and export enhancements on page 25
Directory synchronization enhancements on page 25
Scheduler enhancements on page 25
Security enhancements on page 26
VMware enhancements on page 26
WebLM enhancements on page 26
Reports on page 27
Discover survivable servers on page 27
Software Management on page 27
Avaya Multimedia Messaging element on page 29
NRP sync feature on page 29
Simplified Communication Manager upgrades on page 29
Communication Manager templates on page 30
Supported servers on page 31
Software Management infrastructure enhancements on page 31

Common console enhancements

For enhanced user experience, System Manager Release 6.3.8 provides the following common console changes:

- Provides the **Settings** icon (🔧) to navigate to **Help**, **About**, and **Change Password** links.
- Provides the feature to add a corporate logo on the web console.

- User Preference: You can add a page as your preference by using the plus sign (+) in the top-right corner. The web console displays the link to the page to System Manager. You can delete the user preferences.
- Quick Navigator: You can type the name of the link that you want to search. The web console displays all related links with the search text in the top-right corner of the page. You can click a link to navigate to the specific page.
- The look and feel of the UCM webpages matches with System Manager webpages.

Bulk import and export enhancements

System Manager supports:

- Granular export with user attribute filtering options
- More than one communication profile set
- User provisioning rule name for a user
- Changing login name by using bulk user import using XML and Excel
- Import and export of all attributes of Communication Manager station communication profile by using the Excel file
- Import and export of the Collaboration Environment communication profile by using the Excel file
- Import and export of the CallPilot communication profile by using the Excel file
- Import and export of the Presence communication profile by using the Excel file

Directory synchronization enhancements

LDAP synchronization and authentication with Active Directory 2012.

Scheduler enhancements

System Manager supports:

- Scheduling of the sequential jobs
- Rerunning of the failed jobs
- Rescheduling the failed jobs

Security enhancements

System Manager supports:

- Generation of SHA-2 algorithm-based certificates
- Generation of certificates by using 2048 key size
- Subject Alternative Name for certificate generation. Enables Subject Alternative Name values in the URI format for all System Manager-CA issued identity certificates.

VMware enhancements

With System Manager Release 6.3.8, you can deploy System Manager on VMware vSphere ESXi 5.5.

WebLM enhancements

- Centralized licensing on VMware in Virtualized Environment on System Manager WebLM
- WebLM generates a warning when a system administrator installs a new license file without the non-capacity feature that was present in the existing license file. The system prompts the administrator to confirm or cancel the license file installation. If the administrator chooses to continue, WebLM proceeds with the new license file installation after logging the warning event.

  The log includes details of the license installation, the user name of the person installing the license, and the status whether the administrator confirmed or cancelled the warning. This enhancement applies to the standalone WebLM and System Manager WebLM.

  For example, the customer might have a non-capacity feature, such as ASAI on Communication Manager (FEAT_CM_ASAI_PCKG), in the installed Communication Manager license file on WebLM. When this customer tries to install a new license file without this feature, the customer gets a warning message. The message is to confirm whether the customer intentionally dropped this feature from the license file.

Reports

Avaya Aura® System Manager supports the Reports feature for communication objects. System Manager6.3.8 can add about 350 predefined List and Display Communication Manager configuration reports.

Use Reports to:

- Generate Communication Manager object reports in various formats such as CSV, PDF, and HTML.
- Create and manage reports.
- Edit report parameters.
- Rerun reports.
- Customize the contents of a report.
- Save reports in the System Manager server.
- View and delete reports that are stored in System Manager.
- Save reports to a local computer.
- Email reports to one or more addresses. You can configure an email server to send reports.

You can assign permissions for reports and generate reports for specific custom user.

Discover survivable servers

Create profile and discover SRS and SCS servers

Use the **Create Profiles and Discover SRS/SCS** option to automatically discover survivable remote servers (SRS) and survivable core servers (SCS) from the main Communication Manager. System Manager uses the `list survivable-processor` command to discover the SRS and SCS servers that are associated with the main Communication Manager. The servers that are discovered are stored in **Inventory** > **Manage Elements**.

Additionally, the SRS and SCS servers are automatically added in the System Manager inventory. The Communication Manager servers are automatically identified as survivable servers in **Inventory**.

Software Management

Software Management, a centralized upgrade solution, provides an automatic upgrade of Communication Manager and associated devices, such as Gateways, TN boards, and media modules from a single view. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

The Software Inventory page consists of a collective inventory of different devices arranged in a hierarchy.

When more than one element is selected within a hierarchy, the system creates one scheduler job for the upgrade. Each hierarchy can have only one job scheduled. The system determines the sequence in which the elements must be upgraded. The devices might include:

- Communication Manager
- Communication Manager Messaging
- Utility Server
- Branch Session Manager
- Gateways
- TN Boards
- Media modules

If one of the devices fails to upgrade within the hierarchy, the system might proceed or process the job as failed based on the compatibility of the failed device with the subsequent device.

Important:

You cannot select Communication Manager 5.2.1 and System Platform-based Communication Manager 6.x together. You can upgrade either Communication Manager 5.2.1 systems together or all System Platform-based Communication Manager 6.x systems.

You can perform the following operations by using Software Inventory:

- Get Inventory.
- Analyze software.
- Download.
- Perform a preupgrade check.
- Reset or backup Communication Manager.
- Sequence upgrades.
- Upgrade the following:
    - System Platform-based Communication Manager 6.x
    - Communication Manager 5.2.1
    - All devices and components that run on Communication Manager
- Commit, rollback, or cancel the template upgrade.

Important:

Note that you cannot perform updates by using the **Software Management** > **Software Inventory** link.

However, you can perform the following operations by using **Manage Software** > **Communication Manager**:

- Update Communication Manager, SAMP firmware, and MPC firmware.
- Upgrade Communication Manager 5.x to 5.2.1.

  Note:

  Install System Platform on the supported server before you upgrade Communication Manager.
- Upgrade Gateways, TN boards, and media modules.

Avaya Multimedia Messaging element

System Manager supports Avaya Multimedia Messaging as an element and provides the alarm management service.

NRP sync feature

By using the NRP synchronization feature, users with H.323 phones can move between offices and have appropriate E911 routing for their location.

For the NRP sync feature, ensure that the authoritative Communication Manager **IP Network Region** information is configured in the Session Manager routing table. A Communication Manager server is authoritative for a location if the location contains media gateways and SIP endpoints that are administered on that Communication Manager server.

Therefore, if you make any change to the **IP Network Map** for the **IP Network Region** that are controlled by Communication Manager, the updates are automatically detected. These updates are replicated to the corresponding **Location** entries in the Session Manager routing table.

Simplified Communication Manager upgrades

Avaya Aura® System Manager Release 6.3.8 Software Management has enhanced infrastructure to simplify and automate Avaya Aura® Communication Manager upgrades.

Customers and business partners can avail the following benefits while performing Communication Manager upgrades:

- Fully automated upgrade from Communication Manager Release 6.0, 6.1, and 6.2 to 6.3.6 by using Software Management. System Platform and the Communication Manager template and patches are automatically upgraded from System Manager.
- Partially automated upgrade from Communication Manager Release 5.2.1 to 6.3.6. System Platform is not automatically installed as part of the upgrade. Only the Communication Manager template and patches are automatically upgraded from System Manager when you install System Platform on the supported server.
- Preupgrade checks to ensure that the Communication Manager hardware and IP network environment support the Communication Manager upgrade. This function increases, the rate of successful upgrade.
- Job sequencing and job chaining of all Communication Manager component upgrades, which minimizes the wait time and delay between different upgrade tasks. For example, upgrades of media modules, TN Boards, and gateways that are associated with the upgraded Communication Manager. The result is a faster Communication Manager upgrade.
- Eliminated or reduced human intervention during the upgrade of Communication Manager and associated elements, reducing the potential for errors.
- Starting and monitoring upgrades that centrally reduces or eliminates the need for onsite visits
- Scheduling of Communication Manager upgrades during off-hour maintenance windows, with System Manager performing the entire upgrade.

Communication Manager templates

Using System Manager Software Management, you can upgrade the following Communication Manager templates:

- Duplex CM Main/Survivable Core with SAL and Communication Manager.
- Simplex CM Main/Survivable with SAL,Communication Manager, Communication Manager Messaging, and Utility Services.
- Simplex Survivable Remote with SAL, Communication Manager, Branch Session Manager, and Utility Services.
- Embedded CM Main with SAL, Communication Manager, Communication Manager Messaging, and Utility Services.
- Embedded Survivable Remote with SAL, Communication Manager, Branch Session Manager, and Utility Services.

You can use the templates in both the fully automated process and the partially automated process. However, in the partially automated process:

- You cannot upgrade System Platform from Software Management.
- To automatically upgrade the Communication Manager template and patches from System Manager, you must install System Platform.

For more information about the two processes, see Simplified Communication Manager upgrades on page 29.

Supported servers

For full and partial automated upgrades, you can perform upgrades on the following Avaya Aura® Communication Manager servers:

- Servers that support upgrade of Communication Manager 6.0, 6.1, and 6.2 to Release 6.3.6:
    - S8510 with increased 8GB memory and HDD
    - S8800 with increased 8GB memory and HDD
    - S8300D
    - Common Server R1 Dell R610, HP DL 360 G7
    - Common Server R2 Dell R620, HP DL 360p G8
- Servers that support upgrade of Communication Manager 5.2.1 to Release 6.3.6:
    - S8510 with increased 8GB memory and HDD
    - S8800
    - S8300D

Software Management infrastructure enhancements

Avaya Aura® System Manager provides the following infrastructure enhancements to simplify the Communication Manager upgrade process and to support other Avaya Aura® applications in future releases of System Manager:

- System Manager collects all the needed upgraded information from the administrator at the beginning of the upgrade process workflow. Communication Manager and other Avaya Aura® applications then do not need to continually interact with System Manager during a Communication Manager upgrade.
- Where possible, steps that are part of the System Platform and Communication Manager templates upgrade are automated.

- The Element Inventory page in Software Management shows all Communication Manager instances, gateways, media modules, TN boards, and System Platform server information in a single hierarchical view. In previous versions of Software Management, all elements were on separate tabs. Administrators can now select the Communication Manager instances and associated elements to be upgraded.
- The Element Inventory page provides a list of common element information in a single table structure, for example, hardware, platforms, release, and versions.

System Manager also provides the following new features:

- New SNMP Access Profile configuration area : To centrally configure access credentials for an SMNP discovery. This feature is added to the System Manager web console and is now a part of the Software Management discovery and inventory process.
- Preupgrade checks: To ensure that all aspects of the upgrade environment are correct. The checks are as follows:
    - RAID battery check
    - Hardware compatibility check
    - Required files download check
    - CDOM credentials check
    - Disk space check
    - Sufficient memory check
    - Version compatibility check
    - Version compatibility check
    - Bandwidth is sufficient check
- Rollback and Failure Scenario feature options: To run **Auto Rollback** for the Communication Manager template that has a System Platform error during the upgrade process.

  A Manual **Rollback** / **Commit** option is available if the **Auto Commit** option is not selected during the upgrade. The **Rollback** / **Commit** feature applies to Communication Manager 6.x Release upgrades.
- Simultaneous upgrade: For System Manager Software Management to simultaneously upgrade a maximum of five Communication Manager and all associated elements.

Chapter 3: Interoperability

Product compatibility

For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Chapter 4: Security

Security specification

As the management console for some of the Avaya products, System Manager must be resilient to attacks that might cause service disruption, malfunction, or unauthorized access or modification of the data. System Manager as part of the Avaya Aura® solution must be protected from security threats such as the following:

- Unauthorized access or modification of data
- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Web-based attacks that includes Cross-Site Scripting and Cross-Site Forgery

For information about security-related considerations, features, and services for System Manager, see *System Manager Release 6.3 Security Guide* available on the Avaya Support website at https://support.avaya.com/security.

Related topics:

Trust Management on page 35

Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices thereby enabling a secure, inter-element communication. Trust Management provides Identity (Server) and Trusted (Root/CA) certificates that applications can use to establish mutually authenticated TLS sessions.

System Manager uses a third-party open source application as a Certificate Authority, Enterprise Java Beans Certificate Authority (EJBCA), to issue Identity and Trusted certificates to applications through SCEP.

External authentication

You can configure System Manager to authenticate administrative users using external authentication services, such as an enterprise directory, Kerberos, or a RADIUS server. An administrative account is provisioned within System Manager during installation for initial access.

System Manager supports the following authentication authorities:

- Local users
- External RADIUS users
- External LDAP users
- External Security Assertion Markup Language (SAML) users

The authentication scheme policy determines the order in which you can use the authentication authorities. The authentication servers policy controls the settings for the external SAML, LDAP, RADIUS and KERBEROS servers.

Related topics:

SAML authentication on page 36

SAML authentication

For enterprise level Single Sign On, System Manager provides Security Assertion Markup Language (SAML) authentication. System Manager uses SAML implementation version 2.0 of OpenAM Release 9.5.4 to provide SAML based authentication with external Identity Providers. System Manager uses Web Browser Single Sign On profile of SAML authentication.

Role Based Access Control

In System Manager, you require appropriate permissions to perform a task. The administrator grants permissions to users by assigning appropriate roles. Role Based Access Control (RBAC) in System Manager supports the following types of roles:

- Built-in
- Custom

Using these roles, you can gain access to various elements with specific permission mappings.

Built-in roles are default roles that authorize users to perform common administrative tasks. You can assign built-in roles to users, but you cannot delete roles or change permission mappings in the built-in roles.

Port utilization

System Manager 6.3 Port Matrix lists all the ports and protocols that System Manager uses. Avaya Direct, BusinessPartners, and customers can find the port matrix document at http://support.avaya.com/security. On the Web page, select the Avaya Product Port Matrix Documents link, and click the System Manager 6.3 Port Matrix document.

You can gain access to the port matrix document only after you log in to the Avaya Support site using the valid support site credentials.

Chapter 5: Performance specifications

Capability and scalability specification

Capacity	Maximum limit	Notes
Administrator logins	250	
Simultaneous logins	50	
Endpoints	250,000	Includes all types of endpoints
SIP endpoints	125,000	
End users	250,000	
Messaging mailboxes	250,000	
Contacts per user	250	
Public contacts	1000	
Personal contact lists per user	1	
Members in a personal contact list	250	
Groups	300	
Members in a group	400	
Elements	25,000	
Communication Managers	500	
Session Managers	12	
Branch Session Managers	250	
B5800 Branch Gateways	2000	
Roles	200	
Roles per user	10	
Licensing clients	1000	
Trust management clients	2500	

Capacity	Maximum limit	Notes
Tenants (System Manager Multi Tenant)	250	

Redundancy and high availability

System Manager supports three types of redundancy: cold standby, High Availability (HA), and Geographic Redundancy.

Cold Standby:

In cold standby, a backup server acts as a failover server when the main server fails. The two servers must be on the same IP subnet and must have the same IP address and Hostname. When the main server is active, turn off the power to the cold standby server. You must create a regular backup of the main server database such that you activate the cold backup server using the most recent information. You must manually perform the backup and activate the cold standby server.

High Availability:

In High Availability, the active and standby System Manager servers must be on the same IP subnet and must the same IP address and Hostname. In addition, the two System Manager servers must be within 100 meters distance. The system automatically activates the standby System Manager.

Geographic Redundancy:

System Manager Geographic Redundancy service replicates Avaya Aura® element support for two geographically distant System Manager sites with separate subnetworks and across a WAN so that you can change the System Manager management services from one site to another when one of the sites or servers fails. The System Manager Geographic Redundancy sites are set up in pairs, with each site in a System Manager standalone or System Manager HA configuration. One of the server from the pair is designated as the primary System Manager server and the other is designated as the secondary System Manager server.

Chapter 6: Licensing requirements

Licensing requirements

When you place an order for the following products using the Avaya Solution Designer or Enterprise Configurator, you can choose to include a new System Manager or an upgrade of System Manager as an entitlement:

- New Communication Manager, Avaya Aura® Session Manager, CS 1000, or B5800 Branch Gateway
- Upgrade of Communication Manager, Avaya Aura® Session Manager, CS 1000, or B5800 Branch Gateway

Additionally, you can add the System Manager DVD and the System Manager server to the order.

Glossary

Active-standby (Auto)

Active-Active: The elements leverage the services of the primary and the secondary System Manager servers. The system functions in this mode when the enterprise network splits.

Active-standby (Manual)

Active-Standby: The elements communicate with the active System Manager server. The mode is also called Active-Standby Auto. In the normal operation scenario, the primary System Manager server is active and the secondary System Manager server is in the standby mode. The primary System Manager server continues to manage elements until the primary System Manager server becomes unavailable. If the primary System Manager server fails and the administrator activates the secondary System Manager server, the elements automatically switch to the secondary System Manager server.

Elements

An element is an instance of an Avaya Aura® network entity managed by System Manager, for example, a Session Manager server or a Communication Manager server.

Geographic Redundancy-aware element

An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3.

Geographic Redundancy-unaware element

An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager release earlier than 6.3.

Primary System Manager server

The first or the master System Manager server in a Geographic Redundancy setup that serves all system management requests.

Secondary System Manager server

The System Manager server that functions as a backup to the primary System Manager server in a Geographic Redundancy setup. The secondary System Manager server provides the full System Manager functionality when the system fails to connect to the primary System Manager server.

Index

Numerics

2048 as default key size 26
  System Manager 26

A

about reports 27
Access Control 36
Access to administrative users 24
  System Manager 24
Active Directory 2012 25
  LDAP authentication 25
  LDAP synchronization 25
application instances 20
architecture 13

B

Built-in roles 36
bulk export 16, 17
bulk import 16, 17
bulk import and export 16
Bulk import and export 25
bulk import and export using Excel 17

C

capability and scalability specification, ... 39
Centralized licensing 21
  Communication Manager 21
Centralized licensing on VMware 24
  WebLM 24
client host ID 26
  WebLM 26
CM station data 17
  export 17
  import 17
CM Station profile 25
  Excel 25
common console 13, 24
  enhancements 24
Communication Manager 30
Communication Manager templates 30
communication manager upgrades 29
company logo 24
compatibility matrix 33
configuration management 20
courses 9
Create profile and Discover SRS and SCS servers ... 27
custom reports 27
Custom roles 36

D

data replication 14
data replication service 14
Directory Synchronization 25
Discover SRS and SCS servers 27
Discover survivable servers 27
DRS 14

E

enhancements 24, 25
  Bulk import and export 25
  common console 24
ESXi 5.5 24
  VMware 24
excel 25
  Bulk import and export 25
Excel 17, 25
  CM Station profile 25
  import 17
export 16, 25
  Excel 25
  user data 16, 17
export CM station data 17
export to Excel 17
  user data 16, 17
external authentication 36

F

failed jobs 25
  rerun 25
  reschedule 25
fault management 15
feature description 13
  overview 13
footprint flexibility 20

G

Geographic Redundancy 14
geographical redundancy 40
granular export 24, 25
    System Manager 24, 25
Granular role-based control 22
Group management 20

H

High Availability 40

I

import 16, 25
    Excel 25
    user data 16, 17
import CM station data 17
import from Excel 17
    user data 16, 17
infrastructure enhancements 31
Install WebLM with client host ID 26
Integrated Management transition 27
intended audience 7

L

LDAP authentication 25
    Active Directory 2012 25
LDAP synchronization 25
    Active Directory 2012 25
legal notice 2
license 41
license management 21
licensing requirements 41
log harvester overview 16
log harvesting 16
log viewer 16
logging 16
logging service 16

M

manage 15
manage application instances 20
manage elements 20
manage license 21
manage users 15
managing users 15
Multi Tenancy 19
Multimedia Messaging 29
    System Manager 29

N

NRP sync 29
NRP sync feature 29

O

overview 13
    System Manager 13
Overview 13, 21
    Communication Manager capabilities overview ... 21
    feature description 13
    System Manager; overview 21

P

port utilization 37
product compatibility 33
provision 19
    users 19
public contacts 15

Q

Quick Navigator 24

R

RBAC 22, 36
Redundancy 14
related documentation 8
reports 27
requirements 41
    licensing 41
rerun 25
reschedule 25
role based access control 36
Roles 36
rules 19

S

SAML authentication 36
schedule sequential jobs 25
scheduler 16
scheduler overview 16

scheduler service 16
security specification 35
sequential job 25
  schedule 25
servers 31
Service Profile Management 20
setting icon 24
SHA-2 algorithm-based certificates 24, 26
  System Manager 24, 26
shared addresses 15
simplified communication manager upgrades 29
Single Sign-On 36
Software Inventory 27
software management 31
Software Management 27
  System Platform-based upgrades 27
software management infrastructure enhancements . 31
specification 39
  capability 39
  scalability 39
support 11
  contact 11
supported 31
supported servers 31
sync 29
System Manager 14, 22, 24–26, 29
  2048 as default key size 24, 26
  Active Directory 2012 24
  Geographic Redundancy 14
  granular export 24, 25
  Granular role-based access control 22
  Multimedia Messaging 29
  RBAC 22
  SHA-2 algorithm-based certificates 24, 26
System Manager overview 13
System Manager support for Communication Manager 6.3 features 23
  capacities 23
System ManagerNew in this release 24
  what is new 24

T

templates 30
Tenant Management 19
training 9
trust management 35

U

UPR 19
User preferences 24
user profile management 15
user provisioning rule 19
users 15

V

VE 24
  ESXi 5.5 24
videos 10
Virtualized Environment footprint flexibility 20
VMware 26
  enhancements 26

W

warranty 11
WebLM 21, 24, 26
  Centralized licensing on VMware 24, 26
  install with client host ID 26