Administering Avaya Aura™ Session Manager

03-603324, Issue 2.1
Release 5.2
August 2010

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

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

Third-party components

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

Preventing toll fraud

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

Avaya fraud intervention

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

Trademarks

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

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: Getting Started

Introduction

This book provides information on setting up Avaya Aura™ Session Manager instances and includes procedures for

- Configuring, and monitoring Session Manager instances
- Using the System Manager Common Console
- Creating administrator accounts
- Administering network routing for Session Manager and various SIP entities

Intended audience

This book is intended primarily for those individuals who are responsible for configuring Session Manager. It is also intended for administrators who configure Network Routing Policy (NRP), Session Manager instances, and network and SIP firewalls.

This book is also useful for those who are interested in information about specific features, and the Avaya personnel responsible for configuring and supporting Session Manager.

Required skills and knowledge

The audience is expected to have some experience installing Avaya products and be able to perform administration procedures. They must also have a basic understanding and working knowledge of the following areas:

Operating systems in general	TCP/IP	SSH	SIP
Graphical and command line interfaces such as Windows and Linux	FTP and SFTP	LAN/WAN	Hostname/DNS

Overview

System Manager is a central management system that delivers a set of shared management services and a common console across multiple products. System Manager includes the following shared management services for Session Manager:

- Asset Management: Manages the resources and licenses.
- User Management: Provides central user administration of all user properties. The centralized administration reduces the need for replicating the user's data across multiple products.
- Monitoring: Provides a central point for receiving alarms from the Secure Access Link (SAL) Agents. Supports alarm monitoring, acknowledgement, configuration, clearing, and retiring. It can also send customer SNMP traps to an external SAL Enterprise or Enterprise Management System (EMS). It also provides a central point for receiving log events formatted in the common log format from the SAL Agents.
- Network Routing Policy: Defines all SIP entities in the network and how calls route to them.
- Applications: Provides an interface to manage the instances of applications running on the different servers.
- Security: The System Manager console provides authentication of administrators and authorization by applying role-based access control. It also provides trust and certificate management where trust management is the definition of trust relationships between hosts and services, and certificate management is the lifecycle management of identity certificates.
- Settings: Provides backup and restore capability including backing up and restoring configuration data, and secure file copy.
- Session Manager: Provides configuration and monitoring of Session Manager instances, setting of tracing properties for security modules, and management of call bandwidth usage.

The System Manager Common Console is the management interface for Session Manager. You must log on to the System Manager Common Console to perform any administration or configuration.

Note:

This book contains extra information about System Manager administration which might not have direct relevance for Session Manager administration. These additional System Manager administration specific sections are listed as follows:

- Asset Management/Licenses (WebLM)
- User Management/Manage Roles

- User Management/Importing of Users
- User Management/Presence ACL
- Administering application instances
- Administering service profiles for applications/IAM fields settings

Logging onto the System Manager web interface

The System Manager web interface is the main interface to the Avaya Aura™ System Manager 5.2. You must log onto the Management Console web interface before you can perform any tasks.

Important:

System Manager does not support the browser back functionality. It is not advisable to use the browser back button to navigate to the previously visited pages. Use of the back button may give unpredictable results. You must use the System Manager menu to navigate across pages.

Prerequisites

You must have a user account to log on to the System Manager 5.2 interface. Contact your system administrator if you do not have an user account.

1. In the browser enter the Avaya Aura™ System Manager URL (`https://<SERVER_NAME>/SMGR`) and click **Enter**.
2. In the **User Name** field enter the user name.
3. In the **Password** field enter the password.
4. Click **Log On**.

   If your user name and password:

   - Match an authorized System Manager user account, System Manager displays the Avaya Aura™ System Manager Home page with Avaya Aura™ System Manager Version *version_number* and the Legal Notice display text box. What you see and can do from there depends on your user role.
   - Do not match an authorized System Manager user account, System Manager displays an error message and prompts you to enter the user name and password so that you can log in again.

SIP Application Server

Overview of SIP Application Server

The SIP Application Server (SIP A/S) is a scalable, highly available and high-performance server for the development and deployment of real-time, multimedia, presence-enabled IP communications applications. The SIP Application Server is composed of the following components:

- Service Director — This performs decision-based routing of incoming SIP messages to the Service Host for processing.
- Service Host — This hosts applications and interacting with external entities. It processes SIP messages received from Service Directors and other SIP end points.
- Management Server — This hosts the SIP Application Server management console for monitoring component statistics.

For Session Manager users, this chapter shows how to monitor the various SIP A/S performance data.

Starting the SIP Application Server management console

1. In the Avaya Aura™ System Manager, click **Applications** > **SIP A/S**.
2. On the SIP A/S Connection Details page, enter the host name and administration port of the primary Management Server of the cluster.

   The default port as 5759 is filled in. This should not be changed.
3. Click **Connect**.

   For more information, see the *Avaya Aura™ System Manager online Help system*.

SIP A/S Connection Details field descriptions

Name	Description
Primary Hostname	The name of the machine hosting the primary Management Server of the SIP Application Server cluster to which you are connecting. This is mandatory.
Primary Port	The administration port of the primary Management Server. This is mandatory.
Backup Hostname	The name of the machine hosting the backup Management Server of the SIP Application Server cluster to which you are connecting.
Backup Port	The administration port of the backup Management Server.
Connect	Connect to the SIP Application Server cluster.

About SIP Application Server Management Console

The SIP Application Server Management Console enables viewing of the following details:

- System Status
- Service Director statistics
- Service Host statistics

Warning:

Changing the existing configurations using the SIP Application Server Management Console voids your product warranty.

The System Status page of the SIP Application Server Management Console shows a graphic representation of the SIP Application Server cluster. A status icon next to each cluster element node specifies the operational status of that element, as defined in the following table.

Status Icon	*Cluster element status*
Green check symbol	The cluster element is running.
Red cross mark symbol	The cluster element is in an error state.
Yellow triangle symbol	Other configuration error.

Viewing Service Director Statistics

1. On the SIP Application Server Management Console, click **Monitoring** > **Statistics** > **Service Directors**.
   The Statistics: Service Directors page opens showing details of the listed Service Director.
2. Select the Service Director instance and click **View**.
   The Service Director Statistics page opens where you can view statistics for the selected Service Director instance.

Statistics: Service Directors field descriptions

Name	Description
Id	A number assigned to the Service Director.
Host Name	The host name or IP address of the Service Director.
Administrator Port	The administration port number of the Service Director.
Version	The version of SIP Application Server.
Status	The operational state of each the Service Director. Options include: • RUNNING: The Service Director has been started and is operating normally. • DOWN: The Service Director is unavailable. • UNKNOWN: The operational status of the Service Director cannot be determined. • RESTARTING: The Service Director is rebooting from a previously up state and will soon become available. • STARTING: The Service Director is starting up from a down state and will soon become available. • TESTING: The Service Director is in testing mode. • HALTED: The Service Director is stopped. • HALTING: The Service Director is stopping.

Name	Description
	• DISABLED: The Service Director is disabled but can still receive configuration. • BOOTERROR: The Service Director has encountered an error during start-up.
Restart Req?	Indicates whether the Service Director requires a restart.

Service Director Statistics field descriptions

Some of the important fields are listed below:

Name	Description
Status	The operational state of the Service Director.
Up Time	The time since Service Director start-up.
Received Request Count	The number of SIP request messages received by the Service Director since start-up.
Sent Response Count	The number of SIP response messages sent by the Service Director since start-up.
Dropped Requests Count	The number of requests not forwarded to a Service Host as a result of traffic throttling initiated by Self Awareness and Preservation rules.
Bounced Requests Count	The number of 503 responses sent as a result of traffic throttling initiated by Self Awareness and Preservation rules.

Viewing Service Host Instance Statistics

1. On the SIP Application Server Management Console, click **Monitoring** > **Statistics** > **Service Hosts**.
   The Statistics: Service Hosts page opens showing the list of Service Hosts.
2. In the section Service Host Instance Statistics, select a Service Host instance and click **View**.
   The Service Host Statistics page opens where you can view statistics for the selected Service Host instance.
3. In the section View Statistics from Last 24 Hours, select a statistic record to view and click **View Data**.

The Statistics Detail View page opens where you can view the 24 hour details for the selected statistics.

4. On the Statistics Detail View page, click **Export CSV** to export the data into comma-separated value format for display in a spreadsheet application.

Statistics: Service Hosts field descriptions

Name	Description
Id	A number assigned to each Service Host.
Host Name	The host name or IP address of the Service Host.
Administrator Port	The administration port number of the Service Host.
Version	The version of SIP Application Server.
Status	The operational state of each Service Host. Options include: • RUNNING: The Service Host has been started and is operating normally. • DOWN: The Service Host is unavailable. • UNKNOWN: The operational status of the Service Host cannot be determined for some reason. • RESTARTING: The Service Host is rebooting from a previously up state and will soon become available. • STARTING: The Service Host is starting up from a down state and will soon become available. • TESTING: The Service Host is in testing mode. • HALTED: The Service Host is stopped. • HALTING: The Service Host is stopping. • DISABLED: The Service Host is disabled but can still receive configuration. • BOOTERROR: The Service Host has encountered an error during start-up.
Restart Req?	Indicates whether the Service Host requires a restart.

View Statistics from Last 24 Hours

Statistic	The statistic being monitored.
Peak (Cross-Cluster Total)	The highest value observed for this attribute from totalling the attribute values across all Service Hosts.
Peak (Individual)	The highest individual value observed for this attribute over the last 24 hours, amongst all individual Service Hosts.
Average	The current average of the attribute's values totalled across all Service Hosts over the last 24 hours.

Some of the important fields are listed below:

CPU Usage Percentage	The percentage CPU usage on the Service Host installation platform.
Total number of requests received	Total number of SIP message requests received by the Service Host.
Active SIP Transactions	The number of new active transactions currently being processed by the Service Host.
Free Physical Memory (Mb)	The amount of free physical memory available on the Service Host hardware platform.
Container Sip Application Sessions	The number of SIP application sessions currently being processed by the Service Host. This equals the sum of the number of sessions which represent subscriptions from endpoints and the number of currently active calls handled by the Session Manager.

Service Host Statistics field descriptions

Some of the important fields are listed below:

Name	Description
SIP Protocol Version	The SIP protocol version used by the Service Host.
Status	The operational state of the Service Host.
Up Time	The time since Service Host initialization.
Running	The running state of the Service Host.

Name	Description
SIP Application Sessions	The number of SIP Application Sessions currently being processed by the Service Host.
Active SIP Application Sessions	The number of SIP transactions currently being processed by the Service Host.

Summary Statistics

Name	Description
SIP Initial Requests Per Second In	SIP initial requests per second received by the Service Host since last reported.
SIP Initial Requests Per Second Out	SIP initial requests per second sent from the Service Host since last reported.
Unsupported URI Count	The total number of unsupported URIs that have sent SIP requests to the Service Host.
Total Requests In	The total number of SIP requests received by the Service Host.
Total Requests Out	The total number of SIP requests sent by the Service Host.
Total Responses In	The total number of SIP responses received by the Service Host.
Total Responses Out	The total number of SIP responses sent by the Service Host.
Transaction Quantity	The total number of transactions that have taken place through the Service Host.

Chapter 2: Asset Management

Licenses (WebLM)

WebLM Overview

Licensing of a software product is a formal permission granted to an individual or an enterprise that purchases the product to use the product. An individual or an organization is obliged to use only the authorized number of copies of the purchased product.

WebLM is an out of box licensing solution and is a part of the Avaya Aura™ System Manager initiative. WebLM ensures that organizations use only the authorized number of licenses of a software product. All Avaya software product houses can use WebLM to track the licenses of their product in an organization.

As WebLM is Web-based, it facilitates easy and faster tracking of licenses. Using WebLM, an administrator can track and manage licenses of multiple Avaya software products installed in an organization from a single location. To track and manage licenses in an organization, WebLM requires a license file.

A license file is an Extensible Markup Language (XML) file. The file contains information regarding the product, major release, the licensed features of the product, and the licensed capacities of each feature purchased by the organization. The licensed capacities of a feature are known as, feature licenses. During the purchase of an Avaya software product, an organization obtains the license file for the product. Avaya issues a license file for the Avaya software product purchased by an organization.

Licenses generated from RFA are tied to the host ID of the WebLM server. The host ID of the server can be viewed in the Viewing Server Properties section.

Accessing WebLM

Prerequisites

You must have permissions to access the WebLM application.

1. Enter the URL for accessing Avaya Aura™ System Manager in the browser.
2. Log in to the Avaya Aura™ System Manager web interface as an administrator.
3. On the System Manager Home page, click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.

Related topics:

WebLM Home field descriptions on page 29

Obtain license file

The WebLM server, when installed in an Avaya software product or solution, requires a license file to provide its license entitlements. License files are first generated using Remote Feature Activation (RFA) by any one of the following individuals:

- An Avaya Business Partner
- An Avaya Global Services (AGS) associate

To generate a new license file, the RFA user requires the following information:

- The primary host ID of the WebLM server
- The customer name
- The SAP order number

Note:

Host ID is the MAC address of the computer on which WebLM is installed. WARNING: The host ID specified to the RFA team is embedded in the license file. The license file can be installed only if the host ID of the target computer matches the host ID in the license file. Therefore, while requesting a license file, companies must specify the correct host ID of the computer where the WebLM server is installed.

Related topics:

Installing license file on page 27

Installing license file

Prerequisites

- You must be logged in as an Administrator to perform the installation
- You must have a standard license file obtained from Remote Feature Activation (RFA) team.
- Ensure that the host ID of the server on which you want to install the license file must match with the host ID specified in the license file.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click **Install License** in the left navigation pane.
4. On the Install License page, enter the license file path. You can also click **Browse** to select the license file.
5. Click **Install** to install the license file.

Result

On the successful installation of the license file, WebLM displays a message that the installation of license file is successful.

Related topics:

Obtain license file on page 26
Install License field descriptions on page 29

Viewing license capacity for a licensed product

Prerequisites

The WebLM Administrator must have installed the standard license file on the WebLM server for the licensed product.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.

3. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
4. Click **View License Capacity** in the left navigation pane.

Related topics:

View License Capacity field descriptions on page 30

Viewing peak usage for a licensed product

Prerequisites

The WebLM Administrator must have installed the standard license file on the WebLM server for the licensed product.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
4. Click **View Peak Usage** in the left navigation pane.

Related topics:

View Peak Usage field descriptions on page 31

Removing license file

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click **Uninstall License** in the left navigation pane.
4. On the Uninstall License page, select the license file that you want to delete.
5. Click Uninstall to remove the license file from the WebLM server.

Related topics:

Uninstall License field descriptions on page 31

Viewing server properties

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click **Server Properties** in the left navigation pane.
   Host ID is the MAC address of the computer on which WebLM is installed.

Note:

The host ID specified to the RFA team is embedded in the license file. The license file can be installed only if the host ID of the target computer matches the host ID in the license file. Therefore, while requesting a license file, you must specify the correct host ID of the computer where the WebLM server is installed.

Related topics:

Server Properties field descriptions on page 32

WebLM Home field descriptions

Use this page to view the information about the product(s) and the associated license file(s) installed on the WebLM server.

Field	Description
Product Name	The name of the product for which the license file is installed.
Product Version	The version of the product for which the license file is installed.
Type of License	The type of license file installed for the product.
Date of Installation	Date and time of installation of license file.

Related topics:

Accessing WebLM on page 26

Install License field descriptions

Use this page to install the license file of a product on the WebLM server.

Field/Button	Description
Enter License Path	The path where you have saved the license file.
Browse	Opens the dialog box that allows you to select the license file.
Install	Installs the product license file.

Related topics:

Installing license file on page 27

View License Capacity field descriptions

Use this page to view the total number of feature licenses of a feature that the organization has purchased and the current allocation of these purchased licenses.

Field	Description
Feature (Keyword)	The display name of the licensed features of the product and the keywords of each feature. These keywords are used to represent the licensed feature in the license file.
Expiration Date	The date when the license for the feature would expire.
Licensed	The number of feature licenses purchased by the organization for each licensed feature. The system gathers the number of feature licenses information from the license file.
Acquired	The Number of feature licenses that are currently in use by the licensed application. The features that are of type Uncounted, the column displays *Not counted*.

The Acquired Licenses table displays information about the licenses acquired by the licensed application. You can view this table only if the licensed product has acquired feature licenses.

Field	Description
Feature	The feature keyword for each licensed feature that is currently acquired by a licensed application.
Acquired by	The name of the licensed application that has acquired the license.
Count	The number of feature licenses that are currently acquired by the licensed application.

Related topics:

Viewing license capacity for a licensed product on page 27

View Peak Usage field descriptions

Use this page to view the usage information of feature licenses of a licensed application for different time intervals.

Field	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. These keywords are used to represent the licensed feature in the license file.
Currently Allocated	The number of feature licenses purchased by the organization.
Usage: qty/%	The number of feature licenses for each licensed feature that a licensed application is currently using. The column also displays the percentage of usage. For example, if 50 is the available feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%.
Peak Usage (last 7 days): qty/%	The highest number of feature licenses for each licensed feature that has been used in the last seven days. For example, if the peak usage for a feature license in the past seven days is 25 and the number of available licenses during these seven days was 50, then the column displays 25/50%.
Peak Usage (last 30 days): qty/%	The highest number of feature licenses for each licensed feature that has been used in the past 30 days. For example, if the peak usage for a feature license in the past 30 days is 50 and the number of available licenses during these 30 days was 50, then the column displays 50/100%
Time of Query	The date and time when the last usage query for WebLM was executed
Status	The success or failure of the last usage query executed for WebLM server.

Related topics:

Viewing peak usage for a licensed product on page 28

Uninstall License field descriptions

Use this page to uninstall a license file from the WebLM server for a licensed product.

Field/Button	Description
Installed License File	The name of the license files that are currently installed on the WebLM Server.

Field/Button	Description
Product(s)	The products for which licenses are installed on the WebLM server..
SID	The System ID of the license file.
Select Checkbox	Allows you to select the license files that you want to un install from the WebLM server.
Unistall	Removes the selected license files from the WebLM server.

Related topics:

Removing license file on page 28

Server Properties field descriptions

Use this page to view the MAC Address of the server. The Server Host ID section displays the MAC Address of the server. The server can have more than one MAC Address assigned to it. The first MAC Address is the primary MAC Address and subsequent MAC Addresses are designated as secondary and so on. The primary MAC Address is recommended for use in the license file.

Note:

In case of a Solaris server where the MAC Address is not available (e.g. in a zoned environment), WebLM retrieves the hostid (8 – digit hexadecimal address) of the server and adds leading zeros before using the resulting 12 – digit ID.

Related topics:

Viewing server properties on page 29

Enterprise Licensing

Viewing feature license information of a product

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.

3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **View by Feature** in the left navigation pane.

Related topics:

View by Feature field descriptions on page 40

Viewing connectivity status of local WebLM servers for a product

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **View by Local WebLM** in the left navigation pane.

Related topics:

View by Local WebLM field descriptions on page 40

Configuring enterprise

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Enterprise Configuration** in the left navigation pane.
5. Enter the appropriate information.
6. Click **Submit**.

Related topics:

Enterprise Configuration field descriptions on page 41

Validating connectivity to local WebLM servers for a product

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Local WebLM Configuration** in the left navigation pane.
5. On the Local WebLM Configuration: View Local WebLMs page, select the local WebLM servers that you want to validate for connectivity.
6. click **Validate Connectivity** to query the selected local WebLM servers.

Result

The **status** column on the Local WebLM Configuration: View Local WebLMs page of the selected WebLM servers displays whether the connection request made to the local WebLM server is successful or not.

Related topics:

View Local WebLMs field descriptions on page 43

Adding a local WebLM server

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Local WebLM Configuration** > **Add Local WebLM** in the left navigation pane.
5. On the Local WebLM Configuration: Add Local WebLM page, enter the appropriate information.
6. Click **Configure and Validate**.

Related topics:

Add Local WebLM field descriptions on page 43

Modifying a local WebLM server configuration

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Local WebLM Configuration** > **Modify Local WebLM** in the left navigation pane.
5. On the Local WebLM Configuration: Modify Local WebLM page, select the local WebLM that you want to configure.
6. Click **Modify**.
7. Modify the information .

   Note:

   You can modify information in the following fields: Name, Description, Protocol, Port, Day and Time of Periodic License Allocation Schedule, Day and Time of Periodic Usage Query Schedule.
8. Click **Modify** to save the changes.

Related topics:

Modify Local WebLM field descriptions on page 44

Removing a local WebLM server

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Local WebLM Configuration** > **Delete Local WebLM** in the left navigation pane.
5. On the Local WebLM Configuration: Delete Local WebLM page, select the local WebLM server that you want to delete.
6. Click **Delete**.

Note:

The system displays a warning message before removing the local WebLM server from the master WebLM server.

7. Click **Ok**.

Related topics:

Delete Local WebLM field descriptions on page 46

Viewing usage by WebLM

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Usages** > **Usage by WebLM** in the left navigation pane.
5. on the Usages: Usage by WebLM page, select the master or local WebLM server from the **Select WebLM** field.
6. Click **Query System**.

Related topics:

Usage by WebLM field descriptions on page 47

Viewing allocations by features

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Allocations** > **View by Feature** in the left navigation pane.

Related topics:

Allocations by Features field descriptions on page 50

Viewing enterprise usage of a license feature

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Usages** > **Enterprise Usage** in the left navigation pane.
5. on the Usages: Enterprise Usage page, select the license feature from the **Select Feature (License Keyword)** field.

Related topics:

Enterprise Usage field descriptions on page 48

Changing license feature allocations for a local WebLM server

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Allocations** > **Change Allocations** in the left navigation pane.
5. In the **New Allocation** column on the Allocations: Change Allocations page, enter the new allocation for the corresponding local WebLM server for the feature.
6. Click **Submit Allocations**.

Related topics:

Change Allocations field descriptions on page 51

Viewing periodic status of master and local WebLM servers

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Periodic Status** in the left navigation pane.

Related topics:

Periodic Status field descriptions on page 52

Specifying overuse limit for licensed features

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
4. Click **Overuse** in the left navigation pane.
5. In the **update percent overuse value** field on the Overuse page, select the percent overuse value.
6. Click **Submit** to set the overuse limit.

Related topics:

Overuse field descriptions on page 53

Querying usage of feature licenses for master and local WebLM servers

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.

3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Usages** > **Query Usage** in the left navigation pane.
5. on the Usages: Query Usage page, select the master or local WebLM server for which you want to view the usage details by feature licenses.
6. Click **Query Usage**.

   If you select all the WebLM severs and click **Query usage**, then the page displays whether the query request is success or failure.

Result

The Usages: Usage by WebLM page displays the details for the selected WebLM servers.

Related topics:

Query Usage field descriptions on page 49

Viewing allocations by local WebLM

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Allocations** > **View by Local WebLM** in the left navigation pane.
5. From the **Select Local WebLM** field on the Allocations: View by Local WebLM, select the local WebLM.

Result

The page displays the allocations details for the selected local WebLM server on the same page.

Related topics:

Allocations by Local WebLM field descriptions on page 50

Viewing usage summary

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Licenses (WebLM)** in the left navigation pane.
3. On the WebLM Home page, click the enterprise product name under the **Licensed Products** in the left navigation pane.
4. Click **Usages** in the left navigation pane.

Related topics:

Usage Summary field descriptions on page 46

View by Feature field descriptions

Use this page to view the license capacity for each feature license of a product.

Name	Description
Feature (License Keyword)	The display name and keyword for the licensed features of the product.
License Capacity	The total number of feature licenses purchased by the organization for each feature.
Currently Available	The number of floating licenses of each feature that is currently available with the master WebLM server. **Note:** In the case of uncounted features, this column displays “Not counted”

Related topics:

Viewing feature license information of a product on page 32

View by Local WebLM field descriptions

Use this page to view information related to local WebLM servers of a product.

Name	Description
Local WebLM Name	The name of the local WebLM server.

Name	Description
IP Address	IP Address of the local WebLM server.
Last Contacted	Date and time when the local WebLM server is last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Related topics:

Viewing connectivity status of local WebLM servers for a product on page 33

Enterprise Configuration field descriptions

Use this page to specify the master WebLM server settings and the default settings for the periodic operations of the server. The settings you specify in the Enterprise Configuration Web page is applicable to the entire enterprise.

Master WebLM Configuration

Name	Description
Name	Name of the server.
Description	A brief description of the server.
IP Address	IP address of the server.
MAC ID	Host ID of the computer where the server is installed.

Default Periodic Operation Settings

Name	Description
Retry Count	This count is the number of times a master WebLM server should try to connect to a local WebLM server for a periodic operation after a connection failure. For example, let us consider that the count is set to 2 and the master WebLM server's attempt to connect to a local WebLM server is not successful. The master WebLM server will make two more attempts to connect to the local WebLM server.
Retry Interval	This interval is the duration, in minutes, within which the retry count specified in the Retry Count field must be carried out. For example, let us consider that the Retry Count is 2 and the Retry Interval is 10 minutes. On failure of a connection attempt, the master WebLM server will make two attempts within 10 minutes to connect to the local WebLM server.

SMTP Server Settings

Name	Description
Server Name	Name of the SMTP server.

Email Notification Settings for Periodic Operation

Name	Description
Email notification	Following are the options: • On: Sends an e-mail notification to the administrator regarding the failure of periodic operations. • Off: No e-mail notification is sent to the administrator regarding the failure of periodic operations.
Email Address	The e-mail address to which the WebLM application sends the e-mail notification if the periodic operations failed to execute.
Email Addresses	The list of e-mail addresses to which the WebLM application sends the e-mail notifications.
Add To List	Adds the e-mail address entered in the **Email Address** field to the **Email Addresses**
Remove Selected	Removes the selected e-mail address from the **Email Addresses** field.

Default Periodic License Allocation Schedule

Name	Description
Day	The day of the week on which master WebLM must send the ALF's again to local WebLM server .
Time	The time of the day specified in the **Day** field when master WebLM must send the ALF's again to local WebLM server.

Default Periodic Usage Query Schedule

Name	Description
Day	The day of the week on which master WebLM must query local WebLM servers for usage reports.
Time	The time of the day specified in the **Day** field when master WebLM must query local WebLM servers for usage reports.

Button	Description
Submit	Saves the enterprise configuration.
Reset	Resets the values in the fields to the default values.

Related topics:

Configuring enterprise on page 33

View Local WebLMs field descriptions

Use this page to validate the local WebLM server connection.

Name	Description
Local WebLM Name	The name of the local WebLM server.
IP Address	IP address of the local WebLM server.
Last Contacted	Date and time when the local WebLM server is last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Button	Description
Validate Connectivity	Validates the connectivity of the selected WebLM server.
Check All	Selects all the local WebLM server.
Clear All	Clears the selections of local WebLM servers.

Related topics:

Validating connectivity to local WebLM servers for a product on page 34

Add Local WebLM field descriptions

Use this page to add a local WebLM server.

Local WebLM Configuration

Name	Description
Name	Name of the server.
Description	A brief description of the server.
IP Address	IP address of the server.
Protocol	Protocol scheme over which the master WebLM server listens to the local WebLM server.
Port	Port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.
MAC ID	Host ID of the computer where the server is installed.

Periodic License Allocation Schedule

Name	Description
Day	The day of the week on which master WebLM must send the ALF's again to local WebLM server . By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server.
Time	The time of the day specified in the **Day** field when master WebLM must send the ALF's again to local WebLM server. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server.

Periodic Usage Query Schedule

Name	Description
Day	The day of the week on which master WebLM must query local WebLM servers for usage reports. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server.
Time	The time of the day specified in the **Day** field when master WebLM must query local WebLM servers for usage reports. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server.

Button	Description
Configure and Validate	Configures the local WebLM server and validates the creation of the local WebLM server.
Back	Navigates back to View Local WebLMs.

Related topics:

Adding a local WebLM server on page 34

Modify Local WebLM field descriptions

Use this page to modify information of a selected local WebLM server.

Local WebLM Configuration

Name	Description
Name	Name of the server.
Description	A brief description of the server.
IP Address	IP address of the server. **Note:** You can only view the information in this field.
Protocol	Protocol scheme over which the master WebLM server listens to the local WebLM server.
Port	Port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.
MAC ID	Host ID of the computer where the server is installed. **Note:** You can only view the information in this field.

Periodic License Allocation Schedule

Name	Description
Day	The day of the week on which master WebLM must send the ALF's again to local WebLM server .
Time	The time of the day specified in the **Day** field when master WebLM must send the ALF's again to local WebLM server.

Periodic Usage Query Schedule

Name	Description
Day	The day of the week on which master WebLM must query local WebLM servers for usage reports.
Time	The time of the day specified in the **Day** field when master WebLM must query local WebLM servers for usage reports.

Button	Description
Modify	Saves the local WebLM server configuration changes.
Back	Discards the configuration changes and takes the user back to theModify Local WebLM web page.

Related topics:

Modifying a local WebLM server configuration on page 35

Delete Local WebLM field descriptions

Use this page to delete a local WebLM server.

Name	Description
Local WebLM Name	The name of the local WebLM.
IP Address	IP Address of the local WebLM.
Select check box	Select the local WebLMs that you want to delete.

Button	Description
Delete	Removes the selected local WebLM server.
Reset	Clears the selection of the local WebLM servers.

Related topics:

Removing a local WebLM server on page 35

Usage Summary field descriptions

Use this page to view the usage summary for master WebLM server, a local WebLM server, or all the WebLM servers of the product.

Name	Description
WebLM Name	This column displays the names of the master WebLM server and the local WebLM servers of the product.
IP Address	The IP address of the master WebLM server and the local WebLM servers of the product.
Time of Query	The date and time when the last usage query was executed for the WebLM server. If the status of the last usage query was Failed, this column also displays the date and time of the usage query that was last successful.
Status	The success or failure of the last usage query executed for each WebLM server. This column of a WebLM server will be empty if the server has not been queried even once for feature license usage. The usage query can be a periodic usage query or a non periodic usage query.

Related topics:

Viewing usage summary on page 40

Usage by WebLM field descriptions

Use this page to query the feature license usage by Master and Local WebLM servers.

Name	Description
Select WebLM	The Master and local WebLM servers for which you can view the usage.
Feature (License Keyword)	The name and keyword of the counted features of the product.
Currently Allocated	The number of feature licenses for each feature that has been currently allocated to the selected WebLM server. For the master WebLM server of the product, this column lists the floating licenses available with the server.
Usage: qty/%	The number of feature licenses for each feature that is currently used by the licensed applications, from the allocated feature licenses. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%.
Peak Usage (last 7 days): qty/%	The highest number of feature licenses for each feature that has been used by the applications in the past seven days. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation was 50, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	The highest number of feature licenses for each feature that has been used by the applications in the past 30 days. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation was 50, the column displays 50/100%.
Time of Query	The date and time when the usage query for the selected WebLM server was executed.
Status	The success or failure of the last usage query process executed for each WebLM server. This column will be empty if the server has not been queried even once for feature license usage. The usage query can be a periodic usage query or a non periodic usage query.

Button	Description
Query System	Queries the selected WebLM server for feature license usage.

Related topics:

Viewing usage by WebLM on page 36

Enterprise Usage field descriptions

Use this page to view the feature license usage of all WebLM servers for the selected feature.

Name	Description
Select Feature (License Keyword)	The license features for which you can view the license usage.
License Capacity	The total number of feature licenses purchased by the organization for each feature.
Available	The number of floating licenses available with the master WebLM server.
WebLM Name	The name of the WebLM servers of the product.
Currently Allocated	The number of feature licenses that have been currently allocated to the WebLM servers for the selected feature.
Usage qty/%	The number of feature licenses that is currently used by the licensed applications, from the allocated feature licenses for the selected feature. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%.
Peak Usage (last 7 days): qty/%	The highest number of feature licenses that has been used by the applications in the past seven days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation was 50, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	The highest number of feature licenses that has been used by the applications in the past 30 days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation was 50, the column displays 50/100%.
Time of Query	The date and time when the usage query was executed for the selected feature.
Status	The success or failure of the last usage query process executed for each WebLM server.

Related topics:

Viewing enterprise usage of a license feature on page 37

Query Usage field descriptions

Use this page to query the master WebLM server, a local WebLM server, or all the WebLM servers of the product for their feature license usage report.

Name	Description
WebLM Name	The names of the master and the local WebLM servers of the product as links. You can view the feature license usage of a server by selecting the name of the required server in this column. **Note:** The table in the Usage by WebLM Web page will be empty if the specified WebLM server has not been queried even once for feature license usage.
IP Address	The IP address of the master WebLM server and the local WebLM servers of the product.
Time of Query	The date and time when the last usage query was executed for the WebLM server. If the status of the last usage query was Failed, this column also displays the date and time of the usage query that was last successful. **Note:** The Time of Query column of a WebLM server will be empty if the server has not been queried even once for feature license usage.
Status	The success or failure of the last usage query executed for each WebLM server. This column of a WebLM server will be empty if the server has not been queried even once for feature license usage. The usage query can be a periodic usage query or a non periodic usage query.
Select Check box	Check the WebLM Server for which you want to determine the usage query.

Button	Description
Check All	Selects all the WebLM servers.
Clear All	Clears the selections for all the WebLM servers.
Query Usage	Queries the selected WebLM servers of the product for their feature license usage report.

Related topics:

Querying usage of feature licenses for master and local WebLM servers on page 38

Allocations by Features field descriptions

Use this page to view the feature license allocation information for each counted type feature of the product.

Name	Description
Feature (License Keyword)	The name and license keyword of the counted features of the product.
Local WebLM Name	The name of the local WebLM servers of the product. By default, this column is empty. The system displays the names of the local WebLM servers only when you select the arrow beside the name of the required feature. If no local WebLM server exist for the product, this column will be empty for all the licensed features.
IP Address	The IP address of the local WebLM servers of the product. By default, this column is empty. The system displays the IP address of the local WebLM servers only when you select the arrow beside the name of the required feature. If no local WebLM server exists for the product, this column will be empty for all the licensed features.
License Capacity	The total number of feature licenses purchased by the organization for the respective feature.
Currently Allocated	The total number of feature licenses of the respective feature that have been allocated to the local WebLM servers of the product. If a licensed feature is not allocated to any local WebLM server, the system displays zero as the value of the column for the licensed feature.
Available	This column lists the number of floating licenses of the respective feature that is currently available with the master WebLM server.

Note:

To view information regarding the number of feature licenses of a feature that is allocated to each local WebLM server, click the arrow beside the name of the required feature. When you select the arrow beside a feature, the system displays new rows below the feature row. These new rows display the feature license allocation information for each local WebLM server to which the feature is allocated.

Related topics:

Viewing allocations by features on page 36

Allocations by Local WebLM field descriptions

Use this page to view the feature license allocation information by Local WebLM.

Name	Description
Select Local WebLM	The local WebLMs for which you can view the feature license allocation information.
Last Allocation	The date and time when feature licenses were last allocated to the selected local WebLM server.
Status	The success or failure of the last license allocation process executed for the selected local WebLM server. The allocation process can be a periodic allocation process or a non periodic allocation process. If the status of the last license allocation process was Failed and there was a previous license allocation process success for the server, the system displays the date and time of the license allocation process that was last successful below the Last Allocation field.
Feature (License Keyword)	The name and license keyword of the counted features that have been allocated to the selected local WebLM server.
License Capacity	The total number of feature licenses purchased by the organization for each feature.
Currently Allocated	The total number of feature licenses of each feature that have been allocated to the selected local WebLM server.
Available	The number of floating licenses of each feature that is currently available with the master WebLM server.

Related topics:

Viewing allocations by local WebLM on page 39

Change Allocations field descriptions

Use this page to change feature-wise current feature license allocation information for each local WebLM server of a product.

Name	Description
Feature (License Keyword)	The name and license keyword of the counted features that have been allocated to the selected local WebLM server.
Local WebLM Name	The name of the local WebLM server.
IP Address	The IP address of the local WebLM servers of the product.
License Capacity	The total number of feature licenses purchased by the organization for each feature.
Currently Allocated	The total number of feature licenses of each feature that have been allocated to the selected local WebLM server.

Name	Description
Currently Used	The total number of feature licenses of each feature that are in use by the product.
Available	The number of floating licenses of each feature that is currently available with the local WebLM server.
New Allocation	The total number of additional feature licenses allocated to a local WebLM server.

Button	Description
Submit Allocations	Allocates the number of feature licenses specified in the New Allocations field to the corresponding local WebLM servers.
Reset	Resets the values specified in the New Allocation fields to their default values.

Related topics:

Changing license feature allocations for a local WebLM server on page 37

Periodic Status field descriptions

Use the Periodic Status option to view the status of the periodic operations such as periodic allocation of feature licenses to the local WebLM server and querying the local WebLM server for usage report.

Periodic Allocation

Name	Description
Local WebLM Name	The name of the local WebLM server of a product.
IP Address	The IP address of all the local WebLM servers of the product.
Last Allocation	The date and time when the last periodic license allocation process was executed for each local WebLM server. If the status of the last periodic license allocation process was Failed, this column also displays the date and time of the periodic license allocation process that was last successful.
Status	The success or failure of the last periodic license allocation process executed for each local WebLM server. The system displays the date and time of the last successful periodic license allocation process in the **Last Allocation** column.

Periodic Usage

Name	Description
WebLM Name	The name of master WebLM server and local WebLM servers of a product.
IP Address	The IP address of master and local WebLM servers of a product.
Last Usage Query	The date and time when the last periodic usage query was executed for each WebLM server. If the status of the last periodic usage query was Failed, this column also displays the date and time of the periodic usage query that was last successful.
Status	The success or failure of the last periodic usage query executed for each WebLM server. This column of a WebLM server will be empty if the server has not been queried even once for feature license usage.

Related topics:

Viewing periodic status of master and local WebLM servers on page 38

Overuse field descriptions

Use this page to specify the overuse value in percent for licensed features of a product.

Name	Description
Update percent overuse value	The overuse values in percent . For example, if there are 10 licenses available for a feature and you have set the overuse value to 50 percent then it indicates that you have 5 buffer licenses for the feature.

Button	Description
Submit	Sets the overuse value.
Reset	Set the values in the **Update percent overuse value** to the default value.

Related topics:

Specifying overuse limit for licensed features on page 38

Chapter 3: Communication System Management

Communication System Management Overview

Communication System Management allows you a common, centralized administration of some of the existing IP Telephony products by consolidating key capabilities of the current suite of Integrated Management administration products with other Avaya Management tools on a common software platform. Communication System Management helps you administer Avaya Aura™ Communication Manager (CM), Communication Manager Messaging (CMM), and Modular Messaging (MM). Communication System Management features include:

- Station Management through Avaya Aura™ System Manager
- Template Management for all stations supported in Communication System Management.
- Mailbox Management through Avaya Aura™ System Manager
- Element Cut Through to native administration screens

Telephony (non-station objects management)

Communication System Management allows you to directly add, edit, view or delete group lists through **Telephony**. Communication System Management also displays a collection of non-station objects under **Telephony**.

Station Management

Communication System Management allows you to create and manage stations. Station Management provides support for CM Station objects. You can add, change, remove and view station data through Station Management.

Templates

Using templates, you can specify specific parameters of a station or a subscriber once and then reuse that template for subsequent add station or subscriber tasks. The system provides default templates, but additionally you can also add your own custom templates.

There are two categories of templates: default templates and user-defined templates. The default templates are available within the application and you cannot edit or remove them. However, you can modify or remove user-defined templates any time.

Subscriber Management

Communication System Management lets you manage subscriber data. Subscriber Management provides support for Communication Manager Messaging (CMM) and Modular Management (MM) objects. You can add, change, remove, and view subscriber data.

Using Communication System Management you can:

1. Add Communication Manager (for stations) and Modular Messaging (for subscribers) to the list of managed elements.
2. Create templates to simplify station and subscriber management.
3. Administer stations, subscribers, and create user profiles (with Communication Profiles).
4. Associate the user profiles with the required stations and subscribers.

Synchronization of Data

Synchronizing Communication Manager / Messaging data

Managed elements can have alternate ways of administering data. For example, you can administer station data from the System Access Terminal (SAT) interface or from another tool such as Site Administration or Native Configuration Manager. Thus it is essential to maintain uniformity in the database of the various tools used for administering data. Synchronization of data ensures this.

Initializing Synchronization

Initializing synchronization allows you to synchronize data in the System Manager database with each managed Communication Manager system. When you add a Communication Manager into the system, Communication System Management automatically initiates an initialization task to get all the Communication Management data that is required, and stores it in the System Manager database.

Incremental Synchronization

Incremental synchronization with selected devices allows you to incrementally synchronize data in the System Manager database with each managed Communication Manager system. This synchronization updates the data in the database that has been changed in Communication Manager since the last time the synchronization was run.

Scheduled Synchronization with Communication Manager

You can create and schedule synchronization jobs using Communication System Management. You can schedule a synchronization job to run at a fixed time and repeat it periodically. Communication System Management provides a default incremental synchronization every 24 hours. You can modify this to your convenience.

On demand Synchronization

Communication System Management allows you to synchronize data with the Communication Manager on demand. Administrators can initiate this at any time. On-demand synchronization can either be initialization synchronization or an incremental synchronization.

Note:

You have to add a new CM/ Messaging entity through the Runtime Topology service (RTS) before you perform synchronization.

Related topics:

Initializing Synchronization on page 57
Incremental Synchronization on page 57
Synchronizing Messaging Data on page 58

Initializing Synchronization

1. Log in to the Avaya Aura™ System Manager Web interface.
2. Click **Synchronize CM Data / Launch Element Cut Through**.
3. In the Communication Manager List page, select **Initialize data for selected devices**.
4. Click **Run Now** to perform the initializing synchronization or do one of the following:
   a. Click **Schedule** to perform the synchronization at a specified time.
   b. Click **Cancel** to cancel the synchronization.

Incremental Synchronization

1. Log in to the Avaya Aura™ System Manager Web interface.
2. Click **Synchronize CM Data/ Launch Element Cut Through**.
3. In the Communication Manager List page, select the Communication Managers you want to synchronize.
4. Select **Incremental Sync data for selected devices**.
5. Click **Run Now** to perform the incremental synchronization or do one of the following:

a. Click **Schedule** to perform the synchronization at a specified time.

b. Click **Cancel** to cancel the synchronization.

Note:

While scheduling incremental synchronization, you must set the logging levels on Communication Manager using the **change logging-levels** option. Select **both** option for the **Log Data Values** field.

Synchronizing Messaging Data

1. Log in to the Avaya Aura™ System Manager Web interface.
2. Click **Synchronize Messaging System Data** in the console page.
3. Select the messaging systems you want to synchronize from the Messaging System List.
4. Click **Run Now** to perform the synchronization or do one of the following:
   a. Click **Schedule** to perform the synchronization at a specified time.
   b. Click **Cancel** to cancel the synchronization.

Telephony

Telephony

Communication System Management allows you to directly add, edit, view or delete group lists through **Telephony**. Communication System Management also displays a collection of non-station objects under **Telephony**. The Communication Manager objects are:

- Call Centre

  Vector Directory Number

  Vector
- Coverage

Coverage Answer Group

Coverage Path

Coverage Time of Day

- Groups

Group Page

Hunt Group

Intercom Group

Pickup Group

Terminating Group Extension

- Network

Automatic Alternating Network

Automatic Route Selection

IP Interfaces

IP Network Regions

Node Names

Route Pattern

Signaling Groups

- Parameters

System Parameter CDR Option

System Parameter Customers Option

System Parameter Features

System Parameter Security

System Parameter Special Applications

- Station

Alias Station

Intra Switch CDR

Off PBX Station Mapping

Site Data

- System

Dialplan Analysis

Dialplan Parameters

Feature Access Codes

Class of Restriction

Location

Uniform Dial Plan

Related topics:

[Adding non-station objects](#) on page 60
[Editing non-station objects](#) on page 61
[Viewing non-station objects](#) on page 61
[Deleting non-station objects](#) on page 62

Adding non-station objects

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Select the Communication Manager element to which you want to add a non-station object.
4. From the Communication Manager list, select a Communication Manager.
5. Click **Show List**.
6. Click **New**.
7. Select the Communication Manager again from the list of Communication Managers.

   Note:
   You have to enter the qualifier number in the **Enter Qualifier** field for some Communication Manager elements.
8. Click **Add**.
   The system displays the Element Cut Through screen where you can enter the attributes of the non-station object you want to add.
9. Click **Enter** to add the non-station object.
   To return to the Communication System Management screen click **Cancel**.

Editing non-station objects

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Select the Communication Manager element you want to edit.
4. Click **Show List**.
5. From the group list, select the device you want to edit.
6. Click **Edit**.
   The system displays the Element Cut Through screen where you can edit the attributes of the device you have chosen.
7. To save the changes and go back to the Communication System Management screen, click **Enter**.

   To undo the changes and return to the Communication System Management screen, click **Cancel**.

Viewing non-station objects

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Select the Communication Manager element you want to view.
4. From the list of Communication Managers, select an option.
5. Click **Show List**.
6. From the group list, select the object you want to view.
7. Click **View**.
   You can view the attributes of the object you have selected in the Element Cut Through screen.
8. To return to the Communication System Management screen, click **Cancel**.

Deleting non-station objects

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Select one of the Communication Manager elements from **Telephony**.
4. Select a Communication Manager from the list of Communication Managers.
5. Click **Show List**.
6. Select the object or objects you want to delete from this group.
7. Click **Delete**.

Filtering non-station objects

You can filter the Communication Manager elements using the **Filter** button in the respective element list. You can apply filters on each of the columns in the element list and you can also filter the Communication Manager elements using one or multiple column filters.

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click the Communication Manager element you want to filter.
4. Select one of the Communication Managers from the Communication Manager list.
5. Click **Show List**.
6. Click the **Filter: Enable** option in the group List.
7. Filter the non-station objects according to one or multiple columns.
8. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

   Note:

   The table displays only those devices that match the filter criteria.

Station Management

Station Management

Communication System Management allows you to create and manage stations using the **Manage Stations** option in **Telephony**. You can also view, edit, and delete stations. Communication System Management provides support for the following set types:

- IP/SIP Set types

  9610SIP/9620SIP/9630SIP/9640SIP/9650SIP

  9610/9620/9630/9640/9650

  1603/1608/1616/16CC

  9600SIP

  4620SIP

  4620SIPCC

  4610/4620/4621/4622/4625/4630

  4602+

  4612CL
- DCP Set types

  2402/2410/2420

  6402/6402D/6408/6408+/6408D/6408D+/6416D+/6424D+

  8403B/8405B/8405B+/8405D/8405D+/8410B/8410D/8411B/8411D/8434D
- Analog Set types

  2500
- BRI Set types

  WCBRI

Adding a Station

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the System Manager console, click **Communication System Management**.
3. Click **Telephony**.
4. Click **Station** > **Manage Stations**.
5. From the list of Communication Managers, choose an option.
6. Click **Show List**.
7. Click **New** from the station list menu.
8. Complete the Add Station page and click **Commit** to add the station.

Note:

You must complete the mandatory fields under the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, **Button Assignment** sections before adding a station.

Note:

As a part of the process for adding a station, you must apply a station template (either default or user-defined). You must select the template based on the set type you want to add. You can modify the fields, if required, before clicking **Commit**.

If you want to add a station with a non supported set type, then you must add the station using Element Cut Through. For “Alias” stations, you can choose the corresponding “Alias” set type from the **Template** field. Communication System Management automatically creates a template for the “Alias” set types based on the “aliased-to” set type. Alias station templates have names beginning with “Alias”. Before the Alias station type Template appears in the pull-down menu, you have to create an alias set type on the managed Communication Manager. You can then use the template to add a station.

Related topics:

Station / Template field descriptions on page 124

Using Native Name

To enter the native name, you must use the Input Method Editor (IME) application. The IME application lets you enter characters in multiple languages such as Japanese, Korean,

Russian, Arabic and Chinese without requiring a special keyboard. However, you must enable the IME application manually. Otherwise, the keyboard input remains in the default language.

The IME icon appears in the Windows system tray and indicates the language you are currently using. For example, if you are using English, the IME icon in the system tray displays **EN**. If you are using French, the IME icon in the system tray displays **FR**.

1. Click the IME icon in the Windows system tray.
   The system displays a menu with the languages installed on your PC.
2. Select the language you want to use.
3. Type the native name in Site Administration Communication System Management.

Editing a Station

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. From the Communication Managers' list, select one of the Communication Managers.
5. Click **Show List**.
6. From the corresponding Station list, select the station you want to edit.
7. Click **Edit** or click **View** > **Edit**.
8. Edit the required fields in the **Edit Station** Web page.
9. Click **Commit** to save the changes.

Related topics:

Station / Template field descriptions on page 124

Viewing a Station

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Select **Station** > **Manage Stations**.
4. From the Communication Managers' list, select one of the Communication Managers.
5. Click **Show List**.
6. From the list of stations, select the station you want to view.
7. Click **View**.
   The system displays the View Station page. You can view the attributes of a station in this page.

Note:
You cannot edit the fields in the View Station Web page. To go to the Edit Station page click **Edit**.

Related topics:

Station / Template field descriptions on page 124

Deleting a Station

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. From the Communication Managers' list, select one of the communication Managers.
5. Click **Show List**.
6. From the station list, select the station or stations you want to delete.
7. Click **Delete**.
   The system displays a confirmation message alerting you to a user associated with a station. The system flags these user-associated stations in yellow color.

Note:

You cannot delete a station associated with a user through station management. You can delete the user associated stations only through User Profile Management.

Editing Station Extensions

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. From the Communication Managers' list, select one of the Communication Managers.
5. Click **Show List**.
6. From the station list, select the station for which you want to edit the extension.
7. Click **More Actions** > **Edit Station Extension**.
8. Complete the Edit Station Extension page and click Commit to save the new extension.

Note:

You can use the **Edit Station Extension** option only to change the station extension. Use the **Edit** option to change the other attributes.

Note:

You can also edit the **Message Lamp Ext** and **Emergency Location Ext** fields through **Edit Station Extension**.

Related topics:

Edit Station Extension field descriptions

Bulk Adding Stations

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. From the Communication Managers' list, select one of the Communication Managers.
5. Click **Show List**.
6. Click **More Actions** > **Bulk Add Stations**.
7. Complete the Bulk Add Station page and click **Commit** to bulk add the stations.

   The **Station Name Prefix** field gives the common prefix which appears for all the stations you bulk add. You can enter any prefix name of your choice in this field.

   Note:

   In the **Enter Extensions** field you can enter the extensions which you want to use. You must enter the extensions in serial order and also check for the availability of an extension before you use it.

Related topics:

Bulk Add Station field descriptions on page 122

Bulk Editing Stations

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. From the Communication Managers' list, select one of the Communication Managers.
5. Select the station or stations which you want to bulk edit.
6. Click **Show List**.
7. Click **More Actions** > **Bulk Edit Stations**.
8. Complete the Bulk Edit Station page and click **Commit** to bulk edit the stations.

The **Station Name Prefix** field gives the common prefix that appears for all the stations you bulk add or edit. You can enter any prefix name of your choice in this field.

Related topics:

Bulk Edit Station field descriptions on page 123

Station List

Station List displays all the stations under the Communication Manager(s) you select. You can perform an advanced search on the station list using the search criteria. You can also apply filters and sort each of the columns in the Station List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Specifies the name of the station.
Extension	Specifies the extension of the station.
Port	Specifies the port of the station.
Set Type	Specifies the set type of the station.
COS	Specifies the COS of the station.
COR	Specifies the COR of the station.
User	If a station is associated with a user, then the system displays the name of the user in this column.
System	Specifies the Communication Manager of the station.

Filtering Stations

You can filter stations using the **Filter** button in the station list. You can apply the filters on each of the columns in the station list and you can also filter the stations using one or multiple column filters.

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. Select one of the Communication Managers from the Communication Manager list.

5. Click **Show List**.
6. Click the **Filter: Enable** option in the Station List.
7. Filter the stations according to one or multiple columns.
8. Click **Apply**.

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

   Note:
   The table displays only those stations that match the filter criteria.

Using Advanced Search

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Telephony**.
3. Click **Station** > **Manage Stations**.
4. From the Communication Manager list select an option.
5. Click **Show List**.
6. Click the **Advanced Search** option in the Station list .
7. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   If you want to add a search condition, click **+** and repeat the sub steps listed in step 6.

   If you want to delete a search condition, click **-** . This button is available if there is more than one search condition.

Templates

Distribution of Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Station**.
4. Select a station template from the list of existing station templates on the Station Template page.
5. Click **More Actions** > **Distribute**.
6. Select the Communication Managers to which you want to distribute the template you have chosen.
7. Click **Commit** to distribute the template value.
   All the station(s) associated with this template for the selected Communication Managers will now have the same field values as that in the template.

Template Management

A template is a file that contains stored settings. You can use templates to streamline the process of performing various routine activities. Templates save the data that you enter so that you can perform similar activities later without re-entering the same data. Communication System Management allows you to create, store, and use templates to simplify tasks like adding, editing, and viewing stations or subscribers. Communication System Management offers several default templates and you can create your own templates as well.

Templates exist in two categories, default templates and user-defined templates. The default templates exist on the system and you cannot edit or remove them. You can, however, modify or remove user-defined templates any time.

Adding Station Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Stations**.
4. On the Station Templates page click **New**.
5. On the New Station Template page, click **Set type**.
6. Enter a name in the **Template Name** field.
7. Complete the mandatory fields under the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.
8. After completing the New Station Template page, click **Commit** to add the station template.

Related topics:

Station / Template field descriptions on page 124

Editing Station Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Station**.
4. From the station template list select the template you want to edit.
5. Click **Edit** or click **View** > **Edit**.
6. Complete the Edit Station Template page.
7. Click **Commit** to save the changes.

Related topics:

Station / Template field descriptions on page 124

Viewing Station Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Station**.
4. Select one of the existing templates from the Station Templates page.
5. Click **View**.
   You can view the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections in the View Station Template page.

Related topics:

Station / Template field descriptions on page 124

Deleting Station Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Station**.
4. From the station template list select the template or templates you want to delete.
5. Click **Delete**.

Note:
You cannot delete any of the default templates.

Duplicating Station Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.

3. Click **Station**.
4. From the station template list select the template you want to copy.
5. Click **Duplicate**.
6. Enter the name of the new template in the **New Template Name** field.
7. Choose the appropriate set type from the **Set Type** field.
8. Complete the Duplicate Station Template page and click **Commit** to copy the template.

Related topics:

Station / Template field descriptions on page 124

Adding Subscriber Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Messaging**.
4. From the list of supported messaging versions, select a messaging version.
5. Click **Show List**.
6. Click **New** from the subscriber list menu.
7. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous** sections in the Add Subscriber Template page.
8. Click **Commit** to add a subscriber template.

   Messaging templates have different versions based on their software version. The subscriber templates you create have to correspond to the MM/CMM software version. When you select a messaging template, the **Software Version** field in the Add Subscriber Template page displays the appropriate version information.

Related topics:

Adding Subscriber Templates (CMM) field descriptions on page 92
Adding Subscriber Templates (MM) field descriptions on page 94

Editing Subscriber Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Messaging**.
4. From the supported messaging version list, select a messaging version.
5. Click **Show List**.
6. Select a subscriber template from the subscriber template list.
7. Click **Edit** or click **View** > **Edit**.
8. Edit the required fields in the Edit Subscriber Template page.
9. Click **Commit** to save the changes.

Note:
You cannot edit any “default” subscriber template.

Related topics:

Editing Subscriber Templates (CMM) field descriptions on page 107
Editing Subscriber Templates (MM) field descriptions on page 109

Viewing Subscriber Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Messaging**.
4. From the supported messaging versions list, select one of the messaging versions.
5. Click **Show List**.
6. Select a subscriber template from the list of subscriber templates.
7. Click **View**.
   You can view the mailbox settings of this subscriber in the View Subscriber Template page.

Note:
You cannot edit any of the fields in the View Subscriber Template page.

Related topics:

Viewing Subscriber Templates (CMM) field descriptions on page 118
Viewing Subscriber Templates (MM) field descriptions on page 120

Deleting Subscriber Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Messaging**.
4. From the list of supported messaging versions, select a supported messaging version.
5. Click **Show List**.
6. From the subscriber template list, select the template or templates that you want to delete.
7. Click **Delete**.

Note:
You cannot delete any “default” subscriber templates.

Duplicating Subscriber Templates

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Messaging**.
4. From the list of supported messaging versions, select a messaging version.
5. Click **Show List**.
6. From the subscriber template list, select the subscriber template you want to copy.

7. Click **Duplicate**.
8. Complete the Duplicate Subscriber Template page.
9. Click **Commit** to copy the subscriber template.

Related topics:

Duplicating Subscriber Templates (CMM) field descriptions on page 97
Duplicating Subscriber Templates (MM) field descriptions on page 99

Viewing Associated Stations

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Station**.
4. Select one of the station templates from the list of station templates.
5. Click **More Actions** > **View Associated Stations**.
   You can view the stations in the System Manager database that are associated with the station template you have chosen on the Associated Stations page.

Viewing Associated Subscribers

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.
3. Click **Messaging**.
4. From the list of supported messaging versions, select a messaging version.
5. Click **Show List**.
6. From the subscriber template list, select a subscriber template for which you want to view the associated subscribers.
7. Click **More Actions** > **View Associated Subscribers**.

You can view all the associated subscribers in the System Management database for the template you have chosen in the Associated Subscribers page.

Template List

You can view the template list when you click the **Template** option in the **Communication System Management** tab. You must click the **Station** or **Subscriber** option to view the station or subscriber template list.

You can apply filters and sort each of the columns in the station or messaging template list. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Name of the template.
Owner	Specifies the name of the user who owns a template. For default templates System is considered to be the owner. For user-defined templates this field specifies the name of the user who created the template.
Version	Specifies the version of the template.
Default	Specifies whether the template is default or user-defined.
Last Modified	Specifies the time and date when the station or messaging template was last modified.
Set type (for station templates)	Specifies the set type of the station template.
Type (for messaging templates)	Specifies whether the messaging type is MM or CMM.
Software Version (for messaging templates)	Specifies the type of messaging version of the messaging template.

Filtering Templates

You can filter station and subscriber templates using the **Filter** button in the station or subscriber template list. You can apply the filters on each of the columns in the templates list and you can also filter the stations using one or multiple column filters.

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Templates**.

3. Click either **Station** or **Subscriber** for station templates and subscriber templates respectively.
4. Select the Communication Manager or supported messaging version, whichever applicable.
5. Click **Show List**.
6. Click the **Filter: Enable** option in the Template List.
7. Filter the station or subscriber templates according to one or multiple columns.
8. Click **Apply**.

   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

Note:

The table displays only those station or subscriber templates that match the filter criteria.

Mailbox Management

Subscriber Management

Communication System Management lets you perform selected messaging system administration activities. You can add, view, edit, and delete subscribers through Communication System Management. Apart from subscriber management, you can also administer mailboxes and modify mailbox settings for a messaging system.

Communication System Management supports CM versions 5.0 and later. It also supports MM versions 4.0, 5.0 and 5.2; CMM version 5.2.

Adding a Subscriber

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Messaging**.
3. Click **Subscriber**.

4. From the list of messaging systems, select one or more of the messaging systems.
5. Click **Show List**.
6. Click **New**.
7. In the Add Subscriber page, complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions**, **Miscellaneous** sections.
8. After completing the Add Subscriber page, click **Commit** to add the subscriber.

Note:

If you select more than one MM or CMM from the list of messaging systems, and then click **New**, the System displays the Add Subscriber page with the first MM or CMM in context.

Related topics:

Adding a Subscriber (CMM) field descriptions on page 86
Adding a Subscriber (MM) field descriptions on page 88

Editing a Subscriber

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Messaging**.
3. Click **Subscriber**.
4. From the list of messaging systems, select one of the messaging systems.
5. Click **Show List**.
6. From the subscriber list choose the subscriber you want to edit.
7. Click **Edit** or **View** > **Edit**.
8. Edit the required fields in the Edit Subscriber page.
9. Click **Commit** to save the changes.

Related topics:

Editing a Subscriber (CMM) field descriptions on page 102
Editing a Subscriber (MM) field descriptions on page 104

Viewing a Subscriber

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Messaging**.
3. Click **Subscriber**.
4. From the list of messaging systems, select one of the messaging systems.
5. Click **Show List**.
6. From the subscriber list, select the subscriber you want to view.
7. Click **View**.
   The system displays the View Subscriber Web page.

Note:
You cannot edit any field in the View Subscriber page.

Related topics:

Viewing a Subscriber (CMM) field descriptions on page 112
Viewing a Subscriber (MM) field descriptions on page 114

Deleting a Subscriber

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Messaging**.
3. Click **Subscriber**.
4. From the Messaging Systems list, select one of the messaging systems.
5. Click **Show List**.
6. From the subscriber list, select the subscriber or subscribers you want to delete.
7. Click **Delete**.
   The system displays a confirmation page for deleting the subscriber.
8. Confirm to delete the subscriber or subscribers.

Note:

You cannot delete a subscriber associated with a user through mailbox management. You can delete the user associated subscribers only through User Profile Management.

Subscriber List

Subscriber list displays all the subscribers under a messaging version (CMM/MM). You can apply filters to each column in the Subscriber List. You can also sort the subscribers according to each of the column in the Subscriber List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

Name	Description
Name	Specifies the name of the subscriber.
Mailbox Number	Specifies the subscriber's mailbox number.
Email Handle	Specifies the subscriber's e-mail handle.
Telephone Number	Specifies the telephone number of the mailbox.
Last Modified	Specifies the time and date when the subscriber's details were last modified.
User	If a subscriber is associated with a user, then the system displays the name of the user in this column.
System	Specifies the subscriber's messaging system.

Filtering Subscribers

You can filter subscribers using the **Filter** button in the subscriber list. You can apply filters on each of the columns in the subscriber list and you can also filter the subscribers using one or multiple column filters.

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Messaging**.
3. Click **Subscriber**.
4. Select one of the supported messaging versions from the list.
5. Click **Show List**.
6. Click the **Filter: Enable** option in the Subscriber List.

7. Filter the subscribers according to one or multiple columns.
8. Click **Apply**.
   To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

   Note:
   The table displays only those subscribers that match the filter criteria.

Viewing Class of Service

1. Log in to the Avaya Aura™ System Manager Web interface.
2. From the **Communication System Management** tab, click **Messaging**.
3. Click **Class of Service**.
4. Choose one or more messaging systems from the Messaging Systems list.
5. Click **Show List**.
   The system displays the corresponding Class of Service list.

   Note:
   This list is read-only.

   Note:
   Click the respective column heading to sort the Class of Service by **Name** (in alphabetical order) or by **Class No.** (by numeric order).

Related topics:

Class of Service List field descriptions on page 124

Configure Options

The Uniform Dial Plan call type works identically with the ext call type, with an exception: if the dialed digits match the call type of UDP, Communication Manager automatically checks the UDP Table first to see if there is a match, regardless of the value in the **UDP Extension Search**

Order field on the Dial Plan Parameters screen. If there is no match, Communication Manager then checks the local server.

If the dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **udp-table-first**, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **local-extensions-first**, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP Table.

The UDP call type allows Communication Manager to recognize strings of 14 to 18 digits, which are longer than the maximum extension length of 13 digits. However, the UDP call type can be used with any length in case this provides a useful new capability to customers.

UDP in Communication System Management

You can select the Uniform Dial Plan option under **Synchronize CM Data and Configure Options** > **Configuration Options**. When you select the **Consider UDP** option, the corresponding dial plan is not considered for the available extension range while adding a station. When you do not select the **Consider UDP** option, the corresponding dial plan is considered for the available extension range while adding a station.

Launching Other Applications

You can launch applications like Fault and Performance Manager, Multisite Administration and Network Management Console through Communication System Management. Login to the Communication System Management console, click the **Applications** tab and then click on the application you want to launch.

You can launch the following applications through Communication System Management:

Network Management

Network Management is a Microsoft Windows server solution for managing Avaya IP Telephony products. Network Management gives you a complete converged solution that helps you manage your VoIP network through a common Web-based user interface. This offer gives you the ability to see your whole voice system structure and hierarchy (show status, fault data, inventory, Software and Firmware updates, backup and restore and so on). You can administer and manage Avaya voice systems and Avaya converged devices (such as media gateways and servers). The Network Management offer includes Avaya Aura™ Communication Manager Branch Edition - Central Manager which is used to administer and manage branch locations in a Branch Office network.

Fault and Performance Manager

Avaya Fault and Performance Manager gives you a network map or system view of your converged network and the tabular tools to monitor the status and performance of the devices

on your network. You can see into the network to examine faults and performance data from the Avaya media servers on the network. Fault and Performance Manager collects configuration, fault, and performance data from Secure Services Gateway (through SNMP) or directly from an IP-enabled voice system using OSSI, and then displays the data in text, tables, and graphic formats.

Fault and Performance Manager alerts you when voice system faults and performance problems occur. Fault and Performance Manager also helps you isolate and identify fault and performance problems and provides tools to help you fix fault and performance problems.

Fault and Performance Manager collects configuration, fault, and performance data from your systems according to a schedule that you specify. Fault and Performance Manager keeps a database of system exceptions and performance measurements, and it allows you to run reports on that data. You can present the data as text, tables, and graphs.

In addition to monitoring your voice systems, Fault and Performance Manager also provides alarm management (not performance monitoring) for several adjuncts related to your voice systems including INTUITY AUDIX, DEFINITY Audix, Call Management System, CONVERSANT, and INTUITY Interchange. Fault and Performance Manager supports up to 300 systems. For more information on filtering alarms, see Filtering Alarms (Alarm Filter Panel)

MultiSite Administration

Avaya MultiSite Administration is a client-server based application that gives you multi-user, graphical, web-based management of multiple converged Avaya media servers and media gateways. MultiSite Administration provides you with centralized management of distributed networks and campus environments. Intuitive, task-based programs (wizards) enable you to rapidly learn and implement administrative tasks that were previously difficult and time consuming. You can set these tasks so that you can implement them immediately or at a specified time.

Avaya MultiSite Administration offers the following features:

- The ability for multiple administrators to administer the same (or separate) Avaya media servers at the same time, remotely.
- Graphical station and system administration screens.
- Easy-to-use wizards for basic administration tasks.
- The ability to cut through (using terminal emulation) to administer other telephony devices.

With MultiSite Administration, you can:

- View and administer system-wide settings.
- Add stations, swap stations, move multiple stations, and delete stations. Using MultiSite Administration, you can also move one or more stations from one voice system to another while maintaining the same extension.
- Change phone types and feature buttons. You can also assign features to phone buttons by clicking a button on the picture.
- Create station templates that will save you time while adding stations.
- Print button labels for your phones.
- Add or delete subscriber accounts on your messaging systems.

- Look up extensions and query the voice system for stations matching specific criteria.
- View log files.
- Collect data and generate reports in real time or at a scheduled time. You can also build a report template.
- Cut through to a voice system or a messaging system.

MultiSite Administration validates the data you enter for extensions and ports, ranges and field types before it sends data to a voice system. Avaya Multisite Administration is provided in the Avaya Integrated Management Release 5.0 System Management offer.

Adding a Subscriber (CMM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Template	Specifies the template for this subscriber. You can choose any template from the drop-down box.
Type	Specifies the messaging type of your subscriber.
Software Version	Specifies the messaging version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank

Field	Description
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Cancel	Takes you to the previous page.

Adding a Subscriber (MM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add. You can choose this option from the drop-down box.
Type	Specifies the messaging type of your subscriber.
Template	Specifies the messaging template of a subscriber. You can choose an option from the drop-down box.
Software Version	Specifies the message version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.

Field	Description
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire

Field	Description
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.

Field	Description
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Cancel	Takes you to the previous page.

Adding Subscriber Templates (CMM) field descriptions

Field	Description
Template name	Specifies the template of this subscriber template.
Type	Specifies the messaging type of the subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the

Field	Description
	voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Cancel	Takes you to the previous page.

Adding Subscriber Templates (MM) field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
Template name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]) .

Field	Description
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.

Field	Description
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Cancel	Takes you to the previous page.

Duplicating Subscriber Templates (CMM) field descriptions

Field	Description
Template name	Specifies the template of the subscriber template you want to copy.
New Template Name	Specifies the new subscriber template name.
Type	Specifies the messaging type of the subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.

Field	Description
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Cancel	Takes you to the previous page.

Duplicating Subscriber Templates (MM) field descriptions

Field	Description
Template Name	Specifies the name of the template which you want to duplicate.
New Template Name	Specifies the name of the new template. You can enter the name of your choice.
Type	Specifies the messaging type of the subscriber template.
Template name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]) .
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.

Field	Description
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Cancel	Takes you to the previous page.

Editing a Subscriber (CMM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Template	Specifies the template for this subscriber.
Type	Specifies the messaging type of your subscriber.
Software Version	Specifies the message version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.

Field	Description
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Reset	Undoes all the changes.
Cancel	Takes you to the previous page.

Editing a Subscriber (MM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Type	Specifies the messaging type of your subscriber.
Template	Specifies the messaging template of the subscriber.
Software Version	Specifies the message version of the subscriber.
Save as Template	Saves your current settings as a template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.

Field	Description
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Reset	Clears all the changes.
Cancel	Takes you to the previous page.

Editing Subscriber Templates (CMM) field descriptions

Field	Description
Template name	Specifies the template of this subscriber template.
Type	Specifies the messaging type of the subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can

Field	Description
	use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Saves all the changes.
Reset	undoes all the changes.
Cancel	Takes you to the previous page.

Editing Subscriber Templates (MM) field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
Template name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.

Field	Description
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]) .
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.

Field	Description
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Saves all the changes.
Reset	Undoes all the changes.
Cancel	Takes you to the previous page.

Viewing a Subscriber (CMM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Template	Specifies the template for this subscriber.
Type	Specifies the messaging type of your subscriber.
Software Version	Specifies the message version of the subscriber.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can

Field	Description
	use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Edit	Allows you to edit the fields.
Done	Takes you to the previous page.

Viewing a Subscriber (MM) field descriptions

Field	Description
System	Specifies the messaging system of the subscriber you want to add.
Type	Specifies the messaging type of your subscriber.
Software Version	Specifies the message version of the subscriber.
Template	Specifies the template chosen for this subscriber.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.

Field	Description
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]) .
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Subscriber Security

Field	Description
Expire Password	Specifies whether your password expires or not. You can choose one of the following: • **yes**: for password to expire • **no**: if you do not want your password to expire

Field	Description
Is Mailbox Locked?	Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: • **no**: to unlock your mailbox • **yes**: to lock your mailbox and prevent access to it

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.

Field	Description
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Edit	Allows you to edit the fields.
Done	Takes you to the previous page.

Viewing Subscriber Templates (CMM) field descriptions

Field	Description
Template name	Specifies the template of this subscriber template.
Type	Specifies the messaging type of the subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Extension	Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local machine.
Password	The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
COS	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Switch Number	Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank. • Leave this field blank if the host switch number should be used. • Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
Account Code	Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the

Field	Description
	voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.
Common Name	Specifies the display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Edit	Allows you to edit the fields.
Done	Takes you to the previous page.

Viewing Subscriber Templates (MM) field descriptions

Field	Description
Type	Specifies the messaging type of the subscriber template.
Template name	Specifies the messaging template of a subscriber template.
Software Version	Specifies the messaging version of the subscriber template.

Basic Information

Field	Description
Last Name	Specifies the last name of the subscriber.
First Name	Specifies the first name of the subscriber.
Numeric Address	Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service	The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box.
Community ID	Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.
Password	Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.

Subscriber Directory

Field	Description
Email Handle	Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an E-mail.
Telephone Number	The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]) .

Field	Description
Common Name	Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.
ASCII Version of Name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.

Mailbox Features

Field	Description
Backup Operator Mailbox	Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: • **urgent first then newest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received. • **oldest messages first**: to direct the system to play messages in the order they were received. • **urgent first then oldest**: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received. • **newest messages first**: to direct the system to play messages in the reverse order of how they were received.
Intercom Paging	Specifies the intercom paging settings for a subscriber. You can choose one of the following: • **paging is off**: to disable intercom paging for this subscriber. • **paging is manual**: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.

Field	Description
Voicemail Enabled	Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: • **yes**: to allow the subscriber to create, forward, and receive messages. • **no**: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Secondary Extensions

Field	Description
Secondary extension	Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.

Miscellaneous

Field	Description
Misc 1	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Edit	Allows you to edit the fields.
Done	Takes you to the previous page.

Bulk Add Station field descriptions

Use this page to bulk add stations.

Field	Description
Template	The template you choose for the stations.
Station name prefix	Specifies the prefix name that appears for each of the stations you add. You can enter a prefix name of your choice in this field.
System	Specifies the list of the Communication Managers.
Available extensions	The list of extensions that are available.
Enter extensions	The extensions that you want to use. You can enter your preferred extensions in this field.

Button	Description
Commit	Bulk adds the stations.
Schedule	Bulk adds the station at the scheduled time.
Clear	Undoes all the entries.
Cancel	Takes you to the previous page.

Bulk Edit Station field descriptions

Name	Description
Template	Specifies the station template. You can choose the template which you want to bulk edit.
Station Name Prefix	Specifies the prefix name which appears before all the stations that you bulk edit. You can enter a prefix name of your choice.

Button	Description
Commit	Bulk edits the stations.
Schedule	Bulk edits the stations at the specified time.
Clear	Undoes the entries.
Cancel	Takes you to the previous page.

Class of Service List field descriptions

Name	Description
Class No	Specifies the number of each class of service.
Name	Specifies the name of the class of service.
Last Modified	Specifies the time and date when the class of service was last modified.
Messaging System	Specifies the type of messaging system.

Note:

Click the respective column heading to sort the Class of Service by **Name** (in alphabetical order) and by **Class No**(by numeric order).

Station / Template field descriptions

You can use these fields to perform station / template tasks. This page has the exclusive fields that occur for stations and templates apart from the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.

Field description for Stations

Name	Description
System	Specifies the Communication Manager of the station.
Template	Specifies all the templates that correspond to the set type of the station.
Set Type	Specifies the set type of the station.
Name	Specifies the name of the station. You can enter the name of your choice in this field.

Field description for Templates

Name	Description
Set Type	Specifies the set type of the station template.

Template Name	Specifies the name of the station template. You can enter the name of your choice in this field.

Chapter 4: Monitoring Services

Scheduler

Scheduler

Scheduler is a schedule management service that provides the ability to monitor the tasks that are scheduled for execution. The scheduled tasks are of three types:

- System scheduled: The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but cannot delete the job.
- Admin scheduled job: The job that the administrator schedules for administering the application.
- On-demand job: The periodic jobs that the administrator may schedule to perform non-routine tasks.

You can browse the history of completed jobs. Using the Disable functionality, you can cancel all the executions scheduled for a task. The following are the important operations that you can perform using the Scheduler:

- View the pending and completed scheduled tasks
- Modify a task scheduled by an administrator or an On Demand Job
- Delete a scheduled task
- Schedule an On Demand Job
- Stop a running task
- Enable or Disable a task
- Search a scheduled task

Accessing scheduler

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.

Viewing logs for a job

Use this functionality to view logs for a pending and completed job.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - To view logs for a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **More Actions** > **View Log**.
   - To view logs for a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **More Actions** > **View Log**.

Result

The log viewer displays the log details for the selected job.

Viewing scheduled jobs

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - To view pending jobs perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **View**.
   - To view completed jobs, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **View**.

Result

The Job Scheduling-View Job page displays the details of the selected job.

Filtering Jobs

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - Click **Pending Jobs** in the left navigation pane and click **Filter: Enable** on the Pending Jobs page.
   - Click **Completed Jobs** in the left navigation pane and click **Filter: Enable** on the Completed Jobs page.

   The page displays the **Filter: Enable** at the upper-right of the page.
4. Select type of the job from the field under the **Job Type** column.
5. Enter the name of job in the field under the **Job Name** field.
6. Select the status of the job from the field under the **Job Status** field.

7. Select the state of the job from the field under the **State** field.
8. Select the frequency of execution of the job from the field under the **Frequency** field.
9. Enter the scheduler of the job in the field under the **Scheduled By** column.

   Note:
   This field is displayed only for the completed jobs.
10. Click **Apply**.

Result

The page displays jobs that match the filter criteria.

Editing a job

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - To edit a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **Edit**.

     Note:
     Alternatively, you can also click **View** > **Edit** to access the Job Scheduling-Edit Job page.
   - To edit a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **Edit**.

     Note:
     Alternatively, you can also click **View** > **Edit** to access the Job Scheduling-Edit Job pagepage.
4. On the Job Scheduling-Edit Job page, modify the appropriate information and click **Commit** to save the changes.

Note:

You can modify information in the following fields: **Job Name**, **Job State** in the **Job Details** sections, and **Task Time**, **Recurrence**, **Range** in the **Job Frequency** section.

Deleting a job

Prerequisites

You must log in as an administrator to delete an administrator scheduled job.

Use this functionality to delete an obsolete job. You can delete an On demand and on demand and administrator scheduled job.

Note:

You can remove only jobs that are of type Schedule On Demand.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - To remove a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job.

     Note:

     If the job that you want to delete is currently running then you must stop the job. To stop the job, click **More Actions** > **Stop**.

     Note:

     If the job that you want to delete is in the enabled state, disable the job.

     iii. Click **Delete**.
   - To remove a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job .

Note:

If the job that you want to delete is in the enabled state, disable the job.

iii. Click **Delete**.

4. On the Delete Confirmation page, click **Ok**.

Result

System Manager deletes the selected job from the database.

Disabling a job

Use this functionality to make a job inactive.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - To disable a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **More Actions** > **Disable**.
   - To disable a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **More Actions** > **Disable**.
4. On the Disable Confirmation page, click **Continue**.

Result

The **State** of the selected job is changed to Disabled.

Enabling a job

Use this functionality to make a job active.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:
   - To enable a pending job, perform the following steps:
     i. Click **Pending Jobs** in the left navigation pane.
     ii. On the Pending Jobs page, select a pending job and click **More Actions** > **Enable**.
   - To enable a competed job, perform the following steps:
     i. Click **Completed Jobs** in the left navigation pane.
     ii. On the Completed Jobs page, select a completed job and click **More Actions** > **Enable**.

Result

The **State** of the selected job is changed to Enabled.

Stopping a Job

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Monitoring** > **Scheduler** link in the left navigation pane.
3. Perform one of the following steps:

   To stop a pending job, perform the following steps:

   i. Click **Pending Jobs** in the left navigation pane.
   ii. On the Pending Jobs page, select a pending job in the running state and click **More Actions** > **Stop**.
   iii. Click **Continue** on the Stop Confirmation page.

Result

Scheduler stops the selected job.

Pending Jobs field descriptions

Use this page to view, edit and delete the scheduled jobs that are pending for execution.

Name	Description
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: 1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The options are: 1. Pending Execution 2. Running
State	The state of a job indicates if the job is an active job. The options are: • Enabled • Disabled
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
View	Opens the Job Scheduling-View Job page that displays the details of the selected pending job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.
Delete	Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.
More Actions > **View Log**	Opens the Logging page that displays the logs for the selected pending jobs.
More Actions > **Stop**	Stops the selected job which is currently in running state.
More Actions > **Enable**	Changes the state of the selected pending job from inactive to active.

Button	Description
More Actions > **Disable**	Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.
More Actions > **Schedule On Demand Job**	Opens the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a pending job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the pending jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the pending jobs that you have selected.
Refresh	Refreshes the pending job information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search the pending jobs. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the pending jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Completed Jobs field descriptions

Use this page to view and edit the completed jobs. In addition, you can also perform the following operations:

- Disable or Enable a job
- View a log
- Schedule and delete an on demand job

Name	Description
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. Following are the job types: 1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The options are: 1. Status Unknown 2. Interrupted 3. Failed 4. Successful 5. Not Authorized
Last Run	The date and time when the job was last run.
State	The state of a job indicates if the job is an active. The options are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
View	Opens the Job Scheduling-View Job page that displays the details and of the selected completed job.

Button	Description
Edit	Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected completed job.
Delete	Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.
More Actions > **View Log**	Opens the Logging page that displays the logs for the selected completed jobs.
More Actions > **Enable**	Changes the state of the selected completed job from inactive to active.
More Actions > **Disable**	Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected completed job.
More Actions > **Schedule On Demand Job**	Opens the Job Scheduling-On Demand Job page that you can use to schedule a On Demand job.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a completed job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the completed jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the completed jobs that you have selected.
Refresh	Refreshes the completed job information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search the completed jobs. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the completed jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: 1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.
Job Status	The current status of the job. The options are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
Job State	The state of a job indicates whether the job is an active job or not. The options are: • Enabled • Disabled

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also displays the frequency of recurrence.
Range	The number of recurrences or a date after which the job stops to recur.

Button	Description
View Log	Opens the Logging page that you can use to view the logs for the selected job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to edit the pending job information.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending or Completed Jobs page.

Job Scheduling-Edit Job field descriptions

Use this page to modify job details and frequency related information of a selected job.

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: 1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks. **Note:** You can only view the information in this field.
Job Status	The current status of the job. The options are:

Name	Description
	1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized **Note:** You can only view the information in this field.
Job State	The state of a job indicates whether the job is an active job or not. The options are: • Enabled • Disabled
Scheduled By	The scheduler of the job. **Note:** You can only view the information in this field.

Job Frequency

Name	Description
Task Time	The date and time of running the job. Use the calendar icon to select a date. The time is in the HH:MM:SS format followed by PM and AM.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field displays the frequency of recurrence.
Range	The number of recurrences or the date after which the job stops to recur.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending or completed Jobs page.

Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on demand job.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also display the time interval of recurrence. The options are: • Execute task one time only. • Task are repeated every day.
Range	The settings define the number of recurrences or date after which the job stops recurring. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules an On-Demand job.
Cancel	Cancels the schedule an On Demand job operation and takes you back to the Pending or completed Jobs page.

Disable Confirmation field descriptions

Use this page to disable selected jobs.

Name	Description
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types:

Name	Description
	1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The options are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
State	The state of a job indicates whether the job is an active job or not. The options are: • Enabled • Disabled
Last Run	The date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Disables the job and cancels the next executions that are scheduled for the job.
Cancel	Cancels the operation of disabling a job and takes you back to the Pending or completed Jobs page.

Stop Confirmation field descriptions

Use this page to stop a running job.

Name	Description
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: 1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The jobs on this page have status Running.
State	The state of a job indicates if the job is an active job. All the jobs on this page are in the Enabled state.
Last Run	The date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Stops the job.
Cancel	Cancels the operation of stopping a job and takes you back to the Pending Jobs page.

Delete Confirmation field descriptions

Name	Description
Job Type	The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types:

Name	Description
	1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job. 2. Admin scheduled job — The job that the administrator schedules for administering the application. 3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.
Job Name	The name of the scheduled job.
Job Status	The current status of the job.
State	The state of a job indicates if the job is an active job. The jobs on this page are in the disabled state.
Last Run	The date and time when the job was last run. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Deletes the selected job.
Cancel	Cancels the operation of deleting a job and takes you back to the Pending or completed Jobs page.

Alarming

Alarming

The Alarming service provides an interface for monitoring alarms generated by System Manager and other components. You can perform the following operations using the Alarming service:

- View an alarm
- Change the status of an alarm
- Export alarms to a Comma Separated Values (csv) file

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation and identify the system component which generated the alarm.

System Manager can be configured to forward alarms to Avaya Services. It can also be configured to send SNMP traps to a customer Network Management System (NMS).

Alarming field descriptions

The Alarming page displays a list of alarms. Use this page to view the alarms in the Auto-Refresh mode. In this mode, the page updates the alarm information automatically.

Field	Description
Time Stamp	Date and time when the alarm is generated.
Severity	Severity of the alarm.
Status	Current status of the alarms.
Host Name	The name of the host computer that generated the alarm.
Message	A short description of the problem that generated the alarm.
Identifier	Unique identifier for an alarm.
M/E Ref Number	A unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm.

Button	Description
Alarm landing Page	Switches the mode from Auto-Refresh to Manual refresh and displays the Alarming Home page. This is a toggle button.

Alarming field descriptions

The Alarming page has two sections; Upper and Lower. The upper section has buttons that you can use to view the details of the selected alarms, change the status of alarms, search for alarms , and set filters to view specific alarms. The lower section displays alarms in a table. The table provides information about the status of the alarms along with their severity. You can click a column title to sort the information in the table in ascending or descending order.

Field	Description
Time Stamp	Date and time when the alarm is generated.
Severity	Severity of the alarm.
Status	Current status of the alarms.
Host Name	The name of the host computer that generated the alarm.

Field	Description
Message	A short description of the problem that generated the alarm.
Identifier	Unique identifier for an alarm.
Agent Reference	The reference number of the agent who has reported the alarm.
M/E Ref Number	A unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • Acknowledged • Clear
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. This is a toggle button.
More Actions > **Export Selected**	Exports the selected alarms to a CSV file, which can be viewed with Wordpad or Excel.
More Actions > **Export All**	Exports all the alarms to to a CSV file, which can be viewed with Wordpad or Excel.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	Displays the logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the upper right corner of page.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Criteria</td><td>Use this section to specify search conditions. Select the search criteria from the first drop-down list. Select the operator from the second drop-down field. Enter the search value in the text field.
Select following search criteria from the first drop-down list:
Time Stamp: Searches all of the alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM.
Severity: Searches all of the alarms that match the specified severity level.
Status: Searches all of the alarms that match the specified status.
Host Name: Searches all of the alarms that are generated from the specified host.
Identifier: Searches all of the alarms that match the specified identifier.
Message: Searches all of the alarms that match the specified message.
M/E Ref Number: Searches all of the alarms that match the specified M/E Ref Number.
The operators available are based on the search criterion that you select in the first drop-down field. The following table list the operators that are available for a search criterion:<table><tr><th>Criterion</th><th>Operators</th></tr><tr><td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr><tr><td>Severity</td><td>Equals, Not Equals</td></tr><tr><td>Status</td><td>Equals, Not Equals</td></tr><tr><td>Host Name</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>Identifier</td><td>=, >, <, >=, <=, >=, !=</td></tr><tr><td>Message</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>M/E Ref Number</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr></table>When you select Begin Date and End Date from the first drop-down list, you are prompted to enter the date in the third field.</td></tr>
</table>

Button	Description
Clear	Clears the entered search criteria and sets the default search criteria.
Search	Searches the alarms based on the search conditions.

Button	Description
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition.

Viewing alarms

1. On the System Manager console, click **Monitoring** > **Alarming** in the left navigation pane.
2. Select an alarm. You can select multiple alarms.
3. Click **View**.

Changing status of an alarm

The status of an alarm can be:

- Acknowledged – Maintenance support must manually set the alarm to this state, indicating the alarm is under investigation.
- Cleared – Maintenance support must manually set the alarm to this state, indicating that the error condition has been resolved.

1. On the System Manager console, click **Monitoring** > **Alarming** in the left navigation pane.
2. On the Alarming page, select an alarm and click **Change Status**.

   You can select multiple alarms.
3. Click on the status that you want to apply to the selected alarms.

Exporting alarms

Alarms can be exported to a Comma Separated Values (csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Excel.

1. On the System Manager console, click **Monitoring** > **Alarming** in the left navigation pane.
2. On the Alarming page, perform one of the following steps:
   - To export a selected alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.
   - To export all the alarms to a CSV file, click **More Actions** > **Export All**.
3. Click **Save** to save the exported file to the local disk.

Filtering alarms

The criteria for filtering the alarms are status, M/E Reference Number, Agent Reference, or severity. You can use more than one filter criterion on the selected alarms.

1. On the System Manager console, click **Monitoring** > **Alarming** in the left navigation pane.
2. On the Alarming page, select the alarms you want to filter.
3. Click **Filter: Enable** at the top right corner of the alarm log table.
4. Select the filter criteria you want to apply to the selected alarms.
   The **Status** and **Severity** fields have drop-down menus.
5. Click **Filter: Apply**.

Note:

A message will be displayed if no records are found which match the specified filter criteria.

Result

The page displays the alarms matching the filter criteria on the Alarm viewer.

Searching for alarms

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays only those alarms which satisfy the search conditions. Multiple search conditions can be specified.

1. On the System Manager console, click **Monitoring** > **Alarming** in the left navigation pane.
2. On the Alarming page, click **Advanced Search**.
3. In the Click to Search to find alarms for the given search conditions section, select the search criterion from each of the drop-down fields.
4. If you want to add another search condition, click the **+** button.

   Note:

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
5. Select the AND or OR from the drop-down field.

   This option appears when you add a search condition using the + button.
6. Click **Search** to find alarms for the given search conditions.

Logging

Logging

The logging service provides an interface for viewing logs and their details generated by System Manager or other components. The System Manager console allows you to monitor log messages. You can view the details of a log, perform a search for logs, and filter specific logs. Log detail includes information about the event which generated the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

Viewing log details

1. On the System Manager console, click **Monitoring** > **Logging** in the left navigation pane.
2. On the Logging page, select a log.
3. Click **View**.

Searching for logs

Use the Advanced Search function to find logs based on certain specified conditions. The system displays only those logs which satisfy the search conditions. Multiple search conditions can be specified.

1. On the System Manager console, click **Monitoring** > **Logging** in the left navigation pane.
2. On the Logging page, click **Advanced Search**.
3. In the *Criteria* section, from the first and second drop-down fields, select the search criterion and the operator.
4. Select or enter the search value in the third field.
5. If you want to add another search condition, click **+** and repeat the steps 4 through 6.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
6. Select the AND or OR operator from the drop-down field.

   This page displays this drop-down field when you specify more than one search condition.
7. Click **Search** to find the logs for the given search conditions.

Filtering logs

You can filter and view logs that meet the specified filter criteria. Applying the filters requires you to specify the filter criteria in the fields provided under select columns in the table displaying the logs. The column titles are the filter criteria. You can filter logs on multiple filter criteria.

1. On the System Manager console, click **Monitoring** > **Logging** in the left navigation pane.
2. On the Logging page, click **Filter: Enable**.
   You can find this button on the top right corner in the table displaying logs.
3. Enter or select the filter criteria.
4. Click **Filter: Apply**.

Note:

If no records matching the filter criteria are found, the Management Console application displays a message that no records matching the search criteria are found.

Result

The page displays the logs that matches the specified filter criteria.

Logging field descriptions

The Logging page has two sections. The upper section contains buttons that allow you to view the details of the selected logs, search for logs, and set filters. The lower section displays logs in a table. The table provides information about the logs. You can click the title of the column to sort the data of the column in ascending or descending order.

Name	Description
Select check box	Use this check box to select a log.
Log ID	Unique identification number that identifies the log.
Time Stamp	Date and time of the log generation.
Host Name	Name of the system from which the log is generated.

Name	Description
Product Type	A code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.
Severity	Severity level of the log. The following are the type of severities: • Emergency : System is unusable • Alert : Action must be taken immediately • Critical : Critical conditions • Error : Error conditions • Warning : Warning conditions • Notice: Normal but significant condition • Informational : Informational messages • Debug: Debug-level messages  **Note:** The colors of severities do not indicate logging severities.
Event ID	Unique identification number assigned to the event that has generated the log.
Message	Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	Process on the device that has generated the message. This is usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Opens the Log - View Log Detail page. Use this page to view the details of a selected log.
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. This is a toggle button.

Button	Description
Advanced Search	Displays fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	Displays logs in the previous page. This button is not available if you are on the first page.
Next	Displays logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the top right corner.

Name	Description
Criteria	Use this section to specify search conditions. Select the search criteria from the first drop-down field. Select the operator from the second drop-down field. Enter the search value in the text field. Select following search criteria from the first drop-down field: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated. • Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message • Time Stamp: Date and time of the log generation. • Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The second drop-down field displays operators. Based on the search criterion that you select in the first drop-down field, only those operators that are applicable for

Name	Description
	the selected criterion are displayed in the second drop-down field. The following are the list of operators: • Equals • Not Equals • Starts With • Ends With • Contains The operators for Time Stamp are: =, >, <, >=, <=, and !=. When you select Time Stamp from the first drop-down field, the page provides date and time fields for entering the date and time in the respective fields. Enter the date in MM/DD/YYYY format . You can select the date from the calender. You need to enter the time in one of the following format: • 24Hr • AM • PM

Button	Description
Clear	Clears the search criterion and set it to the default search criteria.
Search	Searches the logs based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition

Logging field descriptions

Use this page to view logs in the Auto-Refresh mode. In this mode, the page updates the log information automatically.

Name	Description
Log ID	Unique identification number that identifies the log.
Time Stamp	Date and time of the log generation.
Host Name	Name of the system from which the log is generated.

Name	Description
Product Type	A code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.
Severity	Severity level of the log. The following are the type of severities: • Emergency : System is unusable • Alert : Action must be taken immediately • Critical : Critical conditions • Error : Error conditions • Warning : Warning conditions • Notice: Normal but significant condition • Informational : Informational messages • Debug: Debug-level messages  **Note:** The colors of severities do not indicate logging severities.
Event ID	Unique identification number assigned to the event that has generated the log.
Message	Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	Process on the device that has generated the message. This is usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
Logging Landing Page	Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. This is a toggle button.

Chapter 5: User Management

User Management module includes some of the System Manager administration specific features which are not supported for Session Manager administration. Some of these features are listed as follows:

- Manage Roles
- Assign Roles
- Global User Settings

Manage Roles

Manage Roles

The Manage Roles service provides the management interface for administering roles and permissions. To define a role, you need to grant permissions on groups and resources of a particular resource type. The permissions on resources and groups for a role are the operations that a user assigned to this role can perform. You can perform the following important operations using the service:

- Create a role
- View and Modify roles
- Delete roles
- Create a duplicate group by copying the properties of an existing group
- Search a role

Viewing user roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select a role and click **View**.

Related topics:

View Role field descriptions on page 171

Creating a user role

Use this functionality to create a role assign a set of permissions to this role.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, click **New**.
4. On the New Role page, enter the name of the role and description of the role in the **Name** and **Description** fields in the Role Details section.
5. Click **Permission Set** > **Add** to assign permissions on the resources for a role.
6. Click **Commit**.

Related topics:

New Role field descriptions on page 167

Modifying user roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. Perform one of the following steps:

- On the Manage Roles page, select a role and click **Edit**.
- On the Manage Roles page, select a role and click **View** > **Edit**.

4. On the Edit Role, modify the name of the role and description of the role in the **Name** and **Description** fields in the Role Details section.
5. Click **Permission Set** > **Add** to modify the permissions assigned to the role.
6. Click **Commit**.

Related topics:

Edit Role field descriptions on page 169

Creating duplicate roles

You can use this functionality to copy an existing role to create a new role. When you create a duplicate role, the system copies all the information from the existing role to the duplicate user account.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select a role and click **Duplicate**.
4. Enter the appropriate information.
5. Click **Commit** to save the changes to the database.

Related topics:

Duplicate Role field descriptions on page 172

Deleting user roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select a role and click **Delete**.

Searching for roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Role page, click **Advanced Search** displayed at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   Note:
   If you want to add a search condition, click **+** and repeat sub steps a through c listed in step 4.

   Note:
   If you want to delete a search condition, click **-** . This button is available if there are more than one search condition.
5. Click **Search**.

Result

The page displays the roles that matches the value specified for the search criteria.

Related topics:

Manage Roles field descriptions on page 166

Filtering roles

You can apply filter on the Role Name column

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, click **Filter: Enable**.
   You can find the button at the upper-right corner of the table displaying roles.

4. Enter the role name in the field under the **Role Name** column.
5. Click **Apply** .

Note:
To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

Result

The table displays only those roles that matches the filter criteria.

Related topics:

Manage Roles field descriptions on page 166

Assigning users to roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select a user role and click **More Actions** > **Assign User Roles**.
4. On the Assign Users page, select the users displayed in the **Select Users** section.
5. Click **Commit**.

Related topics:

Assign Users To Roles field descriptions on page 174

Removing users from roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select one or more user roles and click **More Actions** > **UnAssign User Roles**.

4. On the UnAssign Roles page, select the users displayed in the Select Users section.
5. Click **Commit**.

Related topics:

UnAssign Roles field descriptions on page 175

Assigning permissions to a role

When you create a role, you need to assign permission to this role. Permissions include actions that a user to which you assign the role can perform over the selected groups and resources. The actions that a user can perform over a resource or group varies with the type of resource. You can add more than one permission that may include groups and resources of a different resource type or of same resource type.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, perform one of the following roles:
   - Click **New**.
   - Select a role and click **Edit**.
   - Select a role and click **View** > **Edit**.
4. Click **Permission Set** > **Add**
5. From the **Resource Type** drop-down field, select a type of resource.
6. From the **Actions** list box, select the actions.
   Use the CTRL and up and down arrow keys to select more than one actions.
7. In the Selected Groups and Resources section, click **Add** to add a group and resources.
8. In the Selected Attributes section, click **Add** to add attributes.
9. Click **Add**.
   You can find the Add button following the label **Permission Set**.

Note:

To add another permission over groups and resources of different resource type or of same resource type with different set of resources and groups, repeat the steps from 5 to 9.

Removing permissions from a role

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, perform one of the following roles:
   - Select a role and click **Edit**.
   - Select a role and click **View** > **Edit**.
4. Click **Permission Set**
5. In the Permission Detail section, select the permission and click **Delete** .

Adding groups and resources to a permission

Use this functionality to specify the groups and resources over which you want to apply the permission. You may choose to apply the permission over all or selected groups and resources.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, perform one of the following roles:
   - Click **New**.
   - Select a role and click **Duplicate**.
   - Select a role and click **Edit**.
   - Select a role and click **View** > **Edit**.
4. Click **Permission Set** > **Add**.
5. In the Selected Groups and Resources section, perform one of the following steps:

   To apply permission over all the groups and resources that exists under the specified Resource Type, click **All**

   To apply permission over the chosen groups and resources that exists under the specified Resource Type:

   i. click **Select**.

   ii. click **Add**

iii. On the Select Groups and Resources page, select group and resources and click **Save**.

Related topics:

Select Groups and Resources field descriptions on page 176

Removing groups and resources from a permission

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, perform one of the following roles:

   Note:

   If you are on the New Role page and have already added a group and/or resource, then proceed to step 4.

   - Select a resource and click **Duplicate**.
   - Select a resource and click **Edit**.
   - Select a resource and click **View** > **Edit**.
4. Click **Permission Set**.
5. In the Selected Groups and Resources section, select the resources and groups that you want to remove from the permission and click **Delete**.

Adding attributes to a role

Use this functionality to add attributes over which you want to apply the permissions. Each resource type has a set of attributes associated with it. All the groups and resources of a resource type inherit the attributes that are defined for that resource type. If you do not specify any attribute, the table in the Selected Attributes section displays none.

Note:

Permission to an attribute woks only when there is minimum one group or resource added to the role.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Log in to the Common Console Management web interface.
3. Click **User Management** > **Manage Roles** in the left navigation pane.
4. On the Manage Roles page, perform one of the following steps:
   - Click **New**.
   - Select a role and click **Edit**.
   - Select a role and click **View** > **Edit**.
5. Click **Permission Set** > **Add**.
6. In the Selected Attributes section, perform one of the following steps:

   To apply permission over all the attributes that exists under the specified Resource Type, click **All**

   To apply permission over the selected attributes that exists under the specified Resource Type:

   i. click **Select**.
   ii. click **Add**
   iii. On the Select Attributes page, select attributes and click **Save**.

Removing attributes from a permission

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, perform one of the following roles:

   Note:
   If you are on the New Role page and have already added an attribute, then proceed to step 4.

   - Select a role and click **Duplicate**.
   - Select a role and click **Edit**.
   - Select a role and click **View** > **Edit**.

4. Click **Permission Set**.
5. In the Selected Attributes section, select the attributes that you want to remove from the permission and click **Delete**.

Manage Roles field descriptions

Use this page to:

- Add, modify, view and delete roles.
- Assign roles to or remove roles from an existing user.

Name	Description
Role name	Name of the role.
Resource Type	The type based on the resources.
Role Type	Type of the role.
Description	Insert a description of this field.

Button	Description
View	Opens the View Role page that displays the details of the selected role.
Edit	Opens the Edit Role page that you can use to modify the selected role.
New	Opens the New Role page that you can use to add a new role and assign permissions to the roles.
Duplicate	Opens the Duplicate Role page to create a duplicate role.
Delete	Deletes a selected role.
More Actions > Assign User Roles	Opens the Assign Users page that you can use to assign roles to the user.
More Actions > UnAssign User Roles	Opens the UnAssign Users page that you can use to unassign roles for a user.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a role.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.

Button	Description
Filter: Apply	Filters roles based on the filter criteria.
Select: All	Selects all the roles in the table.
Select: None	Clears all the check box selections.
Refresh	Refreshes the role's information in the table.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search roles. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value for the search criterion. The Roles Management service retrieves and displays roles that match this value.

New Role field descriptions

Use this page to create a new role and assign permissions to the role. The page has two sections:

- Role Details
- Permission Set

Role Details section

Name	Description
Name	Name of the role.
Description	A brief description of the role.

Button	Description
Commit	Creates a new role.
Cancel	Closes the New Role page and returns to the Manage Roles page.

Permission Set section

Name	Description
Select option button	Use this button to select a permission over groups and resources.
Resource Type	The type based on the resources. The table displays group and resources for the resource type that you specified in the **Resource Type** drop-down field in the Permission Detail section.
Actions	Actions that you can perform over the specified groups and resources.
Groups and Resources	Groups and resources added to this permission.
Attributes	Attributes assigned to this permission.

Button	Description
Add	Adds a permission to the role.
Delete	Deletes a selected permission from the role.

Permission Detail

Name	Description
Resource Type	The type based on the resources.
Actions	Permissions that can be set for the corresponding resource type.

Selected Groups and Resources

Name	Description
Select check box	Use the check box to select group and resource.
Resource Name	The name of the resource.
Resource Type	The type based on the resources.
Resource Description	A brief description about the resource.

Button	Description
Add	Opens the Select Groups and Resources page that you can use to select and add groups and resources to the permission. The user to which you assign this role can perform the operations specified in the **Actions** list box over the selected groups and resources.
Delete	Removes the selected groups and/or resources form the permission.
All	Use this option button to apply permissions over all groups and resources for the specified resource type.

Button	Description
Select	Use this option button to apply permissions over the selected groups and resources for the specified resource type.
Select: All	Selects all the groups and roles in the table.
Select: None	Clears all the check box selections.

Selected Attributes

Name	Description
Name	Name of the Attribute

Button	Description
Add	Opens the Select Attributes page that you can use to select an attribute.
Delete	Removes the selected groups and resources.
All	Use this option button to apply permissions over all the attributes of the specified group and resources.
Select	Use this option button to apply permissions over the selected attributes of the specified group and resources.
Select: All	Selects all the attributes in the table.
Select: None	Clears the check box selections.

Related topics:

Creating a user role on page 158

Edit Role field descriptions

Use this page to edit a role.

Role Details section

Name	Description
Name	Name of the role.
Description	A brief description of the role.

Button	Description
Commit	Creates a new role.
Cancel	Cancels the role modifying operation and returns you to the to the Manage Roles page.

Permission Set section

Name	Description
Select option button	Use this button to select a permission over groups and resources.
Resource Type	The type based on the resources. The table displays group and resources for the resource type that you specified in the **Resource Type** drop-down field in the Permission Detail section.
Actions	Actions that you can perform over the specified groups and resources.
Groups and Resources	Groups and resources added to this permission.
Attributes	Attributes assigned to this permission.

Button	Description
Add	Adds a permission to the role.
Delete	Deletes a selected permission from the role.

Permission Detail

Name	Description
Resource Type	The type based on the resources.
Actions	Permissions that can be set for the corresponding resource type.

Selected Groups and Resources

Name	Description
Select check box	Use the check box to select group and resource.
Resource Name	The name of the resource.
Resource Type	The type based on the resources.
Resource Description	A brief description about the resource.

Button	Description
Add	Opens the Select Groups and Resources page that you can use to select and add groups and resources to the permission. The user to which you assign this role can perform the operations specified in the **Actions** list box over the selected groups and resources.
Delete	Removes the selected groups and/or resources form the permission.
All	Use this option button to apply permissions over all groups and resources for the specified resource type.

Button	Description
Select	Use this option button to apply permissions over the selected groups and resources for the specified resource type.
Select: All	Selects all the groups and roles in the table.
Select: None	Clears all the check box selections.

Selected Attributes

Name	Description
Name	Name of the attribute

Button	Description
Add	Opens the Select Attributes page that you can use to select an attribute.
Delete	Removes the selected attributes.
All	Use this option button to apply permissions over all the attributes of the specified group and resources.
Select	Use this option button to apply permissions over the selected attributes of the specified group and resources.
Select: All	Selects all the attributes in the table.
Select: None	Clears the check box selections.

Related topics:

Modifying user roles on page 158

View Role field descriptions

Use this page to view the details of a selected role.

Role Details section

Name	Description
Name	Name of the role.
Description	A brief description of the role.

Button	Description
Edit	Opens the Edit Role page. Use the page to edit a selected role.
Cancel	Closes the View Role page and returns you to the Manage Roles page.

Permission Set section

Name	Description
Resource Type	The type based on the resources. The table displays group and resources for the resource type that you specified in the **Resource Type** drop-down field in the Permission Detail section.
Actions	Actions that you can perform over the specified groups and resources.
Groups and Resources	Groups and resources added to this permission.
Attributes	Attributes assigned to this permission.

Button	Description
Refresh	Refreshes the permission's information.

User Assignment

Name	Description
Status	The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.
Name	Name of the user.
Login Name	The unique system login name given to the user. It takes the form of username@domain.
User Name	Unique name by which the system identifies the user.
Phone Number	Contact number of the user.
Last Login	Date and time when the user has last logged into the system
User Type	The role of the user.

Button	Description
Refresh	Refreshes the user's information.

Related topics:

Viewing user roles on page 158

Duplicate Role field descriptions

Use this page to create a duplicate role and assign permissions to the role. The page has two sections:

- Role Details
- Permission Set

Role Details section

Name	Description
Name	Name of the role.
Description	A brief description of the role.

Button	Description
Commit	Creates a duplicate role.
Cancel	Closes the New Role page and returns to the Manage Roles page.

Permission Set section

Name	Description
Select option button	Click this button to select a permission.
Resource Type	The type based on the resources.
Actions	Permissions available for the resource type.
Groups and Resources	Groups and resources added to this permission.
Attributes	Attributes assigned to this permission.

Permission Detail

Name	Description
Resource Type	The type based on the resources.
Actions	Permissions that are available for the resource type.

Button	Description
Add	Adds a permission to the role.
Delete	Deletes a selected permission.

Selected Groups and Resources

Name	Description
Select check box	Use the check box to select group and resource.
Resource Name	The name of the resource.
Resource Type	The type based on the resources.

Name	Description
Resource Description	A brief description about the resource.

Button	Description
Add	Opens the Select Groups and Resources page that you can use to select and add a group and resource to the permission.
Delete	Removes the selected groups and/or resources.
Select: All	Selects all the groups and roles in the table.
Select: None	Clears the selections.

Selected Attributes

Name	Description
Name	Name of the Attribute

Button	Description
Add	Opens the Select Attributes page that you can use to select an attribute.
Delete	Removes the selected groups and/or resources.
Select: All	Selects all the groups and roles in the table.
Select: None	Clears the selections.

Button	Description
Add	Adds a permission to the role.
Delete	Deletes a selected permission.

Related topics:

Creating duplicate roles on page 159

Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. The page has two sections:

- Selected Roles
- Select Users

Selected Roles section

The roles to which you can assign users.

Name	Description
Name	Name of the role.
Resource Type	The resource type that the corresponding role is assigned.
Description	A brief description about role.

Select Users section

The table displays the users to which you can assign the roles.

Name	Description
Select check box	Use this check box to select the user.
Status	Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application.
User Name	The unique name that identifies the user
Last Login	Time and date when the user has last logged into the system.
User Type	The type that defines the role of the user.

Button	Description
Commit	Assigns user to the role.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

Related topics:

Assigning users to roles on page 161

UnAssign Roles field descriptions

Use this page to unassign a role form the selected users. The page has two sections:

- Selected Roles
- Select Users

Selected Roles section

The role from which users are unassigned.

Name	Description
Name	Name of the role.
Resource Type	The resource type that the corresponding role is assigned.
Description	A brief description about the role.

Select Users section

The table displays the users for which you can remove the roles.

Name	Description
Select check box	Use this check box to select the user.
Status	Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application.
User Name	The unique name that identifies the user
Last Login	Time and date when the user has last logged into the system.
User Type	The type that defines the role of the user.

Button	Description
Commit	Unassigns the role from the users.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

Related topics:

Removing users from roles on page 161

Select Groups and Resources field descriptions

Use this page to add groups and resources to a role.

Name	Description
Select check box	Use this check box to select groups and resources.
Name	Name of the group and resource
Type	Type of a group and resource. If it is a resource then type is based on the resources it contains. If it is a group then type is based on a group with members belonging to a same resource type or group with no restrictions on the type of members.
Description	A brief description about a group or resource.

Button	Description
Save	Adds the selected resources and groups to the permission.
Cancel	Closes the page and returns to the New Role page.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters roles based on the filter criteria.
Select: All	Select all the groups and roles in the table.
Select: None	Clears the selections.

Related topics:

Adding groups and resources to a permission on page 163

Select Attributes field descriptions

Use this page to select and apply attributes to the selected role.

Name	Description
Select Check box	Use this check box to select the attribute. Use the check box displayed as one of the column header to select all the attributes in the table.
Name	Name of the attribute.

Button	Description
Save	Adds the selected attributes to the permission.
Cancel	Cancels the select attributes operations and takes you back to the New Role or Edit Role page.
Select: All	Select all the attributes in the table.
Select: None	Clears all the check box selections.

User Management

User Profile Management

User Profile Management is a shared management service that provides a central user administration. Centralized administration reduces the need for replicating a user's data across

multiple products. Following is the list of important operations that you can perform using the User Management shared service:

- Add a user profile
- View and Modify an existing user profile
- Delete a user profile
- Assign and remove permission, roles, groups, access control list, contacts and attributes for users
- Search for a user

A system administrator can only add, modify, and delete the user profiles.

Users in Management Console

Access to the Management Console web interface requires a valid user name and password. Avaya recommends that you create a limited number of accounts and ensure that the passwords they use are secure.

Users with login privileges can add, modify, and delete accounts on the Management Console. To obtain a user account and password to the console, see your system administrator.

Viewing user accounts

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the Users page, select a user. You can view only one user account at one time.
4. Click **View** to view the selected user account.

Modifying user accounts

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the Users page, select a user.
   You can edit only one user account at one time.
4. To edit a user account, perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. Modify the information and click **Commit** to save the changes to the database.

Related topics:

User Profile Edit field descriptions on page 211

Creating a new user profile

Use this functionality to create a new user profile.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, click **New**.
4. On the New User Profile page, enter the appropriate information click **Commit**.
   The field names that are marked with * are mandatory fields. You must enter valid information in these fields for the successful creation of the user.

Related topics:

New User Profile field descriptions on page 219

Creating duplicate users

Use this functionality you can create a new user account by copying the information from an existing user account. When you create the new user account, the system copies all the information from the existing user account to the new user account.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, select the user account that you want to duplicate.
4. Click **Duplicate**.
5. On the User Profile Duplicate page, enter the appropriate information and click **Commit**.

Related topics:

User Profile Duplicate field descriptions on page 229

Removing user accounts

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, select a user from the table and click **Delete**.
4. On the User Delete Confirmation page, click **Delete**.

Note:

This operation marks the deleted users as deleted and stores them in the database in a list of deleted users.

Related topics:

User Delete Confirmation field descriptions on page 233

Filtering users

You can apply filter on the following four columns:

- Status
- Name
- User Name
- User Type

You may filter users using one or multiple column filters.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, click **Filter: Enable**.
   You can find the button at the upper-right corner of the table displaying roles.
4. Select the status of the user from the drop-down under the **Status** column.
5. Enter the name of the user in the field under the field **Name** column.
6. Enter the user name in the field under the field **User Name** column.
7. Enter the role of the user in the field under the field **User Type** column.
8. Click **Apply** .

Note:
To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

Result

The table displays only those users that match the filter criteria.

Searching for users

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.

3. On the User Management page, click **Advanced Search** displayed at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   Note:
   If you want to add a search condition, click **+** and repeat sub steps a through c listed in step 4.

   Note:
   If you want to delete a search condition, click **-** . This button is available if there are more than one search condition.
5. Click **Search**.

Result

The page displays the users that match the value specified for the search criteria.

Assigning roles to single and multiple users

To provide access to resources, you need to assign roles to the user accounts.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - To assign roles to a new user, perform the following steps:
     i. On the User Management page, click **New** .
     ii. On the New User Profile page, click **Roles** > **Assign Roles**.
     iii. On the Assign Roles page, select the roles from the **Available Roles** sections.
     iv. Click **Select** to assign the roles to the user.
   - To assign roles to an existing user, perform the following steps:

i. On the User Management page, select a user and click **Edit**.

Note:

You can also select a user and click **View** > **Edit** to access the User Profile Edit page.

ii. On the User Profile Edit page, click **Roles** > **Assign Roles**.

iii. On the Assign Roles page, select the roles from the **Available Roles** sections.

iv. Click **Select** to assign the roles to the selected user.

- To assign roles to multiple users, perform the following steps:

i. On the User Management page, select the users and click **More Actions** > **Assign Roles**.

ii. On the Assign Roles page, select roles from the **Select Roles** section.

iii. Click **Commit** to assign roles to the selected users.

Removing roles from a user

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - If you are creating a new user account and you have already assigned a role, then click **New** > **Roles**.
   - If you are removing a role in the edit mode, on the Users page, select a user and click **Edit** > **Roles**.
   - If you are removing a role in the view mode, on the Users page, select a user and click **View** > **Edit** > **Roles**.
4. Select roles and click **Remove Roles** to remove the assigned roles.

Assigning attribute sets to single and multiple users

To provide access to a set of attributes, you need to assign attribute sets to a user account .

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - To assign attribute sets to a new user, perform the following steps:
     i. On the User Management page, click **New**.
     ii. On the New User Profile page, click **Attribute Sets** > **Assign Attribute Sets**
     iii. On the Select Attributes page, navigate to the **Available Attributes** section and select the attribute sets.
     iv. Click **Select** to assign the attribute sets to the users.
   - To assign attribute sets to an existing user, perform the following steps:
     i. On the User Management page, select a user and click **Edit**.

     Note:
     You can also select an user and click **View** > **Edit** to access the User Profile Edit page.

     ii. On the User Profile Edit page, click **Attribute Sets** > **Assign Attribute Sets**.
     iii. On the Select Attributes page, navigate to the **Available Attributes** section and select the attribute sets.
     iv. Click **Select** to assign the attribute sets to the users.
   - To assign attribute sets to multiple users, perform the following steps:
     i. on the User Management page, select the users and click **More Actions** > **Assign Attribute Sets**.
     ii. On the Assign Attributes Sets page, navigate to the **Select Attribute Sets** section and select the attribute sets.
     iii. Click **Commit** to assign the attribute sets to the users.

Removing attribute sets

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - If you are creating a new user account and you have already assigned an attribute set, then click **New** > **Attribute Sets**.
   - If you are removing an attribute set in the edit mode, on the User Management page, select a user and click **Edit** > **Attribute Sets**.
   - If you are removing an attribute set in the view mode, on the User Management page, select a user and click **View** > **Edit** > **Attribute Sets**.
4. Select the attribute sets and click **Remove Attribute Set** to remove the attribute sets.

Assigning groups to single and multiple users

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - To assign groups to a new user, perform the following steps:
     i. On the User Management page, click **New** .
     ii. On the New User Profile page, click **Group Membership** > **Add To Group**.
     iii. On the Assign Groups page, select the groups from the **Available Groups** section.
     iv. Click **Select** to assign the groups to the user.
   - To assign groups to an existing user, perform the following steps:
     i. On the User Management page, select a user and click **Edit**.

Note:

You can also select a user and click **View** > **Edit** to access the User Profile Edit page.

ii. On the New User Profile page, click **Group Membership** > **Add To Group**.

iii. On the Assign Groups page, select the groups from the **Available Groups** section.

iv. Click **Select** to assign the groups to the user.

- To assign groups to multiple users, perform the following steps:

i. On the User Management page, select the users and click **More Actions** > **Add To Group**.

ii. On the Assign Groups page, select the groups from the **Select Groups** section.

iii. Click **Commit** to assign groups to the selected users.

Removing a user from groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - If you are creating a new user account and you have already assigned a group, then click **New** > **Group Membership**.
   - If you are removing a group in the edit mode, on the User Management page, select a user and click **Edit** > **Group Membership**.
   - If you are removing a group in the view mode, on the User Management page, select a user and click **View** > **Edit** > **Group Membership**.
4. Select the groups and click **Remove From Group** to remove the user from the selected groups.

Viewing deleted users

When you remove a user from the User Management page using the Delete functionality, the User Management page removes the user temporarily and stores this users as Deleted Users. You can use the Viewing deleted users functionality to view temporarily deleted users .

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the Users page, click **More Actions** > **Show Deleted Users**.

Restoring deleted users

Use this functionality to restore the user that you have deleted using the delete functionality.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. Select the users that you want to restore and click **Restore**.
5. On the User Restore Confirmation page, click **Restore**.

Related topics:

User Restore Confirmation field descriptions on page 240

Deleting the deleted users

When you use the Deleting the deleted Users functionality to delete a user, it deletes the user permanently from the database.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. Select the users that you want to delete and click **Delete**.
5. On the User Delete Confirmation page, click **Delete**.

Note:
This operation permanently deletes the users from the database.

Related topics:

User Delete Confirmation field descriptions on page 233
Deleted Users field descriptions on page 238

Adding a mailing address of the user

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - On the Users page, click **New** > **Identity** > **Address** > **New**.
   - On the User Management page, select a user and click **Edit** > **Identity** > **Address** > **New**.
   - On the User Management page, select a user and click **View** > **Edit** > **Identity** > **Address** > **New**.
4. Enter the appropriate information.
5. Click **Commit**.

Related topics:

Add Address field descriptions on page 239

Modifying a mailing address

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - Select a user and click **Edit** > **Identity** > **Address** > **Edit**.
   - Select a user and click **View** > **Edit** > **Identity** > **Address** > **Edit**.
4. On the **Edit Address** page, modify the information.
5. Click **Commit**.

Removing a mailing address

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - If you are on the New User Profile page or on the User Profile Duplicate page and have added a mailing address , then navigate to **Identity** > **Address** .
   - On the User Management page, select a user and click **Edit** > **Identity** > **Address** .
   - On the Users page, select a user and click **View** > **Edit** > **Identity** > **Address** .
4. Select the mailing address and click **Delete**.

Choosing a shared address

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - On the Users page, click **New** > **Identity** > **Address** > **Choose Shared Address**.
   - If you are in the edit mode, on the Users page, select a user and click **Edit** > **Identity** > **Address** > **Choose Shared Address**.
   - If you are in the view mode, on the Users page, select a user and click **View** > **Edit** > **Identity** > **Address** > **Choose Shared Address**.
4. Enter the appropriate information.
5. Click **Select**.

Related topics:

Choose Address field descriptions on page 240

Assigning users to roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select a user role and click **More Actions** > **Assign User Roles**.
4. On the Assign Users page, select the users displayed in the **Select Users** section.
5. Click **Commit**.

Related topics:

Assign Users To Roles field descriptions on page 174

Removing users from roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Manage Roles** in the left navigation pane.
3. On the Manage Roles page, select one or more user roles and click **More Actions** > **UnAssign User Roles**.
4. On the UnAssign Roles page, select the users displayed in the Select Users section.
5. Click **Commit**.

Related topics:

UnAssign Roles field descriptions on page 175

Overriding Permissions

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click **Override Permissions New** .
5. On the New Permission page, enter the appropriate information.
6. Click **Add**.

Removing override permissions

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.

3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, select a permission and click **Override Permissions** > **Delete**.

Creating a new communication profile

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, click **New**.
4. Perform one of the following steps:
   - If you are creating a new user account, on the User Management page, click **New**
   - On the User Management page, select a user and click **Edit** for an existing user account.
   - On the User Management page, select a user and click **View** > **Edit** for an existing user account.
5. Click the **Communication Profile** link at the top of the page.
6. In the communication profile section, click **New**.
7. In the **Name** field, enter the name of the communication profile.
8. If you want to make the profile default profile, select the **Default** check box.
9. Click **Save**.
10. Click **Commit**.

Creating a new communication address for a communication profile

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. On the User Management page, click **New**.
4. Perform one of the following steps:
   - If you are creating a new user account, on the User Management page, click **New**
   - On the User Management page, select a user and click **Edit** for an existing user account.
   - On the User Management page, select a user and click **View** > **Edit** for an existing user account.
5. Click the **Communication Profile** link at the top of the page.
6. In the Communication Profile section, click a communication profile.
7. In the communication address section, click **New**.
8. From the **Type** drop-down, select a communication protocol.
9. From the **Sub Type** drop-down, select a application type.
10. In the **Fully Qualified Address** field, enter the contact address in the format supported by the value that you selected in the **Sub Type** field. Contact address can be an e-mail id, instant messenger id, sip address of a sip enabled device and so on.
11. From the drop-down field next to **Fully Qualified Address** field, select or enter the domain name.
12. Click **Save**.
13. Click **Commit**.

Modifying a communication address of a user

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - On the User Management page, select a user and click **Edit**.
   - On the User Management page, select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the Communication Profile link at the top of the page.
5. In the Communication Profile section, select a profile.
6. In the Communication Address section, select a communication address.
7. Click **Edit**.
8. Modify the information in the respective fields.
9. Click **Save** .
10. Click **Commit**.

Related topics:

User Profile Edit field descriptions on page 211

Deleting a communication profile

You cannot delete the default communication profile.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - On the User Management page, select a user and click **Edit**.
   - On the User Management page, select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the Communication Profile link at the top of the page.

5. In the communication profile section, click a profile.
6. Click **Delete**.
7. Click **Commit**.

Result

When you delete a communication profile, the System Manager application deletes all the communication addresses associated with the communication profile.

Related topics:

User Profile Edit field descriptions on page 211

Deleting a communication address in a communication profile

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
3. Perform one of the following steps:
   - On the User Management page, select a user and click **Edit**.
   - On the User Management page, select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the Communication Profile link at the top of the page.
5. In the Communication Profile section, click a Communication Profile.
6. In the Communication Address section, select a communication address.
7. Click **Delete** .
   You can find the **Delete** button in the Communication Address section.
8. Click **Save**.
   You can find the **Save** button in the Communication Profile section.
9. Click **Commit**.

Related topics:

User Profile Edit field descriptions on page 211

Adding a contact in a contact list

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, perform one of the following steps:
   - Click **New** if you are adding a new contact for the user.
   - Select a user and click **Edit** if you are adding a new contact for an existing user.
3. Click the **Default Contact List** link at the top of the page.
4. Click **Add**.
5. On the Attach Contact page, select one or more contacts and click **Select**.

Result

You can view the new contacts in the table displayed in the Associated Contacts section.

Modifying a contact in a contact list

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, select a user and click **Edit**.
3. On the User Profile Edit page, click the **Default Contact List** link at the top of the page.
4. Select a contact from the Associated Contacts section and click **Edit**.
5. Modify the information in the fields in the Contact Membership Details section.
6. Click **Add** to save the changes.

Viewing the details of a contact in the contact list

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, select a user and click **View**.
3. On the User Profile Edit page, click the **Default Contact List** link at the top of the page and select a contact.
4. In the **Last Name** column, click the last name link.

Result

The View Contact List Member page displays the details of the contact whose last name you have clicked.

Deleting contacts from the contact list

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, select a user and click **Edit**.
3. On the User Profile Edit page, click the **Default Contact List** link at the top of the page.
4. Select one or more contacts from the Associated Contacts section and click **Delete**.

Adding a private contact for a user

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, perform one of the following steps:
    - Click **New** if you are adding a private contact for a new user.

- Select a user and click **Edit** if you are adding a private contact for an existing user.

3. Click the **Private Contacts** link at the top of the page and click **New**.
4. On the New Private Contact page, enter the appropriate information in the respective fields.

   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
5. Click **Add** to add the private contact.
6. Click **Commit**.

Note:

Ensure that all the mandatory fields that is fields marked with red asterisk have valid information, before you click **Commit**.

Modifying the details of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, Select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**
5. On the Edit Private Contact page, modify the contact's information.
6. Click **Add** to save the modified information.

Deleting private contacts of a user

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, Select a user and click **Edit**.

3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select one or more contacts.
4. Click **Delete**.

Adding a contact address of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, perform one of the following steps:
   - Click **New** if you are adding a contact address of a private contact for a new user.
   - Select a user and click **Edit** if you are adding a contact address of a private contact for an existing user.
3. Click the **Private Contacts** link at the top of the page and perform one of the following steps:.
   - Click **New** if you are adding a contact address for a new private contact.
   - Select a public contact and click **Edit** if you are adding a contact address for an existing private contact.
4. On the New Private Contact page, click **New** in the Contact Address section.
5. On the Add Address page, enter the appropriate information in the respective fields.

   The fields marked with asterisk are mandatory. You must enter a valid information in these fields to successfully create a private contact.
6. Click **Add** to create a new contact address for the private contact.

Modifying a contact address of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, Select a user and click **Edit**.

3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**
5. On the Edit Private Contact page, select a contact address from the Contact Address section.
6. Click **Edit**.
7. On the Edit Address page, modify the information in the respective fields.

   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
8. Click **Add** to save the modified address.
9. On the User Profile Edit page, click **Commit**.

Note:

Ensure that all the mandatory fields that is fields marked with red asterisk have valid information, before you click **Commit**.

Viewing the details of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, select a user and click **View**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. In the **Last Name** column, click the last name link.

Result

The View Contact page displays the details of the contact whose last name you have clicked.

Deleting contact addresses of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, Select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**
5. On the Edit Private Contact page, select one or more addresses from the Contact Address section.
6. Click **Delete**.

Choosing a shared address for a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, perform one of the following steps:
   - Click **New** if you are choosing a shared address for a private contact of a new user.
   - Select a user and click **Edit** if you are choosing a shared address for a private contact of an existing user.
3. Click the **Private Contacts** link at the top of the page perform on of the following actions:
   - Click **New** if you are adding the address for a new contact.
   - Select a contact and click **Edit** if you are adding the address for an existing contact.
4. Click **Choose Shared Address** in the Postal Address section.
5. On the Choose Address page, select one or more shared addresses.
6. Click **Select** to add these addresses for the private contact.

Adding a postal address of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, perform one of the following steps:
   - Click **New** if you are adding a postal address of a private contact for a new user.
   - Select a user and click **Edit** if you are adding a postal address of a private contact for an existing user.
3. Click the **Private Contacts** link at the top of the page and perform one of the following steps:.
   - Click **New** if you are adding a postal address for a new private contact.
   - Select a private contact and click **Edit** if you are adding a postal address for an existing private contact.
4. On the New Private Contact page, click **New** in the Postal Address section.
5. On the Add Address page, enter the appropriate information in the respective fields.

   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
6. Click **Add** to create a new postal address for the private contact.

Modifying a postal address of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, Select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**
5. On the Edit Private Contact page, select an address from the Postal Address section.
6. Click **Edit**.
7. On the Edit Address page, modify the information in the respective fields.

The fields marked with asterisk are mandatory. You must enter valid information in these fields.

8. Click **Add** to save the modified address.

Deleting postal addresses of a private contact

1. Click **User Management** > **User Management** in the left navigation pane on the System Manager console.
2. On the User Management page, Select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**
5. On the Edit Private Contact page, select one or more addresses from the Postal Address section.
6. Click **Delete**.

User Management field descriptions

The User Management module is the primary master of the user profile. It provides Avaya's customers and Avaya's products with a single point of administration for creating, viewing, modifying, and deleting users. The page has two sections. The upper section contains buttons that you can use to:

- create, view, modify and delete users
- assign roles, attributes to a user
- add a user to a group
- perform Lightweight Directory Access Protocol (LDAP) synchronization

The lower section contains a table that displays information about the user.

Name	Description
Status	The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.

Name	Description
Name	Name of the user.
User Name	Unique name that gives access to the system.
Last Login	Date and time when the user has successfully logged into the system
Handle	A unique communication address of the user.

Button	Description
View	Opens User Profile View page that you can use to view the details of the selected user.
Edit	Opens the User Profile Edit page that you can use to modify the details of the selected user.
New	Opens the New User Profile page that you can use to create a new user.
Duplicate	Opens the User Profile Duplicate page that you can use create a duplicate user.
Delete	Opens the User Delete Confirmation page that you can use to temporarily delete the selected users.
More Actions > **Assign Roles**	Opens the Assign Roles page that you can use to assign roles to the selected users.
More Actions > **Assign Attribute Sets**	Opens the Assign Attribute Sets page that you can use to assign attribute sets to the selected users.
More Actions > **Add To Group**	Opens the Assign Groups page that you can use to assign groups to the selected users .
More Actions > **Show Deleted User**	Opens the Deleted Users page that you can use to view, permanently delete, and restore the deleted users .
Advanced Search	Displays fields that you can use to specify the search criteria for searching a user.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters users based on the filter criteria.
Select: All	Selects all the users in the table.
Select: None	Clears the check box selections.
Refresh	Refreshes the user's information in the table.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search users. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value for the search criterion. The Users Management service retrieves and displays users that match this value.

User Profile View field descriptions

Use this page to view the details of the selected user account.

General section

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Description	A brief description about the user.
User Type	The primary user types. You can associate an user account with the following user types: • enduser • administrator

Identity section

Name	Description
Login Name	The unique system login name given to the user. It takes the form of username@domain. You can use the login name to create the user's primary handle.
Authentication Type	Authentication type defines how the system performs user's authentication. The options are:

Name	Description
	• **enterprise** — User's login is authenticated by the enterprise. • **avayaservices** — User's login is authenticated by an Avaya Service. • **basic** — User's login is authenticated by an Avaya Authentication Service.
Password	The initial password for logging in to the system.
Confirm Password	The initial password for verification.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Honorific	The personal title for address a user. This is typically a social title and not the work title.
Language Preference	The user's preferred written or spoken language.
Time Zone	The preferred time zone of the user.

Identity > Address section

Name	Description
Name	The name of the user.
Address Type	Type of the address. The following are the types: • Office • Home
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Communication Profile section

Name	Description
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Address section

Name	Description
Type	The type of the handle.
SubType	The sub type of the handle.
Handle	.A unique communication address for the user.
Domain	The name of the domain with which the handle is registered.

Session Manager

Note:

You may see these fields only if they are configured for the user.

Name	Description
Session Manager Instance	Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected Session Manager instance will be used as the access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Origination Application Sequence	An application sequence invoked when calls are routed from this user. A selection is optional.
Termination Application Sequence	An application sequence invoked when calls are routed to this user. A selection is optional.

Messaging Profile

Note:

You may see these fields only if they are configured for the user.

Name	Description
System	The Messaging System on which you need to add the subscriber.
Template	The template (system defined and user defined) you want to associate with the subscriber.

Name	Description
Use Existing Subscriber on System	Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.
Existing Mailbox Number	The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Mailbox Number	The mailbox number of the subscriber.
Password	The password for logging into the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user.

Station Profile

Note:

You may see these fields only if they are configured for the user.

Name/Button	Description
System	The Communication Manager on which you need to add the station.
Use Existing Station	Use the check box if you want to use an existing station extension to associate with this profile. If you do not select this check box, the available extensions are used.
Extension	The extension of the station you want to associate.
Search	Lists the stations (existing or available) based on check box status of the **Use Existing Station** field.
Template	The template (system defined or user defined) you want to associate with the station. Select the template based on the set type you want to add.
Set Type	The set type of the station you want to associate. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the station.
Port	The relevant port for the set type you select.
Search	Lists the possible ports based on the selected set type.
Delete Station on Unassign of Station from User	Use this check box to specify whether you want to delete the station from the Communication Manager Device or Communication System Management when you remove the association between the station and the user or when you delete the user.

Roles section

Name	Description
Name	The name of the role.
Description	A brief description about the role.

Group Membership section

Name	Description
Select check box	Select the group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Attribute Sets section

Name	Description
Select check box	Select the attribute set.
Attribute Set	Name of the attribute set.
Attribute Set Instance	Name of the attribute set instance.
Application	Name of the application that owns the attribute set.
Description	A brief description about the attribute set.

Default Contact List section

Name	Description
Name	Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name.
Description	A brief description of the contact list.

Associated Contacts section

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Scope	Categorization of the contact based on whether the contact is a public or private contact.

Name	Description
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	First name of the private contact.
Display Name	Display name of the private contact.
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Button	Description
Edit	Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account.
Done	Closes the User Profile View page and takes you back to the User Management page.

User Profile Edit field descriptions

Use this page to modify the details of a user account.

General section

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Description	A brief description about the user.
User Type	The primary user types. You can associate an user account with the following user types: • enduser • administrator

Identity section

Name	Description
Login Name	This is the unique system login name given to the user. It takes the form of username@domain. It is used to create the user's primary handle.
Authentication Type	Authentication type defines how the system performs user's authentication. The options are: • **enterprise** — User's login is authenticated by the enterprise. • **avayaservices** — User's login is authenticated by an Avaya Service. • **basic** — User's login is authenticated by an Avaya Authentication Service.
Password	The initial password for logging in to the system.
Confirm Password	The initial password for verification.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Honorific	The personal title for address a user. This is typically a social title and not the work title.
Language Preference	The user's preferred written or spoken language.

Name	Description
Time Zone	The preferred time zone of the user.

Identity > Address section

Name	Description
Select check box	Use this check box to select the address.
Name	The name of the user.
Address Type	The type of address. The values are: • Office • Home
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens the Add Address page that you can use to add the address details.
Edit	Opens the Edit Address page that you can use to modify the address details.
Delete	Deletes the selected address.
Choose Shared Address	Opens the Choose Address page that you can use to choose a address.

Communication Profile section

Use this section to create, modify and delete a communication profile for the user. A communication profile contains communication address and

Name	Description
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile.

Name	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.

Name	Description
Save	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

The page displays the following fields when you click the **Add** button in the Communication Profile section.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user. Each communication profile may contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
SubType	The sub type of the handle.
Handle	.A unique communication address for the user.
Domain	The name of the domain with which the handle is registered.

Name	Description
New	Displays the fields for adding a new communication address.
Edit	Use this button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

Name	Description
Type	The types of the handle. The following are the different handle types: • sip: Indicates that the handle supports SIP based communication. • smtp: Indicates that the handle is an e-mail address and supports Simple Mail Transfer Protocol (SMTP) based communication. • ibm: Indicates that the handle is an IBM address. • xmpp: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication.

Name	Description
SubType	The sub types of the handle. The following are the subtypes: • Subtypes for SIP based handles: a. e164: Type signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. b. username: Type signifies that the handle is an alphanumeric value. For example, 1234567, xyz, or abc.xyz c. msrtc: Type signifies that the handle supports communication with the Microsoft RTC server. • Subtypes for SMTP: msexchange: Type signifies that the handle supports communication with Microsoft SMTP server. • Subtypes for ibm: a. lotusnotes: Type signifies that handle is for lotus notes and domino calender. b. ibmsametime: Type signifies that handle is for IBM sametime • Subtypes for xmpp: a. jabber: Type signifies that handle supports communication with the Jabber service. b. googletalk: Type signifies that handle supports communication with the googletalk service.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.

Name	Description
Add	Saves the new communication address or modified communication address information to the database.
Cancel	Cancels the adding a communication address operation.

Session Manager

Note:

You may see these fields only if they are configured for the user.

Name	Description
Session Manager Instance	Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected Session Manager instance will be used as the access

Name	Description
	point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Origination Application Sequence	An application sequence that is invoked when calls are routed from this user. A selection is optional.
Termination Application Sequence	An application sequence that is invoked when calls are routed to this user. A selection is optional.

Messaging Profile

Note:

You may see these fields only if they are configured for the user.

Name	Description
System	The Messaging System on which you need to add the subscriber.
Template	The template (system defined and user defined) you want to associate with the subscriber.
Use Existing Subscriber on System	Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.
Existing Mailbox Number	The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Mailbox Number	The mailbox number of the subscriber.
Password	The password for logging into the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user.

Station Profile

Note:

You may see these fields only if they are configured for the user.

Name/Button	Description
System	The Communication Manager on which you need to add the station.
Use Existing Station	Use the check box if you want to use an existing station extension to associate with this profile. If you do not select this check box, the available extensions are used.

Name/Button	Description
Extension	The extension of the station you want to associate.
Search	Lists the stations (existing or available) based on check box status of the **Use Existing Station** field.
Template	The template (system defined or user defined) you want to associate with the station. Select the template based on the set type you want to add.
Set Type	The set type of the station you want to associate. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the station.
Port	The relevant port for the set type you select.
Search	Lists the possible ports based on the selected set type.
Delete Station on Unassign of Station from User	Use this check box to specify whether you want to delete the station from the Communication Manager Device or Communication System Management when you remove the association between the station and the user or when you delete the user.

Roles section

Name	Description
Select check box	Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Opens the Assign Role page that you can use to assign roles to the user account.
Remove Roles	Removes the selected role from the list of roles associated with the user account.

Override Permissions section

Name	Description
Select Check Box	Use this check box to select a permission.
Resource Type	The type of resource for which you have overridden the permission.
Actions	The actions that the user can perform on the selected resources and attributes.

Name	Description
Groups and Resources	The groups and resources on which the user can perform the actions.
Attributes	The attributes on which the user can perform the actions.

Button	Description
New	Opens the New Permission page that you can use to assign a new permission to the user account.
Delete	Removes the selected permissions from the user account.

Group Membership section

Name	Description
Select check box	Use this check box to select the group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Opens the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Attribute Sets section

Name	Description
Select check box	Use this check box to select the attribute set.
Attribute Set	Name of the attribute set.
Attribute Set Instance	Name of the attribute set instance.
Application	Name of the application that owns the attribute set.
Description	A brief description about the attribute set.

Button	Description
Assign Attribute Sets	Opens the Select Attribute page that allows you to assign attribute sets to the user.
Remove Attribute Set	Removes the selected attribute sets for a user .

Default Contact List

Name	Description
Name	Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name.
Description	A brief description of the contact list.

Associated Contacts

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Scope	Categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact.

Button	Description
Edit	Opens the **Edit Contact List Member** page. Use this page to modify the information of the selected contact.
New	Opens the **Attach Contacts** page. Use this page to select one or more contacts from the list of contacts.
Remove	Removes one or more contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	First name of the private contact.
Display Name	Display name of the private contact.

Name	Description
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Opens the **Edit Private Contact** page. Use this page to modify the information of the selected contact.
New	Opens the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Button	Description
Commit	Modifies the user account. **Note:** While restoring a deleted user, use this button to restore a deleted user.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.

Related topics:

Modifying user accounts on page 179
Modifying a communication address of a user on page 194
Deleting a communication profile on page 194
Deleting a communication address in a communication profile on page 195

New User Profile field descriptions

Use this page to create a new user. This page has the following sections:

- General
- Identity
- Communication Profile
- Roles
- Group Membership

- Attribute Sets
- Default Contact List
- Private Contacts

Note:

The asterisk marked fields are mandatory and you must enter appropriate information in these fields.

General section

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Description	A brief description about the user.
User Type	The primary user types. You can associate an user account with the following user types: • administrator • communication_user • agent • supervisor • resident_expert • service_technician • lobby_phone

Identity section

Name	Description
Login Name	A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle.
Authentication Type	Authentication type defines how the system performs user's authentication. The options are: • **enterprise** — The enterprise authenticates user's login. • **basic** — The Avaya Authentication Service authenticates user's login.
Password	The initial password for logging in to the system.
Confirm Password	The initial password for verification.

Name	Description
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Honorific	The personal title for address a user. This is typically a social title and not the work title.
Language Preference	The user's preferred written or spoken language.
Time Zone	The preferred time zone of the user.

Identity > Address section

Name	Description
Select check box	Use this check box to select a address in the table.
Name	The name of the addressee.
Address Type	The type of address. The values are: • Office • Home
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens the Add Address page. Use the page to add the address details.
Edit	Allows you to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Opens the Choose Address page that you can use to choose a address.

Communication Profile section

Use this section to create, modify and delete a communication profile for the user. A communication profile contains communication address and

Name	Description
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile.

Name	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Save	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

This page displays the following fields when you click the **Add** button in the Communication Profile section.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user. Each communication profile may contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
SubType	The sub type of the handle.
Handle	A unique communication address of the user.
Domain	The name of the domain with which the handle is registered.

Name	Description
New	Displays the fields for adding a new communication address.
Edit	Use this button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

Name	Description
Type	The types of the handle. The following are the different handle types: • sip: Indicates that the handle supports SIP based communication. • smtp: Indicates that the handle is an e-mail address and supports Simple Mail Transfer Protocol (SMTP) based communication. • ibm: Indicates that the handle is an IBM address. • xmpp: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication.
SubType	The sub types of the handle. The following are the subtypes: • Subtypes for SIP based handles: a. e164: Type signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. b. username: Type signifies that the handle is an alphanumeric value. For example, 1234567, xyz, or abc.xyz c. msrtc: Type signifies that the handle supports communication with the Microsoft RTC server. • Subtypes for SMTP: msexchange: Type signifies that the handle supports communication with Microsoft SMTP server. • Subtypes for ibm: a. lotusnotes: Type signifies that the handle is for lotus notes and domino calender. b. ibmsametime: Type signifies that the handle is for IBM sametime • Subtypes for xmpp: a. jabber: Type signifies that the handle supports communication with the Jabber service. b. googletalk: Type signifies that the handle supports communication with the googletalk service.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.

Name	Description
Add	Saves the new communication address or modified communication address information to the database.
Cancel	Cancels the adding a communication address operation.

Session Manager

Note:

You may see these fields only if they can be configured for the user.

Name	Description
Session Manager Instance	Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected Session Manager instance will be used as the access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Origination Application Sequence	An application sequence invoked when calls are routed from this user. A selection is optional.
Termination Application Sequence	An application sequence invoked when calls are routed to this user. A selection is optional.

Messaging Profile

Note:

You may see these fields only if they can be configured for the user.

Name	Description
System	The Messaging System on which you need to add the subscriber.
Template	The template (system defined and user defined) you want to associate with the subscriber.
Use Existing Subscriber on System	Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.
Existing Mailbox Number	The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Mailbox Number	The mailbox number of the subscriber.
Password	The password for logging into the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user.

Station Profile

Note:

You may see these fields only if they can be configured for the user.

Name/Button	Description
System	The Communication Manager on which you need to add the station.
Use Existing Station	Use the check box if you want to use an existing station extension to associate with this profile. If you do not select this check box, the available extensions are used.
Extension	The extension of the station you want to associate.
Search	Lists the stations (existing or available) based on check box status of the **Use Existing Station** field.
Template	The template (system defined or user defined) you want to associate with the station. Select the template based on the set type you want to add.
Set Type	The set type of the station you want to associate. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the station.
Port	The relevant port for the set type you select.
Search	Lists the possible ports based on the selected set type.
Delete Station on Unassign of Station from User	Use this check box to specify whether you want to delete the station from the Communication Manager Device or Communication System Management when you remove the association between the station and the user or when you delete the user.

Roles section

Name	Description
Select check box	Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Opens the Assign Role page that you can use to assign the roles to the user account.
Remove Roles	Removes the selected role from the list of roles associated with the user account.

Group Membership section

Name	Description
Select check box	Use this check box to select the group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Opens the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Attribute Sets section

Name	Description
Select check box	Use this check box to select the attribute set.
Attribute Set	Name of the attribute set.
Attribute Set Instance	Name of the attribute set instance.
Application	Name of the application that owns the attribute set.
Description	A brief description about the attribute set.

Button	Description
Assign Attribute Sets	Opens the Select Attribute page that you can use to assign attribute sets to the user.
Remove Attribute Set	Removes the selected attribute sets for a user .

Default Contact List

Name	Description
Name	Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name.
Description	A brief description of the contact list.

Associated Contacts

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Scope	Categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact.

Button	Description
Edit	Opens the **Edit Contact List Member** page. Use this page to modify the information of the selected contact.
New	Opens the **Attach Contacts** page. Use this page to select one or more contacts from the list of contacts.
Remove	Removes one or more contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	First name of the private contact.
Display Name	Display name of the private contact.
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Opens the **Edit Contact List Member** page. Use this page to modify the information of the selected contact.

Button	Description
New	Opens the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Button	Description
Commit	Creates the user account.
Cancel	Cancels the user creation operation.

Related topics:

Creating a new user profile on page 179

Select Resources field descriptions

Use this page to select a resource and assign permissions to the user for the resource.

Selected Resources section

Name	Description
Name	The name of the resource for which user can perform the actions.
Type	The type of resource.
Description	A brief description about the resource.

Available Resources section

Name	Description
Select Check box	Use this check box to select a resource.
Name	The name of the resource for which user can perform the actions.
Type	The type of resource.
Description	A brief description about the resource.

Button	Description
Select	Assign permissions to the user for the selected resources.

Button	Description
Cancel	Cancels the resource selection operation and takes you back to the User Profile Edit page.

User Profile Duplicate field descriptions

Use this page to create a duplicate user. This page has the following sections:

- General
- Identity

General section

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Description	A brief description about the user.
User Type	The primary user types. You can associate an user account with the following user types: • enduser • administrator

Identity section

Name	Description
Login Name	This is the unique system login name given to the user. It takes the form of username@domain. It will typically be used to create the user's primary handle.
Authentication Type	Authentication type defines how the system performs user's authentication. The options are: • **enterprise** — User's login is authenticated by the enterprise. • **avayaservices** — User's login is authenticated by an Avaya Service. • **basic** — User's login is authenticated by an Avaya Authentication Service.
Password	The initial password for logging in to the system.
Confirm Password	The initial password for verification.

Name	Description
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Honorific	The personal title for address a user. This is typically a social title and not the work title.
Language Preference	The user's preferred written or spoken language.
Time Zone	The preferred time zone of the user.

Identity > Address section

Name	Description
Select check box	Use this check box to select the address.
Name	The name of the user.
Address Type	The type of address. The values are: • Office • Home
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens the Add Address page that allows you to add the address details.
Edit	Opens the Edit Address page that you can use to modify the address details.
Delete	Deletes the selected address.
Choose Shared Address	Opens the Choose Address page that you can use to choose a address.

Button	Description
Commit	Creates the duplicate user.

Button	Description
Cancel	Cancels the duplicate user creation and returns to the User Management page.

Communication Profile section

Name	Description
Option button	Use this button to view the details of the selected communication profile.
Name	Name of the communication profile.

Name	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Save	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

The page displays the following fields when you click the **Add** button in the Communication Profile section.

Name	Description
Name	Name of the communication profile for the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Address section

Name	Description
Type	Type of the communication protocol to be used for the user.
SubType	Sub type of the communication protocol.
Handle	A unique communication address for the user.
Domain	Name of the domain with which the handle is registered.

Name	Description
New	Displays the fields for adding a new communication address.
Edit	Use this button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

Name	Description
Type	Type of the communication protocol used for establishing communication with the user. The following are the communication protocols for the user: • sip • smtp • ibm • xmpp
SubType	Displays the sub types of the communication protocol.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.

Name	Description
Add	Saves the new communication address or modified communication address information to the database.
Cancel	Cancels the adding a communication address operation.

Session Manager

Note:

These fields are for extended communication profile and are available only if the communication profile is installed.

Name	Description
Session Manager Instance	Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected Session Manager instance will be used as the access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Origination Application Sequence	An application sequence that is invoked when calls are routed from this user. A selection is optional.
Termination Application Sequence	An application sequence that is invoked when calls are routed to this user. A selection is optional.

Related topics:

Creating duplicate users on page 180

User Delete Confirmation field descriptions

Use this page to delete an user account.

Name	Description
Status	The status indicates whether the user is currently online or offline.
Name	The name that identifies the group to which the user belongs.
User Name	The unique name of the user account.
Last login	The date and time of last successful login into System Manager.

Button	Description
Delete	Deletes an user.
Cancel	Closes the User Delete Confirmation page and takes you back to the User Management page.

Related topics:

Removing user accounts on page 180
Deleting the deleted users on page 187

Assign Roles to Multiple Users field descriptions

Use this page to assign roles to multiple users. The page has the following two sections:

- Selected Users
- Select Roles

Selected Users

Name	Description
Status	The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.
Name	Name of the user.
User Name	Unique name that gives access to the system .
Last login	Time and date when the user has logged in to the system.

Select Roles

Name	Description
Select Check box	Use this check box to select a role.
Name	Name of the role.
Description	A brief description about the role.

Button	Description
Commit	Assigns roles to the selected users.
Cancel	Cancels the role assignment operation and takes you back to the User Management page.

Assign Roles field descriptions

Use this page to assign a role to the user. The page has the following two sections:

- Selected Roles
- Available Roles

Selected Roles section

The table in this section displays roles that you have assigned to the user account.

Name	Description
Name	The roles that you have assigned to the user account.
Resource Type	The type based on the resources.
Description	Displays a brief description about the roles.

Available Roles section

The table in this section displays roles that you can assign to the user account.

Name	Description
Name	The roles that you can assign to the user account.
Resource Type	The type based on the resources.
Description	Displays a brief description about the roles.

Button	Description
Select	Assigns the role to the user.
Cancel	Cancels the role assignment operation and returns to the New User Profile page.

Button	Description
Select: All	Selects all groups in the table.
Select: None	Clears the role selections.

Select Attributes field descriptions

Use this page to assign attribute sets to the user account. The page has the following two sections:

- Selected Attributes
- Available Attributes

Selected Attributes section

The table in this section displays attributes that you have assigned to the user account.

Name	Description
Name	Name of the assigned attribute.
Attribute Set	Name of the attribute set that contains the attribute.
Application	Name of the application that owns the attribute set.
Description	A brief description about the attribute set.

Available Attributes section

The table in this section displays roles that you can assign to the user account.

Name	Description
Select check box	Select the attribute set.
Name	Name of the attribute.
Attribute Set	Name of the attribute set that contains the attribute.
Application	Name of the application that own the attribute set.
Description	A brief description about the attribute set.

Button	Description
Select	Assigns the attributes set to the user.
Cancel	Cancels the attribute set assignment operation and returns to the New User Profile page.
Select: All	Selects all attributes in the table.
Select: None	Clears the attributes selections.

Assign Groups field descriptions

Use this page to assign a group to the user account. The page has the following two sections:

- Selected Groups
- Available Groups

Selected Groups section

The table in this section displays groups that you have assigned to the user account.

Name	Description
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Available Groups section

The table in this section displays groups that you can assign to the user account.

Name	Description
Select Check box	Select the group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Select	Assigns the selected groups to the user
Cancel	Cancels the group assignment operation.
Select: ALL	Selects all groups in the table
Select: None	Clears the selection

Related topics:

Assigning groups to single and multiple users on page 185

Assign Groups to Multiple Users field descriptions

Use this page to add users to the selected groups. This page has the following two sections:

- Selected Users
- Select Groups

Selected Users

Name	Description
Status	The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.
Name	Name of the user.
User Name	Unique name that gives access to the system .
Last login	Time and date when the user has last logged in to the system.

Select Groups

Name	Description
Select Check box	Use this check box to select a group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group within the groups.
Description	A brief description about the group.

Button	Description
Select: All	Selects all the groups displayed in the table.
Select: None	Clears the selected check boxes.
Commit	Assigns groups to the selected users.
Cancel	Cancels the group assignment operation and takes you back to the User Management page.

Related topics:

Assigning groups to single and multiple users on page 185

Assign Attribute Sets field descriptions

Use this page to assign attribute sets to the user. This page has the following two sections:

- Selected Users
- Select Attribute Sets

Selected Users section

The table in this section displays the details of the user account.

Name	Description
Status	The status indicates whether the user is currently online or offline.
Name	The name that identifies the group to which the user belongs.
User Name	The unique name of the user account.
Last login	The date and time of last successful login into System Manager.

Select Attribute Sets section

The table in this section displays attribute sets that you can assign to the user account.

Name	Description
Select Check box	Use the Check box to select an attribute set. Use the check box provided as the column heading to select all the attribute sets
Name	The roles that you can assign to the user account.
Attribute Set	The name of the attribute set.
Application	Name of the application that owns the attribute set.
Description	A brief description about the attribute set.

Button	Description
Commit	Assigns the selected attribute sets to the user.
Cancel	Cancels the attribute sets assignment operation and returns you back to the User Management page.

Deleted Users field descriptions

You can view the users that you have deleted using the Delete functionality. Use this page to view, delete, and restore users that you have deleted.

Name	Description
Select check box	Use this check box to select a deleted user.
Status	The current login status of the deleted user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.
Name	Name of the deleted user.
User Name	The unique name that identifies the user in the system.
Last login	Date and time when the user has last successfully logged into the system.

Button	Description
Delete	Deletes the user permanently from the database.
Restore	Restores the deleted user.
Show Regular User	Returns to the User page and display the active users.

Related topics:

Deleting the deleted users on page 187

Add Address field descriptions

Use this page to add the mailing address of the user.

Name	Description
Name	The unique label that identifies the address.
Address Type:	The type that identifies whether mailing address is a home or office address.
Building	The name of the building.
Room	The number or name of the room.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code or zip code used by postal services to route mail to a destination. In the United States this is the Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
Commit	Adds the mailing address of the user.
Cancel	Cancels the add address operation.

Related topics:

Adding a mailing address of the user on page 188

Choose Address field descriptions

Use this page to choose the mailing address.

Name	Description
Name	The unique label that identifies the address.
Address Type	The type of address. The values are: • Office • Home
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
Select	Adds the selected mailing address as the shared contact for the user account.
Cancel	Cancels the choose address operation.

Related topics:

Choosing a shared address on page 190

User Restore Confirmation field descriptions

Use this page to restore a deleted user.

Name	Description
Status	The status indicates whether the user is currently online or offline.

Name	Description
Name	The name that identifies the group to which the user belongs.
User Name	The unique name of the user account.
Last login	The date and time of last successful login into System Manager.

Button	Description
Restore	Removes the user from the list of deleted users and restores the user as an active user.
Cancel	Closes the User Restore Confirmation page and returns you back to the Deleted Users page.

Related topics:

Restoring deleted users on page 187

Change Password field descriptions

Use this page to change the password for your account.

Name	Description
Old Password	The existing password.
New Password	The new password that you want to set.
Confirm Password	The new password that you want to set.

Button	Description
Save	Changes the password.
Cancel	Cancels the change password operation and closes the Change Password page.

Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. The page has two sections:

- Selected Roles
- Select Users

Selected Roles section

The roles to which you can assign users.

Name	Description
Name	Name of the role.
Resource Type	The resource type that the corresponding role is assigned.
Description	A brief description about role.

Select Users section

The table displays the users to which you can assign the roles.

Name	Description
Select check box	Use this check box to select the user.
Status	Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application.
User Name	The unique name that identifies the user
Last Login	Time and date when the user has last logged into the system.
User Type	The type that defines the role of the user.

Button	Description
Commit	Assigns user to the role.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

Related topics:

Assigning users to roles on page 161

UnAssign Roles field descriptions

Use this page to unassign a role form the selected users. The page has two sections:

- Selected Roles
- Select Users

Selected Roles section

The role from which users are unassigned.

Name	Description
Name	Name of the role.
Resource Type	The resource type that the corresponding role is assigned.
Description	A brief description about the role.

Select Users section

The table displays the users for which you can remove the roles.

Name	Description
Select check box	Use this check box to select the user.
Status	Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application.
User Name	The unique name that identifies the user
Last Login	Time and date when the user has last logged into the system.
User Type	The type that defines the role of the user.

Button	Description
Commit	Unassigns the role from the users.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

Related topics:

Removing users from roles on page 161

New Permission field descriptions

Use this page to assign new permission to the user account for the selected resources and attributes.

Name	Description
Resource Type	The type of resources for which you want to set the permissions.
Actions	The operations that the user can perform on the groups or resources.

Selected Groups and Resources section

Name	Description
Name	The name of the resource or group for which the user can perform the operations as selected in the **Actions** field.
Type	The type of resource.
Description	A brief description about the resource.

Button	Description
Assign	Opens the Select Resources page. Use this page to select the resources for which you want to override the permission.
Remove	Removes the selected resources from the list of selected resources for which user can perform actions selected in the **Actions** field.

Selected Attributes section

Name	Description
Name	The name of the attribute.

Button	Description
Assign	Opens the Select Attributes page. Use this page to select attributes and to assign permission to the user for the resource.
Remove	Removes the selected attributes from the list of selected attributes for which user can perform actions selected in the **Actions** field.

Button	Description
Select	Assigns new permission on the page
Cancel	Cancels the permission assignment operation and takes you back to the User Profile Edit page.

Select Attributes field descriptions

Use this page to assign permission to the attribute for the user. The page has the following two sections:

- Selected Attributes
- Available Attributes

Selected Attributes

Name	Description
Name	Name of the attribute.

Available Attributes

Button	Description
Select Check box	Use this check box to select attributes.

Button	Description
Name	Name of the attribute.

New System Rule field descriptions

New System Rule

Use this section to set a priority for the new rule.

Name	Description
Priority	Defines a priority for the new rule. The options are: • High • Low The rule with high priority has more weight than the rule with low priority.

Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set. The options are • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.

Name	Description
Action	Defines the access control permission over the presence information. The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Name	Description
Commit	Creates the new system rule for the users.

Edit System Rule field descriptions

Use this page to edit a system rule.

Edit Access Level Along With Action

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set. The options are • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Name	Description
Commit	Saves the changes to the database.

Attach Contacts field descriptions

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Scope	Categorization of the contact based on whether the contact is a user, public or private contact.
Display/Login Name	Unique login name or display name of the contact.

Name	Description
Contact Address	Address of a private or public contact. No contact address is associated with a contact type user.
User Handles	Communication handles associated with the user. These handles are defined in the communication profile of a user.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.
Advanced Search	Displays fields that you can use to specify the search criteria to search for contacts.

Button	Description
Select	Adds the selected contact in the list of associated contacts.

The page displays the following field when you click the **Advanced Search** button at the upper-right corner of the contact table.

Name	Description
Criteria	Defines the search criteria for searching the contacts. Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search the contacts. • Drop-down 2 – The operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field. • Field 3 – The value for the search criterion.

Edit Contact List Member field descriptions

Contact Membership Details

Name	Description
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.
Description	A brief description about the contact.

Name	Description
Presence Buddy	Use this check box to indicate whether you want to allow monitoring of the presence information of the contact.
Speed Dial	Use this check box to indicate whether you want to allow speed dial for the contact.
Address/Handle	A fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	The reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	Postal code of the locality of the city or town.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Add	Saves the modified information in the database.

View Contact List Member field descriptions

Contact Membership Details

Name	Description
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.
Description	A brief description about the contact.
Presence Buddy	Use this check box to indicate whether you want to allow monitoring of the presence information of the contact.
Speed Dial	Use this check box to indicate whether you want to allow speed dial for the contact.
Address/Handle	A fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	The reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.

Name	Description
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	Name of the contact's company.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Global User Settings

Adding a shared address

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Global User Settings** in the left navigation pane.
3. On the Global User Settings page, click **New** in the **Shared Address** section.
4. On the Add Address page, enter the appropriate information.
5. Click **Commit**.

Result

The new address is available as shared address and you can specify this address when you create, modify a user account.

Modifying a shared address

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Global User Settings** in the left navigation pane.
3. On the Global User Settings page, select the address and click **Edit** in the **Shared Address** section.
4. On the Edit Address page, modify the appropriate information.
5. Click **Commit**.

Deleting a shared address

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Global User Settings** in the left navigation pane.
3. On the Global User Settings page, select the address and click **Delete** in the **Shared Address** section.

Viewing details of a high priority enforced ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select a high priority ACL rule from the list of high priority ACL rules displayed in the High Priority Enforced User ACL section.
3. Click **View**.

Result

The View Enforced User ACL page displays the details of the selected ACL rule.

Modifying a high priority enforced ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select a high priority ACL rule from the list of high priority ACL rules in the High Priority Enforced User ACL section.
3. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.

4. On the Edit High Priority Enforced User ACL page, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit**.
5. Click **Commit** to save the changes.

Creating a new high priority enforced ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New** in the High Priority Enforced User ACL section.
3. On the New High Priority Enforced User ACL page, click **New**.
4. Create an access level.
5. Select presentities from the Select Presentity section.
6. Select watchers from the Select Watcher section.
7. Click **Commit**.

Deleting high priority enforced ACL rules

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select one or more high priority ACL rules from the list of high priority rules displayed in the High Priority Enforced User ACL section.
3. Click **Delete**.

Viewing details of a low priority enforced ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select a low priority ACL rule from the list of low priority ACL rules displayed in the Low Priority Enforced User ACL section.
3. Click **View**.

Result

The View Enforced User ACL page displays the details of the selected ACL rule.

Modifying a low priority enforced ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select a low priority ACL rule from the list of low priority enforced ACL rules displayed in the Low Priority Enforced User ACL section.
3. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the Edit Low Priority Enforced User ACL page, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit**.
5. Click **Commit** to save the changes.

Creating a low priority enforced ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New** in the Low Priority Enforced User ACL section.
3. On the New Low Priority Enforced User ACL page, click **New**.
4. Create an access level.
5. Select presentities from the Select Presentity section.
6. Select watchers from the Select Watcher section.
7. Click **Commit**.

Deleting low priority enforced ACL rules

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select one or more low priority ACL rules from the list of low priority ACL rules displayed in the low Priority Enforced User ACL section.
3. Click **Delete**.

Viewing details of a System ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select a system ACL rule from the list of System ACL rules displayed in the System ACL section.
3. Click **View**.

Result

The View System ACL page displays the details of the selected ACL rule.

Modifying a System ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select a system ACL rule from the list of System ACL rules displayed in the System ACL section.
3. Perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the Edit System ACL page, perform one of the following steps:
   - Click **New** and create a new access level.
   - Select an existing access level and click **Edit**.
5. Click **Commit** to save the changes.

Creating a new System ACL rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New** in the System ACL section.
3. On the New System ACL page, click **New**.
4. Create an access level.
5. Select watchers from the Select Watcher section.
6. Click **Commit**.

Deleting System ACL rules

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, select one or more System ACL rules from list of System ACL rules in the System ACL section.
3. Click **Delete**.

Adding a new access level rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, perform one of the following steps:
   - Click **New** .
   - Select a rule and click **Edit** .
3. Click **New**.
4. From the **Access Level** drop-down field, select an access level.

5. From the **Action** drop-down field, select an action.
6. Click **Save**.

Modifying an access level rule

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, perform one of the following steps:
   - Click **New** .
   - Select a rule and click **Edit** .
3. Select an access level rule.
4. Click **Edit**.
5. Modify the information in the respective fields.
6. Click **Save**.

Deleting access level rules

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, perform one of the following steps:
   - Click **New** .
   - Select a rule and click **Edit** .
3. Select one or more access level rules.
4. Click **Delete**.

Filtering presentities

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New**.
3. On the Create new ACL page, select the presentities that you want to filter.
4. Click **Filter: Enable** located at the top right corner of the presentities.
5. Select the filter criteria you want to apply to the selected presentity.
6. Enter or select the search value in the third field from the left.
7. Click **Filter:Apply**.

Searching for presentities

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New**.
3. On the Create new ACL page, click **Advanced Search** in the Select Presentity section.
4. Select the search criteria and operator from the respective drop down fields.
5. Enter or select the search value in the third field.
6. Click the + button if you want to add another search condition.

   To delete a search condition, click the – button. You can delete a search condition only if you have more than one search condition specified.
7. Select the AND or OR operator from the drop-down field.

   This option appears when you add a search condition using the + button.
8. Click **Search** to find presentities for the given search conditions.

Result

The page displays the presentities which meet the search criteria in the Select Presentity section.

Filtering watchers

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New**.
3. On the Create new ACL page, select the presentities that you want to filter.
4. Click **Filter: Enable** located at the top-right corner of the watcher table.
5. Select the filter criteria you want to apply to the selected watchers.
6. Click **Filter:Apply**.

Searching for watchers

1. Click **User Management** > **Global User Settings** > **Presence ACL** in the left navigation pane on the System Manager console.
2. On the Presence ACL page, click **New**.
3. On the Create new ACL page, click **Advanced Search** in the Select Watcher section.
4. Select the search criteria and operator from the respective drop down fields.
5. Enter or select the search value in the third field.
6. Click the + button if you want to add another search condition.

   To delete a search condition, click the – button. You can delete a search condition only if you have more than one search condition specified.
7. Select the AND or OR operator from the drop-down field.

   This option appears when you add a search condition using the + button.
8. Click **Search** to find watchers for the given search conditions.

Result

The page displays the watchers that meet the search criteria in the Select Watcher section.

Adding a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and click **New**.
3. On the New Public Contact page, enter the appropriate information in the respective fields.

   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
4. Click **Add** to add the private contact.
5. On the Global User Settings page, click **Commit**.

Note:

Ensure that all the mandatory fields that is the fields marked with red asterisk have valid information, before you click **Commit**.

Modifying the details of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and select a contact.
3. click **Edit**
4. On the Edit Private Contact page, modify the contact's information.
5. Click **Add** to save the modified information.
6. On the Global User Settings page, click **Commit**.

Note:

Ensure that all the mandatory fields that is the fields marked with red asterisk have valid information, before you click **Commit**.

Deleting public contacts

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and select one or more contacts.
3. Click **Delete**.
4. Click **Commit**.

Viewing the details of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and select a contact.
3. Click **View**.

Result

The View Public Contact page displays the details of a public contact.

Adding a postal address of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and perform one of the following steps:
   - Click **New** if you are adding a postal address for a new public contact.
   - Select a public contact and click **Edit** if you are adding a postal address for an existing public contact.

3. On the New Public Contact page, click **New** in the Postal Address section.
4. On the Add Address page, enter the appropriate information in the respective fields.
   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
5. Click **Add** to create a new postal address for the public contact.

Modifying a postal address of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page.
3. Select a public contact and click **Edit**.
4. On the Edit Public Contact page, select an address from the Postal Address section.
5. Click **Edit**.
6. On the Edit Address page, modify the information in the respective fields.
   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
7. Click **Add** to save the modified address.

Deleting postal addresses of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page.
3. Select a public contact and click **Edit**.

4. On the Edit Public Contact page, select one ore more addresses from the Postal Address section.
5. Click **Delete**.

Choosing a shared address for a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and perform one of the following steps:
   - Click **New** if you are adding a shared address for a new public contact.
   - Select a public contact and click **Edit** if you are adding a shared address for an existing public contact.
3. Click **Choose Shared Address** in the Postal Address section.
4. On the Choose Address page, select one or more shared addresses.
5. Click **Select** to add these addresses for the public contact.

Adding a contact address of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page and perform one of the following steps:
   - Click **New** if you are adding a contact address for a new public contact.
   - Select a public contact and click **Edit** if you are adding a contact address for an existing public contact.
3. On the New Public Contact page, click **New** in the Contact Address section.
4. On the Add Address page, enter the appropriate information in the respective fields.

The fields marked with asterisk are mandatory. You must enter a valid information in these fields to successfully create a private contact.

5. Click **Add** to create a new contact address for the public contact.

Modifying a contact address of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page.
3. Select a public contact and click **Edit**.
4. On the Edit Public Contact page, select an address from the Contact Address section.
5. Click **Edit**.
6. On the Edit Address page, modify the information in the respective fields.

   The fields marked with asterisk are mandatory. You must enter valid information in these fields.
7. Click **Add** to save the modified address.

   Note:

   Ensure that all the mandatory fields that is fields marked with red asterisk have valid information, before you click **Add**.

Deleting contact addresses of a public contact

1. Click **User Management** > **Global User Settings** > **Global User Settings** in the left navigation pane on the System Manager console.
2. On the Global User Settings page, click the **Public Contacts** link at the top of the page.
3. Select a public contact and click **Edit**.

4. On the Edit Public Contact page, select one or more addresses from the Contact Address section.
5. Click **Delete**.

Global User Settings field descriptions

Shared Address

Name	Description
Select check box	Use this check box to select an address.
Name	The name of the person or entity associated with the address.
Address Type	The type of address indicates whether the address is an Office or home address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In the United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Opens Add Address page . Use this page to add an address.
Edit	Opens Edit Address page. Use this page to modify the mailing address information.
Delete	Deletes a selected address.

Public Contacts

Use this section to add new public contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the public contact.
First Name	First name of the public contact.
Display Name	Display name of the public contact.
Contact Address	Address of the public contact.
Description	A brief description about the contact.

Button	Description
View	Open the **View Public Contact** page. Use this page to view the details of the selected public contact.
Edit	Opens the **Edit Public Contact** page. Use this page to modify the information of the selected contact.
New	Opens the **New public Contact** page. Use this page to add a new public contact.
Delete	Deletes the selected contacts.
Filter: Advanced Search	Displays fields that you can use to specify the search criteria for searching a public contact.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Criteria section

The page displays the following fields when you click **Advanced Search** . You can find the **Advanced Search** link at the at the upper-right corner of the public contact table.

Name	Description
Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search public contacts. The options are: a. Last Name: Searches public contacts by last name. b. First Name: Searches public contacts by first name. c. Displays Name: Searches public contacts by display name. d. Contact Address: Searches public contacts by contact address. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The search value for the search criterion selected in the Drop-down 1 field.

Presence ACL field descriptions

High Priority Enforced User ACL (Access Control List)

This section displays the high priority enforced user ACL rules for users. You can add a new rule, modify and delete an existing rule for users.

Name	Description
Presentity Last Name	Last name of the presentity
Presentity First Name	First name of the presentity.
Watcher Last Name	Last name of the watcher.
Watcher First Name	First name of the watcher.
Watcher Type	Categorization of the watcher based on whether the watcher is a public or private contact.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
View	Opens the View Enforced User ACL page. Use this page to view the high priority enforced user ACL rules set for the watchers.
Edit	Opens the Edit High Priority Enforced User ACL page. Use this page to edit a high priority enforced user ACL rule set for a watcher.
New	Opens the New High Priority Enforced User ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers.
Delete	Deletes the selected high priority enforced user ACL rules.

Low Priority Enforced User ACL

This section displays the low priority enforced user ACL rules for users. You can add a new rule, modify and delete an existing rule for users.

Name	Description
Presentity Last Name	Last name of the presentity
Presentity First Name	First name of the presentity.
Watcher Last Name	Last name of the watcher.
Watcher First Name	First name of the watcher.
Watcher Type	Categorization of the watcher based on whether the watcher is a public or private contact.

Name	Description
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
View	Opens the View Enforced User ACL page. Use this page to view the low priority enforced user ACL rules set for the watchers.
Edit	Opens the Edit Low Priority Enforced User ACL page. Use this page to edit a low priority enforced user ACL rule set for a watcher.
New	Opens the New Low Priority Enforced User ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers.
Delete	Deletes the selected low priority enforced user ACL rules.

System ACL

This section displays the system ACL rules for watchers. You can add a new rule, modify and delete an existing rule for watchers.

Name	Description
Watcher Last Name	Last name of the watcher.
Watcher First Name	First name of the watcher.
Display Name / Login Name	Display or login name of the watcher.
Watcher Type	Categorization of the watcher based on whether the watcher is a public or private contact.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
View	Opens the View System ACL page. Use this page to view the system ACL rules set for the watchers.
Edit	Opens the Edit System ACL page. Use this page to edit a system ACL rule set for a watcher.
New	Opens the New System ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers.
Delete	Deletes the selected System ACL rules.

System Rule

This section displays the system rules. You can add a new rule, modify and delete an existing system rule.

Name	Description
Priority	Priority set for the rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Opens the Edit System rule page. Use this page to edit a system rule.
New	Opens the New System rule page. Use this page to create a new system rule by adding one or more access control rules.
Delete	Deletes the selected system rules.

Define Policy

You can use this section to define your personal rules for accessing your presence information by one or more watchers.

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set. The options are • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information.

Name	Description
	The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

New Enforced User ACL field descriptions

Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set.

Name	Description
	The options are • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Select Presentity

Name	Description
Status	The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status.
Name	Name of the user.
User Name	Unique name that gives access to the system.
Last Login	Date and time when the user has successfully logged into the system.
Advanced Search	Displays fields that you can use to specify the search criteria to search for presentities.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters presentities based on the filter criteria.
Select: All	Selects all the presentities in the table.

Name	Description
Select: None	Clears the check box selections.
Refresh	Refreshes the presentity information in the table.

Select Watcher

Name	Description
Last Name	Last name of the watcher.
First Name	First name of the watcher.
Display Name/Login Name	Display or login name of the watcher
Contact Type	Identifies whether the watcher is a private or public contact.
Description	A brief description about the watcher.
Advanced Search	Displays fields that you can use to specify the search criteria to search for watchers.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters watchers based on the filter criteria.
Select: All	Selects all the watchers in the table.
Select: None	Clears the check box selections.
Refresh	Refreshes the watcher information in the table.

The page displays the following field when you click the **Advanced Search** button above the presentity and watcher table at the upper-right corner.

Name	Description
Criteria	Use the fields to define the search criteria for searching the watchers and presentities in the database. Displays the following three fields: • Drop-down 1 - Lists the search criteria. • Drop-down 2 – The operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field. • Field 3 – The value for the search criterion

Name	Description
Commit	Creates the new enforced user ACL rule for the watchers.

Edit Enforced User ACL field descriptions

Edit Access Level Along With Action

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set. The options are: • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Presentity

Name	Description
Last Name	Last name of the presentity.
First Name	First name of the presentity.
Middle Name	Middle name of the presentity
Description	Brief description about the presentity.
Login Name	A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle.
Localized Display Name	Localized display name of the presentity. It is the localized full name.
Endpoint Display Name	Display name that identifies the presentity for an endpoint.

Contact Address

Name	Description
Handle	Unique contact address for communication with the presentity.
Handle Type	Qualifier that represents the type of handle.
Sub Type	Sub type defines the format of the address for the handle
Domain	Domain to which the handle belongs.

Watcher

Name	Description
Last Name	Last name of the watcher.
First Name	First name of the watcher.
Middle Name	Middle name of the watcher.
Description	Brief description about the watcher.
Company	Company name of the watcher.
Localized Display Name	Localized display name of the watcher. It is the localized full name.
Endpoint Display Name	Display name that identifies the watcher for an endpoint.

Contact Address

Name	Description
Address	Contact address of the watcher.
Type	Qualifier that represents the type of address.
Category	Category defines whether the address is an official or residential address.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Name	Description
Commit	Saves the changes to the database.

View Enforced User ACL field descriptions

View Access Level Along With Action

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Presentity

Name	Description
Last Name	Last name of the presentity.
First Name	First name of the presentity.
Middle Name	Middle name of the presentity
Description	Brief description about the presentity.
Login Name	A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle.
Localized Display Name	Localized display name of the presentity. It is the localized full name.
Endpoint Display Name	Display name that identifies the presentity for an endpoint.

Contact Address

Name	Description
Handle	Unique contact address for communication with the presentity.
Handle Type	Qualifier that represents the type of handle.
Sub Type	Sub type defines the format of the address for the handle
Domain	Domain to which the handle belongs.

Watcher

Name	Description
Last Name	Last name of the watcher.
First Name	First name of the watcher.
Middle Name	Middle name of the watcher.
Description	Brief description about the watcher.
Company	Company name of the watcher.
Localized Display Name	Localized display name of the watcher. It is the localized full name.
Endpoint Display Name	Display name that identifies the watcher for an endpoint.

Contact Address

Name	Description
Address	Contact address of the watcher.
Type	Qualifier that represents the type of address.
Category	Category defines whether the address is an official or residential address.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Name	Description
Edit	Opens the Edit High Priority Enforced User ACL page. Use this page to edit the high priority ACL for a watcher.

New System ACL field descriptions

Use this page to add enterprise wide permissions on the presence information of presentties in an enterprise and associate these permissions with the watchers.

Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set. The options are • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Select Watcher

Name	Description
Last Name	Last name of the watcher.
First Name	First name of the watcher.
Display Name/Login Name	Display or login name of the watcher.
Contact Type	Identifies whether the watcher is a private or public contact.
Description	A brief description about the watcher.
Advanced Search	Displays fields that you can use to specify the search criteria to search for watchers.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters watchers based on the filter criteria.
Select: All	Selects all the watchers in the table.
Select: None	Clears the check box selections.
Refresh	Refreshes the watcher information in the table.

The page displays the following field when you click the **Advanced Search** button above the presentity and watcher table at the upper-right corner.

Name	Description
Criteria	Search criteria for searching the watchers or presentities.

Name	Description
Commit	Creates the new system ACL rule for the watchers.

Edit System ACL field descriptions

Edit Access Level Along With Action

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Button	Description
Edit	Use this button to modify an existing rule.
New	Use this button to add a new rule for the watchers.
Delete	Deletes the selected rule from the list of rules added for the watchers.

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

Name	Description
Access Level	Presence information for which access control rules are set. The options are • Telephony: Telephony related presence information for which you can set an access permission. • All: Contains all the presence information types for which you can set an access permission.
Action	Defines the access control permission over the presence information. The options are: • Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher. • Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher. • Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information. • Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.

Button	Description
Save	Saves the rules information in the database when you add or modify a rule for watchers.

Watcher

You can only view information in these fields.

Name	Description
Last Name	Last name of the watcher.
First Name	First name of the watcher.
Middle Name	Middle name of the watcher.
Description	Brief description about the watcher.
Company	Company name of the watcher.
Localized Display Name	Brief description about the watcher.
Endpoint Display Name	Display name that identifies the watcher for an endpoint.

Contact Address

You can only view information in these fields.

Name	Description
Address	Contact address of the watcher.
Type	Qualifier that represents the type of address.
Category	Category defines whether the address is an official or residential address.
Label	Need Information
Alternative Label	Need Information

Name	Description
Commit	Saves the changes to the database.

View System ACL field descriptions

View Access Level Along With Action

Name	Description
Select Check box	Use this check box to select a rule.
Access Level	Presence information for which access control rules are set.
Action	Defines the access control permission over the presence information.

Watcher

Name	Description
Last Name	Last name of the watcher.
First Name	First name of the watcher.
Middle Name	Middle name of the watcher.
Description	Brief description about the watcher.
Company	Company name of the watcher.
Localized Display Name	Brief description about the watcher.
Endpoint Display Name	Display name that identifies the watcher for an endpoint.

Contact Address

Name	Description
Address	Contact address of the watcher.
Type	Qualifier that represents the type of address.
Category	Category defines whether the address is an official or residential address.
Label	Need Information
Alternative Label	Need Information

Name	Description
Edit	Opens the Edit High Priority Enforced User ACL page. Use this page to edit the high priority ACL for a watcher.

New Private Contact field descriptions

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company

Name	Description
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town of the contact.
Postal Code	Postal code of the of the city or town where the contact's office or home is located.
Province	The full name of the province where the contact's office or home is located.
Country	The name of the country where the contact's office or home is located.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the private contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the private contact.
Delete	Deletes the selected private contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the private contact.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.

Name	Description
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the private contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the private contact.
Delete	Deletes the selected private contacts.

Button	Description
Add	Creates a new contact. **Note:** You must enter valid information in the mandatory fields to successfully create a new contact.

Edit Private Contact field descriptions

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.

Name	Description
Source	The source of provisioning the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	Postal code of the of the city or town where the contact's office or home is located.
Province	The full name of the province where the contact's office or home is located.
Country	The name of the country where the contact's office or home is located.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the private contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the private contact.
Delete	Deletes the selected private contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the private contact.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the private contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the private contact.
Delete	Deletes the selected private contacts.

Button	Description
Add	Saves the modified information in the database.

View Private Contact field descriptions

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.

Name	Description
Postal Code	Name of the contact's company.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the View Private Contact page. You can use this page to edit the details of the contact.

Add Address field descriptions

Use this page to add communication address of the contact.

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address, sip or IM of the contact. The format of the address must conform to the type of address that you selected in the **Type** field.
Type	Type of address. The following are the types of address: • phone: An address of this type supports phone numbers. • sip: An address of this type supports sip based communication. • msrtc An address of this type supports communication with a Microsoft RTC Server. • ibmsametime: An address of this type supports communication with IBM Sametime,

Name	Description
	• xmpp: An address of this type supports xmpp based communication. • smtp: An address of this type supports communication with the SMTP server.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Add	Adds the contact address of the public contact in the database.

Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address, sip or IM of the contact. The format of the address must conform to the type of address that you selected in the **Type** field.
Type	Type of address. The following are the types of address: • phone: An address of this type supports phone numbers. • sip: An address of this type supports sip based communication. • msrtc An address of this type supports communication with a Microsoft RTC Server. • ibmsametime: An address of this type supports communication with IBM Sametime, • xmpp: An address of this type supports xmpp based communication. • smtp: An address of this type supports communication with the SMTP server.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Add	Saves the modified information in the database.

View Public Contact field descriptions

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	Name of the contact's company.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Edit Public Contact field descriptions

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	Name of the contact's company.

Name	Description
Province	The full name of the contact's province.
Country	The name of the contact's country.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the public contact.
Delete	Deletes the selected public contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the public contact.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Add	Saves the modified information in the database.

New Public Contact field descriptions

Contact Details

Name	Description
Last Name	Last name of the contact.
First Name	First name of the contact.
Middle Name	Middle name of the contact.
Description	A brief description about the contact.
Company	Name of contact's company
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Endpoint display name of the contact.
Language Preference	A list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The type that identifies whether mailing address is a home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	Name of the contact's company.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the public contact.
Delete	Deletes the selected public contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the public contact.

Contact Address

Name	Description
Address	An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.
Type	Type signifies the communication medium used to interact with the user.
Category	Categorization of the address based on the location.
Label	A text description for classifying this contact.
Alternative Label	A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Add	Creates a new contact. **Note:** You must enter valid information in the mandatory fields to successfully create a new contact.

Group Management

Group Management

The Group and Lookup Service is a shared service that provides group administration and a lookup service for all managed resources. The Group and Lookup Service supports group administration for common resources shared across elements such as roles and users as well

as element specific resources that are not shared. You can perform the following operations using the Group Management service:

- Create a group
- View and Modify groups
- Create a duplicate group by copying the properties of an existing group
- Assign and remove resources for groups
- Delete groups
- Synchronize groups

As a shared service, Group and Lookup reduces the time and effort involved for defining groups of managed resources that are needed by more than one application or service.

Viewing Groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. On the Group Management page, select a group and perform one of the following steps:
   - If the selected group is a selection based group member, then click **View**.
   - If selected group is a query based group, then on the View Group page click **Execute Query**.

Result

The View Group page displays the selected group details along with the resources assigned to them.

Related topics:

View Group field descriptions on page 308

Creating Groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.

3. Perform any one of the following steps:
   - To create a group, click **New** on the Group Management page.
   - To create a subgroup under a group or a subgroup, select a group or a subgroup and click **New** on the Group Management page. You can click **+** to traverse a group.
4. On the Create Group page, enter the appropriate information.
5. Click **Commit** to create the new group.

Related topics:

Create Group field descriptions on page 309

Modifying Groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. Select a group.
4. To access the **Edit Group** page, perform any one of the following steps:
   - On the Group Management page, click **Edit**.
   - On the Group Management page, click **View** > **Edit**.
5. On the Edit Group page, enter the appropriate information.
6. Click **Commit** to save the changes to the database.

Related topics:

Edit Group field descriptions on page 311

Creating duplicate groups

Use this functionality to copy an existing group to create a new group. When you create a duplicate group, the system copies all the information from the existing group to the new group.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.

3. On the Group Management page, select a group and click **Duplicate**.
4. On the Duplicate Group page, perform any one of the following steps:
   - To create a duplicate group at root level, click **Root** .
   - To create a duplicate group under a group or a subgroup, select a group or a subgroup and click **Selected group** .

     Note:
     Click **+** to view the subgroups of a group.

Result

The duplicate group appears on the Group Management page as copy of the parent group (the parent group from which the group is created).

Note:
Use the edit functionality to change the properties of this group.

Related topics:

Duplicate Group field descriptions on page 313

Deleting groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. Select the groups that you want to delete.

   Note:
   You can not delete more than one group at a time. The page makes the Delete button unavailable if you select more than one group in the table.
4. Click **Delete** on the Group Management page.
5. On the Delete Group Confirmation page, click Delete.

Related topics:

Delete Group Confirmation field descriptions on page 313

Moving groups

You can move a group from one group to an another group or to the root level. You can also move a group from the root level to an another group.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. On the Group Management page, select a group and click **More Actions** > **Move**.
4. On the Move Group page, Perform any one of the following steps:
   - To move a group to the root level, click **Root** .
   - To move a group to another group or a subgroup, select the group or the subgroup and click **Selected group** .

   Note:
   Click **+** to view the subgroups of a group.

Related topics:

Move Group field descriptions on page 314

Synchronizing resources for a resource type

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. On the Group Management page, click **More Actions** > **Sync**.
4. On the Resource Synchronization page, select the type of resources from the **Type** drop-down field.
5. Click **Sync**.

Related topics:

Resource Synchronization field descriptions on page 314

Switching to table view

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. On the Group Management page, click **Switch to Table**.

Note:
Switch to Table is a toggle button.

Switching to tree view

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. On the Group Management page, click **Switch to Tree**.

Note:
Switch to Tree is a toggle button.

Assigning resources to a group

You can assign only resources of the type that is configured for the group. The type of resources that can become the member of a group is set when you create a group. If the type of resource is set to ALL, you can assign all types of resource to the group. If the type is set to a specific resource type, only resources of that type can be assigned to that group.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. Perform one of the following steps:
   - Click **New** > **Assign Resources**.

- Select a group if you are assigning a resource to an existing group and click **Edit** > **Assign Resources**.
- Select a group if you are assigning a resource to an existing group and click **View** > **Edit** > **Assign Resources**.

4. On the Resources page, select a resource.

Note:

The Resources page displays all the resources available in the application, but you can not select the resources that are already assigned to the group.

Note:

You can also search for a resource using the Advance search functionality.

5. Click **Add To a Group** .

Result

The application adds the selected resources to the group.

Related topics:

Resources field descriptions on page 315

Assigning resources to a new group

Use this functionality to create a new group and assign resources to this group. You can choose to create the new group at root level or under an existing group.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Resources** in the left navigation pane
3. Select a resource. You can also click the **Advanced Search** link to search a resource.
4. Click **Add To New Group** .
5. Perform one of the following steps:
   - To add a resource to a new group, perform the following steps:
     i. On the Choose Parent Group page, click **Root** .
     ii. On the Create Group page, enter the appropriate information.
     iii. Click **Commit** to add the selected resource to the new group at root level.

- To add a resource to a new subgroup under a group, perform the following steps:

    i. On the Choose Parent Group , click a group.

    Note:
    If you want to select a subgroup of a group, click **+** and click the subgroup.

    ii. Click **Selected Group**.

    iii. On the Create Group page, enter the appropriate information.

    iv. Click **Commit**.

    Note:
    The Group Management application creates the new group and assigns the selected resources. This group is added under the group that you selected on the Choose Parent Group page.

Related topics:

Create Group field descriptions on page 309

Adding resources to a selected group

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Asset Management** > **Resources** in the left navigation pane
3. Select a resource. You can also click the **Advanced Search** link to search a resource.
4. Click **Add To Group** .
5. On the Choose Parent Group page, click a group.
6. click **Selected Group**.
   The Group Management module assign the selected resources to the groups selected on the Choose Parent Group page.

Searching for resources

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. To access the **Resources** page, perform any one of these steps.
   - On the Group Management page, click **New** > **Assign Resources**.
   - On the Group Management page, click **Edit** > **Assign Resources**.
   - On the Group Management page, click **View** > **Edit** > **Assign Resources**.
4. On the Resources page, click **Advanced Search**.
5. Select resource type from the **Type** drop-down field.
6. In the Resource Attributes section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter search value in the third field.

Note:
If you want to add a search condition, click **+** and repeat substeps a through c listed in step 6.

Note:
If you want to delete a search condition, click **-** . This button is enabled when you have added more than one search condition.

7. Click **Search**.

Result

The Resources section displays the resources matching the search criteria. If no resources are found matching the search criteria, Resource section displays a message No records found.

Searching for resources based on group membership

You can search resources based on group membership. The Advanced Search functionality provided on the Resources page does not allow you to search resources based on group

membership. You can search resources using the Advanced Search functionality on the Group Management page.

1. Log in to the Common Console Management web interface.
2. Click the **User Management** > **Group Management** link in the left navigation pane.
3. On the Group Management page, click **Advanced Search**.
4. In the **Criteria** section, do the following:
    a. Select the search criterion from the first field.
    b. Select the operator from the second field.
    c. Enter the search value in the third field.

Note:
If you want to add a search condition, click **+** and repeat substeps 1 through 3 listed in step 6.

Note:
If you want to delete a search condition, click **-** . This button gets enabled when you have added more than one search condition.

5. Click **Search**.

Result

GLS renders list of groups matching the search criteria.

Related topics:

Resources field descriptions on page 317

Filtering groups

You can apply filter on the following three columns:

- Name
- Type
- Group

You may filter groups using one or multiple column filters.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.

3. On the Group Management page, click **Filter: Enable**.
4. Enter the group name in the field under the **Name** column.
5. Select the resource type from the drop-down field under the **Type** column.
6. Enter the hierarchy level under the **Hierarchy** column.

   When you enter a hierarchy level, the table displays only those groups that you have created under that level. For example, if you want to view all the groups that you have created under root, enter / as hierarchy level.
7. Click **Apply** .

   Note:

   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

Result

The table displays only those groups that matches the filter criteria.

Filtering resources

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. Select a group if you are assigning a resource to an existing group.
4. To access the **Resources** page, perform one of the following steps.
   - On the Group Management page, click **New** > **Assign Resources**.
   - On the Group Management page, click **Edit** > **Assign Resources**.
   - On the Group Management page, click **View** > **Edit** > **Assign Resources**.
5. On the Resources page, click **Filter: Enable**.
6. Enter the resource name in the field under the **Name** column.

   Note:

   You may choose to apply filter on one column or multiple columns.
7. Select the resource type from the field under the **Type** column.

   Note:

   You may choose to apply filter on one column or multiple columns.
8. Click **Apply** .

Note:

To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

Result

The table displays resources that matches the filter criteria.

Searching Groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. On the Group Management page, click **Advanced Search** displayed at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. Select the search criterion from the first drop-down field.
   b. Select the operator from the second drop-down field.
   c. Enter the search value in the third field.

   Note:

   If you want to add a search condition, click **+** and repeat sub steps a through c listed in step 4.

   Note:

   If you want to delete a search condition, click **-** . This button is available if there are more than one search condition.
5. Click **Search**.

Result

The page displays the groups that matches the value specified for the search criteria.

Removing assigned resources from a group

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **User Management** > **Group Management** in the left navigation pane.
3. Perform one of the following steps:
   - If you assigned resources to the group while creating a new group, select the resources and click > **Remove**.
   - Select a group and click **Edit** > **Remove**.
   - Select a group and click **View** > **Edit** > **Remove**.

Group Management field descriptions

Use this page to manage groups. You can use this page to perform the following tasks:

- Create, modify, view and delete a group.
- Create a copy of an existing group.
- Move a selected group from one group to another group.
- Synchronize resources for a resource type.
- Define search conditions to Search for groups.
- Apply column filters in the **Groups section** to view groups matching the filter criteria.

Name	Description
Select check box	Use this check box to select a group.
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.
Dynamic	The value indicates whether resource assignment for the group is dynamic or static. **Note:** You can view this column in Tree view.

Button	Description
View	Opens the View Group page that allows you to see the details of the selected group.
Edit	Opens the Edit Group page you can use to modify the information of the selected group.
New	Opens the Create Group page you can use to create a new group.
Duplicate	Opens the Duplicate Group page that you can use to duplicate a group to another selected group.
Delete	Deletes selected groups.
More Actions > **Move**	Opens the Move page that you can use to move a group to another selected group.
More Actions > **Sync**	Opens the Resource Sync page that you can use to synchronize resources for a resource type.
Switch To Tree	Displays groups in a tree view. This is a toggle button. **Note:** You can view this button when you are in a Tree view.
Switch To Table	Displays groups in a table view. This is a toggle button. **Note:** You can view this button when you are in a Table view.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a group.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters groups based on the filter criteria.
Select: All	Selects all the groups in the table.
Select: None	Clears all the check box selections.
Refresh	Refreshes the groups information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page

Name	Description
Criteria	Displays the following three fields:

Name	Description
	• Drop-down 1 - The list of criteria that you can use to search groups. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value for the search criterion. The Group Management service retrieves and displays groups that match this value.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches group based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

View Group field descriptions

Use this page to view a selected group. You can not modify the information in the fields while you are in view mode.

View Group

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources . The options are: • Creating the group having member of same resource type. • All — Creating the group without any restrictions on its member.
Group Membership	The options are : • Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups. • Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.
Description	A brief description about the group.

Button	Description
Edit	Opens the Edit Group page that you can use to modify the group information.
Done	Closes the View Group page and takes you back to the Group Management page.

Define Query

The page displays these fields when you use **Query Based** option for creating group members.

Name/Button	Description
Define Query	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search resources. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.
+	Adds a search condition row for defining a new search condition.
–	Removes a search condition.
Execute Query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the **Results** section. **Note:** This button is visible only when you create a query based group.

The page displays following fields for assigned resources.

Name	Description
Name	Name of the resource.
Type	Type of the resource.

Related topics:

Viewing Groups on page 295

Create Group field descriptions

Use this page to create a new group.

New Group

Name	Description
Name	Unique name of the group.

Name	Description
Type	Group type based on the resources . The options are: • Creating the group having member of same resource type. • All — Creating the group without any restrictions on its member.
Group Membership	The options are : • Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups. • Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.
Description	A brief description about the group.

Button	Description
Assign Resources	Opens the Resources page that you can use to search and assign resources to a group. **Note:** when you use **Selection Based** option for creating group members in the group.
Commit	Creates a new group with the specified configurations.
Cancel	Closes the Create Group page without saving any information on the page and returns to the Group Management page.

Define Query

The page displays the following fields when you use **Query Based** option for creating group members.

Name/Button	Description
Define Query	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search resources. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.
+	Adds a search condition row for defining a new search condition.
–	Removes a search condition.

Name/Button	Description
Execute Query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the **Results** section. **Note:** This button is visible only when you create a query based group.
Name	Name of the resource.
Type	Type of the resource.

Assigned Resources

The page displays the following fields when you use **Selection Based** option for creating group members.

Name	Description
Name	Name of the resource.
Type	Type of the resource.
Assign Resources	Opens the Resources page that you can use to search and assign resources to a group.
Remove	Remove the selected resources from the list of assigned resources.

Related topics:

Creating Groups on page 295
Assigning resources to a new group on page 300

Edit Group field descriptions

Use this page to modify a selected group. You cannot modify the following fields in the page:

- Type
- Group Membership

Edit Group

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources . The options are: • Creating the group having member of same resource type. • All — Creating the group without any restrictions on its member.

Name	Description
Group Membership	The options are : • Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups. • Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.
Description	A brief description about the group.

Button	Description
Commit	Saves the changes in the database.
Cancel	Closes the Edit Group page without saving any information and returns to the Group Management page.

Define Query

The page displays the following fields when you use **Query Based** option for creating group members.

Name/Button	Description
Define Query	Displays the following three fields: • Drop-down 1 - The list of criteria that you can use to search resources. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field. • Field 3 – The value corresponding to the search criteria.
+	Adds a search condition row for defining a new search condition.
–	Removes a search condition.
Execute Query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the **Results** section. **Note:** This button is visible only when you create a query based group.
Name	Name of the resource.
Type	Type of the resource.

Assigned Resources

The page displays the following fields when you use **Selection Based** option for creating group members.

Name	Description
Name	Name of the resource.
Type	Type of the resource.
Assign Resources	Opens the Resources page that you can use to search and assign resources to a group.
Remove	Remove the selected resources from the list of assigned resources.

Related topics:

Modifying Groups on page 296

Delete Group Confirmation field descriptions

Use this page to delete the groups listed in the table.

Name	Description
Name	Name of the group.
Type	Group type based on the resources.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.
Sub-Group Count	Count of sub groups in the parent group.
Resource Count	Count of the resources in the group.

Button	Description
Delete	Deletes the groups listed in the table.
Cancel	Cancels the delete operation and takes you back to the Group Management page.

Related topics:

Deleting groups on page 297

Duplicate Group field descriptions

Use this page to create a duplicate group from an existing group.

Name	Description
Select	Select a group
Name	The groups under which you can create a duplicate group. Click the **+** to expand a group.

Button	Description
Root	Creates a duplicate group at the root level.
Selected Group	Creates a duplicate group under the selected group.
Cancel	Closes the page and returns to the Group Management page.

Related topics:

Creating duplicate groups on page 296

Move Group field descriptions

Use this page to move a group to another group or to root level.

Name	Description
Select	Select a group
Name	The groups to which you can move the selected group . Click the **+** to expand a group.

Button	Description
Root	Moves the selected group to the root level
Selected Group	Moves the selected group to the group that you have selected in the **Name** column
Cancel	Closes the Move Group page and returns to the Group Management page.

Related topics:

Moving groups on page 298

Resource Synchronization field descriptions

Use this page to synchronize resources for a resource type.

Name	Description
Type	The type based on the resources it contains.
Done	Synchronizes resources for the selected resource type and returns to the Group Management page.
Cancel	Closes the Resource Synchronization page and returns to Group Management page.

Related topics:

Synchronizing resources for a resource type on page 298

Resources field descriptions

Use this page to search and assign a resource to a group. You can use this page to perform the following tasks:

- Assign selected resources to a new or an existing group.
- Apply filters to view only those resources that match filter criteria.
- Define search conditions to search resources that match the search conditions.
- View the details of the attributes for the selected resources.
- View the group membership details for the selected resources.

The page has the following sections:

- Criteria
- Resources
- Attributes of resources
- Resource is member of following groups

Resources section

Name	Description
Select Check box	Use the check box to select a record.
ID	Unique name of the resource. Also known as native id of the resource
Type	The type based on the resources.
View Details	Displays the attributes and membership details of the selected resources on the same page.

Button	Description
Add to Group	Adds the selected resources to the group.

Button	Description
Cancel	Closes the Resources page and take you back to the Create Group page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a resource.
Filter: Enable	Displays fields under the columns, **Name** and **Type**. You can use them to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters resources based on the filter criteria.
Select: All	Selects all the resources displayed in the table in the Resources section.
Select: None	Clears the selection for the resources that you have selected.
Refresh	Refreshes resource information in the table.

Attributes of resources section

Name	Description
Name	Name of the attribute.
Value	Value assigned to the attribute for the resource.

Resource is member of following groups section

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources it contains.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Type	The types based on the resources it contains.
Resource Attributes	Displays the following three fields:

Name	Description
	• Drop-down 1 - The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the **Type** drop-down list. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of attribute selected in the first drop-down list. • Field 3 – The value corresponding to the search criterion.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the resources matching the search conditions.
Close	Closes the Criteria section.
Advanced Search	Cancels the search operation and hides the **Criteria** section.

Related topics:

Assigning resources to a group on page 299

Resources field descriptions

Use this page to search and assign a resource to a group. You can use this page to perform the following tasks:

- Add a selected resource to a new group or to a chosen group.
- Apply filters to view only those resources that matches filter criteria.
- Define search conditions to search resources that matches the search conditions.
- View the details of the attributes for the selected resources.
- View the group membership details for the selected resources.

The page has the following sections:

- Criteria
- Resources
- Attributes of resources
- Resource is member of following groups

Resources section

Name	Description
Select Check box	Use the check box to select a record.

Name	Description
ID	Unique name of the resource. Also known as native id of the resource
Type	The type based on the resources.
View Details	Displays the attributes and membership details of the selected resources on the same page.

Button	Description
Add to Group	Opens Choose Group page. Use this page to choose a group in which you want to add the selected resource.
Add to New Group	Opens Choose Parent Group page. Use this page to add the selected resources to a new group or to a chosen group.
Cancel	Closes the Resources page returns to the Create Group page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a resource.
Filter: Enable	Displays fields under the columns, **Name** and **Type**. You can use them to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters resources based on the filter criteria.
Select: All	Select all the resources in the table.
Select: None	Clears the selection for the resources that you have selected.
Refresh	Refreshes resource information in the table.

Attributes of resources section

Name	Description
Name	Name of the attribute.
Value	Value assigned to the attribute for the resource.

Resource is member of following groups section

Name	Description
Name	Unique name of the group.
Type	Group type based on the resources it contains.
Hierarchy	Position of the group in the hierarchy.
Description	A brief description about the group.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Type	The types based on the resources it contains.
Resource Attributes	Displays the following three fields: • Drop-down 1 - The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the **Type** drop-down list. • Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of attribute selected in the first drop-down list. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the resources matching the search conditions.
Close	Closes the Criteria section.
Advanced Search	Cancels the search operation and hides the **Criteria** section.

Related topics:

Searching for resources based on group membership on page 302

Choose Group field descriptions

Use this page to add resources to the selected groups.

Name	Description
Select	Use this option to select a group.
Name	Name of the group.
Type	Group type based on the type of resources. The options are: • Groups having members of same resource type. • All — Groups having members of any resource types.
Dynamic	The value indicates whether the group uses a query to determine its members or has static members. True indicates that group membership is not permanent and determined when you run the query and false indicates groups with static members.

Name	Description
Description	A brief description about the group.

Button	Description
Expand All	Shows the subgroups of groups listed in the table.
Collapse All	Hides the subgroups of all the expanded groups.
Selected Group	Adds the resource as a member of the selected group.
Cancel	Closes the Choose Group page and takes you back to the Resources page.

Choose Parent Group field descriptions

Use this page to add resources to a selected group or to a new group.

Name	Description
Select	Use this option to select a group.
Name	Name of the group.
Type	Group type based on the type of resources. The options are: • Groups having members of same resource type. • All — Groups having members of any resource types.
Dynamic	The value indicates whether the group uses a query to determine its members or has static members. True indicates that group membership is not permanent and determined when you run the query and false indicates groups with static members.
Description	A brief description about the group.

Button	Description
Expand All	Shows the subgroups of groups listed in the table.
Collapse All	Hides the subgroups of all the expanded groups.
Root	Opens New Group page. Use this page to create a new group. The selected resource is the member of this group.
Selected Group	Adds the resource as a member of the selected group.
Cancel	Closes the Choose Parent Group page and takes you back to the Resources page.

Chapter 6: Network Routing Policy

Administering Session Manager routing

Overview of Session Manager routing

This section details the procedures that are required to set up Session Manager enterprise routing. To complete the administrative procedures, you must use the Network Routing Policy (NRP) selection from the System Manager Common Console navigation pane.

Once the initial setup is completed, administrators can use the same screens and procedures for administering and modifying the various NRP entities as well as Session Manager instances.

The primary task of Session Manager is to route session creation requests from one server to another based on the address specified in the session creation request.

The addresses which are specified to identify the ultimate destination of a session creation request are in the form of a SIP Uniform Resource Identifier (URI). It consists mainly of a user part and a domain part. Session Manager uses both parts in its routing decisions in the following manner:

- The domain part is normally a DNS domain.
- The user part is an alphanumeric string (or handle). Session Manager has special rules for efficiently routing and manipulating handles which consist entirely of digits (for example, telephone numbers).

The servers which send their session creation requests to the Session Manager are called SIP Entities. Session Manager routes these requests to other SIP Entities based on the routing rules you have administered.

Session Manager associates SIP Entities with specific locations and can make different routing decisions based upon the location from which a session creation request arrives.

Prerequisites for Network Routing Setup

This section assumes that the following requirements are met:

- The System Manager server is installed.
- All Session Manager instances are installed.

Refer to the section Session Manager installation for details.

Network Routing Policy

Network Routing Policy

A Network Routing Policy (NRP) tells the system which SIP entity should receive a call that matches the configured dial pattern or regular expression. Administrators can use NRP to administer Session Manager instances and related routing policies. The configuration data is distributed from the NRP database to each remote Session Manager instance.

All calls originate from a SIP entity. Routing policies describe how a call is routed when it comes from a particular location associated with the SIP entity and a distinct pattern is dialed (or a regular expression is given) during a particular time range with a distinct ranking/cost for the route to another SIP entity.

Locations are used for origination-based routing and specifying bandwidth for call admission control.

NRP and Session Manager allow administrators to define routing:

- by combining several locations
- by combining several dial patterns and SIP domains
- for several ToD and rankings
- for a single routing destination

Routing of a call using NRP data

1. It tries to match the domain to one of the authoritative domains.
2. If Session Manager is authoritative for the domain, then it tries to match the digit pattern.

3. If Session Manager is not authoritative for the domain or if a digit pattern match is not found, it tries to use the regular expression table.
4. If no regular expression match is found, it sends the request to a Session Manager-provisioned outbound proxy.
5. If no outbound proxy has been administered for the Session Manager and it is not authoritative for the domain, then it uses DNS to determine where to route the request.
6. If the DNS lookup is not successful, the call fails.

Administering initial setup of the Session Manager

Once you have completed the initial setup as a part of ongoing administration, you can modify the created entities or delete them as required.

The recommended order for the initial set up of the Session Manager using the System Manager Network Routing Policy screens is as follows.

1. Accept or change default personal settings.
2. Create SIP domains.
3. Create locations.
4. Create adaptations.
5. Create SIP entities, some of which are routing destinations:
    - Create other SIP entities.
    - Assign locations and adaptations to the SIP entities.
6. Create entity links:
    - Between Session Managers.
    - Between Session Managers and other SIP entities.
7. Create time ranges.
8. Create routing policies.
9. Create dial patterns and assign them to routing policies and locations.
10. Create regular expressions and assign them to routing policies.
11. Create Session Manager instances using the Session Manager menus on the System Manager navigation pane.

Exporting NRP element data

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > ***<Any NRP element>***.
2. From the NRP Entity screen, click **More Actions** > **Export *<NRP Element>***.

   For example, to export adaptations, from the navigation pane, you can click **Network Routing Policy** > **Adaptations**. From the Adaptations screen, select **More Actions** > **Export Adaptations**.

   To export regular expressions, from the navigation pane, you can click **Network Routing Policy** > **Regular Expressions**. From the Regular Expressions screen, click **More Actions** > **Export Regular Expressions**.
3. Select a check box for the entity to be exported from the list of entities on the screen.
4. Click **Browse** to export files to a required location and click **Export**.

   You must export a file in the XML format. This file can be manually modified.

Importing NRP element data

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **<Any NRP element>**.
2. From the NRP Element screen, click **More Actions** > **Import *<NRP Element>***.

   For example, to import dial patterns, from the navigation pane, click **Network Routing Policy** > **Dial Patterns**. From the Dial Patterns screen, click **More Actions** > **Import Dial Patterns**.
3. Click **Browse** to import files from the required location and click **Import**.

   You must import a file in the XML format. This file can be an exported file, or a manually created or modified file.

Saving, Committing, and Synchronizing configuration changes

Session Manager allows you to save the domain data to the System Manager database and distribute the changes to all the Session Manager instances.

To save the data to System Manager and distribute it to the Session Managers, click **Commit**.

When you click**Commit** , System Manager saves the data to the System Manager database. System Manager synchronizes and distributes the data to all the Session Manager instances. For example, renaming an adaptation also changes that data on the SIP Entity Details screen, or changing dial pattern data also changes that data in the routing policy where that dial pattern is used.

Duplicating NRP Element Data

You can use the **Duplicate** button on the relevant Session Manager NRP screens to duplicate NRP elements. Select the check box for the relevant element and click **Duplicate**. Duplication of data is useful if you want to create elements that are similar and want to rename them or copy an entity and make minimal changes to the entity attributes.

For example, to use a routing policy and to add a dial pattern to the copied routing policy, you can duplicate the routing policy and then add the required dial pattern to it.

Modifying the Default Personal Settings

You can use the Personal Settings screen to change the default values or ranges for parameters that are used by the other NRP menu options

These values are used as defaults when creating new NRP elements. Modifying these values does not change the values of already created entities .

1. From the **Network Routing Policy** menu from the left side of the screen, select **Personal Settings**. The Personal Settings screen is displayed.
2. Under **Adaptations**, specify the minimum and maximum number of characters for pattern-matching. These values are used by the NRP Adaptations option. The default minimum and maximum values are 1 and 36 respectively.
3. Under **Dial Patterns**, specify the minimum and maximum length for dial pattern. These values are used by the **NRP Dial Patterns** option. The default minimum and maximum values are 1 and 36 respectively.
4. Under **Entity links**, specify the port number to be used as a listen port. The default port is 5060. This port is used by the **NRP Entity Links** option.
5. Under **SIP Domains**, specify a domain suffix. The default suffix is avaya.com.
6. Under SIP entities, specify the following:
    a. Select the default SIP entity type from the **Type** pull-down menu. The default type is Session Manager. You can optionally select SBC, CM, Voice Portal, Gateway, SIP Trunk, and Other.
    b. Select the default time zone from the **Time Zone** pull-down menu. The default time zone is America/Denver.

c. Select the default transport protocol for ports. The default protocol is TLS. Optionally, you can select TCP or UDP.

d. With entity links from both the Session Manager instances, checking the Override Port & Transport with DNS SRV check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.

- If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
- If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.

7. Under **Time Ranges**, specify the default start time and end time that should be used by the NRP Time Ranges option. The default is to use a 24-hour time range, that is, the start time is 00:00 hours and the end time is 23:59 hours.
8. Under Application Settings, select the **Show warning message** check box to get a warning message if you try to navigate to another page when a page has unsaved data or when data import is in progress.
9. Click **Apply** to save the changes.

Related topics:

Personal Settings field descriptions on page 326

Personal Settings field descriptions

Use this page to specify personal settings for all the NRP menus on the right-hand side pane and to save them as your personal default.

Name	Description
Matching Pattern Min Length	Minimum length of pattern matched for adaptations. The minimum value can be 1.
Matching Pattern Max Length	Maximum length of pattern matched for adaptations. The maximum value can be 36.
Dial Pattern Min Length	Minimum length of dial pattern to be matched. The minimum value can be 1.
Dial Pattern Max Length	Maximum length of dial pattern to be matched. The maximum value can be 36.

Name	Description
Listen Port	Number of the port to be used for SIP entity links. The default port is 5060.
Default Transport Protocol for Entity Links	The default transport protocol that the entity links use, such as TLS, TCP, or UDP. The default is TLS.
Suffix	The default suffix to be used for the domain name.
Type	Type of the SIP entity, such as ASM, CM, Trunk, Gateway, and so on. The default is ASM.
Time Zone	Default time zone to be used for the SIP entity link.
Default Transport Protocol for Ports	Default transport protocol to be used by the ports. The default is TLS.
Use DNS Routing	Select check box to use DNS routing.
Time Range Start Time	Start time for the time range. Default is 00:00
Time Range End Time	End time for the time range. Default is 23:59.
Show warning message	Displays a warning message if you try to navigate to another page when the displayed page has unsaved data or if a data import is on progress.

Button	Description
Restore Defaults	Restores vendor defaults.
Revert	Reverts to settings before the last applied settings.
Apply	Saves and applies the modified personal settings.

Related topics:

Modifying the Default Personal Settings on page 325

SIP domains

About NRP SIP Domains

The NRP SIP Domains screen is used to create a set of SIP domains and sub-domains to enable the Session Manager enterprise to use domain-based routing. This information is used to determine if a SIP user is part of the SIP network. Domains determine if the Session Manager's dial plan can be used to route a particular call. Subdomains are automatically checked if not provisioned. For example, Session Manager needs to check dial patterns for avaya.com if a request to 123@myserver.avaya.com comes in and myserver.avaya.com is not administered as a domain.

The administrator can create a SIP domain and subdomains based on the corporate requirement.

- Domain name can be `<organization-name.domain>`, for example, avaya.com or abc.org.
- Sub-domain can be named based on the geographical location or any other corporate requirements such as office location, for example, us.avaya.com and fr.avaya.com can be sub-domains for Avaya offices in the US and in France, or dr.avaya.com and br.avaya.com can be sub-domains for Avaya offices in Denver and in Basking Ridge.

Creating NRP SIP domains

Create a SIP Domain or set of SIP Domains if you plan to use domain-based routing.

1. From the **Network Routing Policy** menu from the left side of the screen, select **SIP Domains**.
2. Click **New**.
3. Enter the domain name and notes for the new SIP domain or sub-domain.
4. Click **Cancel** or **Commit**.

Modifying NRP SIP domains

You can also edit or delete the SIP domains using the **SIP domains** option. The SIP Domains screen is displayed.

1. From the **Network Routing Policy** menu from the left side of the screen, select **SIP Domains**.
2. To edit information for existing domains or sub-domains, select the check boxes for the domains that you want to edit and click **Edit**.
3. Make changes to the domain data as required.
4. To copy existing domain data to a new domain, select the domain and click **Duplicate**. You can edit the duplicate domain name as required.
5. Click **Commit**.

Deleting NRP SIP Domains

1. From the **Network Routing Policy** menu from the left side of the screen, select **SIP Domains**.
2. To delete an existing domain or domains, select the check boxes for the domains that you want to edit and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

Related topics:

Delete Confirmation field descriptions on page 329

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected SIP domains.

Button	Description
Delete	Deletes the selected SIP domains.
Cancel	Cancels the deletion of the SIP domains.

Related topics:

Deleting NRP SIP Domains on page 329

SIP Domains field descriptions

Use this page to create, modify, delete, and manage SIP domains.

Button	Description
Edit	Opens the SIP Domains page that you can use to modify the SIP domain details.
New	Opens the SIP Domains page that you can use to create new SIP domains.
Duplicate	Creates a duplicate of the selected SIP domain and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the SIP domain.

Button	Description
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import SIP Domains**	Opens the Import SIP Domains page that allows you to import SIP domains from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export SIP Domains**	Opens the Export SIP Domains page that allows you to export the SIP domains data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export the NRP elements data as a zipped file to a specified location.
Commit	Distributes the selected SIP domain to all the Session Manager instances in the enterprise.

SIP Domains field descriptions

Use this page to create new SIP domains

Name	Description
Name	Name of the SIP domain.
Notes	Additional notes about the SIP domain.

Button	Description
Commit	Saves the SIP domain and distributes it to all the instances of the Session Manager.
Cancel	Cancels the SIP domain creation.

Import SIP Domains field descriptions

Use this page to import SIP domains from a file.

Name	Description
Please select a file:	Browse to the required file from which you wish to import the SIP domains. Selecting the file displays the file name and path in the **Import SIP Domains** page.

Button	Description
Import	Imports SIP domains from the specified file
Cancel	Cancels importing SIP domains from the specified file

Export SIP Domains field descriptions

Use this page to export SIP domains to a file.

Button	Description
Export	Exports the SIP domains data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

NRP Locations

About NRP Locations

You can use the NRP Locations screen to set up and configure gateway and user locations. Call processing uses locations to determine the location of the calling and the called gateways or users. The IP address of the device determines the current physical location of the caller or the called user. Session Manager matches the IP address against the patterns defined on location screens. If there is no match in the IP address patterns, Session Manager uses the SIP entity's location as the location.

Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations.

Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations. Locations are also used to limit the number of calls coming out of or going to a physical location. This is useful for those locations where the network bandwidth is limited. This is also known as Call Admission Control (CAC). You can enable CAC in Session Manager by specifying **Average bandwidth per call** and **Managed Bandwidth** on the**Locations** screen. If the Managed Bandwidth field has a non-blank value, Session Manager keeps track of the bandwidth in use based on the calls coming out of and going to that specific location and denies new calls when the bandwidth in use reaches the limit.

If the Managed Bandwidth field is blank for a location, no CAC is done for that location. Session Manager allows you to use the following wildcard characters to specify a location:

- * (star) is used to specify any number of allowed characters at the end of the string.
- X is used to specify a digit.

The Locations screen can contain one or several IP addresses. Each SIP entity has a particular IP address. Depending on the physical and geographic location of each SIP entity, some of the SIP Entities can be grouped into a single location. For example, if there are two Communication Managers located at Denver, they can form one location named Denver.

Creating NRP Locations

1. From the **Network Routing Policy** menu from the left side of the screen, select **Locations**. The Location Details screen is displayed.
2. Click **New**.
3. Enter the location name in the **Name** field.
4. Enter notes about the location, if required.
5. Specify the managed bandwidth for the location in the **Managed Bandwidth** field.
6. Specify the average bandwidth per call for the location in the **Average Bandwidth per Call** field.
7. Specify the time to live in the **Time to Live (secs)** field.
8. To add a location pattern, click **Add** under **Location Pattern**.
9. Enter an IP address pattern to match.
10. Enter notes about the location pattern, if required.
11. Continue clicking the **Location Pattern Add** button until all the required Location Pattern matching patterns have been configured.
12. Click **Cancel** or **Commit**.

Related topics:

Location Details field descriptions on page 334

Modifying NRP Locations

1. From the **Network Routing Policy** menu from the left side of the screen, select **Locations**.
2. If required, modify the managed bandwidth for the location in the **Managed Bandwidth** field.
3. If required, modify the average bandwidth per call for the location in the **Average Bandwidth per Call** field.
4. If required, modify the time to live in the **Time to Live (secs)** field.
5. To edit a location name or location matching pattern, select a check box for the required location and click **Edit** and make the required changes to the location or location pattern for that location.
6. To add or remove a location pattern, click **Add** or **Remove** under **Location Pattern**.
7. Click **Commit**.

Deleting NRP Locations

1. From the **Network Routing Policy** menu from the left side of the screen, select **Locations**.
2. To delete an existing NRP location or locations, select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

Related topics:

Delete Confirmation field descriptions on page 335

Locations field descriptions

Use this page to create, modify, delete, and manage locations.

Button	Description
Edit	Opens the Location Details page that you can use to modify the location details.
New	Opens the Location Details page that you can use to create new locations.
Duplicate	Creates a duplicate of the selected location and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the location.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import Locations**	Opens the Import Locations page that allows you to import locations from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export Locations**	Opens the Export Locations page that allows you to export the locations data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all the NRP elements as a zipped file to a specified location.
Commit	Distributes the selected location to all the Session Manager instances in the enterprise.

Location Details field descriptions

Use this page to set up and configure locations.

Name	Description
Name	Name of the location.
Notes	Notes about the location.
Managed Bandwidth	Managed bandwidth for the location.
Average Bandwidth per call	Average bandwidth per call for the location.
Time to Live (sec)	Time to Live for accessing the location.
Location Pattern	The IP address pattern that should be matched for the location. For example, • 135.12x.121.* • 13x.1xx.*

Name	Description
	• 135.* • 135.12x.121.123

Button	Description
Add	Adds an IP address pattern to match for the location.
Remove	Removes the IP address pattern to match for the location.

Related topics:

Creating NRP Locations on page 332

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of NRP locations.

Button	Description
Delete	Deletes the selected location.
Cancel	Cancels the deletion of the location.

Related topics:

Deleting NRP Locations on page 333

Denied Location field descriptions

Use this page to specify denied locations for the selected dial pattern

Button	Description
Select	Selects the location as a denied location for the dial pattern.
Cancel	Cancels the selection of the denied location.

Import Locations field descriptions

Use this page to import locations from a file.

Name	Description
Please select a file:	Browse to the required file from which you wish to import the NRP locations. Selecting the file displays the file name and path in the **Import Locations** page.

Button	Description
Import	Imports locations from the specified file
Cancel	Cancels importing the locations from the specified file

Export Locations field descriptions

Use this page to export NRP locations to a file.

Button	Description
Export	Exports the locations data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

NRP adaptations

About NRP Adaptations

You can optionally use Adaptations to modify SIP messages that are leaving a Session Manager instance (egress adaptation) and that are entering a Session Manager instance (ingress adaptation). This adaptation function is needed to convert strings containing calling and called party numbers from the local dialplan of a SIP entity to the dialplan administered on the Session Manager, and vice-versa. Adaptation is also needed when other SIP Entities require special SIP protocol conventions. Each administered SIP Entity may have its own unique adaptation, or one adaptation can be shared among multiple entities.

Adaptations are implemented as software modules that can be created and deployed to fit the needs of the system.

Session Manager includes a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as hostnames in the Request-URI and other headers. It also contains adaptation modules which do protocol conversions, such as for AT&T, Verizon, Cisco, and Nortel systems, as well as the digit conversion. All of these adapters allow for modification of URIs specified using unique name-value pairs for egress adaptation. For example, these can be used to replace the host name in the Request-URI with an administered host name during egress adaptation. Details are explained in the Creating NRP Adaptations

section. An adaptation administered using NRP specifies the module to use as well as the digit conversion that is to be performed on headers in the SIP messages. Different digit conversions can be specified for ingress and egress adaptation.

Additionally, digit conversion can be specified to modify only “origination” type headers, only “destination” type headers, or both. The origination/source type URIs are:

- P-Asserted-Identity
- History-Info (calling portion)
- Contact (in 3xx response)

The destination type URIs are:

- Request-URI
- Message Account (in NOTIFY/message-summary body)
- Refer-To (in REFER message)

Adaptation example

In the following example, an adaptation for AT&T service provider is needed at least for international calls.

For incoming calls, AT&T sends the 10 digit local number. To convert this into E.164, Session Manager must add a plus sign. Specify the following values:

- Matching pattern: 1
- Min: 10
- Max: 10
- Delete Digits: 0
- Insert Digits: +
- Address to modify: both

For outgoing calls to AT&T, Session Manager must convert the E.164 form to a format that AT&T supports, either 1+10 digits for North America calls, or 011+country code + number for international calls. For example, for calls to North America, specify the following values:

- Matching Pattern: +1
- Min: 12
- Max: 12
- Delete Digits: 1
- Insert Digits: <None>
- Notes: Calls to North America

For calls to Germany, specify the following values:

- Matching Pattern: +49
- Min: 13
- Max: 13
- Delete Digits: 1
- Insert Digits: 011
- Address to modify: destination
- Notes: Calls to Germany

Adaptation Module administration

The following is information regarding the **Adaptation Module** field on the Adaptation Details screen. The format of the **Adaptation Module** field is:

```
<Name of adaptation module> <name1=value1> <name2=value2>,...
```

There are currently 4 names defined which can be administered using either the full name or shortcut name:

EGRESS Domain Modification Parameters

- `overrideDestinationDomain (`or abbreviated name `odstd)`: {parameter #1 if not named}, replaces the domain in Request-URI and Notify/message-summary body with the given value for egress only.
- `overrideSourceDomain (`or abbreviated name `osrcd)`: replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only.

INGRESS Domain Modification Parameters:

- `ingressOverrideDestinationDomain (`or abbreviated name i`odstd)`: replaces the domain in Request-URI and Notify/message-summary body with the given value for ingress only.
- `ingressOverrideSourceDomain (` or abbreviated name i`osrcd)`: replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.

Example:

```
CiscoAdapter osrcd=dr.avaya.com odstd=ny.avaya.com
```

The same value in verbose form:

```
CiscoAdapter
overrideSourceDomain=dr.avaya.comoverridenDestinationDomain=ny.avaya.com
```

Creating NRP Adaptations

1. From the **NRP** navigation menu to the left side of the screen, select **Adaptations**. The Adaptations screen is displayed.
2. Click **New**. The Adaptation Details screen is displayed.
3. Enter the Name, Adaptation Module and any other required fields in the first section.
   a. Enter a descriptive name for the adaptation.
   b. Specify an adaptation module. This module is the adaptation module to use and host name adaptations to perform.
   c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.

      URI parameters can be added to the Request-URI. For example, the parameter “user=phone” can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field.

      The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. Entry “;user=phone;custApp=1” is equivalent to “user=phone;custApp=1”.
   d. Enter description about the adaptation module in the Notes field.
4. Click **Add** under Digit Conversion for Incoming Calls if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
5. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
6. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1 or more. The maximum value can be 36.
7. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
8. Enter the digits that you want inserted before the number in the **Insert Digits** field.
9. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. Entries

that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.

10. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
11. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
13. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
14. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

    The minimum value can be 1 or more. The maximum value can be 36.
15. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
16. Enter the digits that you want inserted before the number in the **Insert Digits** field.
17. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.
18. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
19. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
20. Click **Cancel** or **Commit**.

Related topics:

Adaptation Details field descriptions on page 344

Modifying NRP Adaptations

1. From the **NRP** navigation menu to the left side of the screen, select **Adaptations**. The Adaptation screen is displayed.
2. Select the adaptation for modification and click **Edit**

   All adaptation modules have the ability to replace domain (also known as host name) portion of the URI with a specified value for source and destination type URIs

on outgoing calls (egress) and to append parameters to the Request URI on for outgoing calls (egress). This adaptation functionality is expandable to adapt additional deployments needing further flexibility.

3. Edit the Name, Adaptation Module and any other required fields in the first section. Currently there is only one adaptation module named “DigitConversionAdapter”.
    - Enter a descriptive name for the adaptation.
    - Specify an adaptation module. This module is the adaptation module to use and host name adaptations to perform.
    - Enter a list of URI parameters to append to the Request-URI on egress in the Egress URI Parameters field.
4. Click **Add** under **Digit Conversion for Incoming Calls** if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
5. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
6. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1 or more. The maximum value can be any number up to 36.
7. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
8. Enter the digits that you want inserted before the number in the **Insert Digits** field.
9. From the drop-down list, select the value for Address to modify. A setting of both will look for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.
10. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
11. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
13. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
14. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

The minimum value can be 1 or more. The maximum value can be any number up to 36. The minimum value must be less than or equal to the maximum value.

15. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
16. Enter the digits that you want inserted before the number in the **Insert Digits** field.
17. From the drop down list, select the value for Address to modify. A setting of both will look for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.
18. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
19. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
20. Click **Commit**.

Deleting NRP Adaptations

1. From the **Network Routing Policy** menu from the left side of the screen, select **Adaptations**.
2. To delete an existing Adaptation or Adaptations, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.

Related topics:

Delete Confirmation field descriptions on page 347

Installed vendor adapters

Cisco Adapter (CiscoAdapter)

The Cisco Adapter provides two basic header manipulations: converting between Diversion and History-Info headers and converting between P-Asserted-Id and Remote-Party-Id headers. The Diversion and Remote-Party-Id headers have not been accepted by the IETF. They are replaced by History-Info and P-Asserted-Identity respectively, but are still used in the Cisco products. The Cisco Adapter also performs all the conversions available by the Digit Conversion Adapter.

Case 1:

Cisco requires the use of the Diversion header, rather than the History-Info header to provide information related to how and why the call arrives to a specific application or user. The following examples illustrate the adaptations.

Example 1:

Communication Manager user 66600001 forwards to Cisco user 60025.

Communication Manager's outgoing INVITE has this history-info:

```
History-Info: "<sip:66600001@ny.avaya.com>;index=1

History-Info: "stn 66600001"

<sip:66600001@ny.avaya.com?Reason=SIP%3Bcause%3D302%3Btext%3D%22Moved
%20Temporarily%22&Reason=Redirection%3Bcause%3DCFI>;index=1.1

History-Info: <sip:600025@ny.avaya.com>;index=1.2
```

In the message sent to Cisco this is converted to:

```
Diversion: "stn 66600001" <sip:66600001@ny.avaya.com>;reason=no-

answer;privacy=off;screen=no
```

Example 2:

Communication Manager user calls Cisco user 60025. The call is routed to Message Manager at extension 688810.

The INVITE message from the Cisco server contains the Diversion Header:

```
Diversion: "Ken's Desk" <sip:600025@ny.avaya.com>;reason=user-

busy;privacy=off;screen=no
```

The message is adapted and the outgoing INVITE to MM replaces the Diversion header with the following:

```
History-Info: <sip:600025@ny.avaya.com>;index=1

History-Info: "Ken's Desk"

<sip:600025@ny.avaya.com?Reason=SIP%3Bcause%3D486%3Btext%3D%22Bus

y%20Here%22&Reason=Redirection%3Bcause%3DNORMAL%3Bavaya-cm-reason%3D
%22cover-busy%22%3Bavaya-cm-vm-address-digits%3D81080000%3Bavaya-cm-vm-
address-handle%3Dsip:80000%40avaya.com>;index=1.1

History-Info: "MM" <sip:688810@ny.avaya.com>;index=1.2
```

Case 2:

Cisco requires information in the P-Asserted-Identity (PAI) header to be received in the Remote-Party-Id (RPI) header. Any incoming message containing a P-Asserted-Identity header being routed to Cisco will replace that header with the Remote-Party-Id header.

Similarly, calls from Cisco containing the Remote-Party-Id header will be converted to a P-Asserted-Identity header when routed to non-Cisco entities.

Example 3:

A call is placed from 12345 at Communication Manager and routed to the Cisco PBX.

The INVITE from Communication Manager contains:

```
P-Asserted-Identity: "Ryan" <sip:12345@avaya.com>
```

This header is converted to RPI when the request is sent to the Cisco PBX:

```
Remote-Party-Id: "Ryan"
<sip:12345@avaya.com>;party=called;screen=no;privacy=off
```

Example 4:

A call is placed from 23456 at Cisco PBX and routed to Communication Manager.

The INVITE from Cisco PBX contains:

```
Remote-Party-Id: "Ryan"
<sip:23456@avaya.com>;party=called;screen=no;privacy=off
```

This header is converted to PAI when the request is sent to Communication Manager:

```
P-Asserted-Identity: "Ryan" <sip:23456@avaya.com>
```

Verizon Adapter (VerizonAdapter)

The Verizon adapter requires the same History-Info to Diversion adaptations that the Cisco Adapter uses. The Verizon Adapter also performs all the conversions available by the Digit Conversion Adapter.

AT&T Adapter (AttAdapter)

AT&T does not handle the History-Info header. The adaptation module removes, on egress to AT&T, any History-Info headers in a request or response. Messages from AT&T do not change. The AT&T Adapter also performs all the conversions available by the Digit Conversion Adapter.

Adaptation Details field descriptions

Use this page to specify the adaptation details.

General section

Name	Description
Name	Name of the adaptation. Must be unique and be between 3 and 64 characters in length.
Adaptation module	Name of the adaptation module that provides the signalling interface

Name	Description
Egress URI Parameters	The terminating trunk group parameters
Notes	Other details that you wish to add.

Digit Conversion for Incoming Calls section

Name	Description
Select check box	Use this check box to select and use the digit conversion for the incoming calls
Matching Pattern	Pattern to match for the incoming calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched
Max	Maximum number of digits to be matched
Delete Digits	Number of digits to be deleted from the dialled number
Insert Digits	Number of digits to be added before the dialled number
Address to Modify	Selecting both looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both.
Notes	Any other details that you wish to add

Digit Conversion for Outgoing Calls section

Name	Description
Select check box	Use this check box to select and use the digit conversion for the outgoing calls
Matching Pattern	Pattern to match for the outgoing calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched
Max	Maximum number of digits to be matched
Delete Digits	Number of digits to be deleted from the dialled number
Insert Digits	Number of digits to be added before the dialled number
Address to Modify	Selecting both looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both.
Notes	Any other details that you wish to add

Button	Description
Add	Adds digit conversion for incoming or outgoing calls for the adaptations
Remove	Removes digit conversion from incoming or outgoing calls for the adaptations
Commit	Saves the adaptation details and distributes them to the Session Manager instances in the enterprise
Cancel	Cancels changes to the adaptation details and returns to the Adaptations page

Related topics:

Creating NRP Adaptations on page 339

Adaptations field descriptions

Use this page to create, modify, delete, and manage adaptations.

Button	Description
Edit	Opens the Adaptation Details page that you can use to modify the adaptation details.
New	Opens the Adaptation Details page that you can use to create new adaptations.
Duplicate	Creates a duplicate of the selected adaptation and assigns a new state to it
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the adaptation.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import Adaptations**	Opens the Import Adaptations page that allows you to import adaptations from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export Adaptations**	Opens the Export Adaptations page that allows you to export adaptations as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export all the NRP elements data as a zipped XML file to a specified location.
Commit	Distributes the selected adaptation to all the Session Manager instances in the enterprise.

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected adaptations

Button	Description
Delete	Deletes entries for the selected adaptations from the database
Cancel	Cancels the deletion of the selected adaptations

Related topics:

Deleting NRP Adaptations on page 342

Export Adaptations field descriptions

Use this page to export adaptations to a file.

Button	Description
Export	Saves the adaptations data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file and returns to Adaptations page.

Import Adaptations field descriptions

Use this page to import NRP adaptations from a file.

Name	Description
Please select a file:	Browse to the required file location from which you wish to import the adaptations. Selecting the file displays the file name and location in the **Import Adaptations** page.

Button	Description
Import	Imports adaptations data from the specified file.
Cancel	Cancels importing the data from the specified file.

SIP entities

About SIP Entities

SIP Entities are all the network elements that are a part of the SIP System. SIP Entities include Session Manager instances, Communication Managers, Session Border Controllers (SBCs), SIP trunks, and so on.

Authentication of trusted SIP entities

Network Routing Policy (NRP) uses the following information for the authentication of SIP entities by performing validation on IP/Transport Layer and TLS Layer:

- FQDN or IP Address of the SIP entity
- Credential name of the SIP entity
- Protocol of the Entity Links. This is a SIP connection transport type (TCP/TLS/UDP)
- Trust State of the Entity Link (This defines whether the entity link is Trusted or not)

For information about administering these fields, refer to Creating NRP SIP entities.

IP and transport layer validation

When a SIP entity connects to Session Manager over a TCP or TLS port, Session Manager validates that:

- The IP address matches one of the SIP Entities configured in NRP that have trusted entity links with the Session Manager. If the SIP entities are configured as FQDN, Session Manager performs a DNS resolution before doing the verification.
- Transport for the incoming SIP connection matches with one of the entity links associated with this SIP entity and the Session Manager. Also, the Trust State of the entity link must be configured as trusted. Session Manager does not accept connections matching untrusted entity links.

For SIP packets over UDP, above validation is performed for each packet. For SIP TLS connections, further validation is performed as described in the next section.

TLS layer validation

Session Manager applies the following additional validations for SIP TLS connections:

1. During a TLS handshake, mutual TLS authentication is performed, that is, Identity certificate of the SIP entity is validated against the trusted CA certificate repository in the Session Manager for SIP TLS. If this verification fails, Session Manager does not accept the connection.
2. If the mutual TLS authentication is successful, further validation is performed on the SIP entity Identity Certificate as per the Credential Name or the far-end IP address.
    - If the Credential Name string is empty, the connection is accepted.
    - If the Credential Name string is not empty, the Credential Name and the IP address of the far-end is searched for in the following fields in the identity certificate provided by the SIP entity:
        - CN value from the subject
        - subjectAltName.dNSName
        - subjectAltName.uniformResourceIdentifier (For IP address comparison, IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Also, case insensitive search is performed in this case)

With entity links from both Session Manager instances, checking the **Override Port & Transport with DNS SRV** check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.

- If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
- If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.

Creating NRP SIP Entities

Use the NRP SIP Entities screen to create SIP Entities. To administer minimal routing via Session Manager, you need to configure a SIP Entity of type Communication Manager and a second SIP Entity of type Session Manager.

1. Select **SIP Entities** under the NRP navigation menu to the left of the screen.
2. Click **New**.
3. Enter the Name, FQDN (fully Qualified Domain Name) or IP address of the SIP Entity, Type (Session Manager, SBC, CM, VoicePortal, Gateway, SIP Trunk, or Other) and any other required fields in the first section.

4. If you need to specify an Adaptation Module for the SIP Entity, click the drop-down selector for the **Adaptation** field.
5. If you need to specify the Location for the SIP Entity, click the drop-down selector for the **Location** field.
6. If the SIP Entity Type is “Session Manager” and you need to specify an Outbound Proxy for the SIP Entity, click the drop-down selector for the **Outbound Proxy** field.
7. Select the correct time zone from the **Time Zone** drop-down list.
8. Enter a value in seconds in the **SIP Timer B/F (secs)** field.
   This value must be between 1 and 32 seconds, and the default is 4. This is the time Session Manager should await a response from a SIP entity before trying an alternate route.
9. Enter a regular expression string in the **Credential name** field. Credential name is used for TLS connection validation by searching for this string in the SIP Entity identity certificate.
   - If you do not want to perform the additional validation on SIP Entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
   - If you want to verify that a specific string or SIP Entity FQDN is present within the SIP Entity identity certificate, enter that string or SIP Entity FQDN using the regular expression syntax.
   - If you want to verify that the SIP entity IP address is present within the SIP Entity identity certificate, enter the SIP Entity IP address using the regular expression syntax. Please note that IP Address is searched by default when any string is configured in the Credential Name.

   Note:

   The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some examples:

   For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”.

   For “192.14.11.22”, use string “192\.14\.11\.22”. You can look for a subset of the string or can create a wild card search. For example, to look for “domain.com” as a substring, use the string “domain\.com”
10. Under Monitoring, from the **Monitoring on/off** field, select **Use Session Manager Configuration** to indicate that the monitoring settings from the Session Manager Administration screen should be used, **Enable Monitoring** or **Disable Monitoring** to indicate if the entity should be monitored or not.
    a. Use Session Manager Configuration – Use the settings under **Session Manager > Session Manager Administration**
    b. Link Monitoring Enabled – Enables link monitoring on this SIP entity.
    c. Link Monitoring Disabled – Link monitoring will be turn off for this SIP entity.

11. If you need to specify the Port parameters, click **Add** under Port. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
12. Enter the necessary Port and Protocol parameters.
13. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
14. Click **Cancel** or **Commit**.

Related topics:

SIP Entity Details field descriptions on page 353

Modifying SIP entities

1. Select **SIP Entities** under the NRP navigation menu to the left of the screen.
2. Select the SIP entity for modification and click **Edit** .
3. Modify the Name, FQDN (fully Qualified Domain Name) or IP address of the SIP Entity, Type (Session Manager, SBC, CM, VoicePortal, Gateway, SIP Trunk, or Other) and any other required fields in the first section.
4. If you need to specify an Adaptation Module for the SIP Entity, click the drop-down selector for the **Adaptation** field.
5. If you need to specify the Location for the SIP Entity, click the drop-down selector for the **Location** field.
6. If the SIP Entity Type is “Session Manager” and you need to specify an Outbound Proxy for the SIP Entity, click the drop-down selector for the **Outbound Proxy** field.
7. Select the correct time zone from the **Time Zone** drop-down list.
8. Enter or modify a value in seconds in the **SIP Timer B/F (secs)** field. This value must be between 1 and 32 seconds. The default is 4. This is the time Session Manager should await a response from a SIP entity before trying an alternate route.
9. Enter or modify a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
    - If you do not want to perform the additional validation on SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.

- If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
- If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. Please note that the system looks for the IP Address by default when any string is configured in the Credential Name.

Note:

The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some of the examples:

- For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain \.com”.
- For “192.14.11.22”, use string “192\.14\.11\.22”.
- You can search a subset of the string or can create a wild card search. For example, for searching for “domain.com” as a substring, use the string “*domain\.com*”

10. Under SIP Link Monitoring, the following options are available from the drop-down menu:
    a. **Use Session Manager Configuration**
    b. **Link Monitoring Enabled** – Enables link monitoring on this SIP entity.
    c. **Link Monitoring Disabled** – Link monitoring will be turn off for this SIP entity.
11. If you need to specify the Port parameters, click **Add** under Port. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
12. Enter the necessary Port and Protocol parameters.
13. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
14. Click **Cancel** or **Commit**.

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the SIP entity.

Button	Description
Delete	Deletes the selected SIP entity or entities.

Button	Description
Cancel	Cancels the deletion of the selected SIP entity or entities.

SIP Entities field descriptions

Use this page to create, modify, delete, and manage SIP entities.

Button	Description
Edit	Opens the SIP Entity Details page that you can use to modify the SIP entity.
New	Opens the SIP Entity Details page that you can use to create new SIP entities.
Duplicate	Creates a duplicate of the selected SIP entity and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the SIP entity.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Display SIP Entity References**	Opens the Overview of References to SIP Entities page which displays the routing policies, adaptations, and locations that correspond to the SIP entity.
More Actions > **Import SIP Entities**	Opens the Import SIP Entities page that allows you to import SIP entities from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export SIP Entities**	Opens the Export SIP Entities page that allows you to export the SIP entity data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all NRP elements as a zipped file to a specified location.
Commit	Distributes the selected SIP entity to all the Session Manager instances in the enterprise.

SIP Entity Details field descriptions

Use this page to specify SIP entity details.

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP entity.
Type	SIP entity type, such as a Session Manager, Communication Manager, SIP trunk, or a gateway.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (secs)	Amount of time the Session Manager should wait for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP Entity identity certificate.
Monitoring On/Off	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (secs)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (secs)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Button	Description
Add	Adds the selected entity.
Remove	Removes the selected entity.
Commit	Saves the SIP entity and distributes it to the Session Managers in the enterprise.
Cancel	Cancels the creation or modification of the SIP entity.

Related topics:

Creating NRP SIP Entities on page 349

SIP Entity List field descriptions

Use this page to select and associate SIP entities to a routing policy.

Name	Description
Name	Select a SIP entity name check box from the list to associate it to the selected routing policy.
FQDN or IP Address	Displays the fully qualified domain name or IP address of the SIP entity.
Type	Displays the type of the SIP entity such as Session Manager, SBC, CM, VoicePortal, Gateway, SIP Trunk, or Other.
Notes	Additional notes.

Button	Description
Select	Confirm selection of the SIP entity for associating to the routing policy.
Cancel	Cancel the selection of the SIP entity.

Export SIP Entities field descriptions

Use this page to export SIP entities to a file.

Button	Description
Export	Exports the SIP entity data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

Import SIP Entities field descriptions

Use this page to import SIP entities from a file.

Name	Description
Please select a file:	Browse to the required file from which you wish to import the SIP entities. Selecting the file displays the file name and path in the **Import SIP Entities** page.

Button	Description
Import	Imports SIP entities from the specified file
Cancel	Cancels importing the SIP entities from the specified file

SIP entity references

About SIP Entity References

Session Manager enables you to see all references to a SIP entity such as its location, the routing policy that is created for the SIP entity, and adaptations, if any. If a single SIP entity has more than one combination of these references, Session Manager displays each of the combinations on a separate row.

Displaying SIP Entity References

1. Select **SIP Entities** under the NRP navigation menu to the left of the screen.
2. From the SIP Entities menu, select the check box for a SIP entity whose references you want to see.
3. From the **More Actions** drop-down list, select **Display SIP Entity References**.
   Session Manager displays the overview of SIP entity references such as the entity location, name of the routing policy attached to the entity, and adaptations, if any.
4. Click **Back** to navigate to the SIP entities.

Related topics:

Overview of References to SIP Entities field descriptions on page 357

Overview of References to SIP Entities field descriptions

Use this page to view information about the SIP entity references associated with the selected SIP entity

Name	Description
SIP Entity Name	Lists the names of the SIP entities
Location Name	Lists the location associated with the specified SIP entity
Routing Policy Name	Lists the routing policy associated with the specified SIP entity
Adaptation Name	Lists the name of the adaptation associated with the SIP entity

Button	Description
Back	Returns to the **SIP Entities** page

Related topics:

Displaying SIP Entity References on page 356

Deleting SIP Entities

1. From the Network Routing Policy menu from the left side of the screen, select **SIP Entities**.
2. To delete an existing SIP entity or entities, select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

NRP entity links

About NRP Entity Links

Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive messages from that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link

to these SIP entities in the network. Session Manager does not need to know the port and NRP entity links Installing and Administering Session Manager June 2009 75 transport protocol if the **Override Port & Transport** box is checked on the SIP entity. Port and transport must be administered even if the **Override Port & Transport** is checked on the SIP entity, although their values will not be used.

NRP entity links connect two SIP entities through the Session Manager. They enable you to define the network topology for SIP routing.

- Entity Links are configured to connect two SIP Entities.
- Trusted Hosts are indicated by assigning the*Trust State* to the link that connects the entities.

Creating NRP Entity Links

Use the Entity Links screen for this task. The general configuration of connections between SIP entities enables NRP and Session Manager to identify specific connection configurations (for example, Trusted Hosts, outbound proxy, and so on) between SIP Entities.

1. Select **Entity Links** under the NRP navigation menu.
2. Click **New**.
3. Enter the name in the **Name** field.
4. Enter the SIP Entity 1 by selecting the required **Session Manager** SIP Entity from the drop-down list and provide the required port. SIP Entity 1 must always be an Session Manager instance.

   The port is the port on the Session Manager to which the remote entity needs to send requests to. Default ports in SIP are 5060 for TCP and UDP and 5061 for TLS. You can specify a port other than these default ports.
5. Enter the SIP Entity 2 by selecting the require non-Session Manager SIP Entity from the drop-down list and provide the required port.

   The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
6. If the SIP entity is trusted, select the **Trusted** check box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7. Select the protocol you require for the link using the **Protocol** drop-down list.
8. Click **Cancel** or **Commit**.

Modifying NRP entity links

1. From the navigation pane on the System Manager Common Console, click **Network Routing Policy** > **Entity Links**
2. Select an entity link for modification and click **Edit**.
3. Modify the name in the **Name** field if required.
4. If required, modify the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port.

   SIP entity 1 must always be a Session Manager instance.
5. If required, modify the SIP entity 2 by selecting the required SIP entity from the drop-down list and provide the required port.
6. If you want to indicate that the link is a trusted link, select the **Trusted** check box.
7. Select the transport protocol you require for the link using the **Protocol** drop-down list.
8. Click **Commit**.

Deleting NRP Entity Links

1. From the **Network Routing Policy** menu from the left side of the screen, select **Entity Links**.
2. To delete an existing link or links, select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of SIP entity links.

Button	Description
Delete	Deletes the SIP entity link entries from the database.

Button	Description
Cancel	Cancels the deletion of SIP entity links and returns to the SIP Entity Links page.

Entity Links field descriptions

Use this page to create, modify, delete, and manage entity links.

Button	Description
Edit	Opens the Entity Links page that you can use to modify the entity link details.
New	Opens the Entity Links page that you can use to create new entity links.
Duplicate	Creates a duplicate of the selected entity link and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the entity link.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import Entity Links**	Opens the Import Entity Links page that allows you to import entity links from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export Entity Links**	Opens the Export Entity Links page that allows you to export the entity links data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export the data for all NRP elements as a zipped file to a specified location.
Commit	Distributes the selected entity links to all the Session Manager instances in the enterprise.

Name	Description
Name	Name of the SIP entity link. This name must be unique and can have 3 to 64 characters.
SIP Entity 1	Select a SIP entity from the drop-down list. This entity must always be a Session Manager instance.
Port	Port to be used for SIP entity 1.
SIP Entity 2	Select a SIP entity from the drop-down list. This entity need not be a Session Manager entity.
Port	Port to be used for SIP entity 2.

Name	Description
Trusted	Specifies that the link between the two SIP entities is trusted.
Protocol	Protocol to be used for the entity link.
Notes	Any details or notes that you wish to add.

Export Entity Links field descriptions

Use this page to export entity links to a file.

Button	Description
Export	Exports the entity links data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

Import Entity Links field descriptions

Use this page to import entity links from a file.

Name	Description
Please select a file:	Browse to the required file location from which you wish to import the entity links. Selecting the file displays the file name and location in the **Import Entity Links** page.

Button	Description
Import	Imports entity links from the specified file.
Cancel	Cancels importing entity links from the specified file.

NRP time ranges

About the NRP Time Ranges

Time ranges indicate when a particular rank or cost of a routing policy is to be used when determining the least-cost route. They do not indicate when routing policies are available to be considered for routing.

You must specify as many time ranges as necessary to cover all hours and days in a week for each administered routing policy.

For example, routing policy A can be in effect on all weekdays from 9:00 a.m. to 5:59 p.m., routing policy B can be in effect on all weekdays from 6:00 pm. to 9 a.m., and routing policy C NRP time ranges can be in effect on weekends. These three time ranges together cover how calls should be routed throughout the week.

Creating NRP Time Ranges

You can use the NRP Time Ranges screen to administer time ranges with start and end times.

1. Select **Time Ranges** from the NRP navigation menu. The Time Ranges screen is displayed.
2. Click **New**.
3. Enter the name, select the required days by entering the start and end times and notes for the new time range. Start times start with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
4. Click **Cancel** or **Commit**.

Related topics:

Time Range List field descriptions on page 363

Modifying NRP Time Ranges

1. Select **Time Ranges** from the NRP navigation menu. The Time Ranges screen is displayed.
2. Select a time range for modification and click **Edit**.
3. If required, modify the name.
4. If required, modify the days by modifying the start and end times and notes. Start times start with the first second of the start hour:minute. End Times go through the last second of the end hour:minute.
5. Click **Commit**.

Deleting NRP Time Ranges

1. From the **Network Routing Policy** menu from the left side of the screen, select **Time Ranges**.
2. To delete an existing time range or ranges, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.

Related topics:

Delete Confirmation field descriptions on page 364

Time Range List field descriptions

Use this page to view time ranges associated to a routing policy.

Name	Description
Name	Name of the time range. This name must be unique and can have between 3 and 64 characters. Select the check box to use the time range for a routing policy.
Mon	Selected check box indicates that the time range is used for Mondays. Similarly, other days of the week for which the time range to be used are selected.
Start Time	Start time for the time range. For a 24–hour time range, the start time is 0.00.
End Time	End time for the time range. For a 24–hour time range, the end time is 23:59.
Notes	Additional notes about the time range.

Button	Description
Select	Associates the selected time range to the routing policy.
Cancel	Cancels the selection of the time range.

Related topics:

Creating NRP Time Ranges on page 362

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of time ranges.

Button	Description
Delete	Deletes the selected time ranges from the database.
Cancel	Cancels the deletion of the selected time ranges.

Related topics:

Deleting NRP Time Ranges on page 363

Time Ranges field descriptions

Use this page to create, modify, delete, and manage time ranges.

Field	Description
Name	Enter a name for the time range. It can have between three and 64 characters. The name cannot contain the following characters: <, >, ^, %, $, @, #, *
Days (Mo to Su)	Select the days of the week for which the time range should be used.
Start Time	Start time for the time range. Use 24–hour time format.
End Time	End time for the time range. Use 24–hour time format.
Notes	Additional notes.

Button	Description
Edit	Opens the Time Ranges page that you can use to modify the time range details.
New	Opens the Time Ranges page that you can use to create new time ranges.
Duplicate	Creates a duplicate of the selected time range and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the time range.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import Time Ranges**	Opens the Import Time Ranges page that allows you to import time ranges from a file that you can specify by browsing.

Button	Description
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export Time Ranges**	Opens the Export Time Ranges page that allows you to export the time ranges data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all the NRP elements as a zipped file to a specified location.
Commit	Distributes the selected time range to all the Session Manager instances in the enterprise.

Import Time Ranges field descriptions

Use this page to import time ranges from a file.

Name	Description
Please select a file:	Browse to the required file from which you wish to import the NRP time ranges. Selecting the file displays the file name and path in the **Import Time Ranges** page.

Button	Description
Import	Imports time ranges from the specified file.
Cancel	Cancels importing time ranges from the specified file.

Export Time Ranges field descriptions

Use this page to export time ranges to a file.

Button	Description
Export	Exports the NRP time ranges data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

NRP routing policies

About NRP Routing Policies

Use the Routing Policies page to create and modify routing policies.

All “Routing Policies” together form the “enterprise wide dial plan”.

Routing Policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “SIP domain” of the called party and the actual time the call occurs.

Optionally, instead of “dialed digits” of the called party and the “SIP domain” of the called party a “regular expression” can be defined.

Depending on one or multiple of the inputs mentioned above a destination where the call should be routed is determined.

Optionally, the destination can be qualified by “deny” which means that the call will not be routed.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Creating NRP Routing Policies

1. Select **Routing Policies** from the NRP navigation menu. The Routing Policies screen is displayed.
2. Click **New**.
3. Enter a policy name and notes in the relevant fields in the General section. Note that the routing policy can be disabled by selecting the **Disabled** check box.
4. Click **Select** under the SIP Entity as Destination section. This is where you can select the destination SIP Entity for this routing policy.
5. Select the required destination and click **Select**.
6. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the Time of Day section.
7. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.

If there are gaps in the Time of Day coverage that you select, Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed

8. Enter the relative Rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.
9. Under Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.

   This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
10. Under Dial Patterns or Regular Expressions, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**. This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
11. Click **Cancel** or **Commit**.

Related topics:

Routing Policy Details field descriptions on page 370

Modifying NRP Routing Policies

1. Select **Routing Policies** from the NRP navigation menu. The Routing Policies screen is displayed.
2. Select a routing policy for modification and click **Edit**.
3. If required, modify the policy name and notes in the relevant fields in the General section. Note that the routing policy can be disabled by selecting the **Disabled** check box.
4. Click **Select** under the SIP Entity as Destination section. This is where you can select the destination SIP Entity for this routing policy.
5. If required, select or modify the required destination and click **Select**.
6. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the Time of Day section.
7. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.

8. Enter the relative rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.
9. If you need to dissociate the Time of Day routing parameters from this Routing Policy, click **Remove** from the Time of Day section.
10. Under Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.

    If you have not specified the dial patterns or regular expressions yet, you can add the routing policy to the dial pattern or regular expression when you add them later.
11. Under Dial Patterns or Regular Expressions, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.
12. Click **Commit**.

Deleting NRP Routing Policies

1. From the Network Routing Policy menu from the left side of the screen, select **Routing Policies**.
2. To delete an existing routing policy or policies, select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

Note:

If you delete a routing policy, all dial patterns and regular expressions that are linked only to this routing policy are also deleted.

Related topics:

Delete Confirmation field descriptions on page 368

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the routing policy.

Button	Description
Delete	Deletes the selected routing policy as well as any dial patterns and regular expressions that are associated *only* with this routing policy.
Cancel	Cancels the deletion of the routing policy.

Related topics:

Deleting NRP Routing Policies on page 368

Routing Policies field descriptions

Use this page to create, modify, delete, and manage routing policies.

Button	Description
Edit	Opens the Routing Policy Details page that you can use to modify the routing policy.
New	Opens the Routing Policy Details page that you can use to create a new routing policy.
Duplicate	Creates a duplicate of the selected routing policy and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the routing policy.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import Routing Policies**	Opens the Import Routing Policies page that allows you to import a routing policy from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export Routing Policies**	Opens the Export Routing Policies page that allows you to export the routing policy data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all the NRP elements as a zipped file to a specified location.
Commit	Distributes the selected routing policy to all the Session Manager instances in the enterprise.

Routing Policy Details field descriptions

Use this page to specify the details for creating or modifying a routing policy.

General section

Name	Description
Name	Name of the routing policy.
Disabled	Selecting this check box specifies that the routing policy is to be disabled and should not be used.
Notes	Additional notes about the routing policy.

SIP Entity as Destination section

Button	Description
Select	Opens the SIP Entity List page. You can use this page to select a SIP entity as a destination and associate it to the selected routing policy.

Time of Day section

Button	Description
Add	Adds a new time of the day to the selected routing policy.
Remove	Removes the selected time of day entry from the selected routing policy.
View Gaps/ Overlaps	Selecting a time of day entry and selecting **View Gaps/Overlaps** generates a Duration Lists report and displays if there are any gaps or overlaps in the time of day entries for each day of the week.

Dial Patterns section

Button	Description
Add	Adds a new dial pattern to the selected routing policy.
Remove	Removes the selected dial pattern from the selected routing policy.

Regular Expressions section

Button	Description
Add	Adds a new regular expression to the selected routing policy.
Remove	Removes the selected regular expression from the selected routing policy.

Button	Description
Commit	Saves the routing policy changes and distributes those to the Session Manager instances in the enterprise.
Cancel	Cancels modifications to the routing policy.

Related topics:

Creating NRP Routing Policies on page 366

Routing Policy List field descriptions

Use this page to select a routing policy that the regular expression should be associated with.

Name	Description
Name	Name of the routing policy to be associated with the selected regular expression.
Disabled	Denotes that the associated routing policy is to be disabled for the selected regular expression.
Destination	Destination SIP entity for the routing policy.
Notes	Additional notes about the routing policy.

Button	Description
Select	Confirms the selection of the routing policy for associating it with the regular expression.
Cancel	Cancels the selection of the routing policy.

Import Routing Policies field descriptions

Use this page to import routing policies from a file.

Name	Description
Please select a file:	Browse to the required file from which you wish to import the routing policies. Selecting the file displays the file name and path in the **Import Routing Policies** page.

Button	Description
Import	Imports routing policies from the specified file
Cancel	Cancels importing routing policies from the specified file

Export Routing Policies field descriptions

Use this page to export routing policies to a file.

Button	Description
Export	Exports the routing policies data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

Dial patterns

About Dial Patterns

A dial pattern specifies which routing policy or policies are used to route a call based on the digits dialed by a user which match that pattern. Session Manager matches these dialed digits after you apply any administered ingress adaptation.

The originating location of the call and the domain in the request-URI also decide how the call gets routed.

Session Manager tries to match the request-URI of a request to a row in the dial pattern table. The rows considered for the match are all rows where:

- The domain in the dial pattern table matches the domain in the request-URI, and,
- The originating location in the dial pattern table row matches the originating location of the request, or, if there are no rows matching the originating location, the originating location in the table is set to -ALL-, or, if there was no originating location, the originating location in the table is -ALL-, and
- The digit pattern in the row matches the user-part of the request-URI, ignoring any parameters that are in the user part of the request-URI

If no rows match using the above criteria, Session Manager modifies the domain in the request URI to remove one level of subdomain. For example, if us.yourcompany.com was tried, then Session Manager tries yourcompany.com.

As another example, you have two Communication Manager instances. Each Communication Manager has a call number range including all direct inward dialing (DID) numbers. Any user on CM-1 has a dial pattern +1301501xxxx. Similarly, any user on CM-2 has a dial pattern +1301601xxxx. You would enter the 2 dial patterns as:

- CM-1: +1301501
- CM-2: +1301601

A call to +13015016789 would match the dial pattern for CM-1.

A call to +13016011234 would match the dial pattern for CM-2.

The pattern matching algorithm works as follows:

- Valid digits are 0-9
- Valid characters for the leading position are,+, *, and #. Any other characters are not matched.
- x (lowercase only) is a wildcard character that matches a character from the allowed characters above. White spaces are not allowed.
- Longer matches get a higher priority over shorter matches. For example, +1601555 has a higher priority as compared to +1601.
- For matches of equal length, exact matches have a higher priority over wildcard matches. For example, +1601555 has a higher priority as compared to +1xxx555.
- For both routing policies and adaptations, the pattern matching works in the same manner.

Creating Dial Patterns

The NRP Dial Patterns screen is used to create Dial Patterns and associate the Dial Patterns to a Routing Policy and Locations.

1. Select **Dial Pattern** under the NRP navigation menu. The Dial Patterns screen is displayed.
2. Click **New**. The Dial Pattern Details screen is displayed.
3. Enter the Dial Pattern General information in the General section. Note that a SIP Domain can be provided to restrict the Dial Pattern to the specified SIP Domain.
4. Click **Add** under the Originating Locations and Routing Policies section.
5. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
6. Click **Select** to indicate that you have completed your selections.
7. If you need to specify that calls from the specified locations will be denied, click **Add** under the Denied Locations section.
8. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
9. Click **Cancel** or **Commit**.

Note:

You cannot save a dial pattern unless you add at least a routing policy or a denied location.

Related topics:

Dial Pattern Details field descriptions on page 376

Modifying Dial Patterns

1. Select **Dial Pattern** under the NRP navigation menu. The Dial Patterns screen is displayed.
2. Select a dial pattern for modification and click **Edit**. The Dial Pattern Details screen is displayed.
3. Enter the Dial Pattern General information in the General section. Note that a SIP Domain can be provided to restrict the Dial Pattern to the specified SIP Domain.
4. Click **Add** under the Locations and Routing Policies sections one after the other.
5. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
6. Click **Select** to indicate that you have completed your selections.
7. Similarly, to remove locations, click **Remove**, select the locations to remove, and click **Select**.
8. If you need to specify that calls from the specified locations will be denied, click **Add** under the Denied Locations section.
9. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
10. Similarly, to remove locations from the denied list, click **Remove**, select the locations to remove, and click **Select**.
11. Click **Commit**.

Note:

You cannot save a dial pattern unless it has at least one routing policy or a denied location associated to it.

Deleting Dial Patterns

1. From the **Network Routing Policy** menu from the left side of the screen, select **Dial Patterns**.
2. To delete an existing dial pattern or patterns, select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

Note:
When you delete a Dial Pattern, it is also deleted from all the Routing Policies that it is associated to.

Related topics:
Dial Pattern Details field descriptions on page 376

Pattern List field descriptions

Use this page to view the dial pattern details for associating with the routing policy

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call.
SIP Domain	SIP domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.

Button	Description
Select	Associate the selected pattern to the routing policy.
Cancel	Cancel the association of the selected pattern to the routing policy.

Dial Pattern Details field descriptions

Use this page to specify the dial pattern details.

General section

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call.
SIP Domain	SIP domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.

Locations and Routing Policies section

Name	Description
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Location Name	Name of the location to be associated to the dial pattern.
Location Notes	Notes about the selected location.
Routing Policy Name	Name of the routing policy to be associated to the dial pattern.
Routing Policy Disabled	Name of the routing policy that should not be used for the dial pattern.
Routing Policy Destination	Destination of the routing policy.
Routing Policy Notes	Any other notes about the routing policy that you wish to add.

Denied Locations section

Name	Description
Select check box	Use this check box to select denied locations for the dial pattern match.

Button	Description
Add	Adds locations, routing policies, or denied locations for the dial patterns.
Remove	Removes locations, routing policies, or denied locations for the dial patterns.

Button	Description
Commit	Saves the dial pattern details and distributes them to the Session Manager instances in the enterprise.
Cancel	Cancels changes to the dial pattern details and returns to the Dial Patterns page.

Related topics:

Creating Dial Patterns on page 373
Deleting Dial Patterns on page 375

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected dial patterns.

Button	Description
Delete	Deletes entries for the selected dial patterns from the database.
Cancel	Cancels the deletion of the selected dial patterns.

Export Dial Patterns field descriptions

Use this page to export dial patterns to a file.

Button	Description
Export	Exports the dial patterns data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

Import Dial Patterns field descriptions

Use this page to import dial patterns from a file.

Name	Description
Please select a file:	Browse to the required file location from which you wish to import the dial patterns. Selecting the file displays the file name and location in the **Import Dial Patterns** page.

Button	Description
Import	Imports dial patterns from the specified file.

Button	Description
Cancel	Cancels importing dial patterns from the specified file.

Dial Patterns field descriptions

Use this page to create, modify, delete, and manage dial patterns.

Button	Description
Edit	Opens the Dial Pattern Details page that you can use to modify the dial pattern details.
New	Opens the Dial Pattern Details page that you can use to create new dial patterns.
Duplicate	Creates a duplicate of the selected dial pattern and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the dial pattern.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import Dial Patterns**	Opens the Import Dial Patterns page that allows you to import dial patterns from a file that you can specify by browsing.
More Actions > **Import Provider Specific Data**	Opens the Import Provider Specific Data page that allows you to import provider—specific data from a file that you can specify by browsing.
More Actions > **Import all data**	Opens the Import all data page that allows you to specify all the files that you want to import data from.
More Actions > **Export Dial Patterns**	Opens the Export Dial Patterns page that allows you to export the dial patterns data as an XML file to a specified location.
More Actions > **Export Provider Specific Data**	Opens the Export Provider Specific Data page that allows you to export provider-specific data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all the NRP elements as a zipped file to a specified location.
Commit	Distributes the selected dial pattern to all the Session Manager instances in the enterprise.

Regular expressions

About Regular Expressions

You can configure routing in Session Manager by creating regular expressions and associating them with a routing policy.

Regular expression syntax is based on Perl version 5.8.

The asterisk character "*" matches any character string.

The dot character "." matches one character.

The backslash character "\ " makes a character lose its special meaning, if any

Some examples are:

- For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”
- For “192.14.11.22”, use string “192\.14\.11\.22”.
- The routing policy with a regular expression .*@.*\.de routes all calls requesting a SIP domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

Creating Regular Expressions

The NRP Regular Expressions screen enables you to create regular expressions and associate them with routing policies. You cannot save a regular expression unless it has a routing policy associated to it.

1. Select **Regular Expressions** from the NRP navigation menu. The Regular Expressions screen is displayed.
2. Click **New**. The Regular Expression Details screen is displayed.
3. Enter the regular expression pattern in the **Pattern** field.
4. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
5. To deny routing for a matched regular expression pattern, select the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.

7. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the policy and click **Remove**.
10. Click **Cancel** or **Commit**.

Modifying Regular Expressions

The NRP Regular Expressions screen enables you to modify regular expressions and associate them with routing policies.

1. Select **Regular Expressions** from the NRP navigation menu. The Regular Expressions screen is displayed.
2. Select a regular expression from the list and click **Edit**. The Regular Expression Details screen is displayed.
3. Modify the regular expression pattern in the **Pattern** field, if required.
4. If required, modify the rank order for the regular expression. A lower rank order indicates a higher priority.
5. To allow or deny routing for a matched regular expression pattern, select or clear the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
7. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the policy and click **Remove**.
10. Click **Cancel** or **Commit**.

Note:

You cannot save a regular expression unless it has a routing policy associated to it.

Deleting Regular Expressions

Deleting a regular expression deletes it from all of the routing policies that it is associated with.

1. From the Network Routing Policy menu from the left side of the screen, select **Regular Expressions**.
2. To delete existing regular expressions, select the respective check boxes and click **Delete**.
3. Click **Delete** or **Cancel** on the confirmation page.

Export Regular Expressions field descriptions

Use this page to export regular expressions to a file.

Button	Description
Export	Exports the regular expressions data as an XML file to a specified location.
Cancel	Cancels exporting the data to a file.

Import Regular Expressions field descriptions

Use this page to import regular expressions from a file.

Name	Description
Please select a file:	Browse to the required file from which you wish to import the regular expressions. Selecting the file displays the file name and path in the **Import Regular Expressions** page.

Button	Description
Import	Imports regular expressions from the specified file
Cancel	Cancels importing regular expressions from the specified file

Chapter 7: Managing Security

Trust management

System Manager Trust Management provisions and manages certificates of various applications (servers/devices), enabling them to have secure inter-element communication. It provides Identity (also known as Server) and Trusted (also known as Root, Issuer, or Certificate Authority (CA)) certificates which applications can use to establish mutually authenticated Transport Layer Security (TLS) sessions.

Session Manager ships with a default identity/server certificate issued by a SIP-Certifying Authority (SIP CA), which is a Certificate Authority that is controlled by Avaya and is only used to issue non-unique certificates to enable out-of-box support for TLS sessions. Additionally, Session Manager also bundles a default set of trusted certificates which are used to verify far-end certificates during a TLS session establishment.

During the installation of Session Manager, the installation script prompts you for an Enrollment Password which enables that Session Manager instance to request unique certificates from the System Manager Certificate Authority for services including SIP-TLS and management.

You can perform the following operations related to Trust Management:

- Obtain an Enrollment Password for application install and deployment
- Assign identity certificates to be used by the security module
- Add, view, and remove trusted certificates to the Session Manager security module
- View and obtain the Identity and Server Certificates of the Session Manager security module

Note:

Please refer to the Avaya Aura™ Session Manager Security Design for details on Security module.

Enrollment password

Applications such as Session Manager use the enrollment password during the initial installation and deployment process. This password is also referred to as the certificate enrollment password.

To ensure that a compromised password is not used, there are two constraints that bind the usage of an enrollment password—expiration time and count. You must keep the security implications in mind before selecting the values for these options.

Setting SCEP enrollment password

Use this functionality to generate the simple certificate enrollment password (SCEP) for adopting products. The adopting products require the SCEP password to request certificates from Trust Management.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Security** > **Trust Management** > **Enrollment Password**.
3. On the Enrollment Password page, select the expiration of password in hours in the **Password expires in** field.
4. In the **Certificate allowed** field, select the number of certificates.
5. Click **Generate**.

   Note:

   The password field displays the generated password.
6. Click **Done**.

   Note:

   When you click **Generate**, the number of certificates displayed next to the **Unused Certificate** label is updated by the number of certificates selected in the **Certificate allowed** field and also the time displayed next to the **Time remaining** label is updated by the value selected in the **Password expires in** field.

Chapter 8: Managing Applications

Applications module includes some of the System Manager administration specific features which are not supported for Session Manager administration. Some of these features are listed as follows:

- FPM
- MSA
- NMC
- SMGR
- SIP AS 8.0
- Entities

Administering certificates

Adding trusted certificates

You need to import the certificates that you want to add as trusted certificate in the trust store of the application. The following are the four methods of importing a trusted certificate in the trust store for an application instance:

1. Import from existing
2. Import from file
3. Import as PEM Certificate
4. Import using TLS

You can add a trusted certificate from a list of an existing certificates, a file, a remote location using TLS connection and by copying the content from a PEM file.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.

3. On the Application Management page, click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. On the **Add Trusted Certificate** page, select store type from the **Store Type** field and perform one of the following steps:
   - To import certificates from existing certificates:
     i. Click **Import from existing** .
     ii. Select the certificate from the Global Trusted Certificate section.
     iii. Click **Commit**.
   - To import certificates from a file:
     i. Click **Import from file** .
     ii. Enter the name of the file. You can also click **Browse** to select a file.
     iii. Click **Retrieve Certificate**.
     iv. Click **Commit**.
   - To import certificates in the PEM format:
     i. Locate the PEM certificate.
     ii. Open the certificate in the Notepad application.
     iii. Select all the contents in the file.
     iv. Perform a copy operation.
     v. Click **Import as PEM Certificate** .
     vi. Perform a paste operation in the box provided at the bottom of the page.

     Note:
     You may include the start and end tags: -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.
     vii. Click **Commit**.
   - To import using TLS:
     i. Click **Import using TLS** .
     ii. Enter the IP Address of the computer in the **IP Address** field.
     iii. Enter the port of the computer in the **Port** field.
     iv. Click **Retrieve Certificate**.
     v. Click **Commit**.

Viewing trusted certificates

Prerequisites

You must have permission to view certificates of an application instance.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **View**.

Result

The **View Trust Certificate** page displays the details of the selected certificate.

Removing trusted certificates

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, select the certificates and click **Remove**.

Result

Trust Management removes the certificates from the list of trusted certificates for the application instance.

Viewing identity certificates

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click **More Actions** > **Configure Identity Certificates**.

Result

The Identity Certificate page displays the identity certificates.

Assigning an identity certificate

Session Manager provides the capability of switching the active certificate being used by the Security Module to the default certificate or the unique certificate issued for that instance by the System Manager CA.

Note:

This operation has critical security implications. Please refer to the *Avaya Aura™ Security Guide* to understand when to select one of the two options.

To switch between these certificates, complete these steps:

1. Log on to the System Manager Common Console.
2. Click **Session Manager** > **System Status** > **Security Module Status**.
3. Under the Security Module Actions section on this screen, use the **Security Module Certificate** button to perform a certificate operation on the selected Session Manager Instance.

   Select one of the following options from the drop-down menu:

   - **Use Default Certificate (Issued By SIP CA)**: use the default identity certificate for the Security Module on that Session Manager instance
   - **Use Certificate from System Manager**: use the unique certificate issued to the Security Module during installation
4. After selecting the option, you should see the status change accordingly in the Statistics section.

The Security Module will use the newly assigned identity certificate for future TLS sessions.

Replacing an identity certificate

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificate page, Click **Replace**.
5. On the Replace Identity Certificate, perform one of the following steps:
   - click **Replace this Certificate with Internal CA Signed Certificate** and do the following:
     - Enter common name, org unit, organization, country in the respective fields.
     - Select key size/type, subjAltname from the respective fields.
     - Click **Commit** to replace the identity certificate with the internal CA signed certificate.
   - Click **Import third party PCKS # 12 file** and do the following:
     - Enter the file name in the **Please select a file** field.
     - Enter the password in the **Password** field.
     - Click **Retrieve Certificate** . The Certificate Details section displays the details of the certificate.
     - Click **Commit** to replace the certificate with the imported third party certificate.

Overview of Session Manager Trust Management Access Point

Session Manager Trust Management Access Point is used for defining application system type for Session Manager which is installed as part of a Session Manager installation. The **Applications** > **Session Manager 5.2** navigation menu link appears after the successful

installation of Session Manager application. An application system instances for Session Manager can be added using this navigation menu link.

Trust Management for application system instances is available through the Runtime Topology Service (RTS) provided on System Manager. Trust Management provides the functionality for managing Third Party Trusted Certificates on a provisioned Session Manager.

Related topics:

Creating a Session Manager Trust Management Access Point on page 390
Configuring Trusted Certificates on page 391
Configuring Identity Certificates on page 391

Creating a Session Manager Trust Management Access Point

1. On the System Manager Common Console, select **Applications** > **Session Manager 5.2**
2. Click **New**.
3. On the**New Session Manager Instance** page, enter the required information in the **Application** section:
   - Enter a **Name** for this TM AP instance.
   - Type is “Session Manager 5.2” and cannot be changed.
   - Enter a Description if so desired.
   - For **Node**, select Other from the drop-down menu.
   - The Other Node field appears. Enter the FQDN value of the TM AP or Session Manager.
4. Skip the **Port** section and navigate to the **Access Point** section.
5. Click on the **Show/Hide** button to open the **Access Point** section if it is not already open.
6. Select the only default available entry in the table with TrustManagement as the Access Point Type.
7. Click the **Edit** button. The Access Point Details section appears.
8. In the Access Point Details section, enter the following information:
   - Name - Use the same Name from the Application section and prefix it with -AP (i.e., -APMyName).
   - Enter the FQDN value for the TM AP in the **Host Name**field.
   - Enter admin in the **Username** and **Password**fields.

- Use the defaults for all of the other fields.

9. Click **Save**, then **Commit**.

Configuring Trusted Certificates

This action displays the currently installed Trusted Certificates for the selected TM AP.

From this page, you can Add new (3rd party) certificates to the TM AP. You can also View, Export or Remove a selected Trusted Certificate from this page.

1. On the System Manager Common Console, select **Applications** > **Session Manager 5.2**.
2. Select the appropriate Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates.**.
4. A list of Trusted Certificates is displayed.

Configuring Identity Certificates

This action displays the currently installed Identity Certificates for the known services on the TM AP.

From this page, you can View, Replace or Export (as .pem certificate file) the Identity Certificate of the selected service.

1. On the System Manager Common Console, select **Applications** > **Session Manager 5.2**.
2. Select the appropriate Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. A list of Identity Certificates is displayed.

Enrollment Password field descriptions

Use this page to generate a simple certificate enrollment password (SCEP).

Name	Description
Existing Password	The current simple certificate enrollment password (SCEP) that the external SCEP clients use to request certificates.
Unused Certificate	The number of certificates available using the password specified in the **Existing Password** field.
Time Remaining	Displays the time in hours and minutes remaining for expiration of the current password.
Password expires in	The duration for which the existing password is valid (in hours).
Certificate allowed	Number of certificates that you can generate using the new password.
Password	The password that the external SCEP clients use to request a certificate. Trust Manager generates this password when you click **Generate**.

Button	Description
Generate	Generates a random password.
Done	Updates the number of unused certificate with the number of certificates selected in **Certificate allowed** field.

Trusted Certificates field descriptions

Use this page to view and delete the trusted certificates listed on the page. You can also use this page to add more certificates in the existing list of trusted certificates

Name	Description
Certificate Name	The name of the trusted certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
View	Open the View Trust Certificate page. Use this page to view the certificate details.
Add	Open the Adds Trusted Certificate page. use this page to import certificates from the selected resource.

Button	Description
Remove	Removes the selected certificate from the list of trusted certificates.

Add Trusted Certificate field descriptions

Use this page to add a trusted certificate.

Name	Description
Store Type	The type of the store based on inbound and outbound connection. The options are: • TM_INBOUND • TM_OUTBOUND
Import from existing	Use this option to import the certificate from your local machine.
Import from file	Use this option to import the certificates from a file. The file format is .cer.
Import as PEM Certificate	Use this option to import the certificate in .pem format.
Import using TLS	Use this option to import a certificate if the application instance requires to contact the certificate provider to obtain the certificate.

Global Trusted Certificate:

The page displays the following fields when you select the **Import from existing** option.

Name	Description
Certificate Name	The fully qualified domain name of the certificate.
Subject Name	The fully qualified domain name of the certificate holder.
Valid To	The date until which the certificate is valid.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters certificates based on the filter criteria.
Select: All	Select all the certificates in the table.
Select: None	Clears all the check box selections.

Name	Description
Refresh	Refreshes the certificates information .

The page displays these fields when you select the **Import from file** option.

Name/Button	Description
Please select a file	The file that contains the certificates.
Browse	Opens the choose file dialog box. Use this dialog box to choose the file from which you want to import the certificates.
Retrieve Certificate	Retrieves the certificate from the file and displays the details of the certificate in the Certificate Details section.

Certificate Details:

The page displays these fields when you click **Retrieve**.

Name	Description
Subject Details	Details of the certificate holder.
Valid From	The date and time from which the certificate is valid.
Valid To	The date and time until which the certificate is valid.
Key Size	The size of the key in bits for encryption.
Issuer Name	The name of the issuer of the certificate.
Finger Print	The finger print that authenticates the certificate.

The page displays these fields when you select the **Import using TLS** option.

Field/Button	Description
IP Address	IP address of the certificate provider that is to be contacted for retrieving the certificate.
Port	Port of the server to be used for obtaining the certificate.
Retrieve Certificate	Retrieves the certificate and displays the details of the certificate in the Certificate Details section.

View Trust Certificate field descriptions

Use this page to view details of a selected certificate.

Name	Description
Subject Details	Details of the certificate holder.

Name	Description
Valid From	The date and time from which the certificate is valid.
Valid To	The date and time until which the certificate is valid.
Key Size	The size of the key in bits for encryption.
Issuer Name	The name of the issuer of the certificate.
Finger Print	The finger print that authenticates the certificate.

Button	Description
Done	Closes the page and takes you back to the Trusted Certificates page.

Delete Trusted Certificate Confirmation field descriptions

Use this page to delete a trusted certificate from the list of trusted certificate maintained by the application instance.

Name	Description
Certificate Name	The name of the trusted certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
Delete	Deletes the trusted certificate from the corresponding store.
Cancel	Cancels the delete operation and takes you back to the Add Trusted Certificate.

Identity Certificates field descriptions

Use this page to view the identity certificates for the application instance.

Name	Description
Service Name	The name of the service that uses the identity certificate.
Common Name	Common name to identify the service.
Valid To	The date until which the certificate is valid.
Service Description	A brief description about the service.

Button	Description
Replace	Opens the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate.
Cancel	Closes the Identity Certificates page and takes you back to the Application Management page.

Replace Identity Certificate field descriptions

Use this page to replace an identity certificate.

Certificate Details section

Name	Description
Subject Details	Details of the certificate holder.
Valid From	The date and time from which the certificate is valid.
Valid To	The date and time until which the certificate is valid.
Key Size	The size of the key in bits for encryption.
Issuer Name	The name of the issuer of the certificate.
Finger Print	The finger print that authenticates the certificate.

Name	Description
Replace this Certificate with Internal CA Signed Certificate	Use this option to replace the current certificate with internal CA signed certificate.
Import third party PCKS #12 file	Use this option if you like to replace the identity certificate with imported third PCKS #12 file.

The page displays following fields when you select **Replace this Certificate with Internal CA Signed Certificate** option

Name	Description
Common Name (CN):	The common name of the certificate holder.
Org Unit (OU):	The name of the organizational unit.
Organization (O):	The name of the organization
Country (C):	The country where the organization is located.
Key Size/Type:	The size of the key in bits or bytes for encryption .
SubjAltName:	The alternative name of the certificate holder.

The page displays following fields when you select **Import third party PCKS #12 file** option

Name/Button	Description
Please Select a file	The full path of the PKCS #12 file where you have saved the certificate.
Password	The password that is used to encrypt the certificate.
Browse	Opens the file dialog box to navigate to the PKCS #12 file.
Retrieve Certificate	Retrieves the details of the imported certificate and displays in the following **Certificate Details** section.

Name/Button	Description
Commit	Replaces the current identity certificate with the selected certificate.
Cancel	Cancels the certificate replacement operation.

Administering application instances

Runtime Topology

Runtime Topology service provides an interface to manage the instances of applications running on different servers. You can perform the following operations using the Runtime Topology service:

- Create an application instance
- Modify an application instance
- Delete an application instance
- Assign and Remove applications
- Issue a certificate to an application instance
- Replace an existing certificate

Creating a trusted application instance

Prerequisites

You must have a Trust Management type entry in the **Access point** section for the application instance.

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click **New**.
4. On the New Application Instance page, enter the appropriate details in the **Application, Port, Access Point, and Attributes** sections.
5. Click **Commit** .

   When you add an application entity through RTS, it in turn starts a synchronization job in the background to bring all the relevant data from the application instances to the Communication System Management database. You can check the status of this synchronization job on the System Manager console by accessing **Monitoring** > **Scheduler** or in the log files on the Communication System Management server.

   Note:

   The following information applies if you are creating an instance of messaging:

   - The details (FQDN or IP address) in the Node field for a messaging instance should correspond to that of MSS (Messaging Storage Server) and not MAS (Messaging Application Server).
   - You have to add the System Manager/ Communication System Management server details in the Trusted Server list on the Messaging box (in Messaging Administration/ Trusted Servers screen), before adding the Messaging box in the System Manager applications.
   - The login credentials between the Messaging box trusted servers screen and the Session Manager application, entity, or attributes for a Messaging type of application have to match.
   - The Trusted Server Name field on the Trusted Server page is mapped to the Login field in the Attributes section. Similarly the Password field on the Trusted Server page is mapped to the Password field in the Attributes section.
   - You should set the **LDAP Access Allowed** field on the trusted server page to yes, to allow LDAP access to this Messaging box from the trusted server that you add.

   The page displays the following three new buttons on the top and bottom of the page: **Issue Certificates**, **Add Untrusted**, and **Cancel**.
6. Click **Issue Certificate**.

Result

The Trust Management service issues certificate to the application instance signed by the System Manager configured certificate authority.

Viewing details of an application instance

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click an instance.
4. click **View**.

Result

The View Application Instance page displays the details of the selected instance.

Modifying an application instance

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click an application instance and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the Edit Application Instance page, modify the appropriate details in the **Application, Port, Access Point, Attributes** sections.
5. Click **Commit** to save the changes.

Deleting an application instance

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, click an instance.

4. click **Delete**.
5. On the Delete Application Confirmation page, Click **Delete**.

Modifying an access point

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Click **New**.
   - If you want to configure an access point for an existing application instance, click an instance and then click **Edit**.
   - If you want to configure an access point for an existing application instance, click an instance and click **View** > **Edit**.
4. Click an access point in the **Access Point** section and click **Edit** .
5. Modify the access point information in the following mandatory fields: **Name, Access Point Type, Protocol, Host, Port, Order**.
6. Click **Save**.

Assigning applications to an application instance

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Select an application instance and then click **Edit**.
   - If you want to assign applications to an existing application instance in the view mode, select an instance and click **View** > **Edit**.
4. Click **Assign Applications** in the Assign Applications section.
5. On the Assign Applications page, select applications and click **Assign**.

Removing assigned applications

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - If you want to remove assigned applications from an existing application instance, click an instance and then click **Edit**.
   - If you want to remove assigned applications from an existing application instance, click an instance and click **View** > **Edit**.
4. Select applications and click **Unassign Applications** in the **Assign Applications** section.

Creating a new port

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Click **New**.
   - If you want to configure a port for an existing application instance, click an instance and then click **Edit**or .
   - If you want to configure a port for an existing application instance, click an instance and click **View** > **Edit**.
4. Click **New** in the **Port** section.
5. Enter the information about the port in the following mandatory fields: **Name, Protocol, Port**.
6. Click **Save**.

Result

The table in the **Port Details** section displays the new port.

Modifying the port information

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Click **New**.
   - If you want to configure a port for an existing application instance, click an instance and then click **Edit**.
   - If you want to configure a port for an existing application instance, click an instance and click **View** > **Edit**.
4. Click **Edit** in the **Port** section.
5. Modify the port information in the following fields: **Name, Protocol, Port, Description**.
6. Click **Save** to save the changes to the database.

Deleting a port

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Click **New**.
   - If you want to configure a port for an existing application instance, click an instance and then click **Edit**.
   - If you want to configure a port for an existing application instance, click an instance and click **View** > **Edit**.
4. Click a port and click **Delete** in the **Port** section.

Result

Deletes the selected port from the table in the **Ports** section.

Creating an access point

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Click **New**.
   - If you want to configure an access point for an existing application instance, click an instance and then click **Edit**.
   - If you want to configure an access point for an existing application instance, click an instance and click **View** > **Edit**.
4. Click **New** in the **Access Point** section.
5. Enter the information about the access point in the following mandatory fields: **Name, Access Point Type, Protocol, Host, Port, Order**.
6. Click **Save**.

Deleting an access point

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click the **Applications** link and then click an application in the left navigation pane.
3. On the Application Management page, perform one of the following steps:
   - Click **New**.
   - If you want to configure an access point for an existing application instance, click an instance and then click **Edit**.
   - If you want to configure an access point for an existing application instance, click an instance and click **View** > **Edit**.
4. Click an access point in the **Access Point** section and click **Delete** .

Note:
You cannot delete an access point that is of type Trust Management.

Application Management field descriptions

Use this page to view the create, edit, view and delete instances of the application.

Name	Description
Name	Name of the application instance.
Node	The node on which the application is running.
Registration	The registration status of the application instance. The values are: • True: Indicates a registered instance. • False: Indicates an unregistered instance
Description	A brief description about the instance.

Button	Description
View	Opens View application page. Use this page to view the details of the selected application instance.
Edit	Opens Edit Application page. Use this page to modify the information of the instance.
Delete	Opens Delete Application Confirmation page. Use this page to delete a selected application instance.
Configure Trusted Certificates	Opens Trusted Certificates page. Use this page to view, add and delete the trusted certificates for the application instance.
Configure Identity Certificates	Opens Identity Certificates page. Use this page to view and replace the identity certificates for the application instance.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters application instances based on the filter criteria.
Select: All	Selects all the application instances in the table.
Select: None	Clears the selection for the users that you have selected.
Refresh	Refreshes the application instance information in the table.

Application Details field descriptions

Use this page to add and edit an application instance.

Application

Name	Description
Name	The name of the instance.
Type	The type of the application to which the instance belongs.
Description	A brief description about the instance.
Node	Select the node on which you want to run the application instance.
Other Node	The node on which you want to run the application instance. **Note:** The page displays this field when you select **Other** from the **Node** field.

Port

Name	Description
Name	The name of the port.
Port	The port on the application instance is running.
Protocol	The protocol associated with the corresponding port.
Description	A brief description about the port.

Button	Description
New	Displays fields in the **Port** section that you can use to add the port details.
Edit	Displays fields in the **Port** section with port information. You can modify the port details in the port mode.
Delete	Deletes the selected configured port.
Save	Saves the port details. **Note:** The section displays this button only when you click **Add** or **Edit** in the **port** section.
Cancel	Cancels the operation of creating or editing an access point and hides the fields that you use to enter or modify the port information. **Note:** The section displays this button only when you click**Add** or **Edit** in the **port** section.

Access Point

Name	Description
Name	The name of the access point.
Access Point Type	The type of the access point. The options are: • EMURL: Use this option to create a URL type access point . • Other
Protocol	The protocol that the application instance supports to communicate with other communication devices.
Host	The name of the host on which the application instance is running.
Port	The port on which the application instance is running.
Order	The order in which the access points are accessed.

Button	Description
New	Displays fields in the **Access Point** section that you can use to add port details.
Edit	Displays fields in the **Access Point** section that allows you to modify the selected port details.
Delete	Deletes the selected access point.

These fields appear when you click **Add** or **Edit** in the **Access Point** section.

Name	Description
Name	The name of the access point.
Access Point Type	The type of the access point. The options are: • EMURL: Use this option to create a URL type access point . • Other
Protocol	The protocol for communicating with the application instance.
Host	The name of the host on which the application instance is running.
Port	The port on which the application instance is running.
Order	The order in which the access points are accessed.
User Name	The name of the user who can access the application instance.
Password	The password that authenticates the user.

Button	Description
Save	Saves the access point details.

Button	Description
	Note: This button is visible only when you click **Add** and **Edit** in the **Access Point** section.
Cancel	Cancels the operation of creating or editing an access point and hides the fields that you use to enter or modify the access point information. **Note:** This button is available only when you click **Add** and **Edit** in the **Access Point** section.

Attributes

This section provides information about attributes fields that you can configure for the selected application.

Name	Description
Login	Login name to be used for connecting to the application instance. **Caution:** Do not use this login to connect to another application or directly to the SAT screens.
Password	Password which authenticates the SSH/ Telnet login name on the application instance. This field is not required for ASG login.
Is SSH Connection	Use this check box to specify whether the SSH connection should be used to connect to the application instance. By default this is selected. If you clear the check box, the connection with the application instance is made using Telnet.
Port	The port on which the service provided by the application instance is running. The default SSH port is 5022.
RSA SSH Key	The RSA SSH key of the CM Server. In case of Duplex servers, RSA SSH Key is the key of the Active server.
DSA SSH Key	The DSA SSH Key of the CM Server used only in case of Duplex servers. This is the key of the Standby server.
Alternate IP Address	Alternate IP address of the application instance. This is the IP address of the standby server in case of duplex servers.
Is AGS Enabled	Use this check box to enable AGS. If you select the **Is ASG enabled** check box, then you should enter the ASG key. Password is not required.
ASG Key	The ASG key used to authenticate the ASG login. You do not have to enter any value in this field if SSH/ Telnet login is used.
Location	The location of the application instance.

The following fields provides information about attributes related to messaging.

Name	Description
Login	Name as given in the Trusted Server Name field of the Trusted Servers page on the Messaging Box for this server.
Password	Password for the login name as given in the Password field of the Trusted Servers page on the Messaging Box for this server.
Confirm Password	You should retype the password for confirmation.
Messaging Type	The type of the Messaging box. The following are the types of messaging: • MM: for Modular Messaging systems • CMM: for Communication Manager Embedded Messaging systems
Version	The version of the Messaging Box. Supported versions are 5.0 and above.
Secured LDAP Connection	Use this check box to specify whether Secure LDAP connection is to be used. Select this check box to use secure LDAP connection, else LDAP will be used.
Port	The port on which the LDAP or secure LDAP service provided by the application instance is running. For LDAP the port is 389 and for secure LDAP the port is 636.
Location	The location of the application instance.

Assign Applications

Name	Description
Name	The name of the application instance.
Type	The type of application.
Description	A brief description about the application instance.

Button	Description
Assign Applications	Opens the Assign Applications page. Use the page to assign an application instance to another application instance.
Unassign Applications	Removes an assigned application.

Button	Description
Commit	Creates or modifies an instance by saving the instance information to the database.

Button	Description
	Note: This button is visible only when you click **New** and **Edit** on the Application Management page.
Cancel	Closes the page without saving the information and takes you back to the **Application Management** page.

Certificate Details

Name	Description
Subject Details	Details of the certificate holder.
Valid From	The date and time from which the certificate is valid.
Valid To	The date and time until which the certificate is valid.
Key Size	The size of the key in bits or bytes for encryption.
Issuer Name	The name of the issuer of the certificate.
Finger Print	The finger print that authenticates the certificate.

Button	Description
Issue Certificates	Adds the application as a trusted application.
Add Untrusted	Adds the application as a non-trusted application.
Cancel	Cancels the operation of issuing certificate to the application.

Delete Application Confirmation field descriptions

Use this page to delete the selected application instance.

Name	Description
Name	Name of the application instance.
Node	The node on which the application is running.
Registration	The registration status of the application instance. The values are: • True: Indicates a registered instance. • False: Indicates an unregistered instance
Description	A brief description about the instance.

Button	Description
Delete	Deletes the selected application instance.
Cancel	Closes the Delete Application Confirmation page.

Assign Applications field descriptions

Name	Description
Select Check box	Use the check box to select application instances.
Name	The name of the application instance.
Type	The type of the application.
Description	A brief description about the application.

Button	Description
Assign	Assigns the selected application instance to another application instance.
Cancel	Cancels the assignment operation and takes you back to the Application details page.

Chapter 9: System Manager Settings

Settings module includes some of the System Manager administration specific features which are not supported for Session Manager administration. Some of these features are listed as follows:

- Service Profile Management > System Manager 5.2 > IAM
- Service Profile Management > System Manager 5.2 > Licenses (WebLM)

Administering service profiles for applications

About Service Profile Management

The Service Profile Management Service provides a configuration repository for the System Manager services. The Service Profile Management service is responsible for storing configuration data for the System Manager services and notifying the services of configuration changes. You can perform the following operations using the Service Profile Management service:

- Store configuration data for services
- View a profile of a service
- Edit a profile of a service

Edit global feature profiles

This topic is about the global feature profiles that Service Profile Manager maintained in System Manager. You must log in as administrator to edit the global profiles.

Following is the global feature profile for System Manager:

Edit Profile System Manager field descriptions

View global feature profiles

This topic is about the global feature profiles that Service Profile Manager maintained in System Manager.

Following is the global feature profile for System Manager:

View Profile System Manager field descriptions

Edit software feature profiles

This topic is about the software feature profiles that Service Profile Manager maintains for global feature profiles in System Manager. You must log in as an administrator to modify the software feature profiles.

Following are the software feature profiles for the System Manager global feature profile:

Edit Profile:Licenses (WebLM) field descriptions on page 413

Edit Profile:Alarming UI field descriptions on page 414

Edit Profile:IAM field descriptions on page 415

Edit Profile: System Manager Element Manager field descriptions on page 429

Edit Profile:Logging field descriptions on page 432

Edit Profile:Scheduler field descriptions on page 434

Edit Profile:SNMP field descriptions on page 435

Edit Common Console Profile field descriptions on page 436

View software feature profiles

This topic is about the software feature profiles that Service Profile Manager maintains for global feature profiles in System Manager.

Following are the software feature profiles for the System Manager global feature profile:

View Profile:Licenses (WebLM) field descriptions on page 413

View Profile:Alarming UI field descriptions on page 414

View Profile:IAM field descriptions on page 422

View Profile: System Manager Element Manager field descriptions on page 428

View Profile:Logging field descriptions on page 431

View Profile:Scheduler field descriptions on page 433

View Profile:SNMP field descriptions on page 435

View Common Console Profile field descriptions on page 436

Edit Profile:Licenses (WebLM) field descriptions

Use this page to edit the parameters in the WebLM profile.

Name	Description
WebLM.Usages.UsageCount	This count represents the number of usage reports the server must maintain and display for each WebLM server.
WebLM.LicenseAllocation.Backup.FileSize	This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Licenses (WebLM) page.

View Profile:Licenses (WebLM) field descriptions

Use this page to view the parameters in the WebLM profile.

Name	Description
WebLM.Usages.UsageCount	This count represents the number of usage reports the server must maintain and display for each WebLM server.
WebLM.LicenseAllocation.Backup.FileSize	This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid.

Button	Description
Edit	Opens the Edit Profile:Licenses (WebLM) page. Use this page to edit the parameters in the WebLM profile.

Button	Description
Done	Closes the View Profile:Licenses (WebLM) page.

Edit Profile:Alarming UI field descriptions

Use this page to edit the parameters in the Alarming profile.

Color Codes

Name	Description
Cleared	The color code for alarms that are cleared.
Critical	The color code for critical alarms.
Informational	The color code for informational alarms.
Intermediate	The color code for the intermediate alarms.
Major	The color code for the major alarms.
Minor	The color code for the minor alarms.
Warning	The color code for the warning alarms.

Auto Refresh

Name	Description
Time Interval (millisec)	The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Alarming UI page.

Related topics:

Edit software feature profiles on page 412

View Profile:Alarming UI field descriptions

Use this page to view the parameters in the Alarming profile.

Color Codes

Name	Description
Cleared	The color code for cleared alarms.
Critical	The color code for critical alarms.
Informational	The color code for informational alarms.
Intermediate	The color code for the intermediate alarms.
Major	The color code for the major alarms.
Minor	The color code for the minor alarms.
Warning	The color code for the warning alarms.

Auto Refresh

Name	Description
Time Interval (millisec)	The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page.

Button	Description
Edit	Opens the Edit Profile:Alarming UI page. Use this page to edit the parameters in the Alarming Profile.
Done	Closes the View Profile:Alarming UI page.

Related topics:

View software feature profiles on page 412

Edit Profile:IAM field descriptions

Use this page to edit the parameters in the IAM profile.

SAML

Name	Description
SAML_ARTIFACT_RESOLUTION_URL	The URL to contact for resolving artifacts to SAML assertions. If the SSL/TLS connection is required, this should point to the HTTPS URL of the server.
SAML_AUTHN_REQ_GET_OR_POST	When sending a redirect URL to the user for authentication, an authentication request is also sent. The sent HTML gets posted automatically and the Idp receives the authentication request.

Name	Description
	When doing this, the form method can be either GET or POST. Some IdPs require one of these explicitly.
SAML_BINDING	The binding for SAML. This binding is mentioned in the Authentication request sent to the Idp as an indication of the binding that the IdP must use when sending the assertion back. The values are: • POST • Artifacts
SAML_COMPRESS_AUTHN_REQ	The parameter specifies whether or not to compress the authentication request when sending to the IdP. Use this option when the SAML_AUTHN_REQ_GET_OR_POST option is GET.
SAML_HTTP_AUTH_USERNAME	The user name to be used at the HTTP level for BASIC authentication when using the artifact resolution by contacting the SAML_ARTIFACT_RESOLUTION_URL.
SAML_IDP_ALIAS	Following are two ways in which this parameter can be used for the signature verification: . • If a value is provided for this parameter , then the signature is verified to have been created using the certificate pointed to by this alias • When the signature element in the assertion does not identify the certificate used for creating the signature, then the certificate pointed to by this alias is used.
SAML_IDP_LOGIN_URL	The URL to which the authentication request is sent.
SAML_NEED_SSL	If the URL for SAML_ARTIFACT_RESOLUTION_URL is HTTPS, then SAML_NEED_SSL must be set to true. If SSL/TLS connection is required between IAM and SAML IdP, then this should be set to TRUE
SAML_PROVIDER_ID	ID of the Identity provider that provides the authentication service.
SAML_SIGNATURE_ALIAS	
SAML_SP_NAME	The configuration name at the IdP that uniquely identifies this instance of IAM.

Name	Description
SAML_URL_ENCODE_AUTHN_REQ	The value indicates whether or not to URL-encode the authentication request when sending to the IdP. This option is used when the SAML_AUTHN_REQ_GET_OR_POST option is GET.
SAML_VERIFY_SIGNATURE	The value indicates whether or not to verify the signatures in the assertions. The parameter accepts a boolean value.

COMMON

Name	Description
AUTHENTICATION_MECHANISM	Determines the type of server to use. The values are: • UPM: Avaya UPM Database • LDAP: An LDAP or AD type server • RADIUS: Radius type server • SAML: the server to be used can act as a SAML ID
AUTHENTICATION_MODE	Determines the type of password to be used for authentication. The values are: • COMMUNICATIONS: Used for SIP authentication • NON-COMMUNICATIONS: Used for non-SIP authentication (for example, web access) **Note:** Administrators are not expected to change this.
BASIC_OR_DIGEST_AUTHENTICATION	Determines if the digest authentication needs to be used. The values are: • DIGEST: Used for SIP authentication • BASIC: Must be used for all non-SIP based authentications **Note:** Administrators are not expected to change this.

Name	Description
DIGEST_NONCE_PRIVATE_KEY	key used to create the NONCE value in the DIGEST mode.
DIGEST_NONCE_VALIDITY_PERIOD	Value determines if a NONCE given by the client is still valid in the DIGEST mode. This should be given in milliseconds.
NUMBER_OF_ACTIVE_SESSIONS	Number of active sessions that each user may have at any given time. This parameter accepts an integer value. For example, 10 means that a particular user is allowed to login through 10 different browser instances at the same time.
REALM_NAME	Realm name to be used for SIP digest authentication. This parameter accepts a string value. For example, sipUsers@domain.com

CONSOLE

Name	Description
LOGIN_PAGE_URI	Determines the URL users are forwarded to for authentication. **Note:** Administrators are recommended not to change the value of this parameter.
LOGIN_SYSTEM_ERROR_REDIRECT_URL	Determines whether to redirect the user to a specific URL page if a system error occurs. The parameter accepts a boolean value: • TRUE • FALSE
LOGIN_SYSTEM_ERROR_REDIRECT_TO_URL	Used in conjunction with **LOGIN_SYSTEM_ERROR_REDIRECT_URL** when **LOGIN_SYSTEM_ERROR_REDIRECT_URL** is set to TRUE. This is the specific URL the user is redirected to on encountering system errors.

LDAP

Name	Description
LDAP_BASE_DN	The base DN value to be used. The complete DN used for the authentication is LDAP_USERNAME_PREFIX + “=” + name entered by user + “,” + LDAP_BASE_DN.
LDAP_PRIMARY_HOST	The hostname or IP address of the primary LDAP/ AD Server.
LDAP_PRIMARY_PORT	The port number of the primary LDAP/AD server.
LDAP_PRIMARY_SSL_REQD	Enables or Disables TLS/SSL connection between IAM module and the primary LDAP server. This parameter accepts boolean value. • True: Enables TLS/SSL connection between the IAM module and the primary LDAP server • False: Disables TLS/SSL connection between the IAM module and the primary LDAP server
LDAP_SECONDARY_HOST	This parameter specifies hostname or IP address of the LDAP secondary host. Authentication is done against this LDAP/AD Server, if the Primary LDAP/ AD server specified above is unreachable.
LDAP_SECONDARY_SSL_REQD	This parameter specifies whether you can establish a TLS/SSL connection between the IAM module and the LDAP/AD server. The parameter accepts boolean value: • True • False
LDAP_USERNAME_PREFIX	The prefix for the username. The complete DN for the authentication is LDAP_USERNAME_PREFIX+ “=” + name entered by user + “,” + LDAP_BASE_DN.

DB

Name	Description
DB_CONNECTION_URL	The JDBC specific connection URL. You can request JDBC vendor to provide information on configuring the parameter. For example, • For Oracle: jdbc:oracle:thin:@192.147.7.215:1521:avayadb, where

Name	Description
	192.147.7.215 is the IP address of the database server and avayadb is the SID of the UPM database. • For PostgreSQL: jdbc:postgresql://192.147.7.215/avayadb, where 192.147.7.215 is the IP address of the database server, and avayadb is the database name. **Note:** If SSL is required when connecting to the database, then the connection URL will look different. Please refer DB_SSL_NEEDED parameter for more information.
DB_DRIVER_CLASSNAME	The JDBC driver class to be used for obtaining the database connection. This class is given by the database vendor. Note that the JAR file containing this class must be present in the system classpath – for example, $JBOSS_HOME/server/<<serverName>>/lib folder. For example, • For Oracle: oracle.jdbc.driver.OracleDriver • For PostgreSQL: org.postgresql.Driver
DB_JNDI_NAME	JNDI name of the datasource object configured in the J2EE server. This datasource must point to the Avaya UPM DB. **Note:** Administrators are strongly recommended not to change the value of this parameter after a successful installation of database.
DB_PASSWORD	Password for connecting to the database.
DB_SCHEMA_NAME	Name of the schema used for creating the Avaya UPM tables.
DB_SSL_NEEDED	Indicates whether or not SSL needs to be used for connecting to the database. This parameter accepts a boolean value.
DB_USERNAME	Unique name that identifies the user when connecting to the database.

Radius

Name	Description
RADIUS_NUM_RETRIES	The number of times the client should attempt to connect to the Radius server if the server does not respond.
RADIUS_PRIMARY_AUTH_PORT	The port number the primary the Radius server uses to receive RADIUS authentication requests.

Name	Description
RADIUS_PRIMARY_HOST	Hostname or IP address of the primary Radius server for authentication. For example, IP address such as 192.168.111.23 or “hostname.rnd.avaya.com”
RADIUS_PRIMARY_SHARED_SECRET	The secret key that is used to sign RADIUS data packets to ensure they are coming from a trusted source. The Radius Server’s clients configuration must be associated with this shared secret.
RADIUS_SECONDARY_AUTH_PORT	The port number on which the server listens for RADIUS authentication requests. Set this parameter when you use a secondary Radius server for fail over, and have provided a value for **RADIUS_SECONDARY_HOST**.
RADIUS_SECONDARY_HOST	The host name or IP address of the secondary Radius server that is used for fail over. Authentication is done against this Radius Server, if the Primary Radius server specified is not reachable.
RADIUS_SECONDARY_SHARED_SECRET	The secret key configured in the secondary Radius Server’s client configuration. This key will be used to sign RADIUS data packets to ensure they are coming from a trusted source. This must be provided if RADIUS_SECONDARY_HOST is provided for failover.
RADIUS_SERVER	The vendor name for the Radius Server. This value helps in loading the dictionary for the Radius Server. Attributes corresponding to this vendor name should be present in the AvayaRadiusClient.dict.
RADIUS_TIMEOUT	The number of seconds to wait for the Radius Server to respond before the client times out the server

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:IAM page.

View Profile:IAM field descriptions

Use this page to view the parameters in the IAM profile.

SAML

Name	Description
SAML_ARTIFACT_RESOLUTION_URL	The URL to contact for resolving artifacts to SAML assertions. If the SSL/TLS connection is required, this should point to the HTTPS URL of the server.
SAML_AUTHN_REQ_GET_OR_POST	When sending a redirect URL to the user for authentication, an authentication request is also sent. The sent HTML gets posted automatically and the Idp receives the authentication request. When doing this, the form method can be either GET or POST. Some IdPs require one of these explicitly.
SAML_BINDING	The binding for SAML. This binding is mentioned in the Authentication request sent to the Idp as an indication of the binding that the IdP must use when sending the assertion back. The values are: • POST • Artifacts
SAML_COMPRESS_AUTHN_REQ	The parameter specifies whether or not to compress the authentication request when sending to the IdP. Use this option when the SAML_AUTHN_REQ_GET_OR_POST option is GET.
SAML_HTTP_AUTH_USERNAME	The user name to be used at the HTTP level for BASIC authentication when using the artifact resolution by contacting the SAML_ARTIFACT_RESOLUTION_URL.
SAML_IDP_ALIAS	Following are two ways in which this parameter can be used for the signature verification: . • If a value is provided for this parameter , then the signature is verified to have been created using the certificate pointed to by this alias • When the signature element in the assertion does not identify the certificate used for

Name	Description
	creating the signature, then the certificate pointed to by this alias is used.
SAML_IDP_LOGIN_URL	The URL to which the authentication request is sent.
SAML_NEED_SSL	If the URL for SAML_ARTIFACT_RESOLUTION_URL is HTTPS, then SAML_NEED_SSL must be set to true. If SSL/TLS connection is required between IAM and SAML IdP, then this should be set to TRUE
SAML_PROVIDER_ID	ID of the Identity provider that provides the authentication service.
SAML_SIGNATURE_ALIAS	
SAML_SP_NAME	The configuration name at the IdP that uniquely identifies this instance of IAM.
SAML_URL_ENCODE_AUTHN_REQ	The value indicates whether or not to URL-encode the authentication request when sending to the IdP. This option is used when the SAML_AUTHN_REQ_GET_OR_POST option is GET.
SAML_VERIFY_SIGNATURE	The value indicates whether or not to verify the signatures in the assertions. The parameter accepts a boolean value.

COMMON

Name	Description
AUTHENTICATION_MECHANISM	Determines the type of server to use. The values are: • UPM: Avaya UPM Database • LDAP: An LDAP or AD type server • RADIUS: Radius type server • SAML: the server to be used can act as a SAML ID
AUTHENTICATION_MODE	Determines the type of password to be used for authentication. The values are:

Name	Description
	• COMMUNICATIONS: Used for SIP authentication • NON-COMMUNICATIONS: Used for non-SIP authentication (for example, web access) **Note:** Administrators are not expected to change this.
BASIC_OR_DIGEST_AUTHENTICATION	Determines if the digest authentication needs to be used. The values are: • DIGEST: Used for SIP authentication • BASIC: Must be used for all non-SIP based authentications **Note:** Administrators are not expected to change this.
DIGEST_NONCE_PRIVATE_KEY	key used to create the NONCE value in the DIGEST mode.
DIGEST_NONCE_VALIDITY_PERIOD	Value determines if a NONCE given by the client is still valid in the DIGEST mode. This should be given in milliseconds.
NUMBER_OF_ACTIVE_SESSIONS	Number of active sessions that each user may have at any given time. This parameter accepts an integer value. For example, 10 means that a particular user is allowed to login through 10 different browser instances at the same time.
REALM_NAME	Realm name to be used for SIP digest authentication. This parameter accepts a string value. For example, sipUsers@domain.com

CONSOLE

Name	Description
LOGIN_PAGE_URI	Determines the URL users are forwarded to for authentication. **Note:**

Name	Description
	Administrators are recommended not to change the value of this parameter.
LOGIN_SYSTEM_ERROR_REDIRECT_URL	Determines whether to redirect the user to a specific URL page if a system error occurs. The parameter accepts a boolean value: • TRUE • FALSE
LOGIN_SYSTEM_ERROR_REDIRECT_TO_URL	Used in conjunction with **LOGIN_SYSTEM_ERROR_REDIRECT_URL** when **LOGIN_SYSTEM_ERROR_REDIRECT_URL** is set to TRUE. This is the specific URL the user is redirected to on encountering system errors.

LDAP

Name	Description
LDAP_BASE_DN	The base DN value to be used. The complete DN used for the authentication is LDAP_USERNAME_PREFIX + “=” + name entered by user + “,” + LDAP_BASE_DN.
LDAP_PRIMARY_HOST	The hostname or IP address of the primary LDAP/ AD Server.
LDAP_PRIMARY_PORT	The port number of the primary LDAP/AD server.
LDAP_PRIMARY_SSL_REQD	Enables or Disables TLS/SSL connection between IAM module and the primary LDAP server. This parameter accepts boolean value. • True: Enables TLS/SSL connection between the IAM module and the primary LDAP server • False: Disables TLS/SSL connection between the IAM module and the primary LDAP server
LDAP_SECONDARY_HOST	This parameter specifies hostname or IP address of the LDAP secondary host. Authentication is done against this LDAP/AD Server, if the Primary LDAP/ AD server specified above is unreachable.
LDAP_SECONDARY_SSL_REQD	This parameter specifies whether you can establish a TLS/SSL connection between the IAM module and the LDAP/AD server. The parameter accepts boolean value:

Name	Description
	• True • False
LDAP_USERNAME_PREFIX	The prefix for the username. The complete DN for the authentication is LDAP_USERNAME_PREFIX+ “=” + name entered by user + “,” + LDAP_BASE_DN.

DB

Name	Description
DB_CONNECTION_URL	The JDBC specific connection URL. You can request JDBC vendor to provide information on configuring the parameter. For example, • For Oracle: jdbc:oracle:thin:@192.147.7.215:1521:avayadb, where 192.147.7.215 is the IP address of the database server and avayadb is the SID of the UPM database. • For PostgreSQL: jdbc:postgresql://192.147.7.215/avayadb, where 192.147.7.215 is the IP address of the database server, and avayadb is the database name. **Note:** If SSL is required when connecting to the database, then the connection URL will look different. Please refer DB_SSL_NEEDED parameter for more information.
DB_DRIVER_CLASSNAME	The JDBC driver class to be used for obtaining the database connection. This class is given by the database vendor. Note that the JAR file containing this class must be present in the system classpath – for example, $JBOSS_HOME/server/<<serverName>>/lib folder. For example, • For Oracle: oracle.jdbc.driver.OracleDriver • For PostgreSQL: org.postgresql.Driver
DB_JNDI_NAME	JNDI name of the datasource object configured in the J2EE server. This datasource must point to the Avaya UPM DB. **Note:** Administrators are strongly recommended not to change the value of this parameter after a successful installation of database.
DB_PASSWORD	Password for connecting to the database.
DB_SCHEMA_NAME	Name of the schema used for creating the Avaya UPM tables.

Name	Description
DB_SSL_NEEDED	Indicates whether or not SSL needs to be used for connecting to the database. This parameter accepts a boolean value.
DB_USERNAME	Unique name that identifies the user when connecting to the database.

Radius

Name	Description
RADIUS_NUM_RETRIES	The number of times the client should attempt to connect to the Radius server if the server does not respond.
RADIUS_PRIMARY_AUTH_PORT	The port number the primary the Radius server uses to receive RADIUS authentication requests.
RADIUS_PRIMARY_HOST	Hostname or IP address of the primary Radius server for authentication. For example, IP address such as 192.168.111.23 or “hostname.rnd.avaya.com”
RADIUS_PRIMARY_SHARED_SECRET	The secret key that is used to sign RADIUS data packets to ensure they are coming from a trusted source. The Radius Server’s clients configuration must be associated with this shared secret.
RADIUS_SECONDARY_AUTH_PORT	The port number on which the server listens for RADIUS authentication requests. Set this parameter when you use a secondary Radius server for fail over, and have provided a value for **RADIUS_SECONDARY_HOST**.
RADIUS_SECONDARY_HOST	The host name or IP address of the secondary Radius server that is used for fail over. Authentication is done against this Radius Server, if the Primary Radius server specified is not reachable.
RADIUS_SECONDARY_SHARED_SECRET	The secret key configured in the secondary Radius Server’s client configuration. This key will be used to sign RADIUS data packets to ensure they are coming from a trusted source. This must be provided if RADIUS_SECONDARY_HOST is provided for failover.

Name	Description
RADIUS_SERVER	The vendor name for the Radius Server. This value helps in loading the dictionary for the Radius Server. Attributes corresponding to this vendor name should be present in the AvayaRadiusClient.dict.
RADIUS_TIMEOUT	The number of seconds to wait for the Radius Server to respond before the client times out the server

Button	Description
Edit	Opens the Edit Profile: IAM page. Use this page to edit the parameters in the IAM profile.
Done	Closes the View Profile: IAM page.

View Profile: System Manager Element Manager field descriptions

Use this page to view the parameters in the System Manager Element Manager profile.

PEM-Container

Name	Description
backupDirectory	The name of the directory on the Database server where Element Manager creates the backup archives. **Note:** The database user should have write privileges on this directory.
databaseDirectory	The name of the directory on the Database server that contains the PostgreSQL backup/restore utilities. **Note:** The database user should have execute permissions on these utilities.
databaseType	Type of the database. For example, Oracle, Postgres.
dbHost	Host name of the database server.
dbPassword	Database super user password.
dbPort	Port number for database server.
dbScpPort	Port on the database server on which the SSH server is running.

Name	Description
dbUser	Database super user. This user should be able to open a SSH connection to the DB.
diskSpaceAllocated	Disk space allocated for backup archives.
diskSpaceThreshold	This is the percentage of the **diskSpaceAllocated** property. When this percentage is reached, an alarm is generated. So, if the **diskSpaceAllocated** is 100 MB and **diskSpaceThreshold** is 90 percent, an alarm is generated when the disk space occupied by the backup archives reaches 90 MB.
jobInterfaceURL	Lookup URL for the Element Manager.
maxBackupFiles	The maximum number of backup files that you can create. Once maximum limit is reached, the backup archives are rotated.
maxDataRetentionLimit	Maximum value allowed for the Data Retention interval.
remoteUtilityDirectory	Directory on the database server that contains the Element Manager backup/restore utilities.
schedulerURL	URL for accessing the scheduler.
scpPassword	Password for accessing the scp server.
scpPort	Port for the scp server.
scpServer	Host name of the scp server.
scpUser	User name for accessing the secure access server.

Button	Description
Edit	Opens the Edit Profile:IMSM Element Manager page. Use this page to edit the parameters in the IMSM Element Manager Profile.
Done	Closes the View Profile:IMSM Element Manager page.

Related topics:

View software feature profiles on page 412

Edit Profile: System Manager Element Manager field descriptions

Use this page to edit the parameters in the System Manager Element Manager profile.

PEM-Container

Name	Description
backupDirectory	The name of the directory on the Database server where Element Manager creates the backup archives.

Name	Description
	Note: The database user should have write privileges on this directory.
databaseDirectory	The name of the directory on the Database server that contains the PostgreSQL backup/restore utilities. **Note:** The database user should have execute permissions on these utilities.
databaseType	Type of the database. For example, Oracle, Postgres.
dbHost	Host name of the database server.
dbPassword	Database super user password.
dbPort	Port number for database server.
dbScpPort	Port on the database server on which the SSH server is running.
dbUser	Database super user. This user should be able to open a SSH connection to the DB.
diskSpaceAllocated	Disk space allocated for backup archives.
diskSpaceThreshold	This is the percentage of the **diskSpaceAllocated** property. When this percentage is reached, an alarm is generated. So, if the **diskSpaceAllocated** is 100 MB and **diskSpaceThreshold** is 90 percent, an alarm is generated when the disk space occupied by the backup archives reaches 90 MB.
jobInterfaceURL	Lookup URL for the Element Manager.
maxBackupFiles	The maximum number of backup files that you can create. Once maximum limit is reached, the backup archives are rotated.
maxDataRetentionLimit	Maximum value allowed for the Data Retention interval.
remoteUtilityDirectory	Directory on the database server that contains the Element Manager backup/restore utilities.
schedulerURL	URL for accessing the scheduler.
scpPassword	Password for accessing the scp server.
scpPort	Port for the scp server.
scpServer	Host name of the scp server.
scpUser	User name for accessing the secure access server.

Button	Description
Commit	Saves the changes to the database.

Button	Description
Cancel	Cancels the edit profile operation for IMSM Element Manager and takes you back to the View Profile: IMSM Element Manager page.

Related topics:

Edit software feature profiles on page 412

View Profile:Logging field descriptions

Use this page to view the parameters in the Logging profile.

Log Severity Levels

Name	Description
Alert	The color code for the log messages that are logged under the Alert severity level.
Critical	The color code for the log messages that are logged under the Critical severity level.
Emergency	The color code for the log messages that are logged under the Emergency severity level.
Error	The color code for the log messages that are logged under the Error severity level.
Informational	The color code for the log messages that are logged under the Informational severity level.
Notice	The color code for the log messages that are logged under the Notice severity level.
Warning	The color code for the log messages that are logged under the Notice severity level.

Auto Refresh

Name	Description
auto_refresh_time_interval	The time interval in milliseconds after which the log messages are auto refreshed on the Logging page .

Button	Description
Edit	Opens the Edit Profile:Logging page. Use this page to edit the parameters in the Logging profile.
Done	Closes the View Profile:Logging page.

Related topics:

View software feature profiles on page 412

Edit Profile:Logging field descriptions

Use this page to edit the parameters in the Logging profile.

Log Severity Levels

Name	Description
Alert	The color code for the log messages that are logged under the Alert severity level.
Critical	The color code for the log messages that are logged under the Critical severity level.
Emergency	The color code for the log messages that are logged under the Emergency severity level.
Error	The color code for the log messages that are logged under the Error severity level.
Informational	The color code for the log messages that are logged under the Informational severity level.
Notice	The color code for the log messages that are logged under the Notice severity level.
Warning	The color code for the log messages that are logged under the Notice severity level.

Auto Refresh

Name	Description
auto_refresh_time_interval	The time interval in milliseconds after which the log messages are auto refreshed on the Logging page .

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Logging page.

View Profile:Scheduler field descriptions

Use this page to view the parameters in the Scheduler profile.

PropertyContainer

Name	Description
pe_noof_retry	A count that defines the number of attempts to start the scheduler MBEAN.
Pe_retry_delay	Delay in time in seconds between each retry.

Container

Name	Description
smm_context_str	Constant that holds the name of the environment property for specifying the initial context factory to use. **Note:** This parameter is currently not in use.
smm_credential	Credential for connecting to the secured Java Naming and Directory Interface (JNDI). **Note:** This parameter is currently not in use.
smm_prinicipal	User name for secured Java Naming and Directory Interface (JNDI).
smm_url	The PROVIDER_URL which gives the server name and port on which a service is running. **Note:** This parameter is currently not in use.

Button	Description
Edit	Opens the Edit Profile:Scheduler page. Use this page to edit the parameters in the Scheduler profile.
Done	Closes the View Profile:Scheduler page.

Related topics:

View software feature profiles on page 412

Edit Profile:Scheduler field descriptions

Use this page to edit the parameters in the Scheduler profile.

PropertyContainer

Name	Description
pe_noof_retry	A count that defines the number of attempts to start the scheduler MBEAN.
Pe_retry_delay	Delay in time in seconds between each retry.

Container

Name	Description
smm_context_str	Constant that holds the name of the environment property for specifying the initial context factory to use. **Note:** This parameter is currently not in use.
smm_credential	Credential for connecting to the secured Java Naming and Directory Interface (JNDI). **Note:** This parameter is currently not in use.
smm_prinicipal	User name for secured Java Naming and Directory Interface (JNDI).
smm_url	The PROVIDER_URL which gives the server name and port on which a service is running. **Note:** This parameter is currently not in use.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Scheduler page.

Related topics:

Edit software feature profiles on page 412

View Profile:SNMP field descriptions

Use this page to view the parameters in the SNMP profile.

Avaya IM System Manager subagent attributes

Name	Description
Master Agent IPAddress	IP address of machine on which master agent is running.
Master Agent TCP Port	The connection between master agent and subagent is established via a TCP port using AgentX protocol. This port has to be configured with both the master agent and the subagent so that the master agent starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port.
Sub Agent IPAddress	IP address of machine on which sub agent is deployed

Button	Description
Edit	Opens the Edit Profile:SNMP page. Use the page to edit the parameters in the SNMP profile.
Done	Closes the View Profile: SNMP page.

Related topics:

View software feature profiles on page 412

Edit Profile:SNMP field descriptions

Use this page to edit the parameters in the SNMP profile.

Avaya IM System Manager subagent attributes

Name	Description
Master Agent IPAddress	IP address of machine on which master agent is running.
Master Agent TCP Port	The connection between master agent and subagent is established via a TCP port using AgentX protocol. This port has to be configured with both the master agent and the subagent so that the master agent starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port.
Sub Agent IPAddress	IP address of machine on which sub agent is deployed

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile: SNMP page.

Related topics:

Edit software feature profiles on page 412

Edit Common Console Profile field descriptions

Use this page to edit the common console profile.

Name	Description
Global session timeout	Timeout period for global session. By default, the timeout period for global session is 30 minutes. The range is minimum -30 minutes and maximum - 480 minutes.
Number of rows	Number of rows to be displayed in table. The default count is 15 . The range of minimum rows is 15 and maximum rows is 100.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation.

Related topics:

Edit software feature profiles on page 412

View Common Console Profile field descriptions

Use this page to view the common console profile.

Name	Description
Global session timeout	Timeout period for global session. By default, the timeout period for global session is 30 minutes. The range is minimum -30 minutes and maximum - 480 minutes.
Number of rows	Number of rows to be displayed in table. The default count is 15 . The range of minimum rows is 15 and maximum rows is 100.

Button	Description
Edit	Opens the Edit Profile: Common Console page. Use this page to edit the parameters in the Common Console profile.

Button	Description
Done	Closes the View Profile: Common Console page.

Related topics:

View software feature profiles on page 412

Administering backup and restore

Backup and Restore

The backup and restore functions are executed on the System Manager. These functions allow you to backup and restore configuration data for the System Manager and all of the Session Manager instances. All of the configuration data for the entire system is kept centrally on the System Manager. This means that individual backups of the Session Manager instances are not needed. After a restore operation, the restored configuration data is automatically propagated to the Session Manager instances.

Associated actions include configuring data retention rules for specifying how long the backup files should remain on the system, and modifying logger and appender information.

Viewing list of backup files

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore**.

Result

The Backup and Restore page displays the list of backup files.

Creating backup of application data

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore**.
3. Click **Backup**.
4. On the Backup page, perform one of the following steps:
   - To back up data to a local drive, do the following:
     i. Click **Local** option.
     ii. In the **File name** field, enter the name of the backup file field that you want to create.
   - To back up data to a remote location, do the following:
     i. Click **Remote** option.
     ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Now**.

Result

If the backup is successful, the Backup and Restore page displays a message Backup created successfully!!.

Scheduling a data backup

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore**.
3. Click **Backup**.
4. On the Backup page, perform one of the following steps:
   - To schedule a local backup, perform the following steps:
     i. Click **Local** option.
     ii. In the **File name** field, enter the name of the backup file field that you want to create.

- To schedule a remote backup, perform the following steps:
    i. Click **Remote** option.
    ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields

5. Click **Schedule**.
6. On the Schedule Backup page, specify the following: Job Name, Task Time, Recurrence and Range in the respective fields.
7. Click **Commit**.

Restoring a backup

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Backup and Restore**.
3. Click **Restore**.
4. On the Restore page, perform one of the following steps:
    - To restore data from a local backup
        i. Click **Local** option.
        ii. Enter the back up file name in the **File name** field.
    - To restore data from a remote backup
        i. Click **Remote** option.
        ii. Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
5. Click **Restore**.

Result

After the successful restore operation, the user who initiated the restore is logged out of the System Manager console.

Viewing data retention rules

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Data Retention** in the left navigation pane.

Result

The Data Retention page displays the data retention rules.

Modifying data retention rules

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Data Retention** in the left navigation pane.
3. Click the option button to select a rule.
4. Click **Edit** .
5. Modify the value in the **Retention Interval (Days)** field.
6. Click **Update** to save the value.

Applying a data retention rule

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Data Retention** in the left navigation pane.
3. Click the option button to select a rule.
4. Click **Apply**.

Viewing loggers for a log file

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Logging Configuration** in the left navigation pane.
3. On the Logging Configuration page, click a log file from the **Select Log File** field.

Result

You can view the loggers in the Logger List section.

Assigning an appender to a logger

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Logging Configuration** in the left navigation pane.
3. On the Logging Configuration page, click a log file from the **Select Log File** field.
4. Click a logger in the **Logger List** section.
5. Click **Edit**.
6. On the Edit logger page, click **Attach** in the **Attached Appenders** section.
7. On the Attach Appender page, click an appender in the **Select Appender** field.
8. Click **Commit**.

Result

The appender is added to the selected logger and you can view the appender on the Logging Configuration page.

Editing a logger

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Logging Configuration** in the left navigation pane.

3. On the Logging Configuration page, select a log file from the **Select Log File** drop-down field.
4. Click a logger in the **Logger List** section.
5. Click **Edit** in the Logger List section.

   The page displays this button at the upper-left side of the table displaying the log files.
6. On the Edit logger page, select a log level from the Log Level drop-down field.
7. Click **Commit** .

   The log level is set for the selected log file.

Editing an appender

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Logging Configuration** in the left navigation pane.
3. On the Logging Configuration page, click a log file from the **Select Log File** field.
4. Click a logger in the **Logger List** section.
5. Click **Edit**.
6. On the Edit logger page, click an appender in the **Attached Appenders** section.
7. Click **Edit**.
8. On the Edit Appender page modify the appender information.

   Note:

   You can modify information in the following fields: **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files**.
9. Click **Commit**.

Removing an appender from a logger

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. Click **Settings** > **Logging Configuration** in the left navigation pane.

3. On the Logging Configuration page, click a log file from the **Select Log File** field.
4. Click a logger in the **Logger List** section.
5. Click **Edit**.
6. On the Edit logger page, click an appender in the **Attached Appenders** section.
7. Click **Detach**.

Backup And Restore field descriptions

Use this page to view the details of backup files.

Name	Description
File Name	Name of the backup file.
Path	Path of the backup file.
Status	Status of the backup. The values are: • SUCCESS • FAILED
Backup Time	Time of backup.
Backup Mode	The mode defines whether the backup is manual or automatic.
Backup Type	The type defines whether the backup is a local or remote backup.
User	The user who has performed the backup.

Button	Description
Backup	Opens the Backup page. Use this page to back up data on a specified local or remote location.
Restore	Opens the Restore page. Use this page to restore data to a specified local or remote location.

Backup field descriptions

Use this page to backup data to a local or a remote location. You can use this page to schedule a back up.

Name	Description
Type	The type based on the location of the computer on which you want to back up the application data. The options are: • **Local**: The data is backed up on a local machine. • **Remote**: The data is backed up on a remote machine.
File Name	The name of the file that identifies the backup. If you specify only the filename, System Manager creates a backup file in the home directory of the specified user. If you want to create the backup file in a directory other than the home directory, specify a complete path including the filename. **Note:** This option is available when you select **Local** as **Type**.
SCP Server IP	IP address of the SCP server. **Note:** This option is available when you select **Remote** as **Type**.
SCP Server Port	Port of the SCP server. **Note:** This option is available when you select **Remote** as **Type**.
User Name	User name for logging in to the SCP server. **Note:** This option is available when you select **Remote** as **Type**.
Password	Password for logging in to the SCP server. **Note:** This option is available when you select **Remote** as **Type**.
File Name	The name that identifies the backup file. **Note:** This option is available when you select **Remote** as **Type**.
Use Default	Select this check box to use the default configured values. **Note:** This option is available when you select **Remote** as **Type** .

Button	Description
Now	Backs up the data to the specified location immediately.
Schedule	Opens the Schedule Backup page. Use this page to schedule a back up.
Cancel	Closes the Backup page and takes you back to the Backup and Restore page.

Schedule Backup field descriptions

Use this page to schedule a job for backup of data by specifying the date and time of running the job.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one time activity. In the case of a recurring job, the field also displays the time interval of recurrence. The options are: • Execute task one time only. • Task are repeated.
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules the backup job.
Cancel	Closes the Schedule Backup page and takes you back to the Backup Restore page.

Restore field descriptions

Use this page to restore the application data from a local or a remote location.

Name	Description
Type	The type based on location of the computer from which you want to restore the application data. The options are: • **Local**: The data is restored from a local machine. • **Remote**: The data is restored from a remote machine.
File Name	The name of the backup file that you want to restore. **Note:** This field is available when you select **Local** as **Type**.
SCP Server IP	IP address of the SCP server. This field is available when you select **Remote** as **Type**.
SCP Server Port	Port of the SCP server. This field is available when you select **Remote** as **Type**.
User Name	User name for logging in to the SCP server. This field is available when you select **Remote** as **Type**.
Password	Password for logging in to the SCP server. This field is available when you select **Remote** as **Type**.
File Name	The name of the backup file that you want to restore. This field is available when you select **Remote** as **Type**.
Use Default	Select this check box to use the default configured values. This field is available when you select **Remote** as **Type**.

Button	Description
Restore	Restores the data from the specified backup file.
Cancel	Closes the Restore page and takes you back to the Backup and Restore page.

Data Retention field descriptions

Use this page to view and edit data retention rules.

Name	Description
Option button	Click the option button to select a data retention rule.
Rule Name	Name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	The number of days the data is retained.

Button	Description
Edit	Modifies the selected rule.
Update	Updates the rule with changes made to the rule.
Cancel	Cancels the editing operation.
Apply	Applies the selected rule.

Logging Configuration field descriptions

Use this page to view and edit log levels and appenders for a logger defined in a log file.

Log Configuration

Name	Description
Select Log File	The field lists the log files that you can configure.

Logger List

Name	Description
Logger	The loggers in the selected log files.
Log level	Log level defines as to what level of logging is set for the corresponding logger.
Attached Appenders > Name	Name of the appender.
Attached Appenders > File Path	The path of the file to which the appender logs the information.

Button	Description
Edit	Opens the Edit Logger page that you can use to edit loggers.

Edit Logger field descriptions

Use this page to edit logger and appender information. You can also add and remove appenders from the loggers.

Logger

Name	Description
Logger	The name of the logger.
Log level	The level of logging for which the logger logs the information.

Attached Appender

Name	Description
Appender	The name of the appender.
Threshold Log Level	The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .
File Path	The path of the file where the appender logs the information.
Max File Size	The maximum size in KB, MB, and GB reserved for the appender file.
# Backup Files	The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.

Button	Description
Edit	Opens the Edit Appender page. Use this page to modify the appender information.
Attach	Opens the Attach Appender page. Use this page to add an appender to the logger.
Detach	Removes the selected appender from the logger.
Commit	Saves the changes in the logger information to the database.
Cancel	Closes the Edit Logger page and takes you back to the Logging Configuration page.

Edit Appender field descriptions

Use this page to edit information of an appender.

Name	Description
Logger	The name of the logger. **Note:** You can only view this information.

Name	Description
Appender	The name of the appender. **Note:** You can only view this information.
Threshold Log Level	The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .
File Path	The path of the file where the appender logs the information.
Max File Size	The maximum KB, MB, and GB reserved for the appender file.
# Backup Files	The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes Edit Appender page and takes you back to the Edit Logger page.

Attach Appender field descriptions

Use this page to assign an appender to the logger.

Name	Description
Logger	The name of the logger.
Log Level	The level of logging for which the logger logs the information.
Select Appender	The list of appenders that you can assign to the logger.

Button	Description
Commit	Assigns the appender to the logger.
Cancel	Closes the **Attach Appender** page and takes you back to the Edit Logger page.

Chapter 10: Session Manager

Session Manager Administration

About Session Manager Administration

Select the Session Manager Administration menu option to add a SIP entity as a Session Manager instance. Once added, these Session Manager instances form a link with the Session Manager Element Manager and can be used for obtaining and monitoring the status of that Session Manager instance.

Data replication and monitoring operations are possible only after these Session Manager instances are added and configured.

In addition to creating new Session Manager instances, the Session Manager Administration screen also allows you to view, edit, or delete the Session Manager instances that you have created.

Note:

Although the PPM Connection Timeout (mins) parameter is mentioned in the chapter and is present on the Session Manager Administration module as a required parameter, it is not yet used by Personal Profile Manager (PPM) in Session Manager 5.2 release.

Adding a SIP entity as a Session Manager instance

Prerequisites

Before starting this procedure, make sure that the SIP entity that you want to add was created and is in a synchronized state. Refer to the section Creating NRP SIP entities to create the SIP entity. Also for a Session Manager type SIP entity, the customer has to administer the listen ports on the SIP entity form. These listen ports are used by endpoints to connect to SM and they can be used to map different ports to different domains.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Session Manager Administration**.
2. Click **New** on the Session Manager Administration screen. The system displays the Add Session Manager screen.
3. Under the **General** section, enter the following information:
   - Select the **SIP Entity Name** from the drop-down list.
   - In the **Description** field for this entity, add a comment if required.
   - In the **Management Access Point Host Name/IP** field, add the IP address of the host on which the management agent is running; that is, the host on which the Session Manager is installed.
   - Select the **Direct Routing to Endpoints** from the drop-down list.

   Note:

   To be a part of the Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point. This is the network mask of the domain name of the server that hosts the Session Manager application. The address is passed to the SM100 agent to allow the agent to query the server for the required information.
4. Under the **Security Module** section, enter the following information to configure the security module:
   - The **SIP Entity IP Address** field, shows the name of the SIP entity that is added as a Session Manager instance. The entity must be of type Session Manager and it must be in Sync state.
   - In the **Network Mask** field, enter the value for the network mask. The network mask is passed to the SM100 agent. The agent configures the network mask to define the subnet that the SM100 card is to be associated with.
   - In the **Default Gateway** field, add the correct IP address.
   - In the **Call Control PHB** field, enter a value.

     The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 that you may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence—they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.

- The **Speed & Duplex** field allows the configuring of the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
- In the **QOS Priority** field, enter a 802.1q priority value.

  This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
- In the **VLAN ID** field, enter an integer value. This is the VLAN that the Session Manager is to be associated with. Call traffic segregation could be based on the VLAN associated with the Session Manager.

5. Under the **Monitoring** section, enter the following information to configure how this Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Session Manage instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default is 900 seconds. Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default is 120 seconds.

     This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

     Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities screen for a specific entity.
   - Type an integer value in **Number of Retries**. The default is 1. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default is 1.
6. Under the **CDR** section, specify related information:
   a. Select the **Enable CDR** check box to enable Call Detail Recording. This controls whether CDR is enabled at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.
   b. Type a password that must be used to access the CDR record and retype to confirm the password. This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR

files. Normally the adjunct logs in as “CDR_User” user ID, with a default password. The password that you specify here becomes the default password. Once the CDR adjunct logs in using “sftp”, it is automatically placed in the Session Manager CDR home directory of the CDR_User, which is `/var/home/ftp/CDR`.

7. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all SM instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM client connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Specify the value of **PPM Connection Timeout (mins)**. Valid values are integers between 1 and 600. Default value is 5.
   d. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
   e. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value: 50.
8. **Event Server** section specifies the option to clear Subscription on Notification Failure.
9. Click **Commit** .

Related topics:

Session Manager Administration page field descriptions on page 458
Add Session Manager page field descriptions on page 458

Viewing the Session Manager administration settings

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Session Manager Administration**.
2. Select a Session Manager from the Session Manager Instances list and click **View**. The View Session Manager screen displays information about the selected Session Manager instance.
3. After you have viewed the information, click **Return**.

Related topics:

Session Manager Administration page field descriptions on page 458
View Session Manager page field descriptions on page 461

Modifying the Session Manager administration settings

This option allows you to modify the configuration settings for an already configured Session Manager.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Session Manager Administration**.
2. Click **Edit** on the Session Manager Administration screen.
3. Under the **General** section, change the following information, if required:
   - Add a comment in the Description field for the Session Manager SIP entity.
   - Change the IP address of the host on which the Session Manager is installed in the **Management Access Point Host Name/IP** field. This is the IP address of the domain name of the server that hosts the Session Manager application. Session Manager passes the address to the SM100 agent to allow the agent to query the server for the required information. To be a part of the Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point.
   - Select the **Direct Routing to Endpoints** from the drop-down list.
4. Under the **Security Module** section, change the following information, if required
   - Modify the network mask in the **Network Mask** field. Session Manager passes this network mask to the SM100 agent. The agent configures the network mask to define the subnet that the SM100 card is to be associated with.
   - Modify the IP address in the **Default Gateway** field.
   - Modify the value for **Call Control PHB**. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 that you may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.

- Select the **Speed & Duplex** value to configure the security module interface speed and duplex values.
- Modify the **QOS Priority** value. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
- Modify the value for **VLAN ID**. This is the VLAN that the Session Manager is to be associated with. Call traffic segregation could be based on the VLAN that the Session Manager is associated with.

5. Under the **Monitoring** section, modify the following information as required to configure how this Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default is 900 seconds.
   - Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default is 120 seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

     Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities screen for a specific entity.
   - Type an integer value in **Number of Retries**. The default is 1. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable.
6. Under the **CDR** section, change the following information, if required
   - Select the **Enable CDR** check box to enable Call Detail Recording. This enables CDR at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.
   - Type a password that must be used to access the CDR record and retype to confirm the password. This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR files. Normally the adjunct logs in with the “CDR_User” user ID with a default password. The password that you specify here becomes the default password. Once the CDR adjunct logs in using “sftp”, it is automatically placed in the

Session Manager CDR home directory of the CDR_User, which is `/var/home/ftp/CDR`.

7. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all SM instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM client connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Specify the value of **PPM Connection Timeout (mins)**. Valid values are integers between 1 and 600. Default value is 5.
   d. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
   e. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value: 50.
8. **Event Server** section specifies the option to clear Subscription on Notification Failure.
9. Click **Commit**.

Related topics:

Session Manager Administration page field descriptions on page 458
Edit Session Manager page field descriptions on page 464

Deleting a SIP entity as a Session Manager instance

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Session Manager Administration**.
2. Select a Session Manager instance from the list and click **Delete**.
3. On the Delete Confirmation screen, click **Delete** to delete the Session Manager instance.

Related topics:

Session Manager Administration page field descriptions on page 458
Delete Confirmation page field descriptions on page 467

Session Manager Administration page field descriptions

Name	Description
New	Opens the Add Session Manager page that enables you to add a SIP entity as a new Session Manager instance
View	Opens the View Session Manager page that enables you to view an already added Session Manager instance
Edit	Opens the Edit Session Manager page that enables you to edit the properties of an already added Session Manager instance
Delete	Opens the Delete Confirmation page that allows you to delete a SIP entity that is added as a Session Manager instance

Related topics:

Adding a SIP entity as a Session Manager instance on page 451
Viewing the Session Manager administration settings on page 454
Modifying the Session Manager administration settings on page 455
Deleting a SIP entity as a Session Manager instance on page 457

Add Session Manager page field descriptions

General

Name	Description
SIP Entity Name	Select a name of the SIP entity that you wish to add as a Session Manager instance. The entity must be of type Session Manager and it must be in Sync state.
Description	Description of the entity added. Optional.
Management Access Point: Host Name / IP	The IP address of the host on which the management agent is running, that is, the host on which the Session Manager is installed.
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.

Security Module

Name	Description
SIP Entity IP Address	Shows the name of the SIP entity that is added as a Session Manager instance.

Name	Description
Network Mask	Allows you to enter the value of the Network mask. The network mask is passed to the SM100 agent. The agent configures the network mask to define the subnet that the SM100 card is to be associated with.
Default Gateway	IP address of the default gateway.
Call Control PHB	The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.
QOS Priority	This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, lower the QOS priority number. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7.
Speed & Duplex	Allows the configuring of the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
VLAN ID	The VLAN that the Session Manager should be associated with. Call traffic segregation could be based on the VLAN that the Session Manager is associated with.

Monitoring

Button	Description
Enable Monitoring	Select to enable monitoring of the administered SIP entities by the added Session Manager instance. Clear the check box to disable monitoring.
Proactive cycle time (secs)	Enter a value in seconds for polling the administered SIP entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. These default values are used for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.
Reactive cycle time (secs)	Enter a value in seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

Button	Description
	Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.
Number of Retries	Enter an integer value. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default is 1. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.

CDR

Name	Description
Enable CDR	This controls whether CDR is enabled at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.
User	User name.
Password	This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR files. Normally the adjunct logs in as "CDR_User" user ID, with a default password. The password that you specify here becomes the default password. Once the CDR adjunct logs in using "sftp", it is automatically placed in the Session Manager CDR home directory of the CDR_User, which is /var/home/ftp/CDR.
Confirm Password	Enter the same password to confirm.

Personal Profile Manager (PPM) - Connection Settings

Name	Description
Limited PPM client connection	Enables selecting **Maximum Connection per PPM client**. Default value is Enabled.
Maximum Connection per PPM client	Valid values are integers between 1 and 10. Default value is 3.
PPM Connection Timeout (mins)	Valid values are integers between 1 and 600. Default value is 5.
PPM Packet Rate Limiting	Enables selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
PPM Packet Rate Limiting Threshold	This value is applied per PPM client. Value Range: 1-500, default value: 50.

Event Server

Name	Description
Clear Subscription on Notification Failure	Specifies the option to clear Subscription on Notification Failure.

Button	Description
Cancel	Cancels the Session Manager addition operation.
Commit	Saves the added SIP entity as a Session Manager instance with the selected configuration options.

Related topics:

Adding a SIP entity as a Session Manager instance on page 451

View Session Manager page field descriptions

General

Name	Description
SIP Entity Name	Name of the SIP entity that you wish to add as a Session Manager instance. The entity must be of type Session Manager and it must be in Sync state. This is a view-only field.
Description	Description of the entity added. Optional. View-only field.
Management Access Point: Host Name	The IP address of the host on which the management agent is running, that is, the host on which the Session Manager is installed. View-only field.
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.

Security Module

Name	Description
SIP Entity IP Address	IP address of the Session Manager. View-only field.
Network Mask	Network mask. The SM100 agent configures the network mask to define the subnet the SM100 board will be associated with. View-only field.
Default Gateway	IP address of the default gateway. View-only field.
Call Control PHB	View-only field. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 may expect as it travels

Name	Description
	through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.
QOS Priority	This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, lower the QOS priority number. The default is 6. View-only field.
Speed & Duplex	Allows the configuring of the security module interface speed and duplex values. View-only field.
VLAN ID	The VLAN that the Session Manager should be associated with. Call traffic segregation could be based on the VLAN that the Session Manager is associated with. View-only field.

Monitoring

Button	Description
Enable Monitoring	If this check box is selected, it enables monitoring of the administered SIP entities by the added Session Manager instance. If the check box is not selected, monitoring is disabled. View-only.
Proactive cycle time (secs)	Time in seconds for polling the administered SIP entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. These default values are used for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.
Reactive cycle time (secs)	Time in seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.
Number of Retries	This integer value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default is 1. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.

CDR

Name	Description
Enable CDR	This controls whether CDR is enabled at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail recording for specific SIP entities using the Call Detail Recording drop-down menu.
User	User name.
Password	This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR files.

Personal Profile Manager (PPM) - Connection Settings

Name	Description
Limited PPM client connection	Enables selecting **Maximum Connection per PPM client**. Default value is Enabled.
Maximum Connection per PPM client	Valid values are integers between 1 and 10. Default value is 3.
PPM Connection Timeout (mins)	Valid values are integers between 1 and 600. Default value is 5.
PPM Packet Rate Limiting	Enables selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
PPM Packet Rate Limiting Threshold	This value is applied per PPM client. Value Range: 1-500, default value: 50.

Event Server

Name	Description
Clear Subscription on Notification Failure	Specifies the option to clear Subscription on Notification Failure.

Button	Description
Return	Returns you to the Session Manager Administration page

Related topics:

Viewing the Session Manager administration settings on page 454

Edit Session Manager page field descriptions

General

Name	Description
SIP Entity Name	Name of the SIP entity that is added as a Session Manager instance. The entity must be of type Session Manager and it must be in Sync state. This is a view-only field.
Description	Description of the entity added. Optional.
Management Access Point: Host Name	Specifies the IP address of the host on which the Session Manager is installed in the Management Access Point Host Name/IP field. This is the IP address of the domain name of the server that hosts the Session Manager application. Session Manager passes the address to the SM100 agent to allow the agent to query the server for the required information. To be a part of the Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point.
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.

Security Module

Name	Description
SIP Entity IP Address	IP address of the Session Manager. View-only field.
Network Mask	Specifies the network mask in the Network Mask field. Session Manager passes this network mask to the SM100 agent. The SM100 agent configures the network mask to define the subnet the SM100 board will be associated with.
Default Gateway	IP address of the default gateway.
Call Control PHB	The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.

Name	Description
QOS Priority	This specifies the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number..
Speed & Duplex	Allows the configuring of the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
VLAN ID	The VLAN that the Session Manager should be associated with. Call traffic segregation could be based on the VLAN that the Session Manager is associated with.

Monitoring

Button	Description
Enable Monitoring	If this check box is selected, it enables monitoring of the administered SIP entities by the added Session Manager instance. If the check box is not selected, monitoring is disabled.
Proactive cycle time (secs)	Time in seconds for polling the administered SIP entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. These default values are used for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.
Reactive cycle time (secs)	Time in seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.
Number of Retries	This integer value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default is 1. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the NRP SIP Entities page for a specific entity.

CDR

Name	Description
Enable CDR	This controls whether CDR is enabled at the system level for that Session Manager instance. If CDR is enabled, you can individually control call detail

Name	Description
	recording for specific SIP entities using the Call Detail Recording drop-down menu.
User	User name.
Password	This password is used to access the CDR record and retype to confirm the password. This password is used by an external CDR processing adjunct for connecting to Session Manager and to transfer the generated CDR files. Normally the adjunct logs in with the "CDR_User" user ID with a default password. The password that you specify here becomes the default password. Once the CDR adjunct logs in using "sftp", it is Local host name resolution Installing and Administering Session Manager June 2009 91 automatically placed in the Session Manager CDR home directory of the CDR_User, which is /var/home/ftp/CDR.
Confirm Password	Type the same password to confirm if you changed the password in the **Password** field.

Personal Profile Manager (PPM) - Connection Settings

Name	Description
Limited PPM client connection	Enables selecting **Maximum Connection per PPM client**. Default value is Enabled.
Maximum Connection per PPM client	Valid values are integers between 1 and 10. Default value is 3.
PPM Connection Timeout (mins)	Valid values are integers between 1 and 600. Default value is 5.
PPM Packet Rate Limiting	Enables selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
PPM Packet Rate Limiting Threshold	This value is applied per PPM client. Value Range: 1-500, default value: 50.

Event Server

Name	Description
Clear Subscription on Notification Failure	Specifies the option to clear Subscription on Notification Failure.

Button	Description
Cancel	Cancels the Session Manager editing operation.
Commit	Saves the Session Manager instance with the modified configuration options.

Related topics:

Modifying the Session Manager administration settings on page 455

Delete Confirmation page field descriptions

Button	Description
Delete	Deletes the selected SIP entity earlier added as a Session Manager instance, but does not delete the entity itself
Cancel	Cancels the deletion of the selected SIP entity as a Session Manager instance

Related topics:

Deleting a SIP entity as a Session Manager instance on page 457

Saving Global Session Manager Settings

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Session Manager Administration** to open the Session Manager Administration screen.
2. On the Session Manager Administration screen, click **Save Global Settings** to configure global settings of all the configured session manager instances.
3. Click the **Authenticate Emergency Calls** checkbox to specify whether emergency calls need to authenticated or not. If the user needs to support emergency calling from unregistered phones, they can uncheck this option to support this functionality.

Network Configuration

Local Host Name Resolution

About Local Host Name Resolution

To route a SIP INVITE, Session Manager needs the IP addresses corresponding to the Fully Qualified Domain Name (FQDN) in the INVITE. To resolve a host name by replacing it with its IP address, Session Manager checks for the host name on the local network. When the host name cannot be resolved through broadcasting on the local network, Session Manager

searches for it in the host names file or by querying the DNS server that maintains the host name to IP address mapping.

Resolving local host name

The Local Host Name Resolution screen allows you to create, edit, and delete local host name entries. Host name entries on this screen override the information provided by DNS.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. To add a host name entry, click **New**.
3. Enter host name information on the New Local Host Name Entries screen as follows.

   You can enter a maximum of ten host names.

   - **Host name**: Name of the host that is to be modified in the local host name table. The host name entries override the information provided by DNS.
   - **IP Address**: IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
   - **Port**: Port number that the host should use for routing using the particular IP address.
   - **Priority**: If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
   - **Weight**: If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
   - **Transport**: The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default is TLS.
4. Click **Commit** to save the host name entry to the host name table.

Local Host Name Resolution page field descriptions

Button	Description
New	Opens the New Local Host Name Entries page that allows you to add new local hosts

Button	Description
Edit	Opens the Edit Local Host Name Entries page that allows you to modify the selected local hosts
Delete	Opens the Delete Local Host Name Entries Confirmation page that allows you to confirm or cancel the deletion of the selected local hosts

Name	Description
Host name	Is the name of the host that is to be modified in the local host name table. The host name entries override the information provided by DNS.
IP Address	Shows the IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
Port	Shows the port number that the host should use for routing using the particular IP address.
Priority	If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
Transport	Shows the transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default is TLS.

New Local Host Name Entries page field descriptions

Name	Description
Host Name	Name of the host that is to be added to the local host name table. The added host name entries override the information provided by DNS. You can add a maximum of ten entries on a page.
IP address	IP address that the host name is mapped to
Port	Port number that the host should use for routing using the particular IP address
Priority	If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
Transport	The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default is TLS

Button	Description
Cancel	Cancels the addition of the new host name entry to the local host name table
Commit	Saves the addition of the new host name entry to the local host name table

Edit Local Host Name Entries page field descriptions

Name	Description
Host Name	Name of the host that is to be modified in the local host name table. The host name entries override the information provided by DNS.
IP address	IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
Port	Port number that the host should use for routing using the particular IP address.
Priority	If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
Transport	The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default is TLS.

Button	Description
Cancel	Cancels the modification of the host name entry to the local host name table
Commit	Saves the modified host name entry to the local host name table

Delete Local Host Name Entries Confirmation page field descriptions

Button	Description
Cancel	Cancels the deletion of the selected local host name from the local host name entries table
Delete	Deletes the selected local host name from the local host name entries table

SIP Firewall

About SIP Firewall Configuration

SIP firewall controls the SIP traffic. The SIP firewall sits at the front end of the Session Manager to control what SIP traffic is allowed into the SIP Application Server. SIP firewall secures the SIP traffic by using rules to allow or drop SIP messages based on their sender, location, and other defined criteria.

Session Manager stores the current firewall settings for each Session Manager instance in a separate file on the System Manager. System Manager uses this file to display the firewall Configuration. It also stores and displays a previous and default configuration. You can modify the displayed firewall configuration.

Configuring the SIP Firewall

1. From the System Manager navigation pane, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Click the **Session Manager Instances** button to display the list of Session Manager instances.

   Select a Session Manager instance from the list. Select **More Actions** to retrieve current, default, or backup configuration or to save a configuration as a backup configuration. By default, the system displays the default configuration of the SIP Firewall.
3. To use the default rules, select **Retrieve Default Configuration** under **More Actions** and click **Save** to save the configuration to the selected Session Manager instance(s).
4. Under Rules, you can perform the following Rule-based operations:
   - **New** —To create a new rule, click **New**. You can define up to 50 rules. For information about creating rules, see .
   - **Edit** —To modify an existing rule, select the left-most check box and click **Edit**.
   - **Delete** —To delete a rule, select a rule and click **Delete**.
   - **Enabled** —To enable or disable all the rules, select or clear the **Enabled** check box.
   - Select a rule from the list and click **Up** or **Down** to move the rule and change the order in which it gets executed.

5. Under Blacklist, specify the following:
    - **Enabled**—Select **Enabled** to drop messages from untrusted hosts.
    - **Key**—Select a key for filtering messages for blacklisting from Remote IP address, CONTACT, and FROM.
    - **Value**—Value of the Key. Specify the following values.
        - Remote IP address—IP address of the host from where the messages are sent.
        - CONTACT—String to look for in the “Contact” SIP Header in the SIP message. This string need not be an exact match with the “Contact” SIP header content and can be a subset of the string present in the “Contact” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
        - FROM—String to look for in the “From” SIP Header in the SIP message. This string need not be an exact match with the “From” SIP header content and can be a subset of the string present in the “From” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
    - **Mask**—Specify the Subnet mask only when you have used the Remote IP address in the Key. This can be used to Blacklist an entire IP subnet.
    - **New**—Create a new rule to drop messages from untrusted hosts. You can create up to 200 Blacklist rules.
    - **Delete**—Delete a selected blacklist rule.
6. Under Whitelist, specify the following:
    - **Enabled**—Select **Enabled**to allow messages from trusted hosts to bypass the SIP Firewall.
    - **Key**—Select a key for filtering messages for whitelisting from Remote IP address, CONTACT, and FROM.
    - **Value**—Value of the Key. Specify the following values.
        - Remote IP address—IP address of the host from where the messages are sent.
        - CONTACT—String to look for in the “Contact” SIP Header in the SIP message. This string need not be an exact match with the “Contact” SIP header content and can be a subset of the string present in the “Contact” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
        - FROM—String to look for in the “From” SIP Header in the SIP message. This string need not be an exact match with the “From” SIP header

content and can be a subset of the string present in the “From” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.

- **Mask**—Specify the Subnet mask only when you have used the Remote IP address in the Key. This can be used to Whitelist an entire IP subnet.
- **New**—Create a new rule to allow messages from trusted hosts.
- **Delete**—Delete a selected whitelist rule.

7. Before enabling SIP Firewall, you must add the following IP addresses to the Whitelist.

   These IP addresses are used by the Session Manager SIP Server. Adding them to the Whitelist ensures that SIP filtering rules are not applied on the outgoing traffic from Session Manager SIP Server and are only applied to the incoming SIP traffic from Network.

   - 19.2.11.13.2 (added as a part of default rules)
   - Session Manager Management IP address

8. Click **Save** to save the SIP Firewall configuration.

   After saving, you can review the results of the configuration changes to the SIP Firewall using **Monitoring** > **Logging** from the System Manager navigation pane. (See *Maintaining and Troubleshooting Avaya Aura™ Session Manager* for specific details of the log messages.)

Related topics:

Firewall Configuration page field descriptions on page 473
Blacklist on page 476
Whitelist on page 476
Rules on page 476
Rule precedence and traversal on page 483

Firewall Configuration page field descriptions

Name	Description
Version	The version of the XML file.
Description	Description for the SIP firewall.
Session Manager Instances: More Action	Allows you to select a Session Manager instance from the list and to retrieve current, default, or backup configuration or to save a configuration as a backup configuration. By default, the default configuration of the SIP firewall is displayed.
Rules: Enabled	Allows you to select or clear the check box to enable or disable rules.

Name	Description
Rules: Name	Name of the SIP firewall rule. The name can have a maximum of 80 characters.
Rules: Action Type	Allows you to select one of the following action types for the rule: • None — No specific action required. This action can be used when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the None action. • Permit — If the rule conditions are fulfilled, allow the SIP message to pass through the SIP Firewall. • Drop — If the rule conditions are fulfilled, drop the SIP message • Rate Block —If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout (as defined by the Threshold parameters). • Rate Limit-If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of remaining period (as defined by the Threshold parameters).
Rules: Log Type	Allows you to specify if a log is to be generated or not, and if an alarm should be sent. You must specify Log Type when the Action Type is None. • No — Do not save the rule to a log file • Yes — Save the rule to a log file • Alarm — If it is possible, generate an alarm when the rule conditions are met
Rules: Log Message	The message that should be logged when the log type is “Yes” or “Alarm”
Blacklist: Enabled	Enables the dropping of messages from untrusted hosts.
Blacklist: Key	Allows you to select a key for filtering messages for blacklisting from the following: Remote IP address, CONTACT, and FROM.
Blacklist: Value	Value of the Key • Remote IP address — IP address of the host from where the messages are sent. • CONTACT ——String to look for in the “Contact” SIP Header in the SIP message. This string need not be an exact match with the “Contact” SIP header content and can be a subset of the string present in the “Contact” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. • FROM — String to look for in the “From” SIP Header in the SIP message. This string need not be an exact match with the “From” SIP header content and can be a subset of the string present in the “From”

Name	Description
	SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
Blacklist: Mask	Specify the Subnet mask only when you have used the Remote IP address in the Key. This can be used to Blacklist an entire IP subnet.
Whitelist: Enabled	Enables the allowing of messages from trusted hosts to bypass the SIP firewall.
Whitelist: Key	Allows you to select a key for filtering messages for whitelisting from the following: Remote IP address, CONTACT, and FROM.
Whitelist: Value	Value of the Key • Remote IP address — IP address of the host from where the messages are sent. • CONTACT —String to look for in the “Contact” SIP Header in the SIP message. This string need not be an exact match with the “Contact” SIP header content and can be a subset of the string present in the “Contact” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. • FROM — String to look for in the “From” SIP Header in the SIP message. This string need not be an exact match with the “From” SIP header content and can be a subset of the string present in the “From” SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
Whitelist: Mask	Subnet mask used for the whitelist operation.

Button	Description
Rules: New	Opens the Rules page which enables you to define a new SIP firewall rule.
Rules: Edit	Opens the Rules page which enables you to edit the selected SIP firewall rule.
Rules: Delete	Allows you to delete a selected rule or rules.
Rules: Up	Allows you to move a selected rule up in the list.
Rules: Down	Allows you to move a selected rule down in the list.

Button	Description
Blacklist: New	Allows you to create a rule for dropping messages from untrusted hosts.
Blacklist: Delete	Deletes the selected Blacklist rule.

Button	Description
Whitelist: New	Allows you to create a rule for allowing messages from trusted hosts to bypass the SIP firewall.
Whitelist: Delete	Deletes the selected Whitelist rule.

Button	Description
Save	Saves the changed SIP firewall configuration settings.

Blacklist

SIP Blacklist enables you to block any known bad SIP elements. The SIP Firewall drops any SIP packet matching a rule in the Blacklist.

Whitelist

SIP Whitelist enables you to allow any known good SIP elements. SIP Firewall allows any SIP packets matching a rule in the Whitelist; no other filtering rule is applied.

Rules

Each SIP Firewall rule has the capability to send log or alarm messages to the Secure Access Link (SAL). You can combine logging with other actions. Avaya recommends that you always enable logging in each SIP Firewall rule to have a record of what actions were taken by the SIP Firewall. Logging can be used independently (with the None action) and can generate logs and alarms for flood-tracking. Note that SIP Firewall log messages are rate-limited. Each rule can log a maximum of 1 log message per second. This rate-limiting of log messages provides protection from flooding the logging system which may occur because of bad configuration of the SIP Firewall rule.

You can apply SIP filtering and DoS protection to:

- SIP gateway/proxy connections (SIP Multiplexed connection/trunk). For example, a SIP Firewall rule can set rate limit on a number of INVITE messages from a specific user within a SIP connection from a SIP gateway without affecting the traffic from other users in that gateway.
- SIP TLS connection. SM100 decrypts all the incoming SIP TLS packets before any filtering rules are applied by the SIP Firewall.
- Reporting using the Secure Access Link (SAL)

Related topics:

Specifying a new SIP Firewall rule on page 477
Rule page field descriptions on page 479
Deep inspection filtering on page 482
Denial of Service protection on page 483
SIP Firewall default rule set on page 483

Specifying a new SIP Firewall rule

1. From the navigation pane, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. On the Firewall Configuration screen, under Rules, click **New**.
3. Under General, specify the following options:
    - Enabled—Select or clear the check box to enable or disable this rule for the selected Session Manager.
    - Name—Name of the rule. The name can have a maximum of 80 characters.
    - Action Type—Specify the action to be taken if rule conditions are met. The valid action types are:
        - None—No specific action required. This action can be used when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the None action.
        - Permit—If the rule conditions are fulfilled, allow the SIP message to pass through the SIP Firewall.
        - Drop—If the rule conditions are fulfilled, drop the SIP message.
        - Rate Block—If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout (as defined by the Threshold parameters).
        - Rate Limit—If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of remaining period (as defined by the Threshold parameters).
    - Log Type—Specify if a log is to be generated or not, and if an alarm should be sent. You must specify Log Type when the Action Type is None.
4. Under IP Layer Match Options, specify the following:
    - Protocol—Select a protocol if you want the rule to be used for a specific protocol.
    - Remote IP Address—For any incoming SIP message, select Any to use the rule for all IP addresses, or select Specify to use the rule for a specific IP address.
    - IP Address—Type the IP address if you selected Specify for Remote IP Address.
    - Mask—Network mask for the specific IP address.
    - Remote Port—For any incoming SIP message, select Any to use the rule for all ports, select Specify to use a single port, or select Specify Range for a range of ports.

- Start—For the Specify option, select a port number. For the Specify Range option, specify the port number to start the range.
- End—For the Specify Range option, specify the port number to end the range. The range includes both the Start and End port numbers specified.
- Local Port—For any incoming SIP message, select Any to use the rule for all ports, select Specify to use a single port, or select Specify Range for a range of ports.
- Start—For the Specify option, select a port number. For the Specify Range option, specify the port number to start the range.
- End—For the Specify Range option, specify the port number to end the range. The range includes both the Start and End port numbers specified.

5. Under SIP Layer Match Options, specify the following:
   - Key Type—Select the key type that the rule should match from the list. You can add up to five key type match options. If more than one match options are defined, then logically, AND of the options is used to create a search pattern.
     - All SIP Headers—This option searches for the Value within all the SIP headers for the SIP packet
     - All SIP Headers/Body—This option searches for the Value in the SIP headers & body portions for the SIP packet
     - REQUEST-METHOD, RESPONSE-CODE—All the remaining entries in the Key Type list are SIP headers and look for the value within the specified SIP header only.
   - Value Type—Specify whether the key type is a string or a regular expression. You can create regular expressions using the PERL version 5.8 syntax.
   - Value—Value of the selected key type. This string need not be an exact match and can be a subset of the string present in the SIP header being used for search.
6. Under IP/SIP Layer Track, select an option for tracking SIP messages only if you have selected either Rate Block or Rate Limit in the Action Type field or with None in the Action Type with Log Type enabled. You cannot use IP/SIP Layer Track with Permit/Drop Actions. This option provides advanced flood tracking in the SIP Firewall. Refer to the SIP Firewall Configuration Section in the Avaya Aura Security Guide for details and examples on using IP/SIP Layer Track
   - None—No tracking used.
   - Remote IP address—Track messages for a specific IP address of the remote host.
   - Local Port—Track messages for a specific local port.
   - From—Track messages for a specific sender.
   - To—Track messages sent to a particular receiver.

- Contact—Track messages for a specific contact.
- Request URI—Track messages for a specific request-URI.

7. Under Threshold, specify the following options only if you have selected either Rate Block or Rate Limit in the Action Type field or with None in the Action Type with Log Type enabled. You cannot use Threshold with Permit/Drop Actions.
   - Count (packets)—Threshold for the number of matching packets. The value can range from 10 to 100000. The default value is 20.
   - Period (secs)—Threshold for the period for matching packets. The value can range from 1 to 60. The default value is 20.
   - Timeout (secs)—Action timeout in seconds. Specify Timeout only if you have selected the Rate Block action. The value can range from 30 to 36000. The default value is 900.
8. Under Connection Type, select from one of the following options:
   - **Any:** This is a default choice. If this option is selected, SIP Firewall rule will be matched against all incoming SIP Traffic
   - **SIP UA Connection:** If this option is selected, SIP Firewall rule will be matched against the incoming SIP traffic from entities that are not the Trusted SIP Entity (as defined by the Network Routing Policy). This option is suitable for creating SIP Firewall filtering rules for SIP telephones that are directly connected to Session Manager.

   NRP Trusted SIP Entity: If this option is selected, SIP Firewall rule will be matched against the incoming SIP traffic from entities that are marked as Trusted SIP Entity in the Network Routing Policy.

   Note:

   If there are any untrusted SIP Entities connected to the Session Manager (as defined by Network Routing Policy), these entities will be treated/filtered as SIP UA connection by SIP Firewall (if there are any rules defined and enabled in SIP Firewall with connection type as SIP UA connection). If this behavior is undesirable, specific rules can be added for the untrusted SIP Entity IP Address/port. These rules shall be defined before SIP Firewall rules for SIP UA connection (Note: SIP Firewall traverse rules in the rule list from top to bottom).
9. Click **Commit** to save the rule or **Cancel** to cancel the changes.

   This does not save the SIP Firewall configuration to the Session Manager. To save the configuration to the Session Manager after creating or editing the configuration, return to the SIP Firewall Configuration screen and click **Save**.

Rule page field descriptions

General:

Name	Description
Enabled	Allows you to select or clear the check box to enable or disable this rule.
Name	Name of the SIP firewall rule. The name can have a maximum of 80 characters.
Action Type	Allows you to select one of the following action types for the rule: • None — No specific action required. This action can be used when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the None action. • Permit — If the rule conditions are fulfilled, allow the SIP message to pass through the SIP Firewall. • Drop — If the rule conditions are fulfilled, drop the SIP message • Rate Block —If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout (as defined by the Threshold parameters). • Rate Limit-If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of remaining period (as defined by the Threshold parameters).
Log Type	Allows you to specify if a log is to be generated or not, and if an alarm should be sent. You must specify Log Type when the Action Type is None. • No — Do not save the rule to a log file • Yes — Save the rule to a log file • Alarm — If it is possible, generate an alarm when the rule conditions are met
Log Message	The message that should be logged when the log type is “Yes” or “Alarm”

IP Layer Match Options:

Name	Description
Protocol	Allows you to select the protocol for which the rule is to be used.
Remote IP Address	For any incoming SIP message, you can select **Any** for using the rule for all IP addresses, or select **Specify** to use the rule for a specific IP address.
IP Address	Allows you to type the IP address if you selected **Specify** for Remote IP Address.
Mask	Network mask for the specified IP address
RemotePort	Allows you to select **Any**, **Specify**, or **Specify Range** to enter a single port or a range of ports
Start	For the **Specify** option, you can select a port number.

Name	Description
	For the **Specify Range** option, you can specify the port number to start the range.
End	For the Specify Range option, you can specify the port number to end the range.
Local Port	Allows you to select **Any**, **Specify**, or **Specify Range** to enter a single port or a range of ports.
Start	For the **Specify** option, you can select a port number. For the **Specify Range** option, you can specify the port number to start the range.
End	For the **Specify Range** option, you can specify the port number to end the range. The range includes both the Start and End port numbers specified.

SIP Layer Match Options:

Name	Description
KeyType	Allows you to select the key type that the rule should match from the list. You can add up to five key type match options. If more than one match options are defined, then logically, AND of the options is used to create a search pattern. All SIP Headers—This option searches for the Value within all the SIP headers for the SIP packet All SIP Headers/Body—This option searches for the Value in the SIP headers & body portions for the SIP packet REQUEST-METHOD, RESPONSE-CODE—All the remaining entries in the Key Type list are SIP headers and look for the value within the specified SIP header only.
ValueType	Allows you to specify whether the key type is a string or a regular expression. You can create regular expressions using the PERL version 5.8 syntax.
Value	Value of the selected key type. This string need not be an exact match and can be a subset of the string present in the SIP header being used for search.

IP/SIP LayerTrack:

Name	Description
Track	Allows you to select an option for tracking SIP messages only if you have selected either Rate Block or Rate Limit in the Action Type field or with None in the Action Type with Log Type enabled. You cannot use IP/SIP Layer Track with Permit/ Drop Actions. This option provides advanced flood tracking in the SIP Firewall.

Name	Description
	Refer to the SIP Firewall Configuration Section in the Avaya Aura Security Guide for details and examples on using IP/SIP Layer Track. • None — No tracking required • Remote IP address — Track messages for a specific IP address of the remote host. • Local Port — Track messages for a specific local port • From — Sender of the message • To — Receiver of the message • Contact ——Track messages for a specific contact. • Request URI — URI of the called party

Threshold:

Name	Description
Count (packets)	Threshold for matching packets. The value can range from 10 to 100000. The default value is 20. Specify this value only for the Rate Block and Rate Limit Action Types.
Period (secs)	Threshold for period for matching packets. The value can range from 1 to 60. The default value is 20. Specify this value only for the Rate Block and Rate Limit Action Types.
Timeout (secs)	Action timeout in seconds. The value can range from 30 to 36000. The default value is 900. Specify this value only for the Rate Block and Rate Limit Action Types.

Button	Description
SIP Layer Match Options: New	Allows you to create up to five SIP layer match options
SIP Layer Match Options: Delete	Deletes the selected SIP layer match options
Cancel	Cancels the defining of the rule
Commit	Saves the defined rule and saves it when the SIP firewall configuration is saved

Deep inspection filtering

SIP Firewall rules provide the following filters for deep inspection:

- SIP Layer content
- IP/Transport layer parameters such as IP address, protocol, port, and so on

You can combine both SIP Layer content and IP transport layer parameters in a single firewall rule. For example, a SIP Firewall rule can limit the high rate of INVITE packets from a remote IP address.

Denial of Service protection

SIP Firewall provides protection from the Denial of Service (DoS) attacks as follows:

- Flood Protection from a specified source
- Advanced Flood Protection—A rule may be defined to detect/mitigate flood attacks within the live SIP Stream without knowing the flood source in advance. In other words, the host causing the flood need not be known when the rule is configured. A high performance database tracks all matched messages.
- Rate-Limiting—A “Rate Limit” action may be configured to limit the number of SIP packets that are forwarded within a given period. Refer to the section Specifying a new SIP Firewall rule for details on how to configure Rate Limit rules.
- Rate-Blocking—A “Rate Block” action may be configured to completely block an offending SIP source once the traffic reaches a specified threshold within a given period. Traffic is then blocked until the configured timeout expires. Refer to the section Specifying a new SIP Firewall rule for details on how to configure the Rate Block rules.
- Signature Detection—A rule may be configured to perform signature detection and drop those packets matching signature. Both simple and regular-expression string searching is supported across the entire SIP header region of the message or across the full message (headers and body).

SIP Firewall default rule set

SIP Firewall provides a default rule set. Avaya recommends that default rules be used after the initial installation of Session Manager.

- 192.11.13.2 (added as a part of default rules)
- Session Manager Management IP address

Rule precedence and traversal

The precedence order for using the rules is:

- Blacklist
- Whitelist
- Rules

Each list above can contain more than one rule. Session Manager traverses the rules within any of the above lists from top to bottom.

SIP Firewall is a packet-based filtering engine. Any time a packet is matched with a rule, the rule traversal is stopped and the packet is either permitted or dropped as per the rule action. The only exception to this is the rules defined with a None Action.

Device and Location Configuration

Device Settings Groups

Device Settings Groups

Device Settings Groups module allows you to manage some of the configuration data for Avaya terminals. These device settings are associated in groups or in a default group and can be assigned to one or more terminals or locations. Location Device Settings Groups can be associated with Locations while Terminal Device Settings Groups can only be associated with terminals respectively. When the terminal is set up for the first time, it is set up with a pre-provisioned group called Default Group which provides the global settings across locations and terminals.

A terminal can be individually associated with a set of Device Settings.

- The endpoint configuration of a terminal depends on the "Default Device Settings" if the terminal
  - does not belong to an “Network Routing Policy Location”
  - or the “Network Routing Policy Location” where the terminal is located has no specific set of Personal Profile Manager (PPM) attributes
  - is administered with Default GROUP of "0"
- The endpoint configuration of a terminal depends on the set of attributes defined for a “Network Routing Policy Location” if the terminal
  - is located in that “Network Routing Policy Location”
  - and the terminal is not individually associated with a specific set of PPM attributes
- The endpoint configuration of a terminal depends on a specific set of PPM attributes if the terminal

  is individually associated with a set of PPM attributes

Viewing Device Settings Groups

From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open

Device Settings Groups screen. The Device Settings Groups screen displays the list of Device Settings Groups.

Related topics:

Device Settings Groups field descriptions on page 488

Creating a Device Settings Group - Location Group

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups screen.
2. Click **New** > **Location Group** to open the Device Settings Group screen.
3. On the Device Settings Group screen, enter the appropriate information about the Location Group.
4. Click **Save** to create a Location Group.
5. Click **Restore** to clear the data entered in the fields.

Related topics:

Device Settings Groups field descriptions on page 488
Device Settings Group - Location Group field descriptions on page 489

Modifying a Device Settings Group - Location Group

You can modify only one Location Device Settings Group at a time.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open the Device Settings Groups screen.
2. Select an Location Group and click **Edit** to open the Device Settings Group screen.
3. On the Device Settings Group screen, modify the appropriate information to update the Location Group details.
4. Click **Save** to save the changes to the Location Group.
5. Click **Restore** to clear the data entered in the fields

Related topics:

Device Settings Groups field descriptions on page 488
Device Settings Group - Location Group field descriptions on page 489

Removing Device Settings Groups - Location Groups

You cannot delete the default Location Device Settings Group.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups screen.
2. Select one or more Location Groups and click **Delete** to delete one or more Location Groups.

Related topics:

Device Settings Groups field descriptions on page 488
Device Settings Group - Location Group field descriptions on page 489

Creating a Device Settings Group - Terminal Group

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups screen.
2. Click **New** > **Terminal Group** to open the Device Settings Group screen.
3. On the Device Settings Group screen, enter the appropriate information of the new Terminal Group.
4. Click **Save** to create a new Terminal Group.
5. Click **Restore** to clear the data entered in the fields.

Related topics:

Device Settings Groups field descriptions on page 488
Device Settings Group - Terminal Group field descriptions on page 490

Modifying a Device Settings Group - Terminal Group

You can modify only one Terminal Device Settings Group at a time.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open the Device Settings Groups screen.
2. Select an Terminal Device Setting Group and click **Edit** to open the Device Settings Group screen.
3. On the Device Settings Group screen, modify the appropriate information.
4. Click **Save** to save the changes to the Terminal Device Setting Group.
5. Click **Restore** to clear the data entered in the fields.

Related topics:

Device Settings Groups field descriptions on page 488
Device Settings Group - Terminal Group field descriptions on page 490

Removing Device Settings Group - Terminal Group

You cannot delete the default Terminal Device Settings Group.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups screen.
2. Select one or more Terminal Groups and click **Delete** to delete one or more Terminal Device Settings Groups.

Related topics:

Device Settings Groups field descriptions on page 488
Device Settings Group - Terminal Group field descriptions on page 490

Purpose and usage of SIP subscriptions

SIP Subscription and Notification requests update connected SIP endpoints on state changes related to services that the endpoints consume. For example, when a new voice message

arrives in a mailbox, Session Manager sends a SIP notification request to notify the related endpoints about the arrival of a new voice mail message.

For an endpoint to receive SIP notifications, it first needs to subscribe to the relevant subscription package. Each subscription package is related to a specific service that the network delivers to the endpoint. The SIP endpoints automatically establish all required subscriptions upon logging into the network.

When a subscription to an event package (service) is established, it is assigned with a subscription expiration timer. The endpoint continues to receive notifications as long as the expiration timer does not expire. The endpoints automatically refresh any subscriptions before their expiration timer expires. A lower subscription expiration timer generates more SIP traffic related to subscription refresh events. Refreshing a subscription updates the state of the subscription.

Session Manager allows administration of the subscription expiration timer for each type of event package.

Device Settings Groups field descriptions

Device Settings Groups page enables the user to create and manage device configuration groups.

Name	Description
Name	Is the name of the Device Settings Group.
Terminal Group Number	Is a numeric ID for this group. Using a group ID you can identify different phones on your network for ease of administration. With the exception of the field Group ID, Group parameters are the same as those for common phone parameters. Numeric IDs must be between 0 and 999.
Description	Shows the details of Device Settings Group.

Related topics:

Viewing Device Settings Groups on page 484
Creating a Device Settings Group - Location Group on page 485
Modifying a Device Settings Group - Location Group on page 485
Removing Device Settings Groups - Location Groups on page 486
Creating a Device Settings Group - Terminal Group on page 486
Modifying a Device Settings Group - Terminal Group on page 487
Removing Device Settings Group - Terminal Group on page 487

Device Settings Group - Location Group field descriptions

General section—these fields cannot be edited for Default Group

Name	Description
Name	Is the name of the Location Device Settings Group.
Description	Shows Location Device Settings Group details.
Group Type	Is a non-editable field specifying the type of Device Setting as Location Group

Server Timer section

Name	Description
Avaya Feature Status - Subscription Expiration Timer (secs)	Is a required field and shows the duration for a SIP client to be subscribed. This event package is used to update the endpoint on state changes related to features the logged-in user is associated with. For example, a notification is generated when any of call forwarding preferences associated with the logged-in user changes. Range is 1 to 86400 seconds and the default is 86400 seconds.
Dialog State - Subscription Expiration Timer (secs)	Is a required field and shows the duration for a SIP client to be subscribed. This event package is used to update the endpoint on state changes related to line and call appearances used by the logged-in user. Range is 1 to 86400 seconds and the default is 86400 seconds.
Message Waiting - Subscription Expiration Timer (secs)	Is a required field and shows the duration for a SIP client to be subscribed. This event package is used to update the endpoint on the state of the voicemail mailbox associated with the logged-in user. Range is 1 to 86400 seconds and the default is 86400 seconds.
PPM - Subscription Expiration Timer (secs)	Is a required field and shows the duration for a SIP client to be subscribed.) This event package is used to update the endpoint on the state changes to the centrally stored profile of the logged-in user. For example, a notification is generated upon change to the feature list associated with the logged-in user. Range is 1 to 86400 seconds and the default is 86400 seconds.
Reg Event - Subscription Expiration Timer (secs)	Is a required field and shows the duration for a SIP client to be subscribed. This event package is used to update the endpoint on the state of registration events associated with the logged-in user. For example, a notification is generated when the logged-in user establishes a registration through another device. Range is 1 to 86400 seconds and the default is 86400 seconds.

Assigned Location section

Name	Description
Name	Is the name of the location to which the Device Group Settings is associated.

Related topics:

Creating a Device Settings Group - Location Group on page 485
Modifying a Device Settings Group - Location Group on page 485
Removing Device Settings Groups - Location Groups on page 486

Device Settings Group - Terminal Group field descriptions

General section—these fields cannot be edited for Default Group

Name	Description
Name	Is the name of the Terminal Device Settings Group.
Description	Shows Terminal Device Settings Group details.
Group Type	Is a non editable field specifying the type of Device Setting as Terminal Group

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Is a required field and specifies the maximum duration, range is 30 to 240 seconds, for a SIP server that a SIP line appearance can be reserved for. If no value is entered, the default value is 30 seconds.
Dialog State - Subscription Expiration Timer (secs)	Is a required field and specifies how often (in seconds) the phone attempts to register with a proxy server when it is not reachable or available. Range is 10 to 3600 seconds. The default is 60 seconds.
Message Waiting - Subscription Expiration Timer (secs)	Is a required field and specifies how long (in seconds) the phone waits for a provisional response after transmitting a SIP INVITE to a proxy server before checking that proxy is unavailable/ unreachable and proceeding to another proxy. The range is 0 to 32 seconds. (0 disables this feature.) The default is 2 seconds.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	Specifies the IP address of a server that can query the phone for SNMP messages. This server must have the correct community string. If this field is blank, any server can query the phone.

Name	Description
SNMP Community	Specifies the SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified, both the server and the phone must have the same community name administered. Only alphabetic characters are allowed and length cannot exceed 32 characters.
Station Admin Password	Specifies the code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted as code and length cannot exceed 32 digits.
Quick Login Status: Password Entry Required Quick Login Allowed	Specifies the whether users must enter a password when logging in to the phone. There are 2 choices: Password Entry Required or Quick Login Allowed

VoIP Monitoring Manager section

Name	Description
IP Address	Specifies the IP address of the Avaya Voice over IP Monitoring Manager server.
Port	Specifies the port used by the Avaya Voice over IP Monitoring Manager server. The range is 1 through 65,535. The default is 5005.
Reporting Period	Specifies how often an endpoint should send its RTCP packets to the Avaya Voice over IP Monitoring Manager server. The range is 5 through 30 seconds. The default is 5.

Volume Settings section

Name	Description
Receiver Volume	Sets the volume in the handset rather than the speaker. This is a required field and range is 0-10. The default value is 5.
Ringer Cadence	Sets the cadence of the ring tone. This is a required field and range is 1-8. The default value is 3.
Ringer Volume	Sets the ringer setting for the stations bridged appearance buttons. This is a required field and range is 1-10. The default value is 5.
Speaker Volume	Sets the volume on the speaker rather than the handset. This is a required field and range is 0-10. The default value is 5.

Related topics:

Creating a Device Settings Group - Terminal Group on page 486
Modifying a Device Settings Group - Terminal Group on page 487
Removing Device Settings Group - Terminal Group on page 487

Location Settings

Location Settings

Location Settings module enables you to assign a Device Setting Group to a Location.

Viewing location settings

From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Location Settings** to open Location Settings screen. The Location Settings screen displays the list of location settings.

Related topics:

Location Settings field descriptions on page 492

Modifying Location Settings

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Device and Location Configuration** > **Location Settings** to open the Location Settings screen.
2. Associate a location with the respective Device Settings Group.
3. Click **Save** to save the changes.

Related topics:

Location Settings field descriptions on page 492

Location Settings field descriptions

Name	Description
Name	Is the name of the Location.

Name	Description
Device Setting Group	Is the name of the Device Setting Group.

Related topics:

Viewing location settings on page 492
Modifying Location Settings on page 492

Application Configuration

Applications

Applications

Enterprise Linux Installer

Subscriber Options

Modular Messaging Web Client

Web Client

Outlook Client

Web Subscriber Options

Data Collection Tool

DCT

Avaya Voice Player

Voice Player

Script Builder

IVR Designer

IVR-D

Message Storage Server (MSS)

Message Application Server (MAS)

System Platform Web Console

one-X Portal

Administration application

Administration Web Client

Administration Command Line Client

Administration Command Line Interface

one-X Portal

one-X Portal Extensions

Avaya Phone Interface

Avaya one-X Portal Message Recorder

Voice Portal

Avaya Voice Browser

Application Interface web service

Application Logging web service

Media Processing Platform

MPP Service Menu

Voice Portal Management System

Viewing applications

From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Applications** to open Applications screen. The Applications screen displays the list of applications.

Creating an application

Prerequisites

Creating a new application entry requires that a non-Session Manager SIP entity first be administered. Refer to the section Creating NRP SIP entities to create the SIP entity.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Applications** to open the Applications screen.
2. Click **New**. The Application Editor screen appears.
3. On the Application Editor screen, enter the appropriate information for the new application.
4. Click **Commit** to create the application.

Related topics:

Applications field descriptions on page 496
Application Editor field descriptions on page 496

Modifying an application

You can modify only one application at a time.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Applications** to open the Applications screen.
2. Select an application and click **Edit** to open the Application Editor screen.
3. On the Application Editor screen, modify the appropriate information.
4. Click **Commit** to save the changes.

Related topics:

Applications field descriptions on page 496
Application Editor field descriptions on page 496

Removing applications

You cannot delete an application if it is a member of an Application Sequence. If you try to delete it, a warning appears, and the application entry remains.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Applications** to open the Applications screen.
2. Select one or more applications and click **Delete** . Delete Confirmation screen appears.
3. On the Delete Confirmation screen, click **Delete** to remove the application entries.

Related topics:

Applications field descriptions on page 496

Applications field descriptions

Use each field to sort or filter records by enabling or disabling Filter feature. Records are filtered on the basis of partial string match and can also be filtered as a combination of one or more fields.

Name	Description
Application Name	Is the name of the application.
SIP Entity	Is the name of the associated SIP Entity.
Description	Provides details about the application.

Related topics:

Creating an application on page 494
Modifying an application on page 495
Removing applications on page 495

Application Editor field descriptions

Application Editor section

Name	Description
Name	Is the name of the application entries. This is a mandatory field.
SIP Entity	Provides a list of previously provisioned SIP entities. This is a mandatory field.
Description	Provides details about the application.

Application Attributes (optional) section — User defined attributes which can only be updated

Name	Description
Application Handle	Is a unique handle for the application. This handle is inserted in the Route header sent by Session Manager when it sequences a call to an application. It is mainly used to distinguish between multiple applications running on the same host.
URI Parameters	Provides a list of URI parameters.

Related topics:

Creating an application on page 494
Modifying an application on page 495

Application Sequences

Application Sequences

Application Sequence enables defining and managing a (sequence ordered) set of applications used in call sequencing. These application sets can be associated as the originating and terminating sets for a registered user's "Communication Profile" in the User Management module. Application sequencing parameters defines the interaction of the user with SIP applications.

Viewing application sequences

From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen. The Application Sequences screen displays the list of Application Sequences.

Creating an Application Sequence

An Application Sequence can contain a maximum of up to 10 applications.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen.
2. Click **New**. The Application Sequence Editor screen appears.
3. On the Application Sequence Editor screen, enter the appropriate information.
4. Click **Commit** to create the Application Sequence.

Related topics:

Application Sequences field descriptions on page 500
Application Sequence Editor field descriptions on page 500

Modifying an Application Sequence

You can modify only one Application Sequence at a time.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen.
2. Select an application sequence and click **Edit** to open the Application Sequence Editor screen.
3. On the Application Sequence Editor screen, modify the appropriate information.
4. Click **Commit** to save the changes.

Related topics:

Application Sequences field descriptions on page 500
Application Sequence Editor field descriptions on page 500

Removing Application Sequences

You cannot delete an Application Sequence, if it is defined as an originating or terminating application set of a communication profile.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen.
2. Select one or more application sequence and click **Delete** . Delete Confirmation screen appears.
3. Click **Delete** to remove the selected application sequences.

Related topics:

Application Sequences field descriptions on page 500
Application Sequence Editor field descriptions on page 500

Rearranging Applications in an Application Sequence

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen.
2. Select an Application Sequence and click **Edit** to open the Application Sequence Editor screen.
3. In the section *Applications in this Sequence* do the following:
   - Click the buttons in the top panel to move selected Applications to the front or back of the Application Sequence or to remove Applications from the Application Sequence.
   - Click the buttons under *Sequence Order (first to last)* to change the relative sequence order of the Applications or to remove Applications from the Application Sequence.

Related topics:

Application Sequences field descriptions on page 500
Application Sequence Editor field descriptions on page 500

Adding Applications in an existing Application Sequence

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen.
2. Select an application sequence and click **Edit** to open the Application Sequence Editor screen.
3. In the section *Available Applications*, click the + button to add the application to the application sequence at the end.

Related topics:

Application Sequences field descriptions on page 500
Application Sequence Editor field descriptions on page 500

Application Sequences field descriptions

The Application Sequence screen enables you to add, edit, or remove sequences of applications.

Name	Description
Name	Is the name of the application sequence.
Description	Provides details about the application sequence.

Related topics:

Creating an Application Sequence on page 497
Modifying an Application Sequence on page 498
Removing Application Sequences on page 498
Rearranging Applications in an Application Sequence on page 499
Adding Applications in an existing Application Sequence on page 500

Application Sequence Editor field descriptions

Sequence Name section

Name	Description
Name	Is the name of the application sequence. This is a mandatory field.

Name	Description
Description	Shows the details about the application sequence .

Applications in this Sequence section — Buttons at the top panel allow you to move selected applications to the front or back of the sequence

Name	Description
Sequence Order (first to last)	Allows you to change the relative sequence order of the applications or to remove applications from the application sequence.
Name	Is the name of the selected application.
SIP Entity	Is the name of the SIP entity associated with the selected application
Mandatory	Specifies whether the application is mandatory or not. If Session Manager fails to reach the application during the sequencing, Session Manager will stop sequencing and send an error response upstream.
Description	Shows the description of the selected application

Available Applications section — This section allows sorting and filtering by application names or SIP entity name. Default sort is by application name and then by SIP entity name.

Name	Description
+	Adds the selected application to the application sequence in the table Application in this Set above.
Name	Is the name of the application.
SIP Entity	Is the name of the SIP entity associated with the application
Description	Shows the description of the application

Related topics:

Creating an Application Sequence on page 497
Modifying an Application Sequence on page 498
Removing Application Sequences on page 498
Rearranging Applications in an Application Sequence on page 499
Adding Applications in an existing Application Sequence on page 500

Implicit Users

Implicit Users

Implicit Users module allows you to administer certain dial patterns for originating and terminating application sequences as rules defined for implicit users. This functionality is used to provide application sequencing for calls either from or to SIP entities and trunks."

Viewing Implicit User Rules

From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Implicit Users** to open Implicit Users screen. The Implicit Users screen displays the list of Implicit User rules.

Related topics:

Implicit User Rules field descriptions on page 503

Creating an Implicit User

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Implicit Users** to open the Implicit Users screen.
2. Click **New**. The Implicit User Rule Editor screen appears.
3. On the Implicit User Rule Editor screen, enter the appropriate information.
4. Click **Commit** to create a new Implicit User rule.

Related topics:

Implicit User Rules field descriptions on page 503
Implicit User Rule Editor field descriptions on page 504

Modifying an existing Implicit User

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Implicit Users** to open the Implicit Users screen.
2. Select an Implicit User rule and click **Edit** to open the Implicit User Rule Editor screen.
3. On the Implicit User Rule Editor screen, modify the appropriate information.
4. Click **Commit** to save the changes to the Implicit User rule.

Related topics:

Implicit User Rules field descriptions on page 503
Implicit User Rule Editor field descriptions on page 504

Removing existing Implicit Users

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **Application Configuration** > **Implicit Users** to open the Implicit Users screen.
2. Select one or more Implicit User rules and click **Delete** to delete one or more Implicit User rules respectively . Delete Confirmation screen appears.
3. On the Delete Confirmation screen, click **Delete** to remove the selected Implicit User rules.

Related topics:

Implicit User Rules field descriptions on page 503

Implicit User Rules field descriptions

Name	Description
Pattern	Shows the dial pattern with the same pattern format as the Network Routing Policy Dial pattern.

Name	Description
Min	Shows the minimum value of the dial pattern matching. Valid values are 1-36.
Max	Shows the maximum value of the dial pattern matching. Valid values are 1-36.
SIP Domain	Shows associated SIP Domain
Origination Application Sequence	Shows Origination Application Sequence
Termination Application Sequence	Shows Termination Application Sequence
Description	Shows the description of the Rule

Related topics:

Viewing Implicit User Rules on page 502
Creating an Implicit User on page 502
Modifying an existing Implicit User on page 503
Removing existing Implicit Users on page 503

Implicit User Rule Editor field descriptions

The Implicit User Rule Editor screen enables you to define a new pattern rule or to modify an existing pattern rule.

Name	Description
Pattern	Shows a dial pattern with the same pattern format as the NETWORK ROUTING POLICY Dial pattern. This is a mandatory field.
Min	Shows the minimum value of the dial pattern matching. Valid values are 1-36. This is mandatory field. The value must be higher than the pattern length.
Max	Shows the maximum value of the dial pattern matching. Valid values are 1-36. This is mandatory field.
Description	Shows the description of the Rule.
SIP Domain	Shows the name of the SIP Domain
Origination Application Sequence	Shows the name of the Origination Application Sequence

Name	Description
Termination Application Sequence	Shows the name of the Termination Application Sequence

Related topics:

Creating an Implicit User on page 502
Modifying an existing Implicit User on page 503

SIP A/S Management Console

About SIP A/S Management Console

The SIP A/S Management Console enables you to administer the SIP A/S and perform the following tasks or activities:

- Viewing Service Host statistics
- Deploying an application
- Deploying security extension for application security
- Monitoring SIP entities
- Adding and removing Service Hosts
- Adding and removing Service Directors

Warning:

You must not change any of the configuration settings which can otherwise void the product warranty.

Starting the SIP A/S Management Console

1. From the navigation pane on the System Manager Common Console, click **Applications** > **SIP A/S 8.1**.
2. On the SIP A/S Connection Details screen, enter the host name and administration port of the primary Management Server of the cluster.
3. Optionally, enter the host name and administration port of the backup Management Server of the cluster.

Note:

If you do not enter details for the backup Management Server, the SIP A/S Management Console uses information stored on the Primary Management Server to connect to the backup Management Server, if available.

4. Click **Connect**.
   The system displays SIP A/S Management Console screen. Refer to SIP A/S Management Console online help for detail documentation.

Viewing collected statistics for Service Host

1. In the SIP A/S Management Console, click **Monitoring** > **Statistics** > **Service Hosts**.
2. To view Service Host instance statistics, select a statistic and click **View**.
3. To view statistics from last 24 hours, select a statistic and click **View Data**.
   The Service Host Statistics screen displays the statistics for the selected Service Host. Refer to the online help for field level descriptions.

System Status

System State Administration

About System State Administration

Before you start a software upgrade of System Manager, you must:

- Back up the database
- Put each Session Manager in the Management Disabled management state.

Before you start a maintenance operation or an upgrade of a Session Manager, you must:

- Put the Session Manager in the Management Disabled management state
- Set the Session Manager to block new incoming calls (set the Deny New Service service state) and wait for active calls to terminate.

Similarly, after completing the Session Manager maintenance or upgrade operation, you must:

- Put the Session Manager in the Management Enabled management state
- Set the Session Manager to allow new calls (set the Accept New Service service state).

The System State Administration page enables you to perform these tasks. In addition, you can use this page to view the following information for each of the configured Session Managers:

- Current management and service states
- Software version information
- Time of the last service state change
- Call count for currently active calls.

Accessing the System State Administration page

The System State Administration page displays the current service and management state of configured Session Managers. You can use this page to make state changes in the context of an upgrade or necessary maintenance.

Select **Session Manager** > **System Status** > **System State Administration** on the System Manager console. The System State Administration screen displays current service and management state of configured Session Managers Instances.

System State Administration page field descriptions

Button	Description
Refresh	Refreshes the System State Administration page with the most recent values of fields.
Management State > Management Disabled	Disables administration of the selected Session Manager or Session Managers but allows call processing for them.
Management State > Management Enabled	Enables administration of the selected Session Manager or Session Managers for which the administration has been previously disabled.

Button	Description
Service State > Deny New Service	Blocks incoming calls for the selected Session Manager or Session Managers but leaves active calls “up”.
Service State > Accept New Service	Allows incoming calls for the selected Session Manager or Session Managers which were previously blocked using a **Deny New Service** request.
Shutdown System > Shutdown	Shuts down the selected Session Manager server or servers.
Shutdown System > Reboot	Reboots the selected Session Manager server or servers.

Name	Description
Session Manager	Name of the Session Manager. Select the adjacent check box to select a Session Manager.
Management State	Displays the current management state of the Session Manager, that is, **Management Enabled** or **Management Disabled**.
Service State	Displays the current service state of the Session Manager, that is, **Deny New Service** or **Accept New Service**.
Last Service State Change	Displays the time stamp for the last service change in the state of the Session Manager.
Active Call Count	Displays how many calls are currently being processed by the Session Manager. This can help you take a maintenance decision or a service state change decision. To get the correct number of active calls before you take a decision, click **Refresh** to refresh this field.
Version	Version of the Session Manager software installed.

Management Enabled Confirmation page field descriptions

Button	Description
Cancel	Cancels the enabling of administration of the selected Session Manager instances
Enable Management	Confirms the enabling of administration of the selected Session Manager instances

Management Disabled Confirmation page field descriptions

Button	Description
Cancel	Cancels the disabling of administration of the selected Session Manager instances
Disable Management	Confirms the disabling of administration of the selected Session Manager instances

Accept New Service Confirmation page field descriptions

Button	Description
Cancel	Processing of new calls is still blocked
Accept New Service	Allows Session Manager to process new calls

Deny New Service Confirmation page field descriptions

Button	Description
Cancel	Cancels the blocking of new calls for processing. Processing of new calls continues.
Deny New Service	Blocks new calls from being processed.

Shutdown Confirmation page field descriptions

Button	Description
Cancel	Cancels the shutdown of the selected Session Manager instances
Shutdown	Confirms the shutdown of the selected Session Manager instances

Reboot Confirmation page field descriptions

Button	Description
Cancel	Cancels the rebooting of the selected Session Manager instances.
Reboot	Confirms the rebooting of the selected Session Manager instances.

SIP Entity Monitoring

Session Manager SIP Entity Monitoring

SIP Entity Monitoring provides background detection for monitored connections to improve alternative routing and minimize the call setup time due to SIP link failures. The SIP Monitor periodically tests the status of the SIP proxy servers. If a proxy fails to reply, SIP messages are no longer routed to that proxy. As a result, call delays will be reduced since calls will not be routed to the failed servers. The SIP Monitor will continue to monitor the failed SIP entity. When the proxy replies, SIP messages will again be routed over that link.

You can turn monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity will not be monitored by any instance.

You can also turn monitoring on or off for an entire instance. If monitoring is turned off, none of the SIP entities will be monitored by that instance. If monitoring for the instance is turned on, only those SIP entities for which monitoring is turned on will be monitored.

The SIP entity being monitored should support the SIP OPTIONS method in order to be monitored.

SIP Monitoring can only report problems if the SM100 Security Module is functional.

SIP Monitoring setup is administered through the Network Routing Policy screens on the System Manager.

Accessing the SIP Monitoring Status Summary page

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager and a SIP entity.

If all of these connections are up, then the entity link status is **up**. If one or more connections are down, but there is at least one connection up, then the link status is **partially down**. If all of the connections are down, the entity link status is **down**.

1. Select **Session Manager** > **System Status** > **SIP Entity Monitoring** on the System Manager console.
2. The **SIP Entity Link Monitoring Status Summary**screen displays the summary of SIP Entity Link monitoring status.

SIP Entity Link Monitoring Status Summary page field descriptions

Button	Description
Entity Link Status for All Session Manager Instances: Refresh	Refreshes the status of the entity links for all administered Session Manager instances. The status displays the following details: • Name of the Session Manager instance • Entity links for the Session Manager that are totally down out of the total number of entity links for the Session Manager • Entity links for the Session Manager that are partially down • SIP entities for which monitoring has not yet started (because it is still being initialized by the Session Manager) • SIP entities that are not monitored (because they are not administered to be monitored by the Session Manager) Clicking any of the Session Managers in the list opens the Session Manager Entity Link Connection Status page that displays detailed connection status for all entity links from a Session Manager where at least one connection is currently down. **Note:** An entity link consists of one or more physical connections between a Session Manager and a SIP entity. If all of these connections are up, then the entity link status is “up”. If one or more connections are down, but there is at least one connection up, then the entity link status is “partially down”. If all the connections are down, the entity link status is “down”.
All Monitored SIP Entities: Refresh	Clicking any of the entities in the list opens the SIP Entity, Entity Link Connection Status page that displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

SIP Entity Entity Link Connection Status page field descriptions

Button	Description
Refresh	Refreshes and displays the detailed connection status for all entity links from the selected Session Manager instance to a single SIP entity. The status displays the following details: • Name of the Session Manager instance • Resolved IP address of the SIP entity • Port used for the connection • Protocol used • Connection status • Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”. • Status of the entity link
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.

Session Manager Entity Link Connection Status page field descriptions

Button	Description
Refresh	Refreshes and displays all entity links for a connection that is down for the selected Session Manager. The status displays the following details: • Name of the SIP entity. Clicking the name field for a SIP entity opens the SIP Entity Entity Link Connection Status page for that SIP entity. • Resolved IP address of the SIP entity • Port that is used for connecting with the SIP entity • Protocol used • Connection status • Reason for connection failure. This field explains how the status of a connection was determined, even if the status is “up” or “down”. • Status of the entity link
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.

Managed Bandwidth Usage

About Managed Bandwidth

The Managed Bandwidth Usage displays Managed Bandwidth (Call Admission Control) real-time data. It displays a read-only table containing one row for each administered location where usage is managed. The row contains current bandwidth usage and maximums and provides an estimated usage percentage and number of calls that can be made before the limits are reached.

You can also expand each row to display a breakdown of usage and capacity by Session Manager, which can be helpful in debugging network utilization or the distribution algorithm. If no bandwidth management is administered, this table contains no data.

Viewing managed bandwidth usage

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **Managed Bandwidth Usage**.

   The Managed Bandwidth Usage screen displays system-wide bandwidth usage information for locations where usage is managed. If the Managed Bandwidth field on the location form is blank, this table has no information for that location.

2. On the Managed Bandwidth Usage screen, click **Refresh** to refresh the data.

Managed Bandwidth Usage page field descriptions

This page displays system-wide bandwidth usage information for locations where usage is managed. If there is no bandwidth management implemented, this table has no information.

Button	Description
Refresh	Refreshes the data in the table for the following columns: • Details — Shows the breakdown of usage among the administered Session Managers in the enterprise. You can click the Show or Hide arrow on any row under **Details** to show or hide the detailed usage for that location. • Location — Locations that you have administered in NRP. • Bandwidth per Call (kbit/sec) — This is the value that you enter in the NRP Location Details page.

Button	Description
	• Bandwidth in Use (kbit/sec) — Current bandwidth used. • Total Bandwidth Available. • Percent Used — Percent of the total bandwidth used. • New Call Capacity — Number of calls that can be made before the maximum bandwidth capacity is reached.

Security Module Status

About Security Module Status

The Security Module Status page allows you to view the status of the security module for each administered Session Manager and to perform certain actions on the security module.

You can view the status of the security module such as its IP address, default gateway, the interface that it uses, the VLAN that it is associated with, the QOS priority, trusted hosts configured for that security module, and the certificate authority.

You can also reset and synchronize the security module, or assign a certificate authority.

Security Module Status actions

The following actions can be performed on a selected Session Manager:

- **Reset** – resets the security module for the selected Session Manager. An administrator may choose to reset the security module when a connection cannot be made to the security module.

  Warning:
  The Session Manager cannot process calls while the security module is being reset. Refer to *Administrating Avaya Aura™ Session Manager*, 03–603324 for details on how to disable the Session Manager prior to resetting the security module.

- **Synchronize** – verifies that the administered configuration matches the actual configuration stored on the security module. This action should be performed anytime the values in the security module statistics table do not match the administered data.

- **Security Module Certificate** - Session Manager provides the capability of switching the active certificate being used by the security module to the default certificate or the unique certificate issued for that instance by the System Manager CA. Please refer to *Administrating Avaya Aura™ Session Manager*, 03–603324 for more details about this

operation. Additionally, refer to **Security Design** in *Administrating Avaya Aura™ Session Manager*, 03–603324 to understand the implications of doing this operation.

Investigating Security Module Deployment “Down” status

Possible causes for the Security Module Deployment status to be **Down** include:

- The security module may have recently been reset. A reset can take several minutes to complete.
- The security module may not have received its configuration information from System Manager. See the Data Replication Status screen for the Session Manager to make sure replication is working, since that is the primary reason the SM100 would not have downloaded its configuration information properly.
- There is a problem with the security module that needs attention.

---

1. Select **Session Manager > System Status > Security Module Status** on the System Manager console.
2. Use the **Refresh** button to see the latest status.
3. If the status is still **Down**, synchronize the security module to trigger an update:
   a. Select the appropriate system from the System Name list.
   b. Select the **Synchronize Security Module** button.
   c. Select the **Refresh** button to see the latest status.
4. If the Deployment status is still **Down**, reset the security module:
   a. Select the appropriate system from the System Name list
   b. Select the **Security Module Reset** Button.

   Warning:

   The Session Manager cannot process calls while the security module is being reset . Refer to System State Administration for details on how to disable the Session Manager prior to resetting the security module.
5. Select the **Refresh** button to see the latest status.

Security Module Status page field descriptions

Button	Description
Refresh	Refreshes the following statistics for all the administered Session Manager instances: • Security Module Deployment—Status of the Security Module deployed for the Session Manager (up or down). • IP Address—IP address of the security module used for SIP traffic. This field should match the address administered on the SIP Entity form for the Session Manager instance. • Network Mask—Network Mask of the security module. This value should match the network mask administered on the Session Manager instance form. • Default Gateway—Default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form. • Interface Name—The Ethernet interface used by the security module for SIP traffic. This field is for informational purposes and is not administrable. • Name Servers—DNS Servers used by the security module. This field is for informational purposes and is not administrable. • DNS Search—DNS search string used by the security module. This field is for informational purposes and is not administrable. • Call Control PHB—The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from SM100 that you may expect as it travels through the IP network. All packets containing SIP signaling which leave the SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence—they must either support this by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority. • Speed & Duplex—Allows the configuring of the security module interface speed and duplex values. The drop-down menu contains a list of the valid values. • VLAN—The VLAN ID that the security module is associated with. This field should match the VLAN ID administered on the Session Manager instance form. • QOS—802.1q priority value (Layer 2 QoS) used by the security module. This field should match the QOS priority administered on the

Button	Description
	Session Manager instance form.priority assigned to the Session Manager. • Certificate Used—The identity certificate being used by the security module for establishing TLS sessions. • Trusted hosts (expected/actual)—The expected value is the number of Trusted SIP Entities configured in Network Routing Policy which have Entity Links to the Session Manager. The actual value is the number of Trusted SIP Entities currently configured on the security module. If these values do not match, then the Synchronize action should be performed.
Security Module Reset	Opens the Security Module Reset Confirmation page.
Synchronize Security Module	Synchronizes the security module of the selected Session Manager.
Security Module Certificate	Select one of the three options: • Update Installed Certificates—Update already installed certificates. • Use Default Certificate (Issued By SIP CA)—Use the default certificate issued by the SIP Certificate Authority. • Use Certificate from System Manager—Use the certificate assigned to the associated System Manager.

Security Module Reset Confirmation page field descriptions

Button	Description
Reset	Resets the security module for the selected Session Manager instance. Please note that while the security module is being reset, the Session Manager cannot process the calls.
Cancel	Cancels the resetting of the security module for the selected Session Manager

Registration Summary

Registration Summary

This module enables you to view the registration status for all AST devices registered to the selected Session Manager Instance. These AST devices are reloaded or rebooted based on the following actions:

- Reset of endpoints
- Full reload of endpoints
- Partial reload of endpoints

Related topics:

Viewing Registration Summary on page 518
Rebooting of selected AST devices on page 518
Reloading of selected AST devices on page 519

Viewing Registration Summary

This module provides the ability to view the basic registration information for a particular device.

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **Registration Summary** to open Registration Summary screen. The Registration Summary screen displays the list of registered devices per Session Manager.
2. Click **Refresh** to retrieve the latest Device Summary results.

Related topics:

Registration Summary on page 518

Rebooting of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **Registration Summary** to open Registration

Summary screen. The Registration Summary screen displays the list of registered devices.

2. Click to select the AST Devices and click **Reboot**. The Confirm Reboot Notification screen appears.
3. On the Confirm Reboot Notification screen, click **Confirm**.
4. After user confirmation, a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions

Related topics:

Registration Summary on page 518

Reloading of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **Registration Summary** to open Registration Summary screen.
2. Click the rows to select the SIP AST Devices and do one of the following:
   a. Click **Reload** > **Reload Complete** to force complete reload of selected SIP AST Devices which includes maintenance data, configuration data, and a complete data reload.

      On the Confirm Reload Complete Notification screen, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

   b. Click **Reload** > **Reload Config** to reload only configuration details of selected SIP AST subscribed devices.

      On the Confirm Reload Config Notification screen, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

   c. Click **Reload** > **Reload Contacts** to reload only contact details of selected SIP AST subscribed devices.

      On the Confirm Reload Contacts Notification screen, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Related topics:

Registration Summary on page 518

Registration Summary field descriptions

Name	Description
Session Manager	Shows the Session Manager Instance.
Registrations	Shows the current registration count.
AST Devices	Show the count of registered endpoints which support AST profile notification.

User Registrations

User Registrations

This module sends notification to selected SIP AST devices and displays the summary of the user registration status for the SIP AST Device based on the following actions:

- Reset of endpoints
- Full reload of endpoints
- Partial reload of endpoints

Viewing User Registrations

This module provides the ability to view the basic registration information for a particular user (or groups of users).

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **User Registrations** to open User Registrations screen. The User Registrations screen displays the list of registered users.
2. Click **Refresh** to retrieve the latest user registration summary results.

Related topics:

User Registrations field descriptions on page 522

Rebooting of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **User Registrations** to open User Registrations screen. The User Registrations screen displays the list of registered users.
2. Click to select the AST Devices and click **Reboot**. The Confirm Reboot Notification screen appears.
3. On the Confirm Reboot Notification screen, click **Confirm**.
4. After user confirmation, a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions

Related topics:

User Registrations field descriptions on page 522

Reloading of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Session Manager** > **System Status** > **User Registrations** to open User Registrations screen.
2. Click the rows to select the SIP AST Devices and do one of the following:
   a. Click **Reload** > **Reload Complete** to force complete reload of selected SIP AST Devices which includes maintenance data, configuration data, and a complete data reload.

      On the Confirm Reload Complete Notification screen, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

   b. Click **Reload** > **Reload Config** to reload only configuration details of selected SIP AST subscribed devices.

      On the Confirm Reload Config Notification screen, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

   c. Click **Reload** > **Reload Contacts** to reload only contact details of selected SIP AST subscribed devices.

      On the Confirm Reload Contacts Notification screen, click **Confirm**.

After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Related topics:

User Registrations field descriptions on page 522

User Registrations field descriptions

General section

Name	Description
Registered	Shows whether the SIP registration is active or not.
Address	Is the SIP registration address.
Login Name	Shows the administered user login name.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Session Manager	Shows the Serving Session Manager.
AST Device	Indicates whether the end point can support a reboot or reload operation.

Detailed Information section

Name	Description
Login Name	Is the administered user login name.
Registration Address	Is the address used during login.
Registration Time	Shows the initial or re-registration time.
Event Subscriptions	Shows the details of the event subscription.
User Communication Profile Addresses	Shows the User Communication Profile addresses.

Related topics:

Viewing User Registrations on page 520
Rebooting of selected AST devices on page 521
Reloading of selected AST devices on page 521

Data Replication Status

Session Manager Data Replication Status

The Session Manager Data Replication Status page displays the status of downward data replication from the System Manager database (master) to the Session Manager local databases (replicas). It also allows you to run audit tests and reset the modification counters.

Database changes on the master database are continuously monitored and are sent to the replicas within seconds of being committed on the master.

The Data Replication system can repair itself using automatic connection recovery and replication audits. Replication audits keep the master and the replica databases synchronized if connection problems occur, if database resource problems occur, or after a system has been down for upgrading or recovery. On replicas, the audit process is performed every 15 minutes.

Master/Replica actions

The following actions can be performed on the Session Manager Downward Data Replication Status page:

- Refresh: refreshes the display for the System Manager and the administered Session Manager instances.
- Update on Master: updates the Test String Value in the System Manager database and runs a test to verify that the test string is replicated correctly to each Session Manager database. The Test String Value and Last Update Time should match across all columns within a refresh or two.
- Reset Modification Counters (All): resets the modification counters for System Manager and all of the Session Manager instances to zero. This can be used in combination with on-demand audits to isolate replication problems to the System Manager or a particular Session Manager.
- Start Audit/Update (Selected): starts an update of the master database or runs an audit on both the master and replica databases on selected Session Managers.

  Selecting System Manager triggers an update cycle on the master database. The System Manager looks for any modifications made to the master database and sends updates to the replica databases if necessary. This process happens automatically every few seconds, so it is typically not necessary to do this on demand.

  Selecting a Session Manager triggers a replica database audit. If the audit determines that the replica database is out of sync with the master database, it will request updates from the master database. It may take more than one audit cycle to synchronize the

databases due to the amount of data to be synchronized or if there are complex relationships between the data to be synchronized.

Related topics:

Updating to Master on page 524
Resetting the Modification Counters on page 524
Running an Audit on page 525
Session Manager Downward Data Replication Status page field descriptions on page 525

Updating to Master

1. Select **Session Manager** > **System Status** > **Data Replication Status** on the System Manager console.
2. Enter any desired string in the **New Master Test String Value** field.

   The **New Master Test String Value** can be any string containing up to 10 alphanumeric or special characters.
3. Click the **Update on Master** button.
4. Wait a few seconds, then click the **Refresh** button.
5. Verify that the Test String Value updates on the replicas within a refresh or two, and that the timestamp updates when the test string is updated.

Related topics:

Master/Replica actions on page 523
Session Manager Downward Data Replication Status page field descriptions on page 525

Resetting the Modification Counters

1. Select **Session Manager** > **System Status** > **Data Replication Status** on the System Manager console.
2. Click the **Reset Modification Counters (All)** button.

Related topics:

Master/Replica actions on page 523

Session Manager Downward Data Replication Status page field descriptions on page 525

Running an Audit

1. Select **Session Manager** > **System Status** > **Data Replication Status** on the System Manager console.
2. Select the System Manager or a Session Manager instance.
3. Click the **Start Audit (Selected)** button to begin the database audit of the selected System Manager or a Session Manager instance.

Related topics:

Master/Replica actions on page 523
Session Manager Downward Data Replication Status page field descriptions on page 525

Session Manager Downward Data Replication Status page field descriptions

Name	Description
New Master Test String Value	Enter a test string for testing to ensure that it gets correctly updated on the master (IMSM) database. You can use a maximum of ten characters, and can use alphanumeric as well as special characters on the keyboard.

Button	Description
Refresh	Refreshes the following System Manager (master) database and Session Manager (replica) database Statistics: • Records Currently in Database — Total number of records in each of the databases. The number of records in each replica database should match the number in the System Manager database because the data is replicated from the master database to the replica databases. • Records Pending Update — For the master database column, this means that the database modifications (insert/update/delete) have occurred on the master database, but update messages for these modifications have not yet been sent to the replica databases. For the replica databases, this means that a replica database audit has determined that these records need to be updated in this replica database, but this replica database has not yet received and processed

Button	Description
	the associated messages from the master database to perform these modifications. • Modifications — Total number of database modifications (insert/update/delete operations) that have occurred in the respective databases. • Modifications Resulting from Audits — For the master database column, these are the number of database modifications that were sent as update messages to any of the replica databases in response to a replica audit. For the replica databases, these are the replica database modifications that were performed as a result of a database audit. This means that the replica database determined that it was out of synchronization with the master database and requested and received update messages from the master database. • Failed Modifications (replica only) — Number of database operations that have failed to be committed (insert, update, delete operations). This could be an error or it could be because the replication messages sent from the master to a replica database were received out of order, in which case, the failure is automatically recovered. • Failed Modifications Resulting from Audit (replica only) — Number of database operations that have failed to be committed (insert, update, delete operations) only for those modifications that were executed as a result of a replica database audit. • Elapsed Time Since Last Update/Audit (Days H:M:S) — On the master database, this is the elapsed time since the last time update messages were created and sent, if any, to the replica databases. On the replica databases, this is the elapsed time since the last replica database audit was performed. • Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S) • Last JMS Message Sent (master) / Received (replica) — This allows the master replication system's last message sent time to be compared with the last message received time of the replica systems. This enables you to estimate any delays in messages sent from the master replication system to the replica systems. For the master database this is the last time the master database replication system sent a message to one of the replica systems. For the replica databases, this is the last time this replica system received a message from the master database system. • Last JMS Message Received (master) / Sent (replica) • JMS Connection Status — This is the status of the underlying message transport system used by the data replication system. An OK status means that the message transport system works as intended. Any other status implies that there could be a problem sending messages from the master to the replica and from the replica to the master. • Test String Value — Current value of the test string in the master database. For the replica columns, this is the value of the test string in

Button	Description
	the respective database and should eventually match the master database test string value. • Test String Last Update Time
Update on Master	Updates the test string value in the System Manager database so that you can verify that the test string is replicated to each Session Manager database. This allows you to test the data replication system by verifying that the value of the test string in each Session Manager database (each is a replica database) is the same as the value in the System Manager database (master database).
Start Audit (Selected)	Starts an audit of actions and carries out updates for the selected System Manager as well as Session Manager instances. If you select a Session Manager, this triggers an update cycle on the master database. This means that the master replication system looks for any modifications made to the database and then sends an update message to the replica databases if necessary. This process happens automatically at regular intervals. Clicking this button forces an update on demand. If you select a Session Manager, this triggers a replica database audit. This means that the replica replication system synchronizes the replica database with the master database. If the replica database is not in synchronization, updates are requested from the master database and/or modifications are made so that the replica database is in synchronization with the master. This process happens automatically at regular intervals. Clicking this button forces an update on demand.
Reset Modification Counters (All)	Resets the modification counters for the System Manager as well as all the administered Session Managers to zero

Related topics:

Master/Replica actions on page 523
Updating to Master on page 524
Resetting the Modification Counters on page 524
Running an Audit on page 525

System Tools

Maintenance Tests

About Maintenance Tests

The Maintenance Tests page allows you to perform maintenance tests on the System Manager server and administered Session Manager instances. These maintenance tests test functionality of the System Manager and Session Manager servers. Tested functionality includes data replication and network connectivity to Session Manager instances, database functionality, the Secure Access Link (SAL) component, as well as the security module of each Session Manager.

Maintenance Tests page field descriptions

Name	Description
Select System Manager or Session Manager to test:	Select a System Manager or a Session Manager from the pulldown list on which to perform maintenance tests

Button	Description
Execute Selected Tests	Runs the selected maintenance tests on the selected System Manager or Session Manager You can run the following maintenance tests for a System Manager: • Test connections for all Session Manager instances • Test replication to each Session Manager local database • Test sanity of Secure Access Link (SAL) agent • Test postgres database sanity You can run the following maintenance tests for a Session Manager: • Test replication to System Manager Status • Test Call Processing status • Test Service Hosts status • Test Service Director Status • Test Management Server

Button	Description
	• Test sanity of Secure Access Link (SAL) agent • Test management link functionality • Test Security Module Status • Test postgres database sanity
Execute All Tests	Runs all the maintenance tests on the selected System Manager or Session Manager. See the list of tests that can be performed in the above row.

Related topics:

Test network connections to each Session Manager on page 529
Test data replication to each Session Manager local database on page 529
Test Call Processing status on page 530
Test Service Host status on page 530
Test Service Director Status on page 530
Test SIP A/S Management Server Status on page 530
Test sanity of Secure Access Link (SAL) agent on page 530
Test management link functionality on page 530
Test Security Module Status on page 530
Test Postgres database sanity on page 530
Running maintenance tests on page 531

Test network connections to each Session Manager

This test only runs on the System Manager. It tests the connectivity to each administered Session Manager.

If connectivity is up for each Session Manager, the test passes. Otherwise, the test fails. The server could be down or an upgrade/install is in progress. Check the log, then check Log and Alarm Event IDs for the appropriate troubleshooting action.

Test data replication to each Session Manager local database

This test only runs on the System Manager. It tests if replication is functioning properly by sending a test string to each administered Session Manager. The test string is saved by each Session Manager within its respective database. After a short wait, each Session Manager is queried for the test string value.

If the replication succeeds, the test passes. A failure indicates a possible JMS or secure connection problem. Refer to the Data Replication Status page for more information.

A similar test can be executed on the Data Replication Status page and specifying a custom test string.

The test is not run for a Session Manager if there is a JBoss connection problem or if the current state of the Session Manager is set to **Management Disabled**.

Test Call Processing status

This is a call processing sanity test. If call processing is working properly, the test passes. If the test fails, contact Avaya Technical Support.

Test Service Host status

This test asks for a list of service hosts and determines the running (up/down) status of each. The test passes if all of the hosts are up. The test fails if one or more of the hosts has an invalid status.

If the test fails, contact Avaya Technical Support.

Test Service Director Status

This test checks the status of the SIP A/S Service Director using a connection to SIP A/S. The test passes if the status of the service director is valid. If the test fails, contact Avaya Technical Support.

Test SIP A/S Management Server Status

This test checks the status of the SIP A/S Management Server using a connection to SIP A/S. The test passes if the status of the management server is valid or a particular SIP A/S service is running.

If the test fails, contact Avaya Technical Support.

Test sanity of Secure Access Link (SAL) agent

This test can run on either System Manager or Session Manager. It checks if the Security Access Link agent is running or not on the server. If the link is up and running, the test passes. Otherwise, if the test fails, contact Avaya Technical Support.

Test management link functionality

This test checks the administrative link to a Session Manager. If this test fails, administrative changes will not take effect on Session Manager. Otherwise, the test passes.

Test Security Module Status

Queries the basic status of the SM100 Security Module. If the query is successful, the test passes. Otherwise, it fails.

Test Postgres database sanity

This test runs on either System Manager or Session Manager. System Manager tests the sanity of the master database. Session Manager tests the sanity of its local instance database. A replication test from System Manager indirectly checks the sanity of each Session Manager replica database. The test passes if the test is successful. If the test fails, contact Avaya Technical Support.

Running maintenance tests

The Maintenance Tests page allows you to run maintenance tests on the System Manager or any administered Session Manager in the enterprise.

1. Select **Session Manager** > **System Tools** > **Maintenance Tests** on the System Manager Common Console.
2. Select System Manager or a Session Manager instance to test from the drop-down list.
   a. To run all of the tests, select **Execute All Tests**
   b. To perform only selected tests, select which tests should be run from the list and select **Execute Selected Tests**.

SIP Tracer Configuration

About Tracer Configuration

You can use the Tracer Configuration page to configure the tracing of SIP messages incoming through the security module, SIP messages outgoing from the security module, and also messages dropped by ASSET proxy or by the SIP firewall.

You can also filter these messages based on the user or the call. Session Manager logs all the traced messages to a file based on the configuration.

Tracer Configuration page field descriptions

Name	Description
Enabled	SIP message tracing is enabled by default.
Dropped	SIP message tracing is enabled for calls dropped by the SIP firewall as well as by the ASSET proxy.
From Network to Security Module	SIP message tracing is enabled for ingress calls sent to the Session Manager instance from the network.
From Security Module to Network	SIP message tracing is enabled for egress calls originating from the Session Manager instance and sent to the network.
From Server to Security Module	Local SIP messages originating from the Session Manager.

Name	Description
From Security Module to Server	Local SIP messages originating from the security module.
Max Dropped Message Count	Shows the value for the maximum number of traced dropped messages, if Dropped checkbox is activated.

Button	Description
User Filter: New	Create a new filter for filtering SIP messages based on the users. You can define a maximum of three user filters.
User Filter: Delete	Delete a selected user filter or filters.
Call Filter: New	Create a new filter for filtering all SIP messages that start a new call. You can define a maximum of three call filters.
Call Filter: Delete	Delete a selected call filter or filters.
Commit	Save the configuration changes.

Name	Description
User Filter: From	Filter SIP messages based on the user from whom the message is sent. Type the user string. For example, a rule to trace all messages from user “pqr”: to=”” from=”pqr” stop-count=50
User Filter: To	Filter SIP messages based on the user to whom the message is sent. Type the user string. For example, a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
User Filter: Source	Filter SIP messages based on the source address.
User Filter: Destination	Filter SIP messages based on the destination address.
User Filter: Max Message Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.
Call Filter: From	Filter SIP messages from a specific user. Call tracing identifies a call by capturing the Call ID from the first message that matches the From filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL from user “pqr”: to=”” from=”pqr” request-uri=”” stop-count=50
Call Filter: To	Filter SIP messages based on the user to whom the message is sent. Call tracing identifies a call by capturing the Call ID from the first message that matches the To filter, thereafter tracing all the messages that have the matching call ID.

Name	Description
	For example, a rule to trace all messages related to a CALL to user “xyz”: to=”xyz” from=”” request-uri=”” stop-count=50
Call Filter: Source	Filter SIP messages based on the source address.
Call Filter: Destination	Filter SIP messages based on the destination address.
Call Filter: Max Call Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.
Call Filter: Request URI	Filter calls based on the called party (URI address). A valid Request URI format, for example, is .@192.111.11.111.
Session Manager Network: Name	Select one or more configured Session Managers for which the specific filters should be used. **Note:** If you select only one Session Manager from this list, the **Get** button is activated. Click this button to retrieve the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page. After displaying the configuration, Session Manager closes the display so that no older configuration data is displayed.

SIP Trace Viewer

About SIP Tracing

The SIP tracer allows tracing of SIP messages exchanged between the Session Manager server and remote SIP entities. SIP messages which are dropped by any of the SM100 components such as SIP Firewall are also logged by the SIP tracer. You can trace all the messages belonging to a user, for a call, or for a selected Session Manager instance. The SIP tracer provides statistics of SIP messages within the SM100 framework. SIP tracer is located under Session Manager on the System Manager Common Console navigation pane. SIP tracer user interface has the following components:

- Tracer Configuration defines the characteristics of messages to be traced for the capturing engine in the security module.
- Trace Viewer displays the captured SIP messages.

For details, refer to the section Tracing in *Maintaining and Troubleshooting Avaya Aura™ ™ Session Manager* (03-603325)

Trace Viewer page field descriptions

Use the From and To fields to specify a range of days or time as follows:

Name	Description
From: Date	Date from which you want to filter the trace logs
From: Time	Time from which you want to filter the trace logs
From: Time Zone	Time Zone for the From date that you want to use for filtering trace logs
To: Date	Date up to which you want to filter the trace logs
To: Time	Time up to which you want to filter the trace logs
To: Time Zone	Time Zone for the To date that you want to use for filtering trace logs

Button	Description
Dialog Filter	Allows you to filter trace log entries. Select a trace log and click **Dialog Filter**. This option filters trace log entries and displays entries for the same Call ID, From, and To fields as the trace log that you select. **Note:** You can also click Filter: **Enable** to filter log entries based on a value or to sort them based on selected columns.
Cancel	Cancels the filtering of the trace using Dialog Filter and displays all trace log entries
Hide dropped messages	Hides dropped messages from the trace log entries
Show dropped messages	Displays dropped message in the trace log entries
Commit	Generates the trace log output for the selected Session Managers from the Session Manager list for the selected date range. This output displays the following details: • Details–Click the Show arrow to see the complete message. • Time–Timestamp when the trace record was written. This timestamp entry also displays the date and time zone. • Tracing Entity–Host name of the system where SM100 logged the trace • From–URI from where the traced SIP message originated • Action–Action of the traced SIP message such as INVITE, ACK, or BYE. The SIP message action is surrounded by an arrow to indicate the direction of the action. For example, -- INVITE -> or <- BYE --. Dropped messages have a leading DROPPED, for example, -- DROPPED ACK -> • To–URI to which the traced SIP message was sent

Button	Description
	• Protocol–Protocol that was used by the traced SIP message such as TCP, UDP, or TLS • Call ID–Call ID of the traced SIP message **Note:** Number of retrieved records shows the number of records that matched the filter criteria. If Session Manager displays fewer records than this number, it means that not all the matching records are displayed. Usually this is done to avoid problems caused by running out of memory. In such cases, you can further configure or refine the filter criteria in such a way that all the log entries are displayed.
More Actions > Export Trace Viewer Overview	Creates a tabulator-separated plain text file with all of the overview columns of the Trace Viewer page. You can open this file with editors such as Wordpad and Excel. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.
More Actions > Export Trace Viewer Details	Creates a plain text file with the details of the Trace View records. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.

Call Routing Test

About Call Routing Testing

Call routing tests are used to test routing of a SIP INVITE based on the current Session Manager administration options that you select. You can use it to verify that you have administered the Session Manager as intended before placing it into service, or to get feedback on why a certain type of call is not being routed as expected. The testing of call routing using Session Manager does not send any “real” SIP messages. It invokes call processing in the debug mode to test routing.

Call Routing Test page field descriptions

Name	Description
Calling Party URI	The SIP URI of the calling party. You must specify a handle and a domain, for example, 5552000@domain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.

Name	Description
Calling Party Address	The IP address or host name from which the INVITE is received. For routing, this is the IP address of a SIP Entity. You can enter any IP address that you require, but make sure that it is recognized by Session Manager. If it is not, Session Manager considers it to have come from a non-trusted host and rejects it.
Called Party URI	The SIP URI of the called party. You must specify a handle and a domain, for example, sip:5551000@companydomain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Session Manager Listen Port	The port on which the called Session Manager Instance receives the INVITE.
Day of Week	Day of the week. This is used for testing time of the day routing.
Time (UTC)	Time. This is used for testing time of the day based routing.
Transport Protocol	Protocol used for transportation of the call. This is used in testing the routing based on NRP entity links.
Called Session Manager Instance	The Session Manager instance that receives the INVITE sent for testing routing. This is used in testing the routing based on NRP entity links.

Button	Description
Execute Test	Carries out the routing test based on the parameters that you provide. The Routing Decisions box displays the result of the routing test. This result displays one line per destination choice. For a destination that has alternate routing choices available, the result displays one line per alternate routing choice and the lines are in the same order that the test attempted the destinations. Each line displays not only where the INVITE would be routed, but also what the adapted digits and domain would be. The Routing Decision Process box contains details about how Session Manager made the routing decisions. This gives you a tool to check your routing algorithms.

Appendix A: Default Certificates

Default certificates used for SIP-TLS

The Trusted/CA certificate of the issuer that follows is used to generate the default Identity Certificate for SIP-TLS.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Avaya Inc., OU=SIP Product Certificate Authority, CN=SIP
Product Certificate Authority
        Validity
            Not Before: Jul 25 00:33:17 2003 GMT
            Not After : Aug 17 05:19:39 2027 GMT
        Subject: C=US, O=Avaya Inc., OU=SIP Product Certificate Authority, CN=SIP
Product Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:dc:3b:2b:72:c7:b6:11:cd:3e:d5:60:9a:2f:f0:
                    51:9e:ea:0d:46:27:48:7e:e1:8e:d8:67:3c:e6:80:
                    73:ea:a6:09:fe:da:39:6e:42:2d:4d:34:79:62:30:
                    b6:d8:2e:7a:ef:7f:ab:37:f9:7f:f3:87:b6:4d:0f:
                    6b:72:ac:a6:4c:09:86:88:f0:55:fa:5f:7b:58:4c:
                    e3:59:f4:4a:d3:62:78:12:24:2a:4b:78:2b:a3:73:
                    ea:a0:b7:54:a6:46:cc:9a:d7:ed:45:f6:2e:63:be:
                    b1:71:a0:eb:91:6f:93:74:e5:8b:f7:70:8f:39:48:
                    52:f0:ee:41:2b:e3:57:10:0e:fb:21:44:15:99:7e:
                    8e:ab:7f:76:c1:26:39:6a:45:31:dc:e7:21:9b:5d:
                    77:84:b3:e2:6b:b4:8b:de:10:21:41:d9:0f:f0:dc:
                    48:3f:19:b7:16:1a:13:f5:ba:a1:ea:38:f1:fb:e9:
                    a3:4c:63:24:0f:18:cc:c3:06:da:42:7c:68:7b:1e:
                    40:fb:8e:44:f6:12:5f:80:88:12:89:cb:47:0e:72:
                    3d:b6:f8:02:9b:2e:f8:79:6d:f7:c9:31:37:02:3d:
                    7d:81:6b:1d:82:0f:62:35:ba:c4:3e:a2:c4:c6:f8:
                    57:6f:ba:14:41:c7:e5:8f:a8:13:96:b1:0d:30:44:
                    a1:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114187.7.2.1.1
                  CPS: mailto:sipca@avaya.com;

            X509v3 Subject Key Identifier:
                A0:82:07:29:5C:3A:A0:C4:29:B8:3D:C3:1D:B9:06:55:13:BE:56:2A
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Key Usage:
```

```
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
                keyid:A0:82:07:29:5C:3A:A0:C4:29:B8:3D:C3:1D:B9:06:55:13:BE:56:2A
                DirName:/C=US/O=Avaya Inc./OU=SIP Product Certificate Authority/
CN=SIP Product Certificate Authority
                serial:00

    Signature Algorithm: sha1WithRSAEncryption
        60:3e:b6:92:b6:8f:be:f8:a0:05:32:d5:12:19:59:b8:8e:c6:
        e4:9d:6c:1a:cd:1e:72:17:19:6d:5a:b8:28:a2:c3:0d:fb:5b:
        77:e7:50:04:25:e7:75:0c:2b:d4:5a:26:db:7d:2c:a5:87:5d:
        cf:37:36:0b:85:22:25:98:a3:d1:f7:c2:d5:43:83:f9:97:6e:
        82:da:cb:89:3d:ac:9e:11:45:fc:ef:00:c2:1d:ef:1e:34:d1:
        bd:de:f9:79:e1:4e:1a:40:3b:a6:f7:c1:52:4d:19:58:8d:d4:
        a2:2f:d4:77:b6:b2:8b:3a:28:98:94:b0:44:d6:82:47:04:63:
        e2:17:34:57:81:cd:17:54:65:97:31:f0:2a:b8:d4:34:d6:9c:
        ca:aa:ee:c4:4f:4f:40:5a:c6:1b:51:2e:1c:f8:9e:6d:75:89:
        3d:9d:89:37:e5:8d:56:b4:ac:0e:cf:c3:12:83:09:01:da:77:
        32:d6:b2:3a:22:e5:af:2c:05:1d:77:d0:4a:70:16:06:2d:23:
        15:ba:55:46:8e:5d:ce:8b:45:77:e7:1c:4d:a3:22:0a:43:df:
        11:3c:86:fd:45:c3:04:ce:18:88:92:15:0e:92:d9:9e:60:77:
        bd:05:89:fc:12:7e:fa:ab:9a:0e:5c:7d:02:68:84:0e:95:df:
        55:a2:87:7f
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFBy
b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N
NHliMLbYLnrvf6s3+X/zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj
c+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJjlqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP
GMzDBtpCfGh7HkD7jkT2El+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggEsMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4
PcMduQZVE75WKqF+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSIlmKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/
-----END CERTIFICATE-----
```

The following set of default certificates (in PEM format) are trusted by the Session Manager Security module for SIP-TLS. Append any additional certificates to this list before using the update_ca_cert.sh script:

```
  -----BEGIN CERTIFICATE-----
MIICaDCCAdECBEgQqykwDQYJKoZIhvcNAQEEBQAwezELMAkGA1UEBhMCVUsxEDAO
BgNVBAgTB1MgV2FsZXMxEDAOBgNVBAcTB0NhcmRpZmYxDjAMBgNVBAoTBWF2YXlh MRcwFQYDVQQ
LEw5VSyBFbmdpbmVlcmluZzEfMB0GA1UEAxMWYXZheWEgZGV2ZWxv
cG1lbnQgdGVhbTAeFw0wODA0MjQxNTQ1NDVaFw0xODAzMDMxNTQ1NDVaMHsxCzAJ
BgNVBAYTAlVLMRAwDgYDVQQIEwdTIFdhbGVzMRAwDgYDVQQHEwdD
YXJkaWZmMQ4w DAYDVQQKEwVhdmF5YTEXMBUGA1UECxMOVUsgRW5naW5lZXJpbmcxHzAdBgNVBAMT
FmF2YXlhIGRldmVsb3BtZW50IHRlYW0wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALpOPDPCHq8jpMs+Guaam66i
```

```
BPOeFBB0SNrLu5Ua1K7fkqEmjG6O+xvnb0Dm
2keo87gZkgSnktazUHfqSQmK9UC12GpomBuJPTZPlSrhcovtadTvjBpnYylp7tVZ
cvsuQxVlaICqr067w6uq0woP4cGSG9kyuhzqvtLCmIiZOFKHAgMBAAEwDQYJKoZI hvcN
AQEEBQADgYEAnLwTrvc4WZsDWw3cuCZlTLYEEIoY9oebhx4EEgOKBz/HXjr5 yA0JiSd
+KWdWdfGryhc7YYSbTruO6Hclmq7uJeaFqexdfEYtWQ0ZE1UFAZwLcz5c Vast/vxri4NVsM
+HZ4caayKPAio8csWhiQkfFDp783ho8
dBW9uKQkImd8KU= -----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE3zCCA8egAwIBAgIBWzANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx HjAcBgNVBAMTF
UF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wNzEyMjExMTU0NDBa
Fw0yNzEyMDIxMTU0NDBaMGsxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTErMCkGA1UEAx
MiQXZheWEg TWFudWZhY3R1cmluZyBTdWJvcmRpbmF0ZSBDQTCCASAwDQYJKoZIhvcNAQEBBQAD
ggENADCCAQgCggEBAMNFdBihMGWSsTAx24rWE5sbjMVkHe0ybSAoZZliLrow9Jau
UfasJ7dm49GQAbeVWqYZ15kFjR9vxU
j4ExGt/TcEbBcTau4wkG1tGrf9IsFLzJ9J dWuC3EWuXcUr4N3UTuSuARh+Q/J31AsXOkSY
+N0Tt2QhNedSeqCAXhUKhDp9FySS ICcobqJgS70W34wXvbgXTrWvlWRanphiADN7lUoUtFpqS
+qIfnpTABDG0TUGu9pk ej3/ft
zmfsACdPw5CzLUklglW5c8l6iJYH1stwkTPrrJkLPaCV1NOLZnpiSgQ9ru
3IbVXAn8MUPkiVU91bitZoB1bCS1WgkF+Q4tiM0CAQOjggGbMIIBlzAdBgNVHQ4E
FgQUbuW8D4RGjxrxDTFJElm8Mf7Bz+wwgYYGA1UdIwR/MH2
AFMKatvFzIYImbROw /v5R9l6b3DV7oWKkYDBeMQswCQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5j
LjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kxHjAcBgNVBAMTFUF2YXlhIFBy
b2R1Y3QgUm9vdCBDQYIBADA
MBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjCB0QYD
VR0gBIHJMIHGMIHDBgtghkgBhvwLBwEBATCBszAqBggrBgEFBQcCARYeaHR0cHM6
Ly93d3cuYXZheWEuY29tL3BraS9DUFM7MIGEBggrBgEFBQcCAjB4MBcWEEF2YXlh
 IFByb2R1Y3QgQ0EwAwIBARpdQXZheWEgSW5jLiBMaW1pdGVkIExpYWJpbGl0eSBQ
S0kgQ0EuICBQbGVhc2UgdmlzaXQgaHR0cDovL3d3dy5hdmF5YS5jb20vcGtpL0NQ
UyBmb3IgZGV0YWlscy47MA0GCSqGSIb3DQEBBQUA
A4IBAQBv40OigRG3iXiqmVwX WUdK1DaNQ7wDYCVPteNa9smLrdswAohdqMpyBS0Fut
+QfqWQkn2p4eL90ZICeqlr hPYWUFKSmlpKhf93WH
+0jsfvuzWefFg4JtlNsWgbVdi1wPdG9wddkgs4Bt6GzwOL r0iUuZwnHyUahR8K
EvFnab0+KA5gTIOqNnF0dGzaePzPzIJ2Tp8ybpSYQTjBVZmP /
YwkociqOMjUwbuUqDKlsARbeZMAUxmLx6V8fv96G+OPf3MUuvclTTVCP7+6i35y dV5DG/qP4OpAZcFO/
HNdtzreIYjDnlbplw2Fy9LClBZmUwHTmSzp1nJjk
6Wg3OAD DVSH -----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE1DCCA7ygAwIBAgIBADANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx HjAcBgNVBAMTF
UF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wMzA4MjIxMTI1MzZa
Fw0zMzA4MTQxMTI1MzZaMF4xCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTEeMBwGA1UEAx
MVQXZheWEg UHJvZHVjdCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+EpellesygWvwACRNRh/6FbkPYDGrf5jpqIzgd3KG1w7gvvQ/ID953REm2DS7DEI 4y7l+zY0MLtNv
+I3rASpdxufsFwkHa
5zR1FjpkiaP7XhMKXNpSY7No78rko9uiGt xCx9VdW20kcP4IiEN23jQWfKjGFzkZItCl/
aOf2+peh8bSS2MIprGx4rnCMZN1dU Nnw8nJFGu7IxRlGDA2XqJ7BWBn/
pvPMLdaVU60oI1/4IT9lHPUCaRVAC56jJdtxq F9sNW0
ZsBy05/vtopUiStfq8aMtMWCqGkSwjWB2VDWhWj6HTuGk27YsTsFIREJuT
i7rXYBQqRJN0o15aERM6BwIDAQABo4IBmzCCAZcwHQYDVR0OBBYEFMKatvFzIYIm bROw/
v5R9l6b3DV7MIGGBgNVHSMEfzB9gBTCmrbxcyGCJm0
TsP7+UfZem9w1e6Fi pGAwXjELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xGjAYBgNVBAsT
EUF2YXlhIFByb2R1Y3QgUEtJMR4wHAYDVQQDExVBdmF5YSBQcm9kdWN0IFJvb3Qg
Q0GCAQAwDAYDVR0TBAUwAwE
B/zALBgNVHQ8EBAMCAQYwgdEGA1UdIASByTCBxjCB
wwYLYIZIAYb8CwcBAQEwgbMwKgYIKwYBBQUHAgEWHmh0dHBzOi8vd3d3LmF2YXlh
LmNvbS9wa2kvQ1BTOzCBhAYIKwYBBQUHAgIweDAXFhBBdmF5YSBQcm9kdWN0IENB
 MAMCAQEaXUF2YXlhIEluYy4gTGltaXRlZCBMaWFiaWxpdHkgUEtJIENBLiAgUGxl
YXNlIHZpc2l0IGh0dHA6Ly93d3cuYXZheWEuY29tL3BraS9DUFMgZm9yIGRldGFp
bHMuOzANBgkqhkiG9w0BAQUFAAOCAQEAQYNqOpJS
kAn6tZOAbp7IW2RMFQO2rwNe UFdyWywqWKdoCNv/+9dAkHXp8wSEwRGPuXRJLuSZloRlK7OnT4GBH
```

```
+YaFMarHpUr rChkrmcR9smgN1WvSjvTk1HiFXEyurvpRarLRem3spDdN6Cyu/fhroJJEHc0j97O
U2HTNgz0papOAFxY
N497y3teENVmRBGNKoUo6NxayOCjv55JBxegvd6bOtabRv1L
OCNK8yeomL5ri9jiTLUgEEZIn3aFXetuKxTjhQqbxcpy16t70SQctIzLXqdp9ZZu
xz27CykJXlmexi5qREs+MLV0jrduRE50nTHMhkHKZBX7yKIgEb9GwQ==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDvDCCAqSgAwIBAgIBADANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCVVMx
FzAVBgNVBAoTDk1vdG9yb2xhLCBJbmMuMTkwNwYDVQQLEzBTZWFtbGVzcyBDb252 ZXJnZWQgQ29tb
XVuaWNhdGlvbiBBY3Jvc3MgTmV0d29ya3MxHTAbBgNVBAMTFFND
Q0FOIFNlcnZlciBSb290IENBMB4XDTAzMTIwNTIxMjg0M1oXDTMzMTIwNDIxMjg0
M1owgYAxCzAJBgNVBAYTAlVTMRcwFQYDVQQKEw5Nb3Rvcm9sYSwgSW
5jLjE5MDcG A1UECxMwU2VhbWxlc3MgQ29udmVyZ2VkIENvbW11bmljYXRpb24gQWNyb3NzIE5l
dHdvcmtzMR0wGwYDVQQDExRTQ0NBTiBTZXJ2ZXIgUm9vdCBDQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAN
HrAz5BUuNXL3cH9eAodevZY+5C1IaBtmxe K7+TweCWSljAeX/
e2EKMQatNIOFHO3cXqV7ERBUp0ymmrnnmLeqVfbS9anWOzoGr
MCZ3grohkFWh41uBzxlgYhDoGhGc1H8RZJBEE3Rmo5djZrTzAutSuOi7iAO7S9IC a9RBZF
/db3Z8jkc0ucSi3pDTolIJvjVx5ccztRd133uUyvHSAoXAwyFVx/9trZHp rQr76xUC/
8nOAhXlUlt8Vnp5C30X5WywCOXWelIUaLldH55fxDVcGL5h7Yu8SLb9 iynrlJ6XeDKp
+fDtWCVySIZBCLx0Ho29f8hOmLpg5/vb691
Q6mUCAwEAAaM/MD0w DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUc50Q0MwSbfz43CTFP6gsFsrWv+Uw
CwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBBQUAA4IBAQA956Nf5ldsVXTLbRMRBMuS
y1mdFnbtFN3hd8j8PcqDH9d
u+411JR1DL7cOJEJWDJwO1qlG44A6Mj/JnvwIA0M4 s3AAKV+EBj1du
+TBLhZluuEcvgpX1xiQehIFqTS6fp+CBLL2NYEeze0x1d/IHNNA eBhYfGBNnhbU0YGOlNERYyT
+nTgPgVVwuNaagJPyxHkZKWE2BmMT3OBt3vsdJS7S
 c+8Xiivl/KSfF3003/hQrzFH6mDtqSwLgFzKadZ2QE3HVdcajt/fW9sGyaq5PfWO mwyOTwtrcuo2/
EQqX03XHeTEohEoqMTTiNXxTLOwaPgAf/dkwmqPDjuZohtAUphg -----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIC0DCCAjmgAwIBAgIBADANBgkqhkiG9w0BAQQFADBVMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEVMBMGA1UECxMMTWVkaWEgU2VydmVyMRowGAYD VQQDExFBdmF5Y
SBDYWxsIFNlcnZlcjAeFw0wMjAxMTAwMzQwNDdaFw0zMjAxMDMw
MzQwNDdaMFUxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJbmMuMRUwEwYD
VQQLEwxNZWRpYSBTZXJ2ZXIxGjAYBgNVBAMTEUF2YXlhIENhbGwgU2
VydmVyMIGf MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDABs8TR5L3cDQNZTsA+t1HJZDOM/Sr
Ngq6TRWf3r8KdzUpYZVAxecODQ2gu9ccfLraxhi8Vn1X6DD/uBT90WdqkhpZs0+f
o6WE7fZZqGFJyVHhtqrN58IOOdQTfj
Kywhi0w+GTKfEvS/IHXLNM7Rr55KN4Jqa7 3GzklP0d//it4QIDAQABo4GvMIGsMB0GA1UdDgQWBBQ7f
+X4y7uDnQ2lkDsVYuFr ESzohDB9BgNVHSMEdjB0gBQ7f
+X4y7uDnQ2lkDsVYuFrESzohKFZpFcwVTELMAkG A1UEBh
MCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xFTATBgNVBAsTDE1lZGlhIFNl
cnZlcjEaMBgGA1UEAxMRQXZheWEgQ2FsbCBTZXJ2ZXKCAQAwDAYDVR0TBAUwAwEB /
zANBgkqhkiG9w0BAQQFAAOBgQAa1P7y67oAqwsnM268fXW
KTjhqixG2N2+BVkkk 2CEgKzFIjUuwV0kllR+RkyijKXsEnFBvXDdDDbuK+K9O2KO//i3I1eRIsMeVJ4Jj
wE9iYt8+Fniir4moMidQW9KT7SK0Db4ARY4GWezJQPFVoPng7Ny6rDooUIcNmZc4 YK9Wbw==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm aWNhdGUgQXV0a
G9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECx
MhU0lQIFBy b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8F
Ge6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N NHliMLbYLnrvf6s3+X/
zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj c
+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r f3bBJj
lqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP GMzDBtpCfGh7HkD7jkT2El
+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1 usQ+osTG+FdvuhRBx
+WPqBOWsQ0wRKGNAgMBAAGjggEsMII
```

```
BKDA/BgNVHSAEODA2 MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E CDAGAQH/
AgEBMAsGA1UdDwQ
EAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4 PcMduQZVE75WKqF
+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
 MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo osMN
+1t351AEJed1DCvUWibbfSylh13PNzYLhSIl
mKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS gwkB2ncy1rI6IuWv
LAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/ -----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIBADANBgkqhkiG9w0BAQQFADBvMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUExEDAOBgNVBAcTB0FuZG92ZXIxDjAMBgNVBAoTBUFWQVlBMQ0w CwYDVQQLEwRFT
U1DMSIwIAYJKoZIhvcNAQkBFhNpZ29uemFsZXNAYXZheWEuY29t
MB4XDTA0MTAxMzE1Mzc1N1oXDTMyMDIyOTE1Mzc1N1owbzELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk1BMRAwDgYDVQQHEwdBbmRvdmVyMQ4wDAYDVQQKEw
VBVkFZQTEN MAsGA1UECxMERU1NQzEiMCAGCSqGSIb3DQEJARYTaWdvbnphbGVzQGF2YXlhLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA3+P7zLbpBTyyvhYUsrAuh3x6
emQRxA6QtJlNOMWZKLtLSWuap+KFYO
LtNd36MZl/KavEn6wCChR5IM1GAPwCIvZV
pG907FRxPoxdZOAZZRqgWzG7L9mC30NxBiBwA3DO9GbFqOdeW8zupf5SBZqpQ7k/
DZO7oAuYZE8GFhNkUVECAwEAAaOBzDCByTAdBgNVHQ4EFgQUixd7HNzpgfqPlLcc uhqhDY
ZUX6QwgZkGA1UdIwSBkTCBjoAUixd7HNzpgfqPlLccuhqhDYZUX6Shc6Rx
MG8xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTEQMA4GA1UEBxMHQW5kb3ZlcjEO
MAwGA1UEChMFQVZBWUExDTALBgNVBAsTBEVNTUMxIjAgBgk
qhkiG9w0BCQEWE2ln b256YWxlc0BhdmF5YS5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQF
AAOBgQCLiZfxwyTbfC5C5KRnz9tbDLLEzCHoHqZASlUtIK/cY6fzmEtkNb/k6pdM
0CwYeY5u7rBMhj9UmnhvgGS
qQKAMZHsFDIYZU6H3HmV6P+l7kKiWYvSag+adwYH4 T0m2+rzTOu/
lYioczR5MIrxT3Txrovs8cEYgJNzewPm2/jQeXw== -----END CERTIFICATE-----
```

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W