Administering Avaya Aura™ Session Manager

Issue 3
03-603324
Release 6.0
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 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 routing, Session Manager instances, and network settings.

This book is also useful for understanding specific features, and for Avaya personnel who configure and support 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 of System Manager

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:

- Elements: Provides features for managing individual components of Avaya Aura Unified Communication System including Session Manager element administration.
- Applications: Provides an interface to manage the instances of applications running on the different servers.
- Security: The System Manager console 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.
- User Management: Provides a central user administration of all user properties. The centralized administration reduces the need for replicating the user's data across multiple products.
- Licenses: Provides features to administer licenses for individual components of Avaya Aura Unified Communication System.
- Routing: Provides features to manage routing applications. You can create and manage routing applications that includes Domains, Adaptations, SIP Entities, Entity Links, Time Ranges, Policies, Dial Patterns, and Regular Expressions to configure your network configuration.
- Events: 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.
- System Data: Provides backup and restore capability of configuration data, monitor and schedule jobs, and replicate data from remote nodes.

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.

Log on to System Manager

Logging on to the System Manager Web interface

The System Manager Web interface is the main interface of Avaya Aura™ System Manager. You must log on to the System Manager Web console before you can perform any tasks.

Prerequisites

A user account to log on to the System Manager Web interface. If you do not have a user account, contact your system administrator to create your account.

1. On the browser, type the Avaya Aura™ System Manager URL (`https://<SERVER_NAME>/SMGR`) and press the **Enter** key.
2. In the **Username** 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 the Avaya Aura™ System Manager Version *version_number*. The System Manager home page displays navigation menu in the left navigation pane. The menu provides access to shared services using which you can perform various operations supported by System Manager. The tasks you can perform depends on your user role.

     The content page in the right pane displays shortcut links that provides access to the shared services.
   - If you enter incorrect login credentials in theSystem Manager login page, System Manager displays an error message, and prompts you to re-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 **Elements** > **SIP AS 8.1**.
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: Synchronizing Communication Manager and messaging data with System Manager

Introduction

This chapter explains how to use Communication System Manager feature to synchronize Communication Manager station data to the System Manager database. The system automatically connects to System Manager and Communication Manager in the core and synchronizes provisioning data in the System Manager database with each managed Communication Manager system. You can synchronize the endpoint data in a scheduled and incremental basis as follows:

1. Administration of each Communication Manager as an entity or application instance.
2. Initialization of the synchronization of Communication Manager and messaging data with System Manager.

Creating a Communication Manager instance

1. On the System Manager console, click **Elements** > **Inventory** > **Manage Elements** in the left navigation pane.
2. On the Application Management page, click **New** and select a “CM” entity instance.
3. On the New CM Instance page, enter the appropriate details:
   a. In the **Node** field, specify the management IP address for the Communication Manager (this is the address used for SSH SAT login).
   b. Select “default (none)” for the **SNMP Attributes** section
   c. Under **Attributes** section, enter the SSH SAT login for the **Login** field and the associated password in the **Password** field.
4. Click **Commit** .

When you add an application entity through RTS (Runtime Topology Service), 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 **System Manager Data** > **Scheduler** or in the log files on the Communication System Management server.

Creating a messaging instance

1. On the System Manager console, click **Elements** > **Inventory** > **Manage Elements** in the left navigation pane.
2. On the Application Management page, click **New** and select a “Messaging” entity instance.
3. On the New Messaging Instance page, enter the details as described below:
   - 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 or 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.
4. Click **Commit** .

   When you add an application entity through RTS (Runtime Topology Service), 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 **System Manager Data** > **Scheduler** or in the log files on the Communication System Management server.

Initializing Synchronization

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Synchronization** > **Communication System** on the left navigation pane.
3. Select the Communication Managers you want to synchronize.
4. Select **Initialize data for selected devices**.
5. Click **Now** to perform the initializing synchronization or do one of the following:
    - Click **Schedule** to perform the synchronization at a specified time.
    - Click **Cancel** to cancel the synchronization.

Synchronizing Messaging Data

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Synchronization** > **Messaging Data** on the left navigation pane.
3. Select the messaging systems you want to synchronize.
4. Click **Now** to perform the synchronization or do one of the following:
    - Click **Schedule** to perform the synchronization at a specified time.
    - Click **Cancel** to cancel the synchronization.

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 runs.
Type	The type of the application to which the instance belongs.
Version	Version of the application instance.
Description	A brief description about the instance.

Button	Description
View	Opens the View application page. Use this page to view the details of the selected application instance.
Edit	Opens the Edit Application page. Use this page to modify the information of the instance.
Delete	Opens the Delete Application Confirmation page. Use this page to delete a selected application instance.
Configure Trusted Certificates	Opens the Trusted Certificates page. Use this page to view, add and delete the trusted certificates for the application instance.
Configure Identity Certificates	Opens the 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. 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.

Name	Description
Type	The type of the application to which the instance belongs.
Description	A brief description about the instance.
Node	The node on which the application runs.
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.

Name	Description
	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. **Note:** This button is visible only when you click **Add** and **Edit** in the **Access Point** section.

Button	Description
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. **Note:** craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager. **Note:** Do not use this login to connect to CM from any other application or to connect to the Communication Manager SAT terminal using CLI.
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.
Alternate IP Address	Alternate IP address of the application instance. This is the IP address of the standby server in case of duplex servers.
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the CM Server. In case of Duplex servers, RSA SSH Key is the key of the Active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH Key of the CM Server used only in case of Duplex servers. This is the key of the Standby server.
Is ASG Enabled	Use this check box to enable ASG. 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 non-ASG 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.

SNMP Attributes

You set some basic parameters for specific devices or a range of devices in the SNMP Attributes section. You can choose either SNMP protocol V1 or V3. Based on your selection of SNMP protocol, you can then set certain basic SNMP parameters.

Name	Description
Version	Specifies the SNMP protocol type.
Read Community	The read community of the device.. Only applicable for SNMP protocol V1.
Write Community	The write community of the device. Only applicable for SNMP protocol V1.
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeout	The number of milliseconds an application polls a device without receiving a response before timing out.
Device Type	Specifies the type of the device

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. **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.

Chapter 3: Managing Security

Introduction

Trust Management provisions certificates to applications enabling them to have a secure inter-element communication. It provides Identity and Trusted (root) certificates with which mutually authenticated TLS sessions can be established.

For administering third-party trusted certificates for Session Manager, a "Session Manager 6.0" application needs to be added for a specific Session Manager or Branch Session Manager instance. This application is administered with the “Management Access Point” IP address of the Session Manager instance. Using the Trust Management service, you can perform the following operations for the application instance:

- View trusted and identity certificates currently installed on the Session Manager server.
- Add and remove trusted certificates installed on the Session Manager server.

Note:

Adding, removing and replacing of certificates is not currently supported for either Identity Certificates or for non-third party certificates that is the default certificates provided by Avaya cannot be changed.

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. On the System Manager console, under **Services**, click **Security**.
2. Click **Certificates** > **Enrollment Password**.
3. On the Enrollment Password page, select the expiration of password in hours in the **Password expires in** field.
4. Click **Generate**.

The password field displays the generated password.

5. Click **Done**.

Note:

When you click **Generate**, the time displayed next to the **Time remaining** label is updated by the value selected in the **Password expires in** field.

Adding a Session Manager application

1. On the System Manager console, click **Elements** > **Application Management** > **Session Manager 6.0** in the left navigation pane.
2. On the Application Management page, select a Session Manager application and click **New**.
3. On the New Session Manager Instance page, enter the following details:
   a. Under **Application** section, enter a name in the **Name** field for this Session Manager.
   b. Enter the Management Access Point IP address of this Session Manager in the **Node** field, which is same as the value entered for Session Manager instance during Session Manager administration.
   c. Under **Access Point** section, select the pre-populated Access Point in the table and click **Edit**. Enter name in the **Name** field, Management Access Point IP address in the **Host** field and any text in the **URI** field.
   d. Click **Save**.
4. Click **Commit** .

Viewing trusted certificates

Prerequisites

You must have permission to view certificates of an application instance.

1. On the System Manager console, click **Elements** > **Application Management** > **Session Manager 6.0** in the left navigation pane.
2. On the Application Management page , select a Session Manager instance and click **More Actions** > **Configure Trusted Certificates**.
3. On the Trusted Certificates page, click **View**.

Result

The **View Trust Certificate** page displays the details of the selected certificate.

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. On the System Manager console, click **Elements** > **Application Management** > **Session Manager 6.0** in the left navigation pane.
2. On the Application Management page , select a Session Manager instance and click **More Actions** > **Configure Trusted Certificates**.
3. On the Trusted Certificates page, click **Add**.
4. 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**.

Removing trusted certificates

1. On the System Manager console, click **Elements** > **Application Management** > **Session Manager 6.0** in the left navigation pane.
2. On the Application Management page , select a Session Manager instance and click **More Actions** > **Configure Trusted Certificates**.
3. 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 Session Manager instance instance.

Viewing identity certificates

1. On the System Manager console, click **Elements** > **Application Management** > **Session Manager 6.0** in the left navigation pane.
2. On the Application Management page , select a Session Manager instance and click **More Actions** > **Configure Identity Certificates**.
3. On the Identity Certificates page, click **View**.

Result

The Identity Certificate page displays the identity certificates.

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.
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).
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 **Existing Password** and **Time Remaining** fields

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 runs.
Type	The type of the application to which the instance belongs.
Version	Version of the application instance.
Description	A brief description about the instance.

Button	Description
View	Opens the View application page. Use this page to view the details of the selected application instance.
Edit	Opens the Edit Application page. Use this page to modify the information of the instance.
Delete	Opens the Delete Application Confirmation page. Use this page to delete a selected application instance.
Configure Trusted Certificates	Opens the Trusted Certificates page. Use this page to view, add and delete the trusted certificates for the application instance.

Button	Description
Configure Identity Certificates	Opens the 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. 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	The node on which the application runs.
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. **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. **Note:** craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager. **Note:** Do not use this login to connect to CM from any other application or to connect to the Communication Manager SAT terminal using CLI.
Password	Password which authenticates the SSH/ Telnet login name on the application instance. This field is not required for ASG login.

Name	Description
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.
Alternate IP Address	Alternate IP address of the application instance. This is the IP address of the standby server in case of duplex servers.
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the CM Server. In case of Duplex servers, RSA SSH Key is the key of the Active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH Key of the CM Server used only in case of Duplex servers. This is the key of the Standby server.
Is ASG Enabled	Use this check box to enable ASG. 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 non-ASG 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.

Name	Description
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.

SNMP Attributes

You set some basic parameters for specific devices or a range of devices in the SNMP Attributes section. You can choose either SNMP protocol V1 or V3. Based on your selection of SNMP protocol, you can then set certain basic SNMP parameters.

Name	Description
Version	Specifies the SNMP protocol type.
Read Community	The read community of the device.. Only applicable for SNMP protocol V1.
Write Community	The write community of the device. Only applicable for SNMP protocol V1.
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeout	The number of milliseconds an application polls a device without receiving a response before timing out.
Device Type	Specifies the type of the device

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.

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.

Button	Description
Add	Open the Adds Trusted Certificate page. use this page to import certificates from the selected resource.
Remove	Removes the selected certificate from the list of trusted certificates.
Exports	Exports the selected certificate from the list of trusted certificates.

Related topics:

Removing trusted certificates
Viewing trusted certificates
Adding 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: • All • TM_INBOUND_TLS • TM_OUTBOUND_TLS • TM_INBOUND_TLS_PEM
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.

Name	Description
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.
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.

Field/Button	Description
Retrieve Certificate	Retrieves the certificate and displays the details of the certificate in the Certificate Details section.

Related topics:

Adding trusted certificates

View Trust Certificate field descriptions

Use this page to view details of a selected certificate.

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.

Button	Description
Done	Closes the page and takes you back to the Trusted Certificates page.

Related topics:

Viewing trusted certificates

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.

Related topics:

Removing trusted certificates

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.

Chapter 4: Managing Users

Introduction

This chapter explains adding a user profile for accessing enhanced enterprise call handling facilities using:

- application sequencing (with Communication Manager Feature Server and other applications)
- modular messaging mailbox
- telephone set

Following are the pre-administration steps required for adding the Session Manager Profile of a user:

1. Administer Primary Session Manager by adding a SIP entity of type “Session Manager” and Session Manager instance (with listen ports). See the topics Creating SIP Entities on page 112 and Adding a SIP entity as a Session Manager instance on page 155 for details.
2. Administer Secondary Session Manager by adding a SIP entity of type “Session Manager” and Session Manager instance (with listen ports). See the topics Creating SIP Entities on page 112 and Adding a SIP entity as a Session Manager instance on page 155 for details.

   Note:
   This is an optional step required only for redundancy purposes.
3. Add SIP Domains — Administer the SIP domain using the Routing application. See the topic Creating domains on page 88 .
4. Add applications to be added in the Origination and Termination Application Sequences.
   a. Add Communication Manager Feature Server as an Application
      - Add the Communication Manager Feature Server SIP entity. See the topics Creating SIP Entities on page 112.
      - Administer the Communication Manager Feature Server as an application instance for associating the CM System for SIP entity.

See the topic Creating a Communication Manager instance on page 23 for details.

- Add the Communication Manager Feature Server as an Application. See the topic Creating an application on page 227 for details.

b. Similarly add other Applications to be added in the Application Sequence.

5. Create Application Sequence from existing Applications for specifying “Origination Application Sequence” and “Termination Application Sequence”. See the topic Creating an Application Sequence on page 231 for details.
6. To use a Branch Session Manager as a Survivability Server, add a SIP entity of type “Session Manager” and Branch Session Manager instance (with listen ports). See the topics Creating SIP Entities on page 112 and Adding a SIP entity as a Branch Session Manager instance on page 175 for details.
7. For Home Location which is a mandatory selection, the valid values are those of the configured “Locations”. For adding a new value, add a “Location”. See the topic Creating Locations on page 93 for details.

Before adding user, you need to synchronize Communication Manager station data and messaging data to the System Manager as follows:

1. Administer each Communication Manager and messaging application as an application instance. See the topics Creating a Communication Manager instance on page 23 and Creating a messaging instance on page 24 for details.
2. Synchronize Communication Manager and messaging data with System Manager. See the topics Initializing Synchronization on page 25 and Synchronizing Messaging Data on page 25 for details.

Add a User Profile (SIP end-point). See the topics Adding users on page 50 for details.

System Manager provides bulk importing of user profiles and user attributes. See the on-line help topics under “Managing bulk importing and exporting” for details.

Adding users

The following are the steps for adding users. Any input fields not mentioned in the steps can be ignored. There are a number of input fields which are not necessary for Session Manager user administration.

A user may have more than one Communication Profile. For more information regarding the fields, see the on-line help.

1. Select **Users** > **Manage Users**.
2. In the User Management page, click**New**.
3. In the **General** section, enter the user's last name and first name.
4. Enter a description in the **Description** field. This field is optional.
5. Select a **User Type**.
6. In the **Identity** section, enter a **Login** name.
   This is the unique system login name given to the user. It takes the form of username@domain (enterprise canonical number) and is used to create the user's primary handle.
7. The **Authentication Type** should be `Basic`
8. Enter an **SMGR Login Password** and confirm it. The password must start with an alpha (lower or upper case) character.
9. The **Shared Communication Profile Password** *must* be administered. This is the password that is used when logging in to the phone.
10. Enter the **Localized Display Name** of the user. This is the name that is displayed as the calling party.
11. Enter the full text name of the user for **Endpoint Display Name** .
12. Click on the show/hide button for **Communication Profile**.
13. Click on the show/hide button for **Communication Address**.
14. For each SIP handle:
    a. Click**New**.
    b. Select `Avaya SIP` from the drop-down menu for **Type** if it is not set already.
    c. In the **Fully Qualified Address** field, enter the extension number.
    d. Click**Add**.
15. Assign the user to a Communication Manager station:

    Note:
    This step cannot be done until synchronization of the data has completed. To view the synchronization status, navigate to **Communication System Management** > **Telephony** on the System Manager console. The status is displayed in the **Sync Status** column.

    a. Check the box to the left of **Endpoint Profile**
    b. Select the Communication Manager from the **System** drop-down menu.
    c. Check **Use Existing Stations** if the station already exists on the Communication Manager that is associated with this user.

The box must be checked in order to associate the user with the selected Communication Manager station settings. Otherwise, leave the box unchecked to create a station automatically .

d. Enter the extension that is administered on Communication Manager for the existing or new station in the **Extension** field.

e. Select a phone template for the use's phone in the **Template** field. This selection is required only in case when existing station is not used.

f. Enter a port in the **Port** field.

g. Select the **Delete Station on Unassign of Station from User** box. This optional step applies only if the station is required to be deleted when the user is deleted.

16. Under the Session Manager section:

a. Make sure the **Session Manager Profile** check box is checked.

b. Select the appropriate Primary Session Manager instance from the drop-down menu in the **Primary Session Manager** field.

c. Select the appropriate Secondary Session Manager instance from the drop-down menu in the **Secondary Session Manager** field. This is an optional step required only for redundancy purposes.

d. Select the origination application sequencing from the drop-down menu in the **Origination Application Sequence** field.

e. Select the termination application sequencing from the drop-down menu in the **Termination Application Sequence** field.

f. Specifying a survivability server (e.g. Branch Session Manager) in the **Survivability Server** field. This is optional and is required only for survivability.

g. **Home Location** is a mandatory input field to support mobile users. You can administer locations using **Routing** > **Locations**.

17. Select **Commit**.

Related topics:

New User Profile field descriptions on page 57

Modifying user accounts

You must have permission to modify the user. The **Edit** button for modifying a user details is not available if you select a user for which you do not have the permission to modify the details.

Prerequisites

Permission to modify the user

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, select a user.
   You can edit only one user account at one time.
3. To edit a user account, perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. Modify the information and click **Commit** to save the changes to the database.

Related topics:

User Profile Edit field descriptions on page 65

Viewing details of a user

Prerequisites

You must have permission to view the details of the selected user.

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, select a user.
3. Click **View** to view details of the selected user account.
   You can view details of only one user account at a time.

Related topics:

User Profile View field descriptions on page 74

Removing user accounts

When you remove a user, the system marks the user as deleted and stores them in a list of deleted users. Removing a user removes the roles associated with the user but retains the contacts, addresses, communication profiles of the user.

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, select one or more users from the table, and click **Delete**.
3. 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.

Creating duplicate users

Using this feature, you can create a new user account by copying the information from an existing user account. This feature does not copy the confidential information, such as addresses, private contacts, contact members in the contact list, password, and login name of the source user.

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, select the user account that you want to duplicate.
3. Click **Duplicate**.
4. On the User Profile Duplicate page, enter the appropriate information, and click **Commit**.

Filtering users

You can filter users by:

- Status of the user
- Name of the user
- E164 Handle
- Login Name of the user

You may apply one or more filters to view users that match the filter criteria.

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, click **Filter: Enable**.
   You can find the button at the upper-right corner of the table displaying users.
3. Enter information for one or more of the following filter criteria:
   - To filter users by status, select a status from the drop-down under the **Status** column.
   - To filter users by name, enter the name of the user in the field under the **Name** column.

     To filter names that start with a particular letter, enter the letter in the field. You can enter a string of letters to filter names that start with that string.
   - To filter users by login name, enter the login name in the field under the **Login Name** column.

     To filter login names that start with a particular letter, enter the letter in the field. You can enter a string of letters to filter login names that start with that string.
   - To filter users by the E164 handle, enter the E164 handle of the user in the field under the **E164 Handle** column.
4. Click **Apply** .
   To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.
   To clear the filter criteria, click **Clear**.

Result

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

Searching for users

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, click **Advanced Search** displayed at the upper-right corner of the page.
3. 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.

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

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

Result

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

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. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, click **More Actions** > **Show Deleted Users**.

Result

The Deleted Users table displays the temporarily deleted users.

Restoring a deleted user

You can use this feature to restore a user that you deleted using the Delete feature.

Prerequisites

You must have permission to restore the selected deleted user.

1. On the System Manager console, under User View, click **Manage Users**.
2. On the User Management page, click **More Actions** > **Show Deleted Users**.
3. Select the user that you want to restore, and click **Restore**.
4. On the User Restore Confirmation page, click **Restore**.
5. On the User Profile Edit page, enter a new password in the **Password** field.
6. In the **Confirm Password** field, enter the same password that you entered in step 5.
7. Click **Commit**.

New User Profile field descriptions

Use this page to create a new user. This page has four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Note:

The fields that are marked with an asterisk are mandatory and you must enter appropriate information in these fields.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user.

Name	Description
First Name	The first name of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
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** — User's login is authenticated by the enterprise. • **Basic** — User's login is authenticated by an Avaya Authentication Service.
New Password	The initial password for logging in to the system.
Confirm Password	The initial password n for confirmation.
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 tab — 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.

Name	Description
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 shared or common address.

Communication Profile tab — Communication profile section

Use this section to create, modify and delete a communication profile for the user. Each communication profile may contain one or more communication addresses for a user.

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

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding a communication profile.

The system enables the following fields when you click the **New** 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 Profile tab — Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user.

Name	Description
Type	The type of the handle.

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

Button	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. The following fields define the communication address for the user.

Name	Description
Type	The type of the handle. The following are the different handle types: • Avaya SIP: Indicates that the handle supports Avaya SIP-based communication. • Avaya E.164: Indicates 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. • Microsoft OCS SIP: Indicates that the handle support OCS SIP based communication. • Microsoft Exchange: Signifies that the handle is an e-mail address and supports communication with Microsoft SMTP server. • Lotus Notes: Indicates that the handle is for Lotus Notes and domino calender. • IBM Sametime: Indicates that the handle is for IBM Sametime. • Jabber: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication with the Jabber service. • GoogleTalk: Indicates that the handle supports XMPP-based communication with the Google Talk service. • Other Email: Indicates that the handle is an e-mail address other than MS Exchange e-mail addresses. • Other SIP: Indicates that the handle supports other SIP-based communication than the ones mentioned above. • Other XMPP: Indicates that the handle supports other XMPP-based communication than the ones mentioned above.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or an address of an communication device using which user can send or receive messages.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the adding a communication address operation.

Communication Profile tab — Session Manager

Note:

You may see these fields only if a communication profile for the user can be configured using the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Secondary Session Manager	If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.
Survivability Server	For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.
Home Location	A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with

Name	Description
	an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory.

Communication Profile tab — Endpoint Profile

Note:

You may see these fields only if an endpoint profile can be configured for the user .

Name/Button	Description
System	The Communication Manager on which you need to add the endpoint.
Profile Type	The type of the endpoint profile you want to create.
Use Existing Endpoints	Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used.
Extension	The extension of the endpoint you want to associate. The field lists the endpoints (existing or available) based on check box status of the **Use Existing Endpoints** field.
Template	The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.
Set Type	The set type of the endpoint 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 endpoint.
Port	The relevant port for the set type you select. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you want to associate.
Delete Endpoint on Unassign of Endpoint from User or Delete User	Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.

Communication Profile tab — Messaging Profile

Note:

You may see these fields only if a messaging profile can be configured for the user.

Name	Description
System	The Messaging System on which you need to add 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.
Mailbox Number	The mailbox number of the subscriber. The field takes 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.
Template	The template (system defined and user defined) you want to associate with the subscriber.
Password	The password for logging into the mailbox.
Delete Subscriber on Unassign of Subscriber from User or Delete 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.

Membership tab — Roles section

Name	Description
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.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership section

Name	Description
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.

Contacts tab — 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.

Contacts tab — 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.
Add	Opens the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.
Remove	Removes one or more selected 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.

Contacts tab — 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.
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.

Common buttons

Button	Description
Commit	Creates the user account.
Cancel	Cancels the user creation operation.

Related topics:

Adding users on page 50

User Profile Edit field descriptions

Use this page to modify the details of a user account.

The User Profile Edit page has four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Identity tab — Identity section

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user
Update Time	The time when the user details were last modified.
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. • **basic** — User's login is authenticated by an Avaya Authentication Service.
Change Password	Click this link to change the password for logging into the system.
New Password	Type the new password for logging in to the system.
Confirm Password	Type the password again for confirmation.
Source	
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 tab — Address section

Name	Description
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 common address.

Communication Profile tab — Communication Profile section

Use this section to create, modify and delete a communication profile for the user. Each communication profile may contain one or more communication addresses for a user.

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

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.

Button	Description
Cancel	Cancels the operation for adding a communication profile.

The system enables the following fields when you click the **New** 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 Profile tab — Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user.

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

Button	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: • Avaya SIP: Indicates that the handle supports SIP based communication. • Avaya E.164: 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. • Microsoft Exchange: Signifies that the handle is an e-mail address and supports communication with Microsoft SMTP server. • Lotus Notes: Indicates that the handle is for Lotus Notes and domino calender. • IBM Sametime: Indicates that the handle is for IBM Sametime. • Jabber: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication with the Jabber service.

Name	Description
	• Google Talk: Indicates that the handle supports XMPP-based communication with the Google Talk service. • Other Email: Indicates that the handle is an e-mail address other than MS Exchange e-mail addresses. • Other SIP: Indicates that the handle supports other SIP-based communication than the ones mentioned above. • Other XMPP: Indicates that the handle supports other XMPP-based communication than the ones mentioned above.
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.

Button	Description
Add	Saves the new communication address or modified communication address information to the database.
Cancel	Cancels the adding a communication address operation.

Communication Profile tab — Session Manager

Note:

The page displays the following fields if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Secondary Session Manager	If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.

Name	Description
	Note: If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.
Survivability Server	For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.
Home Location	A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory.

Communication Profile tab — Endpoint Profile

Note:

The page displays the following fields if an endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager on which you need to add the endpoint.
Use Existing Endpoints	Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used.
Extension	The extension of the endpoint you want to associate. The field lists the endpoints (existing or available) based on check box status of the **Use Existing Endpoints** field.
Template	The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.
Set Type	The set type of the endpoint 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 endpoint.
Port	The relevant port for the set type you select.

Name/Button	Description
	The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you want to associate.
Delete Endpoint on Unassign of Endpoint from User	Use this check box to specify whether you want to delete the endpoint from the Communication Manager Device when you remove the association between the endpoint and the user or when you delete the user.

Communication Profile tab — Messaging Profile section

Note:

The page displays the following fields if a messaging profile exists 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.
Mailbox Number	The mailbox number of the subscriber. The field lists the existing subscriber if you select the **Use Existing Subscriber on System** check box.
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.

Membership tab — Roles section

Name	Description
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.

Button	Description
UnAssign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership section

Name	Description
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.

Contacts tab — 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.

Contacts tab — 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.
Add	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.

Contacts tab — 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 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.

Common buttons

Button	Description
Commit	Modifies the user account.

Button	Description
	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 53

User Profile View field descriptions

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

The User Profile View page has four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Identity tab — Identity section

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Description	A brief description of the user.
Status	The login status of the user.
Update Time	The time when the user details were last modified.
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: • **enterprise** — User's login is authenticated by the enterprise. • **basic** — User's login is authenticated by an Avaya Authentication Service.
Source	

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 tab — 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 tab — 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 Profile tab — Communication Address section

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

Communication Profile tab — Session Manager section

Note:

The page displays the following fields if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.
Secondary Session Manager	If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.
Origination Application Sequence	Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.
Termination Application Sequence	Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.
Survivability Server	For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.

Name	Description
Home Location	A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory.

Communication Profile tab — Endpoint Profile

Note:

The page displays the following fields if an endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager on which you need to add the endpoint.
Profile Type	The type of the profile for the user.
Extension	The extension of the station you want to associate.
View Endpoint	Lists the endpoints (existing or available) based on check box status of the **Use Existing Endpoints** field.
Set Type	The set type of the endpoint 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 endpoint.
Port	The relevant port for the set type you select.
Voice Mail Number	The voice mail number of the station you want to associate.
Delete Endpoint on Unassign of Endpoint from User or Delete User	Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.

Communication Profile tab — Messaging Profile

Note:

The page displays the following fields if a messaging profile exists 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.
Mailbox Number	The mailbox number of the subscriber.

Name	Description
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.

Membership tab — Roles section

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

Membership tab — Group Membership section

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.

Contacts tab — 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.

Contacts tab — 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.
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.

Name	Description
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.

Contacts tab — 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.

Common buttons

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.

Related topics:

Viewing details of a user on page 53

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 localized display name of a user. It is typically the localized full name.
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.

Chapter 5: Managing 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 Routing 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 routing 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 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.

Routing

Routing

Routing tells the system which SIP Entity should receive a call that matches the configured dial pattern or regular expression. Administrators can use Routing to administer Session Manager instances and related routing policies. The configuration data is distributed from the Routing 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.

Routing and Session Manager allow administrators to define routing:

- by combining several locations
- by combining several dial patterns and domains
- for several ToD and rankings
- for a single routing destination

Routing of a call using routing policy 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 or the Local Host Name Resolution table to determine where to route the request.
6. If the hostname cannot be resolved to an IP address then 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 Routing screens is as follows.

1. Accept or change default settings.
2. Create 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.

Routing import and export Overview

Overview of exporting and importing routing element data

The Routing screens allow administering of the Avaya Aura Session Manager SIP routing rules. The management screens consist of nine configurable elements that relate to each other in various ways.

It is possible to populate a very large number of the above elements in System Manager by using XML files. It is also possible to export each of the elements or the entire routing configuration to XML files.

PRE-REQUISITES:

- Ensure that System Manager is installed and the server is running.
- Ensure that the user performing the bulk import operation has administrative privileges.
- Before you import a large amount of data, it is highly recommended that you backup the System Manager database. This backup will provide an easy way to restore the original database in case you find that the information you imported is substantially incorrect. Refer to the document Administering Avaya Aura™ System Manager for details about this operation.
- Importing a very large number of elements (thousands and above) can take a very long time and can be CPU intensive to the System Manager server. This information will also need to be synchronized with all the Session Managers. It is highly recommended that you perform large imports at a time where there is reduced platform activity in the network (for example at night or during a maintenance window).

FEATURES:

System Manager Routing Import/Export supports:

- Routing related data:
  - Domains
  - Locations
  - Adaptations
  - SIP Entities

- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions

- Each element can be imported separately as a single XML file containing many entries.
- It is possible to compress the XMLs using ZIP compression in order to decrease the size of the files that need to be uploaded to the System Manager server. Note that this is especially important when importing large files of size exceeding 10 MB or more.
- Several or all the elements can be imported in a single ZIP file containing many XML files.
- It is possible to export a single type of entity or all the entities. When exporting all the entities, the exported files are contained in a single ZIP file.
- It is important to note that the Routing elements depend on each other (see specific elements details in this guide). An import operation will fail if the needed elements do not already exist in the database or exist in the same import operation. For example: Import of a Dial Pattern with domain name avaya.com will fail if there is no such domain in the database, or if an XML file containing this domain is not imported in the same import operation as the Dial Pattern.
- When importing several entities together (either as a list of XML/ZIP files or inside a single ZIP file), the System Manager will import them in the correct order to maintain dependencies. Because of this, it is possible, for example, to import SIP Entities and Entity Links pointing to these SIP Entities in the same import operation. The import order is always:

    a. Domains
    b. Locations
    c. Adaptations
    d. SIP Entities
    e. Entity Links
    f. Time Ranges
    g. Routing Policies
    h. Dial Patterns
    i. Regular Expressions

  The order is decided by analyzing the files internal structure (it must be a well formed XML as described in this guide). Any file name can be used as long as its extension is “xml”.
- The Import operation does not halt if one of the elements fails validation. The failed element will not be added to the database, and the operation will continue to the next one.

- An audit log provides details on the failed and successful import operations.
- If an imported element already exists in the System Manager database, which means that there is an element with the same unique identifiers, then the values in the new element will overwrite the old element.
  - For example: if a domain named “avaya.com” already exist in the database, then the note, type and default values will be overwritten by the new element.
  - Dial Pattern is an exception for this rule. It is not possible to import a dial pattern with elements such as <digitpattern>,<maxdigits>,<mindigits>,<sipdomainName> and <routingoriginationName> already present in the database. Such an attempt will fail.
- Every operation in the Routing application is logged to an audit log including the import operation. A log entry is added for each element that is imported, even if the operation succeeds or fails. The log is located at the following file:**`/var/log/Avaya/mgmt/nrp/nrpaudit.log`**. The file is accessible through the System Manager Linux Shell.

Note:

The Routing elements depend on each other. An import operation will fail if the needed elements do not already exist in the database or exist in the same import operation. For example import of a Dial Pattern with domain name avaya.com will fail if there is no such domain in the database, or if an XML file containing this domain is not imported in the same import operation as the Dial Pattern.

Exporting Routing element data

1. On the System Manager console, select **Routing** > ***<Any Routing element>***.
2. From the Routing Entity screen, click **More Actions** > **Export *<Routing Element>***.
   For example, to export adaptations, select **Routing** > **Adaptations**. From the Adaptations screen, select **More Actions** > **Export Adaptations**.
   To export regular expressions, select **Routing** > **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. To export multiple routing elements, from the routing element screen, click **More Actions** > **Export all data**.
5. Click **Browse** to specify the location and click **Export**.
   You must export a file in the XML format or multiple files as a zipped file.

Importing Routing element data

1. On the System Manager console, select **Routing** > **<Any Routing element>**.
2. To import a single or multiple routing elements, click **More Actions** > **Import** .

   For example, to import dial patterns, select **Routing** > **Dial Patterns**. From the Dial Patterns screen, click **More Actions** > **Import**.
3. Click **Browse** to select files from the required location and click **Import**.

   You must import a file in the XML format. This file can be an XML file or a ZIP file consisting one or more XML files.

   Note:

   - You cannot import data from the later stages in the routing definition process without importing data from the earlier stages (e.g. one must import SIP Entities before or in conjunction with the relevant Entity Links).
   - The import operation can accept any routing element XMLs (e.g. you can import “Locations” even if you clicked on import from the “Domains” screen).
   - The XML files that are created with the “export” operation contains version information as shown below:

     ```
     <buildNumber>0</buildNumber>
     <implementationVersion>0</implementationVersion>
     <specificationVersion>0</specificationVersion>
     ```

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 Entities Details screen, or changing dial pattern data also changes that data in the routing policy where that dial pattern is used.

Duplicating Routing entity data

You can use the **Duplicate** button on the relevant Session Manager Routing screens to duplicate routing entities. Select the check box for the relevant entity and click **Duplicate**.

Duplication of data is useful if you want to create entities 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.

Domains

About Domains

The Domains screen is used to create a set of 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. Sub-domains 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 sub-domains 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 domains

Create a domain or set of domains if you plan to use domain-based routing.

1. On the System Manager console, select **Routing** > **Domains**.
2. Click **New**.
3. Enter the domain name and notes for the new domain or sub-domain.

4. Select “sip” as the domain type from the drop-down list.
5. Click **Commit**.

Modifying domains

You can also edit or delete the domains using the **domains** option. The Domains screen is displayed.

1. On the System Manager console, select **Routing** > **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 domains

1. On the System Manager console, select **Routing** > **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** on the confirmation page.

Related topics:

Delete Confirmation field descriptions on page 89

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected domains.

Button	Description
Delete	Deletes the selected domains.
Cancel	Cancels the deletion of the domains.

Related topics:

Deleting domains on page 89

Domains field descriptions

Use this page to create, modify, delete, and manage domains.

Button	Description
Edit	Opens the Domains page that you can use to modify the domain details.
New	Opens the Domains page that you can use to create new domains.
Duplicate	Creates a duplicate of the selected domain.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the domain.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Domains**	Opens the Export Domains page that allows you to export the 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 routing entities data as a zipped file to a specified location.
Commit	Distributes the selected domain to all the Session Manager instances in the enterprise.

Domain field descriptions

Use this page to create new domains

Name	Description
Name	Name of the domain.

Name	Description
Type	List of the type of domains. Only Domains of type SIP can be used for routing.
Default	Indicates the default domain.
Notes	Additional notes about the domain.

Button	Description
Commit	Saves the domain and distributes it to all the instances of the Session Manager.
Cancel	Cancels the domain creation.

Bulk import for Domains

Please follow these rules when creating an XML bulk import file:

- The domain name must be unique, and is referred to by other elements.
- It is not possible to create a domain with <domainType> of type “sip” that have <defaultDomain> containing the value “true”.
- The values in <domainType> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipdomainFullTOList>
    <SipdomainFullTO>
        <notes>this is a test</notes>
        <defaultDomain>false</defaultDomain>
        <domainName>avaya.com</domainName>
        <domainType>sip</domainType>
        <name>avaya.com</name>
    </SipdomainFullTO>
    <SipdomainFullTO>
        <notes>this is another test</notes>
        <defaultDomain>false</defaultDomain>
        <domainName>avaya2.com</domainName>
        <domainType>sip</domainType>
        <name>avaya2.com</name>
    </SipdomainFullTO>
</sipdomainFullTOList>
```

Locations

About Locations

You can use the Locations screen to set up and configure gateway and user locations. 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 entities 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. 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.

Note:

Pattern can also accept IP address range. Example: 10.0.0.1-10.0.0.5

IP address mask is also a valid pattern. Example: 135.9.0.0/16

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 Locations

1. On the System Manager console, select **Routing** > **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. To add a location pattern, click **Add** under **Location Pattern**.
8. Enter an IP address pattern to match.
9. Enter notes about the location pattern, if required.
10. Continue clicking the **Location Pattern Add** button until all the required Location Pattern matching patterns have been configured.
11. Click **Commit**.

Related topics:

Location Details field descriptions on page 95

Modifying Locations

1. On the System Manager console, select **Routing** > **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. 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.

5. To add or remove a location pattern, click **Add** or **Remove** under **Location Pattern**.
6. Click **Commit**.

Deleting Locations

1. On the System Manager console, select **Routing** > **Locations**.
2. To delete an existing location or locations, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.

Related topics:

Delete Confirmation field descriptions on page 94

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of locations.

Button	Description
Delete	Deletes the selected location.
Cancel	Cancels the deletion of the location.

Related topics:

Deleting Locations on page 94

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.

Button	Description
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**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Locations**	Opens the Export Locations page that allows you to export the location 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 routing entities data 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.
Location Pattern	The IP address pattern that should be matched for the location. For example, • 135.12x.121.* • 13x.1xx.* • 135.* • 135.12x.121.123 **Note:** Pattern can also accept IP address range. Example: 10.0.0.1-10.0.0.5 IP address mask is also a valid pattern. Example: 135.9.0.0/16

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 Locations on page 93

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.

Bulk import for Locations

Please follow these rules when creating an XML bulk import file:

- Locations are referred to as routing origination in the import XML.
- The name of a location is unique and is referred to by other elements.
- Multiple Routing Origination Patterns (<routingoriginationpatterns>) can be configured for one Routing Origination Name.
- The values in <ManagedBandwidthUnitOfMeasurement> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingoriginationFullTOList>
    <RoutingoriginationFullTO>
        <notes>this is a test</notes>
        <name>New York</name>
        <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
        <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
        <ManagedBandwidth>500000</ManagedBandwidth>
        <ManagedBandwidthUnitOfMeasurement>Kbit/sec</
ManagedBandwidthUnitOfMeasurement>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>1.2.3.4-1.2.3.10</ipaddresspattern>
        </routingoriginationpatterns>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>1.2.4.*</ipaddresspattern>
```

```
        </routingoriginationpatterns>
        <TimeToLiveInSec>3600</TimeToLiveInSec>
    </RoutingoriginationFullTO>
    <RoutingoriginationFullTO>
        <notes>this is a test</notes>
        <name>Berlin</name>
        <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
        <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
        <ManagedBandwidth>900000</ManagedBandwidth>
        <ManagedBandwidthUnitOfMeasurement>Kbit/sec</
ManagedBandwidthUnitOfMeasurement>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>3.*</ipaddresspattern>
        </routingoriginationpatterns>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>2.3.4.5</ipaddresspattern>
        </routingoriginationpatterns>
        <TimeToLiveInSec>3600</TimeToLiveInSec>
    </RoutingoriginationFullTO>
</routingoriginationFullTOList>
```

Adaptations

About 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 Adaptations section. An adaptation administered using routing 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)

Note:
Session Manager adaptations do not work on the to and the from SIP headers.

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

On the Adaptation Details screen, the format of the **Adaptation Module** field is:

```
<Name of adaptation module> <name1=value1> <name2=value2>,...
```

- The module name contains only the name
- The module parameters can contain either a single parameter or a list of "`name=value name=value name=value`".

Note:
The list is separated by spaces and not by commas

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.com
overrideDestinationDomain=ny.avaya.com
```

Creating Adaptations

1. On the System Manager console, select **Routing** > **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.
      - **Module name** field contains only the name (4 options)
      - **Module parameter** field contain either a single parameter or a list of "`name=value name=value name=value`".

      Note:
      The list is separated by spaces and not by commas
   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 **Commit**.

Related topics:

Adaptation Details field descriptions on page 107

Modifying Adaptations

1. On the System Manager console, select **Routing** > **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”.
   a. Enter a descriptive name for the adaptation.
   b. Specify an adaptation module.
      - **Module name** field contains only the name (4 options)
      - **Module parameter** field contain either a single parameter or a list of “`name=value name=value name=value`”.

      Note:
      The list is separated by spaces and not by commas
   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 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 Adaptations

1. On the System Manager console, select **Routing** > **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 104

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 Adaptations on page 104

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.

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**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Adaptations**	Opens the Export Adaptation page that allows you to export the adaptation 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 routing entities data as a zipped file to a specified location.
Commit	Distributes the selected adaptation to all the Session Manager instances in the enterprise.

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.
Module name	The module name contains only the name (4 options)
Module parameter	The module parameters contain either a single parameter or a list of "`name=value name=value name=value`"

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 Adaptations on page 100

Bulk import for Adaptations

Please follow these rules when creating an XML bulk import file:

- The name of an adaptation is unique and is referred to by other elements.
- The value of <adaptationmodule> is a combination of the fields “Module Name” and “Module Parameters” in the System Manager user interface. The values are separated by a single space.
- Multiple Ingress and Egress configurations <<EgressadaptationFullTO>, <IngressadaptationFullTO>> can be configured for one Adaptation name.
- The values in <addressToModify> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<adaptationFullTOList>
    <AdaptationFullTO>
        <notes>this is a test</notes>
        <adaptationmodule>VersionModule param1=17 param2=15</adaptationmodule>
        <egressuriparameters>uri1</egressuriparameters>
        <name>VerisonAdaptation</name>
        <EgressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>809</matchingpattern>
            <maxdigits>20</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>origination</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>810</matchingpattern>
            <maxdigits>21</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>destination</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
```

```
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>811</matchingpattern>
            <maxdigits>22</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <IngressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>2</insertdigits>
            <matchingpattern>148</matchingpattern>
            <maxdigits>25</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>origination</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>2</insertdigits>
            <matchingpattern>149</matchingpattern>
            <maxdigits>26</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>destination</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>2</insertdigits>
            <matchingpattern>150</matchingpattern>
            <maxdigits>27</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
    </AdaptationFullTO>
</adaptationFullTOList>
```

SIP Entities

About SIP Entities

SIP entities are all the network entities 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

Routing 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 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 routing 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 SIP Entities

Use the 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. On the System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. Enter the Name of the SIP entity in the **Name** field.
4. Enter the FQDN or IP address of the SIP entity in the **FQDN** or **IP Address** field.
5. Select the type of SIP entity from the drop-down menu in the **Type** field.
6. Enter any other required information in the **General** section.
7. If you need to specify an Adaptation Module for the SIP entity, click the drop-down selector for the **Adaptation** field and select a value.
8. If you need to specify the Location for the SIP entity, click the drop-down selector for the **Location** field and select a location.

9. 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.
10. Enter a regular expression string in the **Credential name** field. The 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 the 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.

    Note:

    IP Address is searched by default when any string is configured in the Credential Name.

    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 you can create a wild card search. For example, to look for “domain.com” as a substring, use the string “domain\.com”
11. Under SIP Link Monitoring, use the drop-down menu to select one of the following:
    - Use Session Manager Configuration – Use the settings under **Session Manager** > **Session Manager Administration**
    - Link Monitoring Enabled – Enables link monitoring on this SIP entity.
    - Link Monitoring Disabled – Link monitoring will be turn off for this SIP entity.
12. 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.
13. Enter the necessary Port and Protocol parameters.
14. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
15. Click **Commit**.

Related topics:

SIP Entity Details field descriptions on page 117

Modifying SIP entities

1. On the System Manager console, select **Routing** > **SIP Entities**.
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 **Commit**.

Deleting SIP Entities

1. On the System Manager console, select **Routing** > **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.

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.
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**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
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 routing entities 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.

Name	Description
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 SIP Entities on page 112

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.

Bulk import for SIP Entities

Please follow these rules when creating an XML bulk import file:

- The name of a SIP Entity is unique and is referred to by other elements.
- <adaptationName> must either be empty or refer to an existing adaptation with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity. SIP Entity of type “ASM” <Avaya Session Manager> cannot contain an adaptation entry.
- <adaptationName> contains the adaptation module name and parameters separated by spaces <examples below>.
- Listen ports (<listenports>) are only relevant for SIP Entity of type “ASM”. Do not include these entries for any other type of SIP Entity.
- Multiple listen ports entries (<listenports>) can be configured for one ASM SIP Entity.
    - <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity.
    - The values in <transportprotocol> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.
- The values of <timezoneName> should be same (being case sensitive) as that of the field “Time Zone” in the SIP Entity user interface in System Manager.
- The field <userfc3263> corresponds to the “Override Port & Transport with DNS SRV” check box in the SIP entity form.
- The value of <entitytype> must contain one of the following values exactly as they appear below being case sensitive.
    - CM — communication manager (CM in the user interface)
    - ASM — Session Manager in the user interface
    - Modular Messaging — Session Manager in the user interface
    - VP — Voice Portal in the user interface
    - Gateway — Gateway in the user interface
    - SIP Trunk — SIP Trunk in the user interface
    - OTHER — Other in the user interface.

- The values in <cdrSetting> must appear exactly same being case sensitive, as they appear in the System Manager user interface.
- The field <do_monitoring> corresponds to the field “SIP Link Monitoring” in the SIP Entity details form. The relation is as follows:
  - In order to enable SIP Link monitoring, <do_monitoring> value must be “yes”
  - In order to enable SIP Link monitoring, <do_monitoring> value must be “no”
  - In order to use the Session Manager configuration, the <do_monitoring> tag must be completely omitted.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipentityFullTOList>
    <SipentityFullTO>
        <notes>this is a test</notes>
        <entitytype>CM</entitytype>
        <fqdnoripaddr>9.8.7.6</fqdnoripaddr>
        <name>BerlinCM</name>
        <adaptationName>VerisonAdaptation param1=12 param2=14</adaptationName>
        <cdrSetting>egress</cdrSetting>
        <credentialname>credential test</credentialname>
        <do_monitoring>yes</do_monitoring>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>Berlin</routingoriginationName>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>Europe/Berlin</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
        <notes>this is a test</notes>
        <entitytype>CM</entitytype>
        <fqdnoripaddr>9.8.7.5</fqdnoripaddr>
        <name>NewYorkCM</name>
        <adaptationName>VerisonAdaptation param1=7 param2=8</adaptationName>
        <cdrSetting>egress</cdrSetting>
        <credentialname>credential test</credentialname>
        <do_monitoring>yes</do_monitoring>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>New York</routingoriginationName>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>America/New_York</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
        <notes>this is a test</notes>
        <entitytype>ASM</entitytype>
        <fqdnoripaddr>4.5.6.7</fqdnoripaddr>
        <name>SessionManager1</name>
        <cdrSetting>egress</cdrSetting>
        <credentialname>credential test</credentialname>
        <do_monitoring>use-instance</do_monitoring>
        <listenports>
            <notes>this is a test</notes>
            <portnumber>5067</portnumber>
            <sipdomainName>avaya.com</sipdomainName>
            <transportprotocol>TLS</transportprotocol>
```

```
        </listenports>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>New York</routingoriginationName>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>America/New_York</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
</sipentityFullTOList>
```

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. On the System Manager console, select **Routing** > **SIP Entities**.
2. From the SIP Entity 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 122

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 121

Entity Links

About 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 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.

Routing 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 Entity Links

1. On the System Manager console, select **Routing** > **Entity Links**.
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 default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Enter the SIP entity 2 by selecting the required 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 **Commit**.

Modifying entity links

1. On the System Manager console, select **Routing** > **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 1 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 Entity Links

1. On the System Manager console, select **Routing** > **Entity Links**.
2. To delete an existing link or links, select the respective check boxes and click **Delete**.
3. Click **Delete** 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.
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.

Button	Description
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**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
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 routing 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.
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.

Bulk import for Entity Links

Please follow these rules when creating an XML bulk import file:

- The name of an Entity Link must be unique.
- <entityName1> , <entityName2> must refer to an existing SIP Entity with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Entity Link.
- The values in <transportProtocol> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entitylinkFullTOList>
    <EntitylinkFullTO>
        <notes></notes>
        <listenPortEntity1>5061</listenPortEntity1>
        <listenPortEntity2>5061</listenPortEntity2>
        <name>SessionManager1_BerlinCM_5061_TLS</name>
        <transportProtocol>TLS</transportProtocol>
        <trusted>true</trusted>
        <entityName1>SessionManager1</entityName1>
        <entityName2>BerlinCM</entityName2>
    </EntitylinkFullTO>
    <EntitylinkFullTO>
        <notes></notes>
        <listenPortEntity1>5061</listenPortEntity1>
        <listenPortEntity2>5061</listenPortEntity2>
        <name>NewYorkCM-SessionManager1-TLS</name>
        <transportProtocol>TLS</transportProtocol>
        <trusted>true</trusted>
        <entityName1>SessionManager1</entityName1>
        <entityName2>NewYorkCM</entityName2>
    </EntitylinkFullTO>
</entitylinkFullTOList>
```

Time Ranges

About the 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 time ranges can be in effect on weekends. These three time ranges together cover how calls should be routed throughout the week.

Creating Time Ranges

You can use the Time Ranges screen to administer time ranges with start and end times.

1. On the System Manager console, select **Routing** > **Time Ranges**.
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 **Commit**.

Related topics:

Time Range List field descriptions on page 129

Modifying Time Ranges

1. On the System Manager console, select **Routing** > **Time Ranges**.
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 Time Ranges

1. On the System Manager console, select **Routing** > **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 128

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 Time Ranges on page 127

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**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.

Button	Description
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 routing entities as a zipped file to a specified location.
Commit	Distributes the selected time range to all the Session Manager instances in the enterprise.

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 Time Ranges on page 126

Bulk import for Time Ranges

Please follow these rules when creating an XML bulk import file:

The name of a Time Range must be unique and is referred to by other elements.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<timerangeFullTOList>
```

```
    <TimerangeFullTO>
        <notes>this is a test</notes>
        <includesFriday>true</includesFriday>
        <includesMonday>true</includesMonday>
        <includesSaturday>false</includesSaturday>
        <includesSunday>false</includesSunday>
        <includesThursday>true</includesThursday>
        <includesTuesday>true</includesTuesday>
        <includesWednesday>true</includesWednesday>
        <name>regularweek</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
    <TimerangeFullTO>
        <notes></notes>
        <includesFriday>false</includesFriday>
        <includesMonday>false</includesMonday>
        <includesSaturday>true</includesSaturday>
        <includesSunday>true</includesSunday>
        <includesThursday>false</includesThursday>
        <includesTuesday>false</includesTuesday>
        <includesWednesday>false</includesWednesday>
        <name>weekend</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
    <TimerangeFullTO>
        <notes>Time Range 24/7</notes>
        <includesFriday>true</includesFriday>
        <includesMonday>true</includesMonday>
        <includesSaturday>true</includesSaturday>
        <includesSunday>true</includesSunday>
        <includesThursday>true</includesThursday>
        <includesTuesday>true</includesTuesday>
        <includesWednesday>true</includesWednesday>
        <name>24/7</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
</timerangeFullTOList>
```

Routing Policies

About 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 “domain” of the called party and the actual time the call occurs.

Optionally, instead of “dialed digits” of the called party and the “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 Routing Policies

1. On the System Manager console, select **Routing** > **Policies**.
2. Click **New**.
3. Enter a routing 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 Entities 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 **Commit**.

Related topics:

Routing Policy Details field descriptions on page 134

Modifying Routing Policies

1. On the System Manager console, select **Routing** > **Policies**. The Routing Policies screen is displayed.
2. Select a routing policy for modification and click **Edit**.
3. If required, modify the routing 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 entities 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 Routing Policies

1. On the System Manager console, select **Routing** > **Policies**.
2. To delete an existing routing policy or routing policies, select the respective check boxes and click **Delete**.
3. Click **Delete** 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 133

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 Routing Policies on page 133

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**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
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 routing entities 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 Routing Policies](#) on page 131

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.

Name	Description
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.

Bulk import for Routing Policies

Please follow these rules when creating an XML bulk import file:

- The name of a routing policy <referred to as routing policy> is unique and is referred to by other elements.
- <sipentityName> must refer to an existing SIP element with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.
- Multiple time of day entries (<timeofdayNames>) can be configured for one Routing Policy.

  <timerangeName> must refer to an existing Time Range with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingpolicyFullTOList>
    <RoutingpolicyFullTO>
        <notes>this is a test</notes>
        <disabled>false</disabled>
        <name>toBerlin</name>
        <sipentityName>BerlinCM</sipentityName>
        <timeofdayNames>
            <rank>1</rank>
            <timerangeName>regularweek</timerangeName>
        </timeofdayNames>
        <timeofdayNames>
            <rank>0</rank>
            <timerangeName>24/7</timerangeName>
        </timeofdayNames>
    </RoutingpolicyFullTO>
</routingpolicyFullTOList>
```

Dial Patterns

About Dial Patterns

A dial pattern specifies which routing policy or routing 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 applying any administered ingress adaptation.

The originating location of the call and the domain in the request-URI also determine 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 Dial Patterns screen is used to create Dial Patterns and associate the Dial Patterns to a Routing Policy and Locations.

1. On the System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**. The Dial Pattern Details screen is displayed.
3. Enter the Dial Pattern General information in the General section. Note that a Domain can be provided to restrict the Dial Pattern to the specified 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 **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 141

Modifying Dial Patterns

1. On the System Manager console, select **Routing** > **Dial Patterns**.
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 Domain can be provided to restrict the Dial Pattern to the specified 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. On the System Manager console, select **Routing** > **Dial Patterns**.
2. To delete an existing dial pattern or patterns, select the respective check boxes and click **Delete**.
3. Click **Delete** 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 141

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.

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 > **Dial Pattern Report**	Displays Dial Patterns and the corresponding Locations, Routing Policies and Domains.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.

Button	Description
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 > **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 routing entities as a zipped file to a specified location.
Commit	Distributes the selected dial pattern to all the Session Manager instances in the enterprise.

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. **Note:** Some of the important constraints on the use of this feature are as follows • Each location should be assigned to only one emergency dial number. • This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.
SIP Domain	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.
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 138
Deleting Dial Patterns on page 139

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.

Name	Description
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call. **Note:** Some of the important constraints on the use of this feature are as follows • Each location should be assigned to only one emergency dial number. • This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.
Domain	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.

Bulk Import for Dial Patterns

Please follow these rules when creating an XML bulk import file:

- A dial pattern is identified by a combination of 5 elements below. This combination must be unique for each dial pattern.
  - <digitpattern>
  - <maxdigits>
  - <mindigits>
  - <sipdomainName>
  - <routingoriginationName>
- <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the dial pattern.
- <routingpolicyNames> must refer to existing Routing Policies with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Dial pattern.
- <routingpolicyNames> must exist if <deny> is false.
- <routingpolicyNames> must exist if <deny> is true.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digitmapFullTOList>
    <DigitmapFullTO>
        <notes>this is a test</notes>
        <deny>true</deny>
        <digitpattern>123</digitpattern>
        <maxdigits>36</maxdigits>
        <mindigits>3</mindigits>
        <routingoriginationName>New York</routingoriginationName>
        <routingpolicyNames>toBerlin</routingpolicyNames>
        <sipdomainName>avaya.com</sipdomainName>
        <treatasemergency>true</treatasemergency>
    </DigitmapFullTO>
    <DigitmapFullTO>
        <notes>this is a test</notes>
        <deny>false</deny>
        <digitpattern>123</digitpattern>
        <maxdigits>36</maxdigits>
        <mindigits>3</mindigits>
        <routingoriginationName>Berlin</routingoriginationName>
        <routingpolicyNames>toBerlin</routingpolicyNames>
        <sipdomainName>avaya.com</sipdomainName>
        <treatasemergency>true</treatasemergency>
    </DigitmapFullTO>
</digitmapFullTOList>
```

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 domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

Creating Regular Expressions

The 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. On the System Manager console, select **Routing** > **Regular Expressions**.
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 routing policy and click **Remove**.
10. Click **Commit**.

Modifying Regular Expressions

The Regular Expressions screen enables you to modify regular expressions and associate them with routing policies.

1. On the System Manager console, select **Routing** > **Regular Expressions**. 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 routing policy and click **Remove**.
10. Click **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. On the System Manager console, select **Routing** > **Regular Expressions**.
2. To delete existing regular expressions, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the regular expression.

Button	Description
Delete	Confirms the deletion of the regular expression and also deletes the regular expression from the routing policy that it is associated to.
Cancel	Cancels the deletion of the regular expression.

Regular Expressions field descriptions

Use this page to create, modify, delete, and manage regular expressions.

Button	Description
Edit	Opens the Regular Expression Details page that you can use to modify the regular expressions.
New	Opens the Regular Expression Details page that you can use to create new regular expressions.
Duplicate	Creates a duplicate of the selected regular expression and assigns a new state to it.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the regular expression.
More Actions > **Refresh all data**	Refreshes all data. Any unsaved modifications are lost.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Regular Expressions**	Opens the Export Regular Expressions page that allows you to export the regular expressions 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 entities as a zipped file to a specified location.
Commit	Distributes the selected regular expressions to all the Session Manager instances in the enterprise.

Regular Expression Details field descriptions

Use this page to specify the regular expression details.

General

Name	Description
Pattern	Regular expression pattern that Session Manager tries to match. Allowed characters are A-Z a-z 0-9 @ - _ and meta characters are - [ ] ( ) { } | ? : + * ^ $. \\ . For example,

Name	Description
	• miller@company.com • company.org • .*@company.com
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Denies routing for a matched regular expression pattern.
Notes	Additional notes about the regular expression pattern.

Button	Description
Add	Associates a routing policy for the matched pattern.
Remove	Dissociates a routing policy from the matched pattern.
Commit	Saves the regular expression and distributes it to the Session Managers in the enterprise.
Cancel	Cancels the creation or modification of the regular expression.

Regular Expression List field descriptions

Use this page to view the regular expression associated with the selected routing policy.

Name	Description
Regular Expression	Displays the regular expression to be used for the selected routing policy.
Rank Order	Priority of the regular expression. Lower rank order means a higher priority.
Deny	Denies routing for a matched regular expression.
Notes	Additional notes for the regular expression.

Button	Description
Select	Associates the selected regular expression to a routing policy or dissociates it based on the Add or Remove option selected earlier.
Cancel	Cancels the association or dissociation of the regular expression.

Bulk import for Regular Expressions

Please follow these rules when creating an XML bulk import file:

- The pattern of a Regular Expression referred to as <regexpmap> must be unique.
- <routingpolicyNames> must refer to an existing Routing Policy with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Regular Expression.
- Multiple Routing Policy entries (<routingpolicyNames>) can be configured for one Regular Expression.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<regexpmapFullTOList>
    <RegexpmapFullTO>
        <notes>this is a test</notes>
        <deny>false</deny>
        <pattern>*.com</pattern>
        <rankorder>0</rankorder>
        <routingpolicyNames>toBerlin</routingpolicyNames>
    </RegexpmapFullTO>
</regexpmapFullTOList>
```

Defaults

Modifying the default settings

You can use the Defaults screen to change the default values or ranges for parameters that are used by the other Routing menu options

These values are used as defaults values of admin personal settings when creating new Routing entities. Modifying these values does not change the values of already created entities .

1. On the System Manager console, select **Routing** > **Defaults**. The Personal Settings screen is displayed.
2. Under **Adaptations**, specify the minimum and maximum number of characters for pattern matching. 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 **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.
5. Under **Domain Management**, specify a domain suffix.
6. Under **SIP Entities**, specify the following:
    a. Select the default SIP entity type from the **Type** drop-down menu. The default type is Session Manager.
    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.
    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 for the time range. 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:

Default Settings field descriptions on page 151

Default Settings field descriptions

Use this page to specify default settings for all the Routing menus on the right-hand side pane and to save them as your default personal settings.

Name	Description
Adaptations	
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 Patterns	
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.
Entity Links	
Listen Port	Number of the port to be used for 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.
Domain Management	
Suffix	The default suffix to be used for the domain name.
SIP Entities	
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 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 Ranges	
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.
Application Settings	

Name	Description
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 default settings.

Related topics:

Modifying the default settings on page 149

Chapter 6: Configuring and monitoring Session Manager instances

Dashboard

About Session Manager Dashboard

Session Manager Dashboard provides a snapshot view of the health and summary of all the administered Session Manager instances.

Session Manager Dashboard page field descriptions

Button	Description
Session Manager	Name of administered Session Manager instance. You can click on the link to go to the Session Manager Administration page.
Type	Shows the type of Session Manager instance, either as Core or Branch Session Manager.
Alarms	Count of raised alarms being demarcated on the basis of status codes as Major & Critical/Minor/Warning.
Tests Pass	Shows current results for periodic maintenance tests, green color suggests as passed and red as failed.
Security Module	Shows possible state of Security Module matching existing Security Module Status page "Up" (green) "Down" (red) "---" (unknown, yellow). You can click on the link to go to the detailed summary of the selected security module in the Security Module Status page.
Service State	Shows current service and management state of the selected Session Manager instance. It can be of the following types: • ME/MD for Management Enabled/Disabled • AN/DN for Accept New Service/Deny New Service

Button	Description
	You can click on the link to go to the Session Manager Administration page.
Entity Monitoring	Shows Monitoring status of selected session manager entity as number of down links and number of total links. You can click on the link to go to the Session Manager Entity Link Connection Status page.
Active Call Count	Shows the current active call counts for this session manager instance.
Registrations	Shows the registration summary. You can click on the link to go to the Registration Summary page.

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.

About NIC Bonding

NIC bonding enables two Ethernet interfaces on the Session Manager Security Module to act as one, providing redundancy. The NIC bonding driver is configured to use "active-backup" mode in which two Ethernet interfaces can be added as slaves to the NIC bonding driver interface. Only one slave in the bond is active and the other slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid any conflict with the switch. The NIC bonding interface needs only one IP Address and uses the public IP address of the Session Manager Security Module. The NIC bonding interface needs only one MAC address and uses the MAC address of the first slave Ethernet interface. More than one of the NICs enable bonding so that traffic can traverse either NIC connected to a separate L2 switch port based on the interface's link state.

The bonding driver supports two schemes for monitoring a slave interface's link state: the ARP monitor and the MII monitor.

Note:

Following is the mapping of the physical Ethernet interfaces:

- Eth0: Management
- Eth1: Services
- Eth2: Security Module (SIP/PPM) - Physical port 3
- Eth3: Backup interface for NIC bonding - Physical port 4

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. For a Session Manager SIP Entity type, you must administer the listen ports on the SIP entity form. These listen ports are used by endpoints to connect to Session Manager and can be used to map different ports to different domains.

1. On the System Manager Common Console, select **Elements > Session Manager** > **Session Manager Administration**.
2. Click **New** on the Session Manager Administration screen.
3. Under the **General** section, enter the following information:
   a. Select the **SIP Entity Name** from the drop-down list.
   b. In the **Description** field, add a description for this entity.
   c. In the **Management Access Point Host Name/IP** field, enter the IP address of the management interface (eth0) of the Session Manager server.
   d. Select the **Direct Routing to Endpoints** from the drop-down list.
   e. For **Adaptation for Trunk Gateway**, select **None** from the drop-down list.
4. Under the **Security Module** section, enter the following information to configure the Security Module:
   a. In the **Network Mask** field, enter the value for the network mask associated with the network that the Security Module network interface will be connected to.
   b. In the **Default Gateway** field, add the IP address of the default gateway.
   c. In the **Call Control PHB** field, use the default value of 46 (forward with highest priority).
   d. In the **QOS Priority** field, enter a 802.1q priority value. The default is 6.

e. In the **Speed & Duplex** field, select a value from the drop-down menu to configure the security module interface speed and duplex values.

f. In the **VLAN ID** field, enter an integer value. This is the VLAN that the Session Manager is to be associated with. Leave this field blank if VLANs are not in use.

SIP Entity IP Address field is populated as per the IP address of the SIP entity.

5. Under the **NIC Bonding** section, enable or disable NIC bonding by selecting or clearing the **Enable Bonding** check box.

6. Under the **NIC Bonding** section, select a monitoring mode for NIC bonding from the drop-down menu for **Device Monitoring Mode**

7. If you selected **ARP Monitoring** for **Device Monitoring Mode**, enter the following information:

   a. ARP Interval (msecs) — Specifies the ARP link monitoring frequency. The range is 50 to 1000. The default value is 100.

   b. ARP Target IP — Specifies the IP target of the ARP request which is sent to determine the health of the link to the targets. You can configure up to 3 IP addresses for ARP monitoring.

Due to a Red Hat Linux kernel limitation, monitor virtual IP addresses using MII mode.

8. If you selected **MII Monitoring** for **Device Monitoring Mode**, enter the following information:

   a. Link Monitoring Frequency (msecs) — Specifies the sampling period. The range is 50 to 500. The default value is 100.

   b. Down Delay (msecs) — Specifies the wait time for disabling a slave if a link failure is detected. The range is 50 to 1000. The default value is 200.

   c. Up Delay (msecs) — Specifies the wait time for enabling a slave if a link recovery is detected. The range is 50 to 1000. The default value is 200.

9. Under the **Monitoring** section, enter the following information to configure how this Session Manager instance should monitor SIP entities:

   a. Select or clear the **Enable Monitoring** check box to enable or disable monitoring of the SIP entities by this Session Manage instance.

   b. In the **Proactive cycle time (secs)** field, enter a value in seconds. The default is 900 seconds. Session Manager uses this value for monitoring and polling an administered SIP entity at this interval until that entity is reachable.

   c. In the **Reactive cycle time (secs)** field, enter a value in seconds. The default is 120 seconds.

   d. Iin the **Number of Retries** field, 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.

10. Under the **CDR** section, enter the following information:

    a. Select the **Enable CDR** check box to enable Call Detail Recording.

b. Enter a password that will be used to access the CDR record, and re-enter the password to confirm it. The password that you enter here becomes the default password for the **CDR_USER** user ID.

11. Under the **Personal Profile Manager (PPM) - Connection Settings** section, enter the following information:
    a. Select the **Limited PPM Client Connection** check box to enable the **Maximum Connection per PPM client** field. The default value is enabled.
    b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. The default value is 3.
    c. Select the **PPM Packet Rate Limiting** check box to enable the **PPM Packet Rate Limiting Threshold** field. The default value is enabled.
    d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. The range is 1-500. The default value is 50.
12. Under the **Event Server** section, select **Yes** or **No** for **Clear Subscription on Notification Failure**.
13. Click **Commit**.

Related topics:

Session Manager Administration page field descriptions on page 161
Add Session Manager page field descriptions on page 163

Viewing the Session Manager administration settings

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 161
View Session Manager page field descriptions on page 167

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 **Elements > 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 **NIC Bonding** section, change the following information if required:
   - To enable or disable NIC bonding, select or clear the **Enable Bonding** check box. NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to SM100 agent public IP Address to be applied on the NIC bonding interface.
   - Select one of the following modes of NIC bonding as supported by NIC bonding driver from the drop-down menu **Device Monitoring Mode**:
     - ARP Monitoring
     - MII Monitoring
   - Modify the following details related to ARP monitoring:
     - ARP Interval (msecs) — Specifies the ARP link monitoring frequency and range is from 50 to 1000 (default value is 100).
     - ARP Target IP — Specifies the IP target of the ARP request which is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring. Due to a Red Hat Linux kernel

     limitation, monitor virtual IP addresses using MII mode.

   - Modify the following details related to MII monitoring:
     - Link Monitoring Frequency (msecs) — Specifies the sampling period with range from 50 to 500 (default value is 100).
     - Down Delay (msecs) — Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).
     - Up Delay (msecs) — Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).
6. 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 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.

7. 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`.

8. **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. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.

   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value: 50.

9. **Event Server** section specifies the option to clear Subscription on Notification Failure.

10. Click **Commit**.

Related topics:

Session Manager Administration page field descriptions on page 161
Edit Session Manager page field descriptions on page 170

Deleting a Session Manager instance

1. From the navigation pane on the System Manager Common Console, click **Elements > 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:

Delete Confirmation page field descriptions on page 161
Session Manager Administration page field descriptions on page 161

Delete Confirmation page field descriptions

Button	Description
Delete	Deletes the selectedSession Manager instance.
Cancel	Cancels the deletion of the selected Session Manager instance

Related topics:

Deleting a Session Manager instance on page 161

Session Manager Administration page field descriptions

Global Settings

Button	Description
Save Global Settings	Configures global settings of all the configured session manager instances.
Allow Unauthenticated Emergency Calls	Specifies whether to allow unauthenticated users to make emergency calls.

Button	Description
Allow Unsecured PPM Traffic	Enables PPM traffic over HTTP so that it can continue to process phone login, download button labels, contact lists, and other services.
Failback Policy	Specifies manual and scheduled failback support for terminals.

Session Manager Instances

Button	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

Name	Description
Name	Name of administered Session Manager
Primary Communication Profiles	The number of Communication Profiles that use this Session Manager as their primary SIP controller.<n1>
Secondary Communication Profiles	The total number of Communication Profiles that use this Session Manager as their secondary SIP controller.<n2>
Maximum Active Communication Profiles	This Session Manager is the primary server for n1 Communication Profile(s) and will support up to additional n2 Communication Profile(s) if a single other Session Manager fails.

Branch Session Manager Instances

Button	Description
New	Opens the Add Branch Session Manager page that enables you to add a SIP entity as a new Branch Session Manager instance
View	Opens the View Branch Session Manager page that enables you to view an already added Branch Session Manager instance
Edit	Opens the Edit Branch Session Manager page that enables you to edit the properties of an already added Branch Session Manager instance
Delete	Opens the Delete Confirmation page that allows you to delete a SIP entity that is added as a Branch Session Manager instance

Name	Description
Name	Name of administered Branch Session Manager
Main CM for LSP	Main CM for the LSP associated with this Branch Session Manager
SIP Communication Profiles	The number of Communication Profiles assigned to this Branch Session Manager.

Related topics:

Adding a SIP entity as a Session Manager instance on page 155
Viewing the Session Manager administration settings on page 157
Modifying the Session Manager administration settings on page 158
Deleting a Session Manager instance on page 161
Adding a SIP entity as a Branch Session Manager instance on page 175
Viewing the Branch Session Manager administration settings on page 178
Modifying the Branch Session Manager administration settings on page 178
Deleting a Branch Session Manager instance on page 181

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	IP address of the Session Manager as specified in the SIP Entity Details screen.
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.

Name	Description
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.

NIC Bonding

Name	Description
Enable Bonding	Enables or disables NIC bonding. NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to SM100 agent public IP Address to be applied on the NIC bonding interface.
Device Monitoring Mode	Allows you to select ARP Monitoring or MII Monitoring as the modes of NIC bonding as supported by NIC bonding driver.
ARP Interval (msecs)	Specifies the ARP link monitoring frequency and range is from 50 to 1000 (default value is 100).
ARP Target IP	Specifies the IP target of the ARP request which is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring.
Link Monitoring Frequency (msecs)	Specifies the sampling period with range from 50 to 500 (default value is 100).

Name	Description
Down Delay (msecs)	Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).
Up Delay (msecs)	Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).

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 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. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the 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 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 login name for CDR access.

Name	Description
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 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 155

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 as specified in the SIP Entity Details screen. 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 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.

Name	Description
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.

NIC Bonding

Name	Description
Enable Bonding	NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to SM100 agent public IP Address to be applied on the NIC bonding interface.
Device Monitoring Mode	Shows ARP Monitoring or MII Monitoring as the modes of NIC bonding as supported by NIC bonding driver.
ARP Interval (msecs	Specifies the ARP link monitoring frequency and range is from 50 to 1000 (default value is 100).
ARP Target IP	Specifies the IP target of the ARP request which is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring.
Link Monitoring Frequency (msecs)	Specifies the sampling period with range from 50 to 500 (default value is 100).
Down Delay (msecs)	Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).
Up Delay (msecs)	Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).

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 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

Button	Description
	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 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 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 login name for CDR access.
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 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 157

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 as specified in the SIP Entity Details screen
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

Name	Description
	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 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.

NIC Bonding

Name	Description
Enable Bonding	Enables or disables NIC bonding. NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to SM100 agent public IP Address to be applied on the NIC bonding interface.
Device Monitoring Mode	Allows you to select ARP Monitoring or MII Monitoring as the modes of NIC bonding as supported by NIC bonding driver.
ARP Interval (msecs)	Specifies the ARP link monitoring frequency and range is from 50 to 1000 (default value is 100).
ARP Target IP	Specifies the IP target of the ARP request which is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring.
Link Monitoring Frequency (msecs)	Specifies the sampling period with range from 50 to 500 (default value is 100).
Down Delay (msecs)	Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).
Up Delay (msecs)	Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000 (default value is 200).

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 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 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 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 login name for CDR access.
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.

Name	Description
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 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 158

Saving Global Session Manager Settings

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Session Manager Administration** to open the Session Manager Administration screen.
2. On the Session Manager Administration screen under Global Settings section, click **Save Global Settings** to configure global settings of all the configured session manager instances.

3. Select the **Allow Unauthenticated Emergency Calls** check box to specify whether emergency calls (based on dial pattern) need to authenticated or not. Check this box to allow unauthenticated users to make emergency calls.
4. Select the **Allow Unsecured PPM Traffic** check box to enable PPM traffic over HTTP so that it can continue to process phone login, download button labels, contact lists, and other services.
5. Select the **Failback Policy** check box to specify manual and scheduled failback support for terminals. Session Manager sends out unsolicited NOTIFY messages to terminals that have previously failed over. Phones uses the unsolicited NOTIFY message to register with the highest priority server in the terminal's administered list of servers. The NOTIFY messages are send out to avoid a re-registration and re-subscription flood upon the failback.

Branch Session Manager Administration

About Branch Session Manager

Branch Session Manager provides a SIP-enabled branch survivability solution. It allows a customer who has deployed SIP phones in a branch to receive LSP-style survivability. For example, when the core Session Manager is unreachable, the SIP phones receive their Communication Manager features from the LSP.

Branch Session Manager supports phones which simultaneously register with both the primary (and secondary, if configured) Session Managers in the core, and also with the Branch Session Manager. The phones accept incoming calls from any of these servers. Thus there is no outage to basic calling when a failure occurs and the phone is ready to receive a call from any of its servers.

A typical branch setup contains the following components:

1. Branch Session Manager provides service to users in case there is a WAN failure between branch and core.
2. Media Gateway provides among other functions the ability to connect branch to PSTN and media services such as conferencing, tones, and announcements.

3. LSP is a survivable processor for branch Media Gateway. The LSP starts to work when the Media Gateway loses connectivity with Trunk Gateway, and register itself to LSP.
4. End user devices (phones) register with the primary Session Manager as a primary controller, but uses Branch Session Manager as a third controller (in case of WAN failure).

Branch Session Manager provides service when the branch loses WAN connectivity. As the result of WAN failure, there are two simultaneous process triggered:

- Branch Media Gateway loses connectivity with Trunk Gateway, and registers itself to Communication Manager LSP. As the result, the LSP starts to provide service.
- The phones detect losing connectivity with core Session Manager and register the Branch Session Manager as the new controller.

Note:

Branch Session Manager may not provide normal service in various partial failure scenarios such as core Communication Manager goes down but Session Manager is up.

Branch Session Manager has the same specifications as a Session Manager, and provides local autonomy or survivability for SIP stations, trunks and applications. When signaling is available to the core Session Manager, branch SIP users can avail sequenced applications. A Branch Session Manager serves at most one user community and does not directly connect to each of the core Session Managers. It only connects to the two core Session Managers which serve its user community.

Adding a SIP entity as a Branch Session Manager instance

Prerequisites

Before starting this procedure, make sure that the SIP entity that you want to add was created. 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 Branch Session Manager and they can be used to map different ports to different domains.

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Session Manager Administration**.
2. Click **New** on the Branch Session Manager Instances section of Session Manager Administration screen. The system displays the Add Branch 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 Branch Session Manager is installed.
- Select the **Main CM for LSP** from the drop-down list. Click the **View / Add CM Entities** link to add new CM applications.
- Select the **Direct Routing to Endpoints** from the drop-down list.
- Select the **Adaptation for Trunk Gateway** from the drop-down list. This selected adaptation is used by the Branch Session Manager for digit conversion when routing calls to or from the Communication Manager LSP trunk gateway.

Note:

To be a part of the Branch Session Manager instances network of an enterprise, a Branch 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 Branch 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:
   - 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, Branch 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 Branch 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 Branch Session Manager is to be associated with. Call traffic segregation could be based on the VLAN associated with the Branch Session Manager.

SIP Entity IP Address field is populated as per the IP address of the SIP entity.

5. Under the **Monitoring** section, enter the following information to configure how this Branch Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Branch 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. Branch 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.

     Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the 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 Branch Session Manager polls a SIP entity before it is deemed unreachable. The default is 1.
6. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Branch Session Manager 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. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value: 50.

During normal operation, Branch Session Manager receives data from a Communication Manager feature server for synchronization to Avaya SIP endpoints.

7. **Event Server** section specifies the option to clear Subscription on Notification Failure.
8. Click **Commit** .

Related topics:

Session Manager Administration page field descriptions on page 161
Add Branch Session Manager page field descriptions on page 182

Viewing the Branch Session Manager administration settings

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Session Manager Administration**.
2. In the Branch Session Manager Instances section, select a Branch Session Manager from the Branch Session Manager Instances list and click **View**. The View Branch Session Manager screen displays information about the selected Branch Session Manager instance.
3. After you have viewed the information, click **Return**.

Related topics:

Session Manager Administration page field descriptions on page 161
View Branch Session Manager page field descriptions on page 184

Modifying the Branch Session Manager administration settings

This option allows you to modify the configuration settings for an already configured Branch Session Manager.

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Session Manager Administration**.
2. Click **Edit** on the Branch Session Manager Instances section of Session Manager Administration screen. The system displays the Edit Branch Session Manager screen.

3. Under the **General** section, change the following information, if required:
    - Add a comment in the Description field for the Branch Session Manager SIP entity.
    - Change the IP address of the host on which the Branch 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 Branch Session Manager application. Branch 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 Branch Session Manager instances network of an enterprise, a Branch Session Manager instance must first be administered as a management access point.
    - Select the **Main CM for LSP** from the drop-down list. Click the **View / Add CM Entities** link to add new CM applications.
    - Select the **Direct Routing to Endpoints** from the drop-down list.
    - Select the **Adaptation for Trunk Gateway** from the drop-down list. This selected adaptation is used by the Branch Session Manager for digit conversion when routing calls to or from the Communication Manager LSP trunk gateway.
4. Under the **Security Module** section, change the following information, if required
    - Modify the network mask in the **Network Mask** field. Branch 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, Branch 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 Branch 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 Branch Session Manager is to be associated with. Call traffic segregation could be based on the VLAN that the Branch Session Manager is associated with.

5. Under the **Monitoring** section, modify the following information as required to configure how this Branch Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Branch 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.
   - Branch 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.

     Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the 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 Branch Session Manager polls a SIP entity before it is deemed unreachable.
6. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Branch Session Manager 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. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value: 50.

   During normal operation, Branch Session Manager receives data from a Communication Manager feature server for synchronization to Avaya SIP endpoints.

7. **Event Server** section specifies the option to clear Subscription on Notification Failure.
8. Click **Commit**.

Related topics:

Session Manager Administration page field descriptions on page 161
Edit Branch Session Manager page field descriptions on page 187

Deleting a Branch Session Manager instance

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Session Manager Administration**.
2. Select a Branch Session Manager instance from the list and click **Delete**.
3. On the Delete Confirmation screen, click **Delete** to delete the Branch Session Manager instance.

Related topics:

Session Manager Administration page field descriptions on page 161
Delete Confirmation page field descriptions on page 181

Delete Confirmation page field descriptions

Button	Description
Delete	Deletes the selected Branch Session Manager instance.
Cancel	Cancels the deletion of the selected Branch Session Manager instance.

Related topics:

Deleting a Branch Session Manager instance on page 181

Add Branch 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 Branch 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 Branch Session Manager is installed.
Main CM for LSP	Main CM for the LSP associated with this Branch Session Manager.
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.
Adaptation for Trunk Gateway	Enables digit conversion when routing calls to or from the Communication Manager LSP trunk gateway.

Security Module

Name	Description
SIP Entity IP Address	IP address of the Branch Session Manager as specified in the SIP Entity Details screen.
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, Branch Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.

Name	Description
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 Branch 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 Branch Session Manager should be associated with. Call traffic segregation could be based on the VLAN that the Branch Session Manager is associated with.

Monitoring

Button	Description
Enable Monitoring	Select to enable monitoring of the administered SIP entities by the added Branch 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 Branch 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 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. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.
Number of Retries	Enter an integer value. This value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable. The default is 1. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.

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 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 Branch Session Manager addition operation.
Commit	Saves the added SIP entity as a Branch Session Manager instance with the selected configuration options.

Related topics:

Adding a SIP entity as a Branch Session Manager instance on page 175

View Branch 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 Branch Session Manager is installed. View-only field.
Main CM for LSP	Main CM for the LSP associated with this Branch Session Manager.

Name	Description
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.
Adaptation for Trunk Gateway	Enables digit conversion when routing calls to or from the Communication Manager LSP trunk gateway.

Security Module

Name	Description
SIP Entity IP Address	IP address of the Branch Session Manager as specified in the SIP Entity Details screen. 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 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, Branch 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 Branch Session Manager should be associated with. Call traffic segregation could be based on the VLAN that the Branch 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 Branch Session Manager instance. If the check box is not selected, monitoring is disabled. View-only.

Button	Description
Proactive cycle time (secs)	Time in seconds for polling the administered SIP entities by the added Branch 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 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. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.
Number of Retries	This integer value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable. The default is 1. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.

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 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 Branch Session Manager administration settings on page 178

Edit Branch Session Manager page field descriptions

General

Name	Description
SIP Entity Name	Name of the SIP entity that is added as a Branch 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 Branch 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 Branch Session Manager application. Branch 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 Branch Session Manager instances network of an enterprise, a Branch Session Manager instance must first be administered as a management access point.
Main CM for LSP	Main CM for the LSP associated with this Branch Session Manager.
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.
Adaptation for Trunk Gateway	Enables digit conversion when routing calls to or from the Communication Manager LSP trunk gateway.

Security Module

Name	Description
SIP Entity IP Address	IP address of the Branch Session Manager as specified in the SIP Entity Details screen.
Network Mask	Specifies the network mask in the Network Mask field. Branch 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

Name	Description
	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, Branch Session Manager uses a default DSCP value of 46 which indicates forwarding with the highest priority.
QOS Priority	This specifies the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Branch 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 Branch Session Manager should be associated with. Call traffic segregation could be based on the VLAN that the Branch 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 Branch 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 Branch 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 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. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.
Number of Retries	This integer value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable. The default is 1.

Button	Description
	Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.

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 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 Branch Session Manager editing operation.
Commit	Saves the Branch Session Manager instance with the modified configuration options.

Related topics:

Modifying the Branch Session Manager administration settings on page 178

Communication Profile Editor

About Communication Profile Editor

Communication Profile Editor provides users with an enterprise view of all configured Session Manager Communication Profiles and provides the following set of functionality:

- viewing the listing of all existing Session Manager Communication Profiles with advanced options of sorting and filtering.
- bulk editing of required Communication Profile attributes across selected Communication Profiles. For example, replacement of a Session Manager instance across all the selected Communication Profiles. This is an enhancement over editing of individual profiles using User Profile Edit screen.
- viewing the background edit job status of bulk editing of Communication Profile.
- viewing Communication Profile edit failures during bulk editing operations.

Important:

A user's SIP phone is added to the Aura Network by assigning the user a Communication Profile containing a Communication Manager endpoint profile and a Session Manager profile. The Communication Manager profile associates the user with a station on a Communication Manager that is in the core network. The Session Manager profile assigns the user's primary and secondary Session Managers, application sequences and survivability server. For correct application sequencing to Communication Manager, the application sequences must reference one and the same Communication Manager as the Communication Manager endpoint profile. For correct survivability configuration, if a Branch Session Manager is specified as the survivability server, the Branch Session Manager must also reference the same Communication Manager as the Communication Manager endpoint profile.

Viewing Communication Profiles

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Communication Profile Editor** to open Communication Profile Editor screen.

The Communication Profile Editor screen displays under the Session Manager Communication Profiles section the list of all the Session Manager Communication Profiles provisioned for all the registered users.

2. To view using sorting option, click a column title to sort the information in the table as the primary sorting order.
3. To view using filtering option, enable **Filter** option. Filtering can be as a compound of one or more fields. On filtering, the table displays only those results that match the filtering criteria.

Modifying Communication Profiles

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Communication Profile Editor** to open Communication Profile Editor screen.
2. In the Session Manager Communication Profiles section, select the rows that need to be modified. Click the **All** link at the bottom left of the table to select all of the rows.
3. In the New Communication Profile Values section, all fields initially have the default value as “Use existing values”. Modify the field values to be set as property values for the selected list of Communication Profiles.

   You cannot set the value for **Primary Session Manager** and **Home Location** fields as “None”. For adding a new value for the **Home Location** field, you need to add location using **Routing** > **Locations** menu selection.
4. Click **Commit Changes** to save the changes. In the Communication Profile Edit Confirmation screen, click **Commit** to save the changes.

Viewing background edit job status

When the number of simultaneous Communication Profile editing operations exceed 15 then these operations are queued as batch jobs.

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Communication Profile Editor** to open Communication Profile Editor screen.
2. Under Background Edit Job Status section, you can view the status of all background edit jobs since the last restart of System Manager.

Viewing Communication Profile edit failures

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **Communication Profile Editor** to open Communication Profile Editor screen.
2. Under Background Edit Job Status section, select the edit job which did not finish running successfully.
3. Click **View Profile Edit Failures** to view the details of all Communication Profiles which could not be modified in the selected job run.
   The Session Manager Communication Profiles section shows the details of those existing profiles which could not be edited due to the failed job run.
4. Click **Return to View All Profiles** for returning to the original Communication Profile Editor screen.

Communication Profile Editor field descriptions

Session Manager Communication Profiles

Name	Description
Login Name	Full login name of the user and is a unique name that gives access to the system.
Address: Handle	Handle part of the Communication Address. **Note:** The displayed address can be either the “E.164 ” or the “Avaya E. 164” address as specified in the User Profile page.

Name	Description
Address: Domain	Domain part of the Communication Address.
Primary Session Manager	Name of the primary Session Manager which acts as the default access point for connecting devices associated with the Communication Profile to the Aura network. This is a mandatory field.
Secondary Session Manager	Name of the secondary Session Manager which provides continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available.
Origination Application Sequence	Defines application sequences for calls from this user.
Termination Application Sequence	Defines application sequences for calls to this user.
Survivability Server	Name of the Survivability Server which provides survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. For a Branch Session Manager, if the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. **Note:** If a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.
Home Location	Name of a Home Location to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules applies to the call based on the home location regardless of the physical location of the SIP device used to make the call. This is a mandatory field. **Note:** A user's call is routed according to the user's home location except for the following cases: • CAC (Call Admission Control) routes based on actual location • Emergency calling routes based on actual location

The field descriptions for **New Communication Profile Values** section are same as mentioned above.

Background Edit Job Status

This section provides a list of Communication Profile editing operations that run as background jobs since the last restart of System Manager. When the number of simultaneous Communication Profile editing operations exceed 15 then these operations are queued as batch jobs.

Name	Description
Start Time	Start time of the background edit job.
Status	Status of completion of the background edit job.
Percent Completed	Percentage completion of the background edit job.
Total Edits to Perform	Number of background edits performed in the job run.
Failed Edits	Number of failed background edits during the job run.
Last Updated	Finish time of the background edit job run.
Job Name	Name of the background edit job.

Button	Description
View Profile Edit Failures	Shows the details of all Communication Profiles which could not be modified in the selected job run. It also states the reason for such editing failures.
Stop Job	This operation stops the current running background edit job.

Communication Profile Edit Confirmation page field descriptions

This page has the following sections —

- Message Area section shows the messages related to those Communication Profile edit operation which run as background jobs.
- New Profile Values and Profiles to Update section shows the new attributes for the selected list of Communication Profiles. Following table shows the field descriptions —

Name	Description
Login Name	Full login name of the user and is a unique name that gives access to the system.
Address: Handle	Handle part of the Communication Address. **Note:** The displayed address can be either the “E.164 ” or the “Avaya E. 164” address as specified in the User Profile page.
Address: Domain	Domain part of the Communication Address.

Name	Description
Primary Session Manager	Name of the primary Session Manager which acts as the default access point for connecting devices associated with the Communication Profile to the Aura network.
Secondary Session Manager	Name of the secondary Session Manager which provides continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available.
Origination Application Sequence	Defines application sequences for calls from this user.
Termination Application Sequence	Defines application sequences for calls to this user.
Survivability Server	Name of the Survivability Server which provides survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. For a Branch Session Manager, if the termination and origination application sequences contain a Communication Manager application, sequencing to this application will continue, locally, to the Communication Manager LSP resident with the Branch Session Manager. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager associated with the application must be the main Communication Manager for the Communication Manager LSP that is resident with the Branch Session Manager.
Home Location	Name of a Home Location to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules applies to the call based on the home location regardless of the physical location of the SIP device used to make the call. **Note:** A user's call is routed according to the user's home location except for the following cases: • CAC (Call Admission Control) routes based on actual location • Emergency calling routes based on actual location

Button	Description
Commit	Saves the changes to the selected Session Manager Communication Profiles.
Cancel	Cancels the changes to the selected Session Manager Communication Profiles.

Network Configuration

Local Host Name Resolution

About Local Host Name Resolution

Session Manager can locally resolve hostnames into an ordered set of (IP address, port, and transport) tuples and can assign priority and weights to each tuple. Local Hostname Resolution is only applied to hostnames provisioned by the administrator and overrides normal DNS resolution. For example, if the Session Manager is attempting to resolve nj.proxy.avaya.com, and that hostname is provisioned as a local hostname, the Session Manager will skip DNS resolution and instead determine the request target using the tuples for nj.proxy.avaya.com that it has been provisioned with. 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 **Elements > 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 (FQDN)**: Enter Fully Qualified Domain Name or IP address of the host. 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.

Note:

You can import or export XML Schema instance file containing LHN entries using **More Actions** menu on the Local Host Name Resolution page.

Local Host Name Schema

XML schema provides the format for generation of XML schema instance file in the event of import of Local Host Name data.

Example

The format of the JAXB-compliant XSD schema of the XML files used in the Local Host Name Import and Export feature is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:jxb="http://java.sun.com/xml/ns/jaxb"
            jxb:version="2.0">

<xsd:annotation>
  <xsd:documentation xml:lang="en">
    XML schema definition for 'Local Host Name Resolution' entries.

    Copyright Avaya Inc., All Rights Reserved
    THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF AVAYA INC
    The copyright notice above does not evidence any
    actual or intended publication of such source code.
    Some third-party source code components may have been modified from
    their original versions by Avaya Inc.
    The modifications are Copyright Avaya Inc., All Rights Reserved.
  </xsd:documentation>
</xsd:annotation>

<xsd:element name="LocalHostNameEntries" type="LocalHostNameEntryListType"/>

<xsd:complexType name="LocalHostNameEntryListType">
```

```
        <xsd:sequence>
              <xsd:element name="LocalHostNameEntry" type="LocalHostNameEntryType"
                                        maxOccurs="unbounded"/>
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="LocalHostNameEntryType">
  <xsd:sequence>
    <xsd:element name="hostName" type="hostNameType"/>
    <xsd:element name="ipAddress" type="ipAddressType"/>
    <xsd:element name="port" type="portType"/>
    <xsd:element name="priority" type="priorityType"/>
    <xsd:element name="weight" type="weightType"/>
    <xsd:element name="transport" type="transportType"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="hostNameType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength  value="1"/>
    <xsd:maxLength  value="255"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="ipAddressType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength  value="7"/>
    <xsd:maxLength  value="15"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="portType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="65535"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="priorityType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="2147483647"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="weightType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="100"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="transportType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="TLS"/>
    <xsd:enumeration value="TCP"/>
    <xsd:enumeration value="UDP"/>
  </xsd:restriction>
</xsd:simpleType>
```

```
</xsd:schema>
```

Example

A sample XML Schema file is provided below for reference purpose:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<LocalHostNameEntries>
        <LocalHostNameEntry>
                <hostName>www.domain1.com</hostName>
                <ipAddress>192.168.1.100</ipAddress>
                <port>1024</port>
                <priority>900</priority>
                <weight>50</weight>
                <transport>TLS</transport>
        </LocalHostNameEntry>
        <LocalHostNameEntry>
                <hostName>www.domain2.com</hostName>
                <ipAddress>192.168.1.101</ipAddress>
                <port>1024</port>
                <priority>600</priority>
                <weight>25</weight>
                <transport>TCP</transport>
        </LocalHostNameEntry>
</LocalHostNameEntries>
```

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
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
More Actions > **Import Local Host Name Entries**	Opens Import Local Host Name Entries page where you can select (for importing or uploading) an XML Schema instance file containing a list of LHN entries for adding to the LHN resolution table.
More Actions > **Export Local Host Name Entries**	Allows you to Export (download) an XML Schema instance file containing a list of LHN entries currently in the LHN resolution table.
More Actions > **Get Local Host Name Schema**	Allows you to get/retrieve the XML Schema for the current version of the Session Manager release. This enables you to understand the XML schema format for a creating new XML schema instance file for import purpose.

Name	Description
Host Name (FQDN)	Enter Fully Qualified Domain Name or IP address of the host. 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 (FQDN)	Enter Fully Qualified Domain Name or IP address of the host. The 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 (FQDN)	Enter Fully Qualified Domain Name or IP address of the host. 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. On the System Manager console, select **Elements > Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Click the **Session Manager Instances** button to display the list of Session Manager instances.
3. Select a Session Manager instance from the list.
4. 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.
5. To use the default rules: Session Manager instance(s).
   a. Click on **More Actions**
   b. Select **Retrieve Default Configuration**.
   c. click **Save** to save the configuration to the selected Session Manager instance(s).
6. 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.
   - **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.
7. 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.

8. 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.

9. 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

10. 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 204
Blacklist on page 207
Whitelist on page 207
Rules on page 207
Rule precedence and traversal on page 215

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.
Rules: Name	Name of the SIP firewall rule. The name can have a maximum of 80 characters.

Name	Description
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” SIP Header. Its value can be a complete or partial SIP URI, for example,

Name	Description
	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.

Related topics:

Configuring the SIP Firewall on page 202

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 208
Rule page field descriptions on page 211
Deep inspection filtering on page 214
Denial of Service protection on page 214

SIP Firewall default rule set on page 215

Specifying a new SIP Firewall rule

1. From the navigation pane, click **Elements > 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.
   - Log Message—Specify the log message to display if Log Type is set to Yes or Alarm.
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 is matched against all incoming SIP Traffic
   - **SIP UA Connection:** If this option is selected, SIP Firewall rule is matched against the incoming SIP traffic from entities that are not the Trusted SIP Entity (as defined by the 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 is matched against the incoming SIP traffic from entities that are marked as Trusted SIP Entity in the Routing Policy.

   Note:

   If there are any untrusted SIP Entities connected to the Session Manager (as defined by 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**.

Related topics:

Rule page field descriptions on page 211

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.

Name	Description
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. 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. 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.

Connection:

Name	Description
Connection Type	Following are the possible connection types: • **Any:** This is a default choice. If this option is selected, SIP Firewall rule is matched against all incoming SIP Traffic • **SIP UA Connection:** If this option is selected, SIP Firewall rule is matched against the incoming SIP traffic from entities that are not the Trusted SIP Entity (as defined by the Routing Policy). This option is

Name	Description
	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 is matched against the incoming SIP traffic from entities that are marked as Trusted SIP Entity in the Routing Policy.

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

Related topics:

Specifying a new SIP Firewall rule on page 208

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. Device Settings Groups of type Location Groups can be associated with Locations while Device Settings Groups of type Terminal Groups can only be associated with a terminal respectively having a Terminal Group ID. 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 which are downloaded and set as per the following criteria.

- The configuration of a terminal is set as the "Default Device Settings" if the terminal
  - does not belong to an “Routing Policy Location”
  - or the “Network Routing Policy Location” where the terminal is located has no specific set of Personal Profile Manager (PPM) attributes
  - and the Terminal is not associated with a specific set of Personal Profile Manager (PPM) attributes
- The configuration of a terminal is set as the set of attributes defined for a “Routing Policy Location” if the terminal
  - is located in that “Routing Policy Location”
  - and the terminal is not individually associated with a specific set of PPM attributes
- The configuration of a terminal is set as a specific set of PPM attributes if the terminal
  - is individually associated with a set of PPM attributes
  - and the selected set of PPM attributes does still exist

Viewing Device Settings Groups

From the navigation pane on the System Manager Common Console, click **Elements > 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 220

Creating a Device Settings Group - Location Group

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 restore the default values of the parameters.

Related topics:

Device Settings Groups field descriptions on page 220
Device Settings Group - Location Group field descriptions on page 223

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 **Elements > 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 restore the default values of the parameters.

Related topics:

Device Settings Groups field descriptions on page 220
Device Settings Group - Location Group field descriptions on page 223

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 **Elements > 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 220
Device Settings Group - Location Group field descriptions on page 223

Creating a Device Settings Group - Terminal Group

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 restore the default values of the parameters.

Related topics:

Device Settings Groups field descriptions on page 220
Device Settings Group - Terminal Group field descriptions on page 223

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 **Elements > 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 restore the default values of the parameters.

Related topics:

Device Settings Groups field descriptions on page 220
Device Settings Group - Terminal Group field descriptions on page 223

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 **Elements > 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 220
Device Settings Group - Terminal Group field descriptions on page 223

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.

Terminal Groups

Name	Description
Name	Shows the name of the Terminal Device Settings Group.
Terminal Group Number	Specifies 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 Terminal Device Settings Group.

Location Groups

Name	Description
Name	Shows the name of the Location Device Settings Group.
Description	Shows the details of Location Device Settings Group.

Related topics:

Viewing Device Settings Groups on page 216
Creating a Device Settings Group - Location Group on page 217
Modifying a Device Settings Group - Location Group on page 217
Removing Device Settings Groups - Location Groups on page 218
Creating a Device Settings Group - Terminal Group on page 218
Modifying a Device Settings Group - Terminal Group on page 218
Removing Device Settings Group - Terminal Group on page 219

Device Settings Group - Default Group field descriptions

General section

Name	Description
Name	Specifies a non—editable field as Default Group.
Description	Specifies a non—editable field as Default Group.
Group Type	Specifies a non—editable field as Location Group
Terminal Group Number	Specifies a non—editable field.

Server Timer section

Name	Description
Subscription Expiration Timer (secs)	Specifies the maximum duration as 86400 and minimum duration as 1500 seconds for a SIP server to keep a SIP client as subscribed.
Registration Expiration Timer (secs)	Specifies the maximum duration as 3600 and minimum duration as 300 seconds for a SIP server to keep a SIP client as registered.

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Specifies 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.
Reactive Monitoring Interval (secs)	Specifies the duration after which (in seconds) the phone attempts to REGISTER with a proxy server when it is not reachable/available. Range is 10 to 3600 seconds. The default is 60 seconds.
Timer B (sec)	Specifies the duration (in seconds) that the phone waits for a provisional response after transmitting a SIP INVITE to a proxy server and after not receiving any response from proxy being unavailable or unreachable, proceeds to another proxy. The range is 0 to 32 seconds. (0 disables this feature.) The default value is 2.

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:	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.

Device Settings Group - Location Group field descriptions

General section

Name	Description
Name	Shows the name of the Location Device Settings Group.
Description	Shows Location Device Settings Group details.
Group Type	Shows a non-editable field specifying the type of Device Setting as Location Group

Server Timer section

Name	Description
Subscription Expiration Timer (secs)	Specifies the maximum duration as 86400 and minimum duration as 1500 seconds for a SIP server to keep a SIP client as subscribed.
Registration Expiration Timer (secs)	Specifies the maximum duration as 3600 and minimum duration as 300 seconds for a SIP server to keep a SIP client as registered.

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 217
Modifying a Device Settings Group - Location Group on page 217
Removing Device Settings Groups - Location Groups on page 218

Device Settings Group - Terminal Group field descriptions

General section

Name	Description
Name	Specifies the name of the Terminal Device Settings Group.
Description	Specifies Terminal Device Settings Group details.
Group Type	Specifies a non editable field specifying the type of Device Setting as Terminal Group

Name	Description
Terminal Group Number	Specifies the Device Settings Group number

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Specifies 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.
Reactive Monitoring Interval (secs)	Specifies the duration after which (in seconds) the phone attempts to REGISTER with a proxy server when it is not reachable/available. Range is 10 to 3600 seconds. The default is 60 seconds.
Timer B (sec)	Specifies the duration (in seconds) that the phone waits for a provisional response after transmitting a SIP INVITE to a proxy server and after not receiving any response from proxy being unavailable or unreachable, proceeds to another proxy. The range is 0 to 32 seconds. (0 disables this feature.) The default value is 2.

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.
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:	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.

Name	Description
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 218
Modifying a Device Settings Group - Terminal Group on page 218
Removing Device Settings Group - Terminal Group on page 219

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 **Elements > 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 226

Modifying Location Settings

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 226

Location Settings field descriptions

Name	Description
Name	Is the name of the Location.
Device Setting Group	Is the name of the Device Setting Group.

Related topics:

Viewing location settings on page 225
Modifying Location Settings on page 226

Application Configuration

Applications

About Applications

Application entries allow you to define and manage single applications with application attributes for inclusion into one or more application sequence.

Viewing applications

From the navigation pane on the System Manager Common Console, click **Elements > 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 topic “Creating SIP entities” to create the SIP entity.

1. On the System Manager console, select **Elements > Session Manager** > **Application Configuration** > **Applications** to open the Applications screen.
2. Click **New**. The Application Editor screen appears.
3. Enter the appropriate information for the new application.
4. Click **Commit** to create the application.

Related topics:

Applications field descriptions on page 229

Application Editor field descriptions on page 229

Modifying an application

You can modify only one application at a time.

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 229
Application Editor field descriptions on page 229

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 **Elements > 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 229

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 227
[Modifying an application](#) on page 228
[Removing applications](#) on page 228

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.
CM System for SIP Entity	Provides a list of previously provisioned CM systems. This is a mandatory field. **Note:** This selection of CM System for SIP entity associates a Communication Manager Feature Server for call sequencing. **Refresh:** Updates the list of CM Systems. **View/Add CM Systems:** Enables adding and viewing of currently provisioned CM Systems.
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 227
Modifying an application on page 228

Application Sequences

Application Sequences

Application Sequence enables defining and managing an ordered set of applications used in call sequencing. These application sets can be associated as the originating and terminating application templates for a registered user's "Communication Profile" in the User Management module and enable routing every incoming, outgoing, or combined call for that user. Applications are assigned based on the user's needs and are irrespective of location or the device used.

Session Manager provides the capability to create a profile for third party PBX users and add applications to be applied to these users to provide services such as block calls based on user preferences, direct calls to these users when they move across the enterprise, and augment caller ID information for incoming and outgoing calls – all without upgrades or code modifications to existing third party PBX-equipment.

Viewing application sequences

From the navigation pane on the System Manager Common Console, click **Elements > 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. On the System Manager console, select **Elements > Session Manager** > **Application Configuration** > **Application Sequences** to open the Application Sequences screen.
2. Click **New**. The Application Sequence Editor screen appears.
3. Enter the appropriate information.
4. Click **Commit** to create the Application Sequence.

Related topics:

Application Sequences field descriptions on page 233
Application Sequence Editor field descriptions on page 233

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 **Elements > 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 233
Application Sequence Editor field descriptions on page 233

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 **Elements > 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 233
Application Sequence Editor field descriptions on page 233

Rearranging Applications in an Application Sequence

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 233
Application Sequence Editor field descriptions on page 233

Adding Applications in an existing Application Sequence

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 233
Application Sequence Editor field descriptions on page 233

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 231
Modifying an Application Sequence on page 231
Removing Application Sequences on page 231
Rearranging Applications in an Application Sequence on page 232
Adding Applications in an existing Application Sequence on page 233

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 231
Modifying an Application Sequence on page 231
Removing Application Sequences on page 231
Rearranging Applications in an Application Sequence on page 232
Adding Applications in an existing Application Sequence on page 233

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 **Elements > 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 236

Creating an Implicit User

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 236
Implicit User Rule Editor field descriptions on page 237

Modifying an existing Implicit User

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 236
Implicit User Rule Editor field descriptions on page 237

Removing existing Implicit Users

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 236

Implicit User Rules field descriptions

Name	Description
Pattern	Shows the dial pattern with the same pattern format as the 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 235
Creating an Implicit User on page 235
Modifying an existing Implicit User on page 236
Removing existing Implicit Users on page 236

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 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
Termination Application Sequence	Shows the name of the Termination Application Sequence

Related topics:

Creating an Implicit User on page 235
Modifying an existing Implicit User on page 236

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 **Elements > 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 data is loaded asynchronously in the background. 'Loading...' message appears when data loading occurs behind the scenes. 'Loading Complete.' message appears when data loading finishes. 'Loading failure. Please try again.' message appears if there is a long waiting time for the data and the user is requested to try again later.

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.
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. It is of the following format: <major release number>.<minor release number>.<service pack number>.<patch number>.<build number>

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 Security Module is functional.

SIP Monitoring setup is administered through the 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 **Elements > 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	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

Button	Description
Instances: Refresh	• 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 **Elements > 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 Routing Policy. • Bandwidth per Call (kbit/sec) — This is the value that you enter in the Routing Location Details page. • 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 the Security Module Status page:

- **Refresh** – refreshes the statistics for all of the administered Session Manager instances..
- **Reset** – resets the security module for the selected Session Manager. You 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.
- **Update Installed Certificates** – provides the capability of switching the active certificate being used by the security module to the default certificate. Additionally, refer to **Security Design** in *Administrating Avaya Aura™ Session Manager*, 03–603324 to understand the implications of doing this operation.
- **Connection Status** — allows you to view the current status of inbound and outbound links between the Session Manager security module and external hosts. It enables general-purpose monitoring and debugging activities such as:
  - identifying if Session Manager is required to be taken out of service
  - determining if links are secured or not
  - viewing link details and statistics

Investigating Security Module “Down” status

Possible causes for the Security Module 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.

---

1. Select **System Manager Data** > **Replication** on the System Manager console.
2. If the **Status** is not **IN_SYNC**,
3. Select **Elements** > **Session Manager** > **System Status** > **Security Module Status**

4. Click the **Refresh** button to see the latest status.
5. If the status is **Down**, synchronize the security module to trigger an update:
   a. Select the appropriate system from the System Name list.
   b. Click the **Synchronize** button.
   c. Click the **Refresh** button to see the latest status.
6. If the status is still **Down**, reset the security module:
   a. Select the appropriate system from the System Name list
   b. Select the **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.
7. 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: • Session Manager—Session Manager instance. • Type—Shows the type of Session Manager instance, either as Core or Branch Session Manager. • Status—Status of the Security Module deployed for the Session Manager (up or down). • Connections—Total count of connections for the Security Module. • 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. • 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. • Default Gateway—Default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form.

Button	Description
	• NIC Bonding—Shows whether NIC bonding is “enabled” or “disabled”. • Trusted Hosts (expected / actual)—The expected value is the number of Trusted SIP Entities configured in 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.
Reset	Opens the Security Module Reset Confirmation page.
Synchronize	Synchronizes the security module of the selected Session Manager and opens the Confirm Security Module Synchronize page.
Update Installed Certificate	Updates already installed certificates.
Connections Status	Enables you to monitor connection links for selected Session Manager instances.

Confirm Security Module Reset page field descriptions

Button	Description
Confirm	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

About Connection Status

Connection Status allows administrator to view current status of inbound and outbound links between Session Manager SM 100 module and external hosts. It enables general-purpose monitoring and debugging activities such as-

- identification of whether Session Manager is required to be taken out of service
- determination of whether links are secured or not
- viewing of link details and statistics

Monitoring Connection Links

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager** > **System Status** > **Security Module Status** to open the Security Module Status screen.
2. Select a system and click **Connections Status** to open the Connections Status screen.

   Summary section shows the count for connection types such as SIP, PPM and Others. The information is categorized as follows:

   - Active Connections
   - Incoming
   - Outgoing
   - TCP
   - TLS
3. Apply the required filters using **Collect Filters** section.
4. Under Connection List, click **Collect Connections** to display the list of connection links.
5. Select a row and click **Show** check-box to view the detailed information about the selected connection.
6. Click **Return** to return to the Security Module Status screen.

Connections Status field descriptions

Summary section

This section shows counters for the number of incoming, outgoing, TCP and TLS connections.

Collect Filters section

This section enables you to define a filter (FQDN or IP Address and mask) and accordingly display the connection list based on the defined filters.

Connection List section

This section shows basic information of all the active connections.

Name	Description
Details	Shows detailed information about the selected connection link in the Connection Details section.
Type	Link type.
Local IP	Local IP address.
Local Port	Local SM100 port.
Remote IP	Remote IP address.
Remote Port	Remote port.
Remote FQDN	Remote FQDN.
Transport	Transport protocol (UDP, TCP, TLS).
Policy	Security Policy.

Connection Details section

This section shows detailed information for the selected connection.

Name	Description
Direction	Link direction
Creation time	Link creation time
Last message received	Last message received time
Last message sent	Last message sent time
Messages/Bytes Received	Received message count, byte count
Messages/Bytes Transmitted	Transmitted message count, byte count
Messages/Bytes Dropped	Dropped message count, byte count

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
- Failback of endpoints to the primary controller

Related topics:

Viewing Registration Summary on page 251
Rebooting of selected AST devices on page 251
Reloading of selected AST devices on page 252

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 **Elements > 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 250

Rebooting of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 250

Reloading of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 250

Failback of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 **Failback**. The Confirm Failback Notification screen appears.
3. On the Confirm Failback Notification screen, click **Confirm**.

Result

This enables failback to the primary Session Manager.

Advanced Searching

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
Advanced Search Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria for the search. • 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.

Registration Summary field descriptions

Name	Description
Session Manager	Shows the name of the Session Manager Instance.
Type	Either as Session Manager (SM) or Branch Session Manager (BSM).
Primary Registered	Show the count of primary registrations for this Session Manager.
Primary AST	Show the count of primary registrations which are “Active Controller” registrations for this Session Manager.

Name	Description
Primary Admin	Show the count of Communication Profiles what are administered to this Session Manager.
Secondary Registered	Show the count of secondary registrations for this Session Manager or for survivable Branch Session Manager.
Secondary AST Failover	Show the count of secondary registrations which are “Active Controller” registrations for this Session Manager or for survivable Branch Session Manager.
Secondary Admin	Show the count of Communication Profiles what are administered to this Session Manager or for survivable Branch Session Manager.
Total Registered	Show the total count of registrations for this Session Manager or for Branch Session Manager.
Total AST	Show the total count of registrations which are “Active Controller” registrations for this Session Manager or for Branch Session Manager.
Total Admin	Show the total count of Communication Profiles what are administered to this Session Manager or for Branch Session Manager.

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
- Failback of endpoints to the primary controller

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 **Elements > 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 257

Rebooting of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 257

Reloading of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 257

Failback of selected AST devices

1. From the navigation pane on the System Manager Common Console, click **Elements > 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 **Failback**. The Confirm Failback Notification screen appears.
3. On the Confirm Failback Notification screen, click **Confirm**.

Result

This enables failback to the primary Session Manager.

Advanced Searching

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
Advanced Search Criteria	Displays the following three fields: • Drop-down 1 - The list of criteria for the search.

	• 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.

User Registrations field descriptions

General section

Name	Description
Address	Shows 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.
Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Registered Primary	Indicates as primary registration.
Registered Secondary	Indicates as secondary registration.
Registered Survivable	Indicates as survivable registration.
AST	Indicates as AST device.

Registration Detailed section

Name	Description
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Login Name	Shows the administered user login name.
Registration Address	The Communication Address/handle user logged in with.
All Addresses	All of the SIP Communication Addresses the user has administered.
Primary SM	Indicates administered primary Session Manager in the user's Communication Profile.

Name	Description
Secondary SM	Indicates administered secondary Session Manager in the user's Communication Profile.
Survivable SM	Indicates administered survivable Session Manager in the user's Communication Profile.
Active Controller	Session Manager currently serving the endpoint SIP signaling and event subscriptions.
Registration Time	Shows the initial or re-registration time.
Event Subscriptions	Shows all subscriptions for the registered endpoint.
IP Address	Indicates numeric IP address of the end point.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.

Related topics:

Viewing User Registrations on page 254
Rebooting of selected AST devices on page 255
Reloading of selected AST devices on page 255

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 • 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 260
Test data distribution and redundancy link on page 260
Test Call Processing status on page 260
Test Service Host status on page 260
Test Service Director Status on page 260
Test SIP A/S Management Server Status on page 260
Test sanity of Secure Access Link (SAL) agent on page 261
Test management link functionality on page 261
Test Security Module Status on page 261

Test Postgres database sanity on page 261
Running maintenance tests on page 261

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 distribution and redundancy link

This test only runs on the Session Manager. It tests if the mechanism by which Session Managers share data 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.

A test failure indicates a potential failure of all link redundancy behaviors and Call Admission Control.

The test is not run for a Session Manager if the current state of the Session Manager is set to **Management Disabled**.

Test Call Processing status

This is a call processing sanity test for a specified Session Manager. If call processing is working properly, the test passes. If the test fails, contact Avaya Technical Support.

Test Service Host status

This test determines the running status (up/down) of a specified Session Manager. The test passes if the service host is up. The test fails if the service host has an invalid status.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to 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. This test runs on a specified Session Manager. The test passes if the status of the service director is valid.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to Avaya Technical Support.

Test SIP A/S Management Server Status

This test runs on a specified Session Manager. It 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, run the statapp command and other corrective actions for associated alarms on the Session Manager before escalating to 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.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on the Session Manager before escalating to 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

This test queries the basic status of the Security Module on a specified Session Manager. 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.

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 **Elements > Session Manager** > **System Tools** > **Maintenance Tests**
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
Tracer Enabled	SIP message tracing is enabled by default.
Trace All Messages	SIP message tracing is enabled for all SIP messages. In this case, other fields get disabled.
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.
From Security Module to Server	Local SIP messages originating from the security module.
Trace Dropped Messages	SIP message tracing is enabled to trace messages ffrom calls dropped by the SIP firewall as well as by the SM100 proxy.
Max Dropped Message Count	Shows the value for the maximum number of traced dropped messages, if Dropped check box is activated.
Send Trace to a Remote Server	Enables or disables SIP Tracing to an external host . This enables Session Manager to send all the (decrypted) SIP traffic out to an external host. Session Manager uses Syslog protocol for sending the SIP traffic (as used currently for SIP Tracing).
Remote Server FQDN or IP Address	FQDN or IP address of the remote syslog server.
Send Trace Method	Method used to transfer syslogs either using Stunnel (encrypted TCP) or Syslog (unsecure UDP) as mentioned below:

Name	Description
	• Syslog (unsecured UDP) — Traffic is send without being encrypted to remote server as specified in the “Remote Server FQDN or IP Address” to default syslog port. • Stunnel (encrypted TCP) — Traffic is send as encrypted (using stunnel) to remote server which is specified in the “Remote Server FQDN or IP Address” to the port specified in the input field ”Stunnel Port”.
Stunnel Port	Port number that remote server's stunnel is listening on. Stunnel provides several modes for far end certificate validation.

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”:

Name	Description
	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. 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 Instance: 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 **Read** 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.

Button	Description
	• 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 • 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.
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 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 entity links. **Note:** These are only core Session Manager instances.

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.

Chapter 7: Managing events

Managing alarms

Alarming

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

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

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation and they identify the system component which generated the alarm. You can configure System Manager to forward alarms to Avaya Services. You can also configure alarms 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.

Field	Description
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.
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.

Button	Description
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.

Name	Description
Criteria	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.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>

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

Viewing alarms

1. On the System Manager console, under **Services**, click **Events** .
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, under **Services**, click **Events** .
2. Click **Alarms** in the left navigation pane.
3. On the Alarming page, select an alarm and click **Change Status**.
   You can select multiple alarms.
4. 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, under **Services**, click **Events** .
2. Click **Alarms** in the left navigation pane.
3. 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**.

4. Click **Save** to save the exported file to the local disk.

Filtering alarms

The criteria for filtering the alarms are Severity, Status, Host Name, Message, Identifier, and M/E Ref Number. You can use more than one filter criterion on the selected alarms.

1. On the System Manager console, under **Services**, click **Events** .
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.

   You can enter the alarm code in the Message field to find all alarms which contain a particular alarm code.
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.

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, under **Services**, click **Events** .
2. On the Alarming page, click **Advanced Search**.
3. In the Criteria section, from the first and second drop-down fields, select the search criterion and the operator.

   The default value in the first drop-down field is **Time Stamp**.
4. Select or enter the search value in the third field.
5. If you want to add another search condition, click **+** and do the following:
   a. Select the AND or OR operator from the drop-down field.
   b. Repeat steps 3 and 4.

   Click **-** to delete a search condition. You can delete a search condition only if you have added more than one search condition.
6. Click **Search** to find alarms for the given search conditions.

Managing logs

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. The log viewer displays a list of logs. You can view details of each 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. Log viewer displays only logs that are of type Audit.

Log Types

Following are some of the log types that you may come across when viewing logs on the System Manager console. You can view the stations specific logs in the `/var/log/Avaya/mgmt/iptcm` directory.

Security

Security loggers gather security logs.

Audit

Audit loggers gather audit logs.

Operation

Operational loggers gather operational logs.

Debug

Debug loggers collect debug information to troubleshoot issues at the customer site. These loggers have been categorized based on the Communication System Management components.

Debug. Station

Debug Station loggers gather debug information for station management related operations.

Debug.Template

Template Debug loggers gather debug information for template management related operations.

Debug.CM

CM debug loggers gather debug information for communication between Communication Manager and the Communication System Management server.

Debug.NCM

NCM debug logger gathers debug information related to Element Cut Through.

Debug.Synch

Synch debug logger gathers debug information for synchronization operations.

Debug.Model

Model debug logger gathers debug information for database operations.

Debug

Debug logger gathers debug information other than that gathered for the debug types mentioned above.

Viewing log details

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs** > **Log Viewer** in the left navigation pane.

3. On the Logging page, select a log.
4. 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. You can specify multiple search conditions.

1. On the System Manager console, under **Services**, click **Events**.
2. Click **Logs** > **Log Viewer** in the left navigation pane.
3. On the Logging page, click **Advanced Search**.
4. In the *Criteria* section, from the first and second drop-down fields, select the search criterion and the operator.
5. Select or enter the search value in the third field.
6. 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.
7. 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.
8. 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, under **Services**, click **Events**.
2. Click **Logs** > **Log Viewer** in the left navigation pane.

3. On the Logging page, click **Filter: Enable**.
   You can find this button on the top right corner in the table displaying logs.
4. Enter or select the filter criteria.
5. 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.

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.
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

Name	Description
	• 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.
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.

Button	Description
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 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:

Name	Description
	• 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.
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

Name	Description
	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 8: Managing system data

Administering backup and restore

Backup and Restore

The backup and restore functions are executed throughSystem Manager. These functions allow you to backup and restore configuration data for System Manager and all of the Session Manager instances. All of the configuration data for the entire system is kept centrally on 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

On the System Manager console, under **Services**, click **Backup and Restore**.

Result

The Backup and Restore page displays the list of backup files.

Creating a data backup on a local computer

1. On the System Manager console, under **Services**, click **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.

3. On the Backup page, click **Local**.
4. In the **File name** field, enter the file path and name of the backup file that you want to create.
5. Click **Now**.

Result

If the backup is successful, the Backup and Restore page displays a message Backup created successfully!!.

Scheduling a data backup on a local computer

1. On the System Manager console, under **Services**, click **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, Click **Local** option.
4. In the **File name** field, enter the name of the backup file that you want to create.
5. Click **Schedule**.
6. Click **Commit**.

Restoring a data backup from a local machine

1. On the System Manager console, under **Services**, click **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File Name** field, type the file name that you want to restore.
5. Click **Restore**.
6. On the Restore Confirmation page, click **Continue**.
   After the backup data is successfully restored, the system logs you out of the System Manager console.

Viewing data retention rules

1. On the System Manager console, under Services, click **Configurations**.
2. Click **Data Retention** in the left navigation pane.
   The system displays the Data Retention page with the Rule list.

Modifying data retention rules

1. On the System Manager console, under Services, click **Configurations**.
2. Click **Data Retention** in the left navigation pane.
   The system displays the Data Retention page with the Rule list.
3. Select a rule from the Rule list.
4. Click **Edit**.
5. Modify the value in the **Retention Interval (Days)** field.
6. Click **Update** to save the value.

Accessing the Data Retention Rules service

1. On the System Manager console, under Services, click **Configurations**.
2. Click **Data Retention** in the left navigation pane.
   The system displays the Data Retention page with the Rule list.

Result

The system displays the Data Retention page.

Viewing loggers for a log file

1. On the System Manager console, under **Events**, click **Logs**.
2. Click **Log Settings** in the left navigation pane.
3. On the Logging Configuration page, click a log file from the **Select Log File** field.
   You can view the loggers in the Logger List.

Assigning an appender to a logger

The appender where logger logs the log messages.

1. On the System Manager console, under **Events**, click **Logs**.
2. Click **Log Settings** in the left navigation pane.
3. On the Log Settings page, select 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**.
   The appender is added to the selected logger and you can view the appender on the Log Settings page.

Editing a logger in a log file

You can set log levels for loggers which define as to what level of logging the logger logs.

1. On the System Manager console, under **Events**, click **Logs**.
2. Click **Log Settings** in the left navigation pane.
3. On the Log Settings page, select 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, in the **Log Level** field select a log level.
7. Click **Commit** .
   The log level is set for the selected logger.

Modifying an appender

1. On the System Manager console, under **Events**, click **Logs**.
2. Click **Log Settings** 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.
   You can modify information in the **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files** fields
9. Click **Commit**.

Removing an appender from a logger

1. On the System Manager console, under **Events**, click **Logs**.
2. Click **Log Settings** in the left navigation pane.
3. On the Log Settings 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 the System Manager data on a local or a remote location. You can also 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.

The page displays the following fields when you choose to create a backup of System Manager data on a local computer.

Name	Description
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.

The page displays the following fields when you choose to create a backup of System Manager data on a remote computer.

Name	Description
Remote Server IP	IP address of the remote server.
Remote Server Port	Port of the remote server.
User Name	User name for logging into the remote server.
Password	Password for logging into the remote server.
File Name	The path and name of the backup file.
Use Default	Select this check box to use the default configured values.

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.

Name	Description
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 the 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.

The page displays the following fields, when you select **Local** as **Type**.

Name	Description
File Name	The name of the backup file that you want to restore.
Select File Name	Lists the name of the backup file that you want to restore.

The page displays the following fields, when you select **Remote** as **Type**.

Name	Description
Remote Server IP	IP address of the SCP server.
Remote Server Port	Port of the SCP server.

Name	Description
User Name	User name for logging in to the SCP server.
Password	Password for logging in to the SCP server.
File Name	The name of the backup file that you want to restore.
Use Default	Select this check box to use the default configured values.

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 Settings field descriptions

Use this page to view and edit loggers 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.
Attached Appenders >Facility	The process running on the machine that created the log message.
Attached Appenders > host	The name of the syslog host where the log output is stored.
Show All	Provides you an option to select the maximum number of logger records that you can view at a time.

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.

Name	Description
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.
Facility	The process running on the machine for which log messages are created.
Host	The name of the syslog host that stores the log output.
Header	The header part of the syslog packet. The header part contains timestamp and host name information.
Facility Printing	The printed message includes the facility name of the application.

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.
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.

Name	Description
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.

Data Replication Service

Data Replication Service

The Data Replication Service replicates data from the master database residing on the server.

The Data Replication Service supports the following two modes of replication:

- Replication in Repair mode: In repair mode, the Data Replication Service replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of the Data Replication Service.
- Automatic synchronization mode: After the database of the replica node is loaded with the requested data, the subsequent synchronizations of the master database and the replica database occur automatically. The Data Replication service replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after each fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. Data Replication Service creates replication batches whenever the data in the master database is added, modified, and deleted.

You can perform the following activities using the Data Replication service:

- View replica nodes in a replica group.
- Replicate requested data from the System Manager master database to the database of the replica nodes if the databases are not synchronized

Viewing replica groups

On the System Manager console, under **Services**, click **Replication**.
The system displays the Replica Groups page.

Result

The system displays the Replica Groups page with the groups in a table.

Related topics:

Replica Groups field descriptions on page 298

Viewing replica nodes in a replica group

You can view the replica nodes in a group.

1. On the System Manager console, under **Services**, click **Replication**.
   The system displays the Replica Groups page.
2. Select a replica group and click **View Replica Nodes**.

Alternatively, you can click a replica group name displayed under the **Replica Group** column to view the replica nodes for that replica group.

The Replica Nodes page displays the replica nodes for the select group.

Related topics:

Replica Nodes field descriptions on page 299

Repairing a replica node

You can replicate data for a replica node whose database is not synchronized with the System Manager database. Repair is necessary if there is a post-install failure of the Data Replication Service.

1. On the System Manager console, under **Services**, click **Replication**.
   The system displays the Replica Groups page.
2. Select a replica group for which you want repair the replica nodes from the table displaying replica groups and click **View Replica Nodes** or click the name of the replica node displayed in the **Replica Group** column.
3. On the Replica Nodes page, select a replica node and click **Repair**.

   The **Synchronization Status** column displays the data replication status for the repairing replica node.

Related topics:

Replica Nodes field descriptions on page 299

Repairing all replica nodes in a replica group

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

1. On the System Manager console, under **Services**, click **Replication**.
   The system displays the Replica Groups page.
2. Select a replica group for which you want repair the replica nodes from the table displaying replica groups.
3. Click **Repair**.

The **Synchronization Status** column displays the data replication status for the replica group.

Viewing replication details for a replica node

You can view the batch related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

1. On the System Manager console, under **Services**, click **Replication**.
   The system displays the Replica Groups page.
2. Select a replica group and click **View Replica Nodes**.
   The Replica Nodes page displays the replica nodes for the selected replica group in a table.
3. Select a replica node and click **View Details**.

   The Data Replication page displays the replication details for the selected replica node.

Related topics:

Data Replication field descriptions on page 300

Removing a replica node

1. On the System Manager console, under **Services**, click **Replication**.
   The system displays the Replica Groups page.
2. Select a replica group in which you want to remove a node.
3. On the Replica Node page, click **Remove**.

Removing a replica node from queue

1. On the System Manager console, under **Services**, click **Replication**.
   The system displays the Replica Groups page.
2. Select the replica group for which you want to remove the node from queue.
3. On the Replica Node page, click **Remove from Queue**.

Replica Groups field descriptions

You can use this page to:

- view all the replica groups in the enterprise. These replica groups are logical grouping of the replica nodes.
- replicate data requested by the replica node from the master database to the database of the replica nodes
- view the replication status of the replica groups

The page displays these fields when you All from the **Replica Group** field.

Name	Description
Select check box	You can use this check box to select a group.
Replica Group	Name of the replica group. This is a hyperlink. When you click a group, the Replica Nodes page opens and displays the replica nodes for that group.
Synchronization Status	Replication status of the replica group. The group displays out of synch status if any one of the replica computer database in the group and master database are not synchronized.

Button	Description
View Replica Nodes	Opens the Replica Nodes page. You can use this page to view replica nodes for a selected group.
Repair	Replicates data for a selected replica node that is not synchronized with the master nodes.

Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group which has requested data replication from the master database of System Manager
- View the replication status of replica nodes in a group

Name	Description
Select check box	You can use this check box to select a replica node.
Replica Node Host Name	The IP address of the replica node
Product	Name of the product running on the replica node
Synchronization Status	The synchronization status of the replica node. The following are the status for when you click the **Repair** button on the page to perform a data replication for a replica node: • Ready for Repair: This status indicates that database of the replica node is not synchronized with the master database. • Queued for Repair: This status indicates that replication request of the replica computer is in queue with other data replication requests. The color code of the status is yellow. • Repairing: This status indicates that the data replication process is in progress. The color code of the status is yellow. • Synchronized: This status indicates that the data requested by the replica node is successfully replicated from the master database to the database of the replica node. The color code of the status is green. • Synchronization Failure: This status indicates an error in data replication for the initial load. Resolving this issue requires manual intervention from the administrator. The system displays the following status during automatic replication of data from the master to the replica node: • Synchronizing: This status indicates that the data replication is in progress for the replica node. The color code of the status is yellow. • Synchronized: This status indicates that the data requested by the replica node is successfully replicated from the master database to the database of the replica node. The color code of the status is green.

Name	Description
Last Synchronization time	The last time when the data synchronization or replication happened for the replica node.

Button	Description
View Details	Opens the Data Replication page. You can use this page to view the synchronization details for a replica node.
Repair	Replicates or synchronizes data from themaster node to a selected replica node.
Remove	Removes the selected nodes from the group.
Show All Replica Groups	Takes you back to the Replica Groups page.

Data Replication field descriptions

General

Name	Description
Replica Node Group	Name of the group of the replica computer.
Replica Node Host Name	The IP address of the replica computer
Last Synchronization Time	The last time and date when the data synchronization or replication happened for the replica node.
Synchronization Status	The synchronization status of the replica computer.

Synchronization Status

Name	Description
Pending Batches	The batches for which data replication is pending.

Statistics

Name	Description
Cause of Error	A brief description of reason for failure to replicate or synchronize data
Time of Error	The time when the error occurred.

Managing scheduled jobs

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 sdministrator 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

On the System Manager console, under **Services**, click **Scheduler**.

Viewing pending jobs

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Pending Jobs** in the left navigation pane.

Related topics:

Pending Jobs field descriptions on page 308

Viewing completed jobs

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.
   The Completed Jobs page displays completed jobs.

Related topics:

Completed Jobs field descriptions on page 310

Viewing details of a pending job

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Pending Jobs** in the left navigation pane.
3. On the Pending Jobs page, select a pending job and click **View**.
   The Job Scheduling-View Job page displays the details of the selected job.

Viewing details of a completed job

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.
3. On the Completed Jobs page, select a completed job and click **View**.
   The Job Scheduling-View Job page displays the details of the selected job.

Viewing details of a pending job

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Pending Jobs** in the left navigation pane.
3. On the Pending Jobs page, select a pending job and click **View**.
   The Job Scheduling-View Job page displays the details of the selected job.

Viewing logs for a job

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

1.
2. 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 completed jobs

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.
   The Completed Jobs page displays completed jobs.

Related topics:

Completed Jobs field descriptions on page 310

Filtering Jobs

1. On the System Manager console, under **Services**, click **Scheduler**.
2. 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 system displays the **Filter: Enable** option at the upper-right corner of the page.
3. Select type of the job from the field under the **Job Type** column.
4. Enter the name of job in the field under the **Job Name** field.
5. Select the status of the job from the field under the **Job Status** field.
6. Select the state of the job from the field under the **State** field.
7. Select the frequency of execution of the job from the field under the **Frequency** field.
8. Enter the scheduler of the job in the field under the **Scheduled By** column.

Note:

The system displays this field only for the completed jobs.

9. Click **Apply**.
   The system displays jobs that match the filter criteria.

Result

Editing a job

1. On the System Manager console, under **Services**, click **Scheduler**.
2. 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.
3. 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 an administrator scheduled job.

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

1. On the System Manager console, under **Services**, click **Scheduler**.
2. 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.

     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**.
3. On the Delete Confirmation page, click **OK**.
   System Manager deletes the job you select from the database.

Disabling a job

Use this functionality to make a job inactive.

1. On the System Manager console, under **Services**, click **Scheduler**.
2. 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**.
3. On the Disable Confirmation page, click **Continue**.
   The **State** of the selected job is changed to Disabled.

Enabling a job

Use this functionality to make a job active.

1. On the System Manager console, under **Services**, click **Scheduler**.
2. 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**.

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

Result

Stopping a Job

1. On the System Manager console, under **Services**, click **Scheduler**.
2. Click **Pending Jobs** in the left navigation pane.
3. On the Pending Jobs page, select a pending job in the running state and click **More Actions** > **Stop**.
4. Click **Continue** on the Stop Confirmation page.
   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:

Name	Description
	• 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.
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.

Related topics:

Viewing pending jobs on page 302

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:

Name	Description
	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.
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.

Button	Description
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.

Related topics:

Viewing completed jobs on page 302

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:

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 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: 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.

Name	Description
	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.

Name	Description
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: 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

Name	Description
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.

Name	Description
	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: 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.

Appendix A: 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

R

S

T

U

V