Installing, Administering, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services

03-600768
Issue 9.0
January 2011

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758, and Avaya Support Notices for Hardware Documentation, Document Number03-600759.

To locate this document on the web site, go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not 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. Customer and/or 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. 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 through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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 identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at http://support.avaya.com/ThirdPartyLicense/.

The disclaimers of warranties and limitations of liability set forth in the Third Party Terms do not affect any express warranty or limitation of liability that may be provided to you by Avaya pursuant to the license terms covering the Product contained in a separate written agreement between you and Avaya. To the extent there is a conflict between the General License Terms or your customer sales agreement and any Third Party Terms, the Third Party Terms shall prevail solely for such Third Party Components.

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: About this document

This document, *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services*, is developed for these reasons:

- Is an update to the R5.2 document *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services*, Doc ID 03-600768
- Contains information about the new version of SES, also known as SIP Enablement Services
- Includes both corrections of earlier information and newly developed information
- Presents additional information about SIP for the R5.2 Communication Manager. See the documents for Communication Manager for non-SIP issues.
- SIP Enablement Services is now known as Avaya Aura® SIP Enablement Services.

This document is available online. For your convenience, consider using the embedded cross-references to locate information. In addition, there is a table of contents and index for your reference. Online readers may also use the search facility of the browser.

Audience

This document is for field technicians, remote service personnel, and user-assigned administrative personnel as a reference to install, configure and administer SES R5.2 in concurrence with its communication manager server.

We recommend having three to five years experience in system administration, and experience with working on both communication manager servers on the Communication Manager system and host servers in the SES system.

This document assumes that the engineer has a working knowledge of telecommunications fundamentals and PBX maintenance practices. This document also assumes that the system was installed and tested properly and brought into service with every fault cleared. Adjuncts and other devices external to the switch are covered by their own service documentation.

If you do not have these experiences and qualifications, please make arrangements for a mentor.

Document set

Although this book is published separately, it is part of a set. Use this document as an adjunct to the following references.

- *Installing the Avaya S8800 Server for Avaya Aura® SIP Enablement Services*, Doc ID 03-603447
- *Installing, Administrating, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services*, Doc ID 03-600768
- *Administering Avaya Aura® SIP Enablement Services on the Avaya S8300 Server for Co Residency*, Doc ID 03-602508
- *SIP Personal Information Manager (SIP PIM)*, Doc ID 03-300441
- The installation and administration guides for the endpoints your site uses
- *Maintaining the Avaya S8800 Server for Avaya Aura® SIP Enablement Services*, Doc ID 03-603448
- *SIP Support in Avaya Aura® Communication Manager*, Doc ID 555-245-206
- *Avaya Aura® SIP Enablement Services Implementation guide*, Doc ID 16-300140
- Using A*vaya Server Availability Management Processor (SAMP)* Doc ID 03-300322
- SES Release notes

Chapter 2: Introduction to SIP and SIP Enablement Services

This section describes SIP Enablement Services, what it is, and what it does. General information is covered in these sections:

Converged Communications Server and SES

SIP Enablement Services establishes the foundation for the Communication Services layer within the Communication Architecture. This layer unifies all enterprise real-time communications over an open SIP-based infrastructure, and provides the “glue” that binds with Avaya Communication Manager Express applications, exposing them as Web service components that can be easily invoked through standards-based clients or business applications, or as open APIs that provide a secure, reliable, and highly scalable application development platform for access to Avaya Communication Manager services.

SIP Enablement Services and Application Enablement Services are modular offerings that can be ordered independently and implemented as needed by the enterprise on separate, dedicated, industry-standard servers. In combination, the new services of the Converged Communications Server create an application environment that combines the loosely coupled multi-modal services and presence capabilities available via a SIP-based architecture with the open APIs that expose the full breadth of features and functions of Communication Manager.

The Converged Communications Server is a family of related product offerings that currently consists of two components:

- SIP Enablement Services
- Application Enablement Services

SIP Enablement Services

SIP Enablement Services (SES) incorporates the SIP functionality previously introduced as Converged Communications Server Release 2.1, combined with new feature and scalability enhancements. The application combines the standard functions of a SIP proxy or registrar server with SIP trunking support and duplicated server features to create a highly scalable, highly reliable SIP communications network supporting telephony, instant messaging, conferencing, and collaboration solutions.

Application Enablement Services

Application Enablement Services (AES) Release 3.1 consolidate Avaya's existing application enablement assets – such as Communication Manager Application Programming Interface (CMAPI) and Avaya CT – into a single, Linux-based platform. This enables enterprises to leverage the tremendous variety of computer-telephony integration and interactive response applications developed for these interfaces. Application Enablement Services allow for powerful new applications to be written and deployed that fully leverage Communication Manager via standards-based APIs and Web service components.

Introduction to the SES Server

Find overview material about Avaya servers that run SIP Enablement Services in these sections:

- SIP Enablement Services definition on page 14
- How does this fit into your system? on page 15
- Standalone and Co-resident configurations on page 20
- SES and Communication Manager Branch Edition on page 16
- SES visiting user on page 16

SIP Enablement Services definition

Avaya servers running SIP Enablement Services perform proxy, registration, and redirection functions associated with SIP applications such as Instant Messaging (IM). SIP is the Session Initiation Protocol, an endpoint-oriented, network messaging standard defined by the Internet Engineering Task Force (IETF). The Avaya servers running AES and SES are referred to specifically as the Converged Communications Servers product families.

When SES hosts communicate with one or more Communication Manager servers, then the SES SIP edge server supports communication among these elements:

- Non-SIP endpoints supported by Communication Manager:
  - Analog, DCP or H.323 stations
  - Analog, digital or IP trunks
- SIP-enabled endpoints configured in Communication Manager as OSI:
  - Toshiba Business Phone SP 1020A
  - Avaya SIP Telephones
  - Avaya SIP Softphone Release 2
  - Avaya IP Softphone R5.1 or later with instant messaging
  - Avaya IP Agent R6 or later.

Advanced SIP telephony extends Communication Manager features to SIP-enabled endpoints.

SIP-enabled endpoints register with the Avaya proxy server. SIP-enabled endpoints can be managed by Communication Manager servers as well. In addition, the SES edge proxy server supports the SIP-enabled instant messaging application between users of IP Softphone R5, and SIP Softphone R2 client software. For voice, the clients also must be logged in to and managed by communication manager servers.

For current, specific phone types, see Supported Phone Types for SES on page 37.

How does this fit into your system?

In addition to the SIP Enablement Services servers, the support for SIP built into Avaya Communication Manager has the following attributes to help it fit into your system:

- It is built around open-source software and published standards (for example, Linux, SIP and H.323).
- It integrates traditional circuit-switched interfaces and IP-switched interfaces. This integration allows the customer to evolve from the current circuit-switched telephony infrastructures to next generation IP infrastructures, including SIP.
- It positions customers to leverage the increasing number and power of SIP-enabled applications, like Instant Messaging and presence.

The modular and extensible system architecture that Avaya has chosen for offering SIP support has a unique benefit for Avaya customers: the set of features supported by SIP itself is augmented by those supported by Communication Manager. A Communication Manager server becomes a telephony feature server, accessible from any SIP-enabled endpoint. This configuration provides access transparently to the many telephony features that the SIP standard currently does not address. Advanced SIP telephony provides value-added features such as bridging, conferencing, unique ringing, and VIP calling.

SES and Communication Manager Branch Edition

SES, along with Communication Manager, is a part of the Communication Manager Branch Edition solution. You may have to administer SES as part of that solution.

Avaya Communication Manager Branch Edition is a highly distributed solution for branch offices. Communication Manager Branch Edition provides:

- Communications applications
- Centralized management of communication and its hardware
- Rapid deployment
- Low cost

Corporate enterprises of any size use Communication Manager Branch Edition.

However, Communication Manager Branch Edition is never configured for the co-resident solution on the S8300.

To find all the documentation, see *Avaya Aura® Communication Manager Branch Edition Documentation Map*, Doc ID 03-602021. This map summarizes the documentation available for Avaya Communication Manager Branch Edition.

SES visiting user

Visiting user presents several new concepts, concerns, and topics of interest for the SES administrator.

Non-roaming or local visiting user

A visiting user can be roaming or non-roaming. If a visiting user is non-roaming, it means the user is logged into a visiting phone that is served by the users usual SES home server. For example, a non-roaming visiting user logs into a phone that is in the office adjacent to the primary phone. No special connections need to be made to serve up the contacts, permissions and buddy list the non-roaming visiting user expects.

Roaming or remote visiting user

If a visiting user is roaming, the visiting user is logged into a phone that uses an SES home server that is different from the user's usual home SES.

During registration, the roaming SES home server retrieves the user’s credentials from the SES data service as the means to enable roaming for that user.

Roaming and non-roaming visiting users

When a new registration arrives from a visiting phone, either roaming or non-roaming, the visiting phone takes priority over the user's primary phone. Now, the visiting phone is both active and registered. Inbound calls are routed to the visiting phone. Note that the user can only be actively visiting at one location, although there might be multiple registrations.

The SIP PIM user web interface manages the user experience for basic SIP telephones, including which device is active. In that interface, check the My Devices screen.

Active / inactive status

- An active phone is one that is registered, and receives inbound and can initiate outbound calls. A primary phone can be active or inactive, a visiting phone can be active or inactive.
- An inactive phone is one that is registered, but cannot receive inbound calls and can only make outbound emergency calls.
- An unregistered phone does not have a valid SIP registration record in any SES home server. An unregistered phone can make outbound emergency calls.
- The last phone that the user logs into becomes the active device, depending on the visiting user mode.
- When the user logs off a phone, the phone becomes unregistered. If a user forgets to log off, the EMU inactivity timer makes the phone inactive after the specified time, but only if it is a visiting phone.
- If the visiting user EMU timer expires and the phone is visiting, the phone unregisters. Administer the EMU timer if any phones will be used as visiting phone stations.
- If another of the user’s phones is already registered and active, becoming a visiting user makes the registered phone inactive.
- The user can make an inactive phone active by:

  -- Using the SIP PIM interface

  -- Logging out of the active phone

  -- Letting the timer act

Calling features and restrictions

- All incoming calls go to the registered, active endpoint.
- No outbound calls are allowed from inactive or unregistered phones except for emergency calls.
- If an active phone becomes inactive during call setup, the phone rejects an incoming call.
- If the active phone becomes inactive during feature invocation, the only allowed user action is to hang up.

- No added features are available when emergency calls are made from inactive or unregistered phones.

EMU Inactivity Timer

EMU timer sets the time a phone must be inactive before the phone is unregistered.

The EMU timer is set in Communication Manager > Feature Related Systems Parameter screen > EMU Timer field. This field times the visiting user sessions in SES for phones designated as visiting.

The SIP visiting user feature audibly and visually notifies the user before a visiting session expires and allows the visiting user to extend the session. After each call the visiting user receives or answers, the inactivity time is reset.

Using the SES Master Administration interface > SIP Phone Settings, the administrator determines, via groups, which phones are governed by the inactivity timer. This is helpful because the administrator can set the primary phone to not use the inactivity timer so that it always remains active.

- Visiting User Mode—Optional. When the Visiting User Mode is optional, the login screen has an addition field where the user can specify if the phone is or is not their primary phone.
- Visiting User Mode—Forced (visiting user phone). When a phone is designated as visiting, the phone is always governed by the inactivity timer (EMU) and the q-value that is 0. Under these two conditions, the phone unregisters and so becomes inactive.
- Visiting User Mode—Off. When the Visiting User Mode is off, the user must select to turn it on. With visiting user mode off, the phone is never governed by the inactivity time or a q-value of 0.

Emergency Calls

A SIP visiting user is able to make emergency calls from any visiting or home location. Unregistered phones, as well as registered phones, both active and inactive, can make this type of call.

To enable PSAP call back, set up a Communication Manager server Map entry to call 911. See Edit Communication Manager Server Map Entry screen on page 251.

Additionally, the SIP VU feature can send a local Calling Party Number (CPN) to the Emergency Response Center/PSAP on emergency calls made by a Visiting User. The CPN identifies the originating building location. The ability for the SIP visiting user implementation to provide a local calling party number when routing an emergency call from a visiting user to the local PSAP depends on the customer provisioning in Communication Manager.

Local outbound proxy sends emergency calls to the local media gateway which has the local PSAP set up.

To make emergency calls, a phone can be:

- Registered and active
- Registered and inactive
- Not registered

A user can make outbound emergency calls from both inactive, registered, as well as unregistered phones, and that phone can receive the PSAP callback.

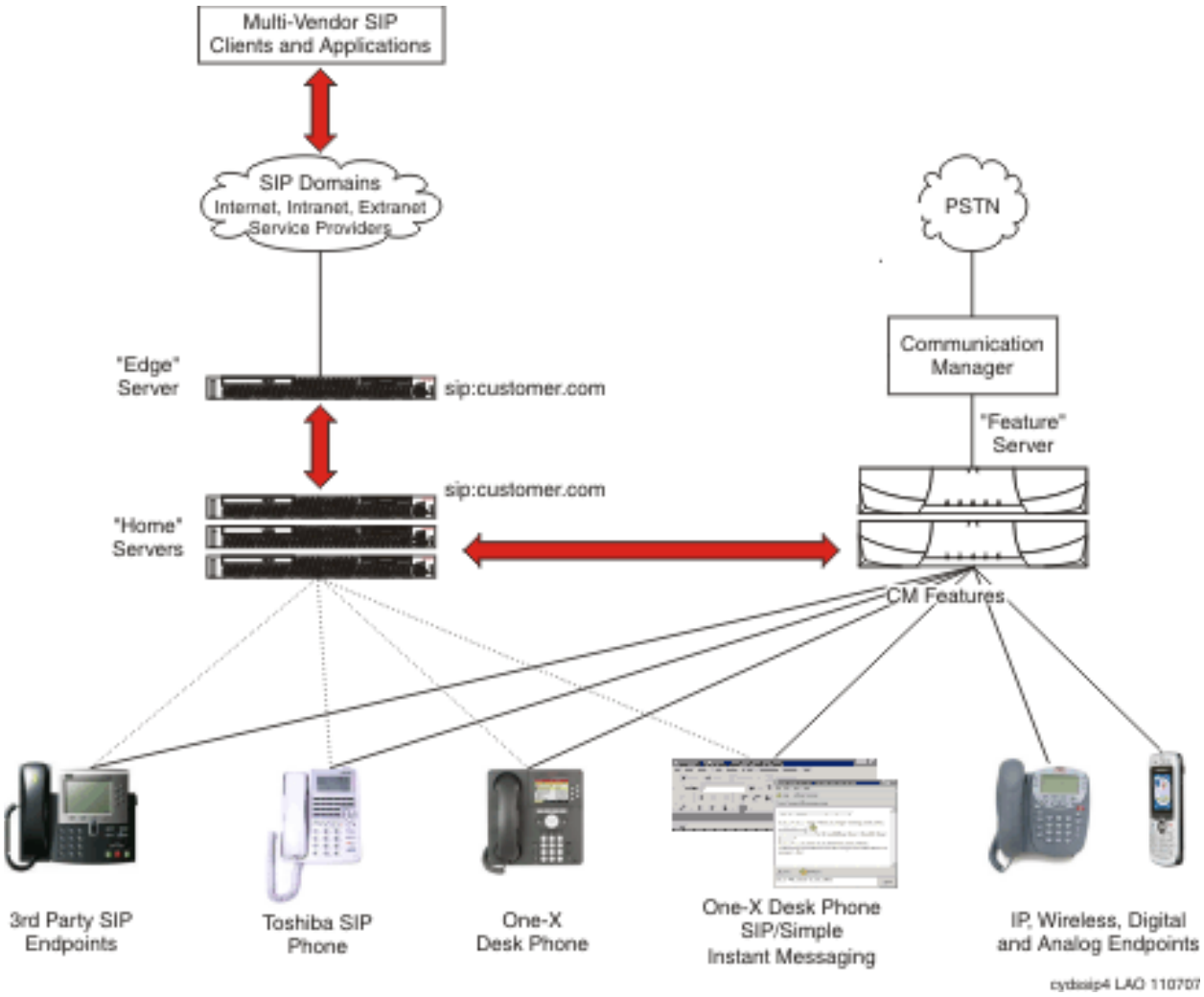
System Architecture

Avaya's SIP architecture supports SES servers of different types, discussed in these sections:

- System topography on page 20
- Standalone and Co-resident configurations on page 20
- SES and Communication Manager Branch Edition on page 16
- Types of SES servers on page 21
- Administrative interfaces on page 23

System topography

Figure 1: Topography of system



Standalone and Co-resident configurations

The SES solution can be implemented as either a standalone or co-resident configuration.

In a standalone installation, SES and Communication Manager reside on separate servers. In the standalone configuration, SES employs the Avaya S8800 Server, Avaya S8500-series servers, and HP ProLiant DL360 G7 server for home and edge servers. Communication

Manager resides on an S8300, S8400, S8500, S8700-series servers, S8800, and HP DL360 G7 server.

In a co-resident installation, SES and Communication Manager reside on the same server, the HP, S8800, S8300C or S8300D server. See the document *Administering SIP Enablement Services on the Avaya S8300 Server*, Doc ID 03-602508.

Types of SES servers

There are several types of architectures using SES servers:

- Single edge server with a single home server
- Single edge server with multiple home servers
- Multiple edge servers with multiple home servers
- A combined home and edge server
- SES combined home/edge or home that is co-resident with Communication Manager on an S8300.
- SES on a server blade i40 or i120

An administrator can change a combination home/edge server to distributed home and edge servers. Allow for any required data backups. In revision R3.x and R5.1 of SES, backup both the Master Administration interface subsystem and the home system to back up all user data. Although administrators view SIP PIM data from the Master Administration interface on the edge, those data are stored on the home server associated with that edge server.

Edge servers

The edge server manages SIP requests from all domains, forwarding requests received from home servers. Along with the edge server, one or more home servers must also exist in this architecture. Only one edge server, either distributed or combined with a home server, is allowed for any one domain.

The S8500B server comes with 0.5 GB of RAM but requires an additional 2.5 GB of RAM for use as an edge server. The S8500C server comes with 1 GB of RAM but requires an additional 2 GB of RAM for use as an edge server. The S8510 server has 4 GB of RAM and does not require a memory upgrade for use as an edge server. The S8800 server has 4 GB of RAM and does not require a memory upgrade for use as an edge server.

Edge servers and combined home/edge servers may be duplicated for data redundancy.

Home servers

A home server manages SIP requests for the specific domain assigned for this server, and it forwards any requests pertaining to other domains to the edge server. One to 20 home servers and exactly one edge server are required in this scenario.

For example, a customer might have one home server for A-users@company.com and another home server for B-users@company.com within its network. Subdomains are not supported.

Home servers may be duplicated for data redundancy.

Home servers support 6000 users each, and 120,000 users across all homes. If a single home must support more than 3500 users, install additional memory to increase RAM to 3 GB.

There can be up to 20 home servers in one SES system.

Home/Edge servers

A combined home/edge server contains software to act as both a home server and an edge server. This is a single-server scenario. No other home or edge servers may exist in this type of architecture.

A home/edge combined server may be duplicated for redundancy.

Note:

Design your system architecture with scalability in mind. A migration or upgrade to a new configuration may disrupt the database.

Server configuration mixes for SES

Your SES network can employ a combination of the four SES servers: S8300C, S8300D, S8500, S8510 or a combination of HP or S8800 Servers. Keep these points in mind when designing or scaling your site:

- You can have a duplicated pair of an S8500 Server, but the server BIOS and SAMP firmware versions of both servers of the duplicated pair must match.
- When SES 5.2.1 runs co-resident with Communication Manager 5.2.1 on an S8300C/D, it cannot be duplicated with any S8500 or S8510 server running SES.
- When SES 5.2.1 runs co-resident with Communication Manager on an S8300C, it cannot act as an edge server (Core Router) in a Communication Manager Branch Edition network. This is because SES 5.2.1 co-resident on the S8300C can be configured only as a home server or home/edge combination server in an SES network.
- When SIP Enablement Services is deployed co-resident with Communication Manager, the server must be configured as a Home server or combined Home/Edge server. Co-resident SIP Enablement Services cannot be configured as a standalone Edge server, and therefore cannot perform the core routing function in an Avaya Communication

Manager Branch Edition solution. A standalone S8500-based SIP Enablement Services Edge 5.2.1 is still required for these larger SIP implementations.

- SES 5.2.1 running co-resident with Communication Manager on the S8300C/D can be configured as a home SIP server at the main location in a Communication Manager Branch Edition network, if needed.
- In SES 5.2.1, the edge functions as a core router for Communication Manager Branch Edition.

Note:

A duplicated pair can be two S8800 servers, two S8500B servers, two S8500C servers, two HP servers, one S8500B server and one S8500C server, or two S8510 servers.

Capacities

Visit the Avaya support web site (http://support.avaya.com) for a latest copy of *Avaya Aura*® *Communication Manager System Capacities Table*, Document Number 03_300511.

When thinking about capacity, keep in mind that some TLS links need to be reserved for failover. See Local failover design on page 28.

Other capacity restrictions concerns the hardware and user aspects of the system.

Certificate synchronization

On a redundant, duplicated system, the trusted certificates repository is synchronized periodically on both servers in the pair.

However, server certificates, whether for Apache or for SIP, are not.

The unique certificates should have the DNS name of the pair, not each server, because the DNS name of the pair will be what the browser checks against to authenticate.

Administrative interfaces

All administrators gain access to SIP Enablement Services through a secure connection, that is, `https`.

Master Administration interface

The Master Administration interface is always on the edge server.

The hardware configuration of your system determines what links appear on the left of the administration interfaces.

The Master Administration interface can add and delete users, and update data on all home or edge servers in a domain. The Limited Administrator interface on home servers cannot update user data, only view it. The limited administration interface on home servers can control reloading and rebooting user endpoints.

The edge server updates all servers and their databases. For a combined home/edge server, these databases co-reside on a single node, and the home/edge cannot be used with additional home servers. The Master Administration interface supports administering both users and communication manager server extensions. The Master Administration interface resides on the edge server (or the combined home/edge server). Only one server or server pair in the network may have the Master Administration interface. All other servers have the Limited Administrator interface.

Limited Administrator interface

The Limited Administrator interface is available on a home server. The Limited Administrator interface cannot update user data, only view it. A home server with the Limited Administrator interface does not support administering users or their extensions, and cannot update the databases on other servers. With the limited interface you can administer maintenance items for the server, for example, and also view a list of registered SIP users on this home server.

Adjunct systems services

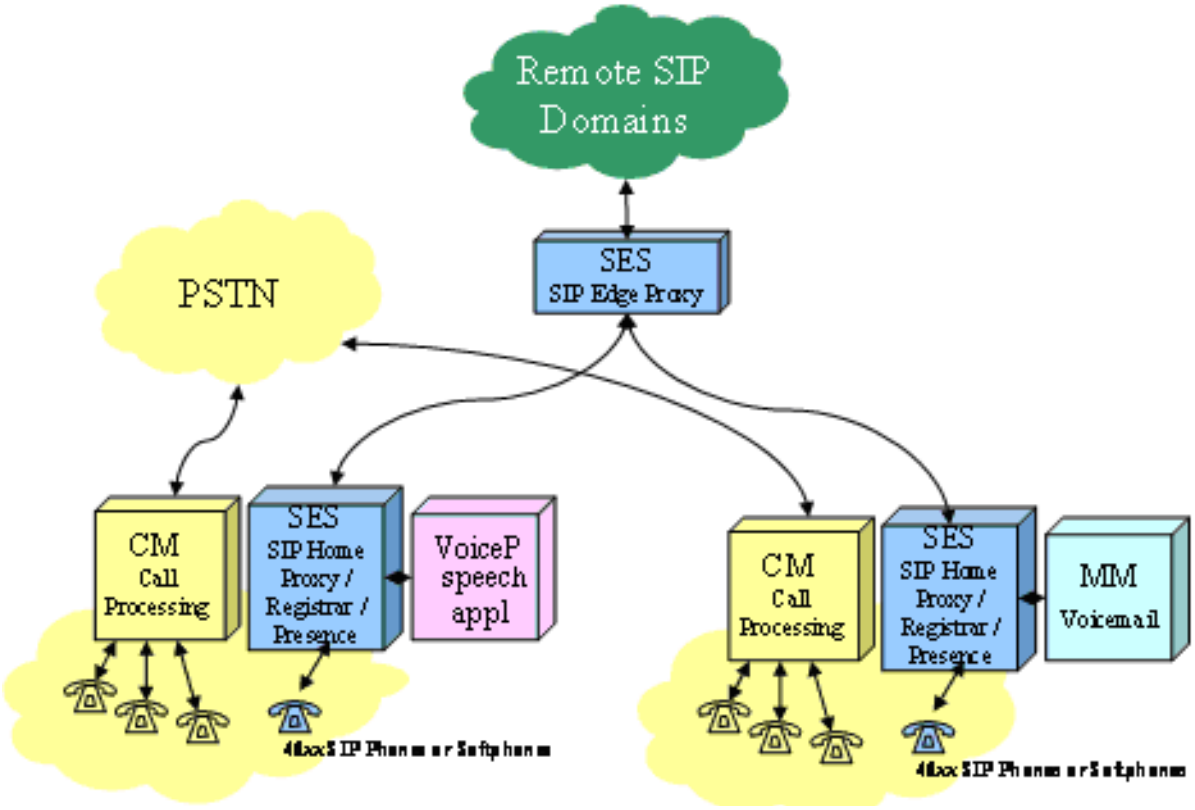
An SES adjunct is an entity that provides some service to SES via a SIP interface.
An adjunct system consists of adjunct servers, which serve an application, perhaps sending an alert on behalf of librarian for all the books due on a specific day. Examples of adjunct systems are Modular Messaging (MM), for voice mail, and Voice Portal for speech applications.

This section describes the system architecture for the SES administrative system to include support for adjunct systems with SIP integration. This includes the web interface infrastructure for managing the entire SIP network as well as the system for maintenance tasks for each host.

The administration of SIP adjuncts is very much like the existing SES administration interface.

A new definition of system is used to support SIP adjuncts to SES. The expanded meaning is multiple servers comprising a system, and perhaps a system of systems. Figure 2 illustrates a distributed example of the adjunct systems concept.

Figure 2: Adjunct systems architecture



The expanded system definition uses common service elements that integrate these individual servers into an overall system. The SES system delivers services on a system basis rather than an individual server basis. To accomplish this, SES sends invites to servers in a given system on a round robin basis.

A concrete example of an adjunct system is Modular Messaging (MM). The MM system is composed of one or more telephony servers (MASs) and a message store. Each MAS represents one SIP adjunct. The message store represents Common Adjunct Service Element.

For MM, SES delivers invites to the MASs in a given system on a rotational basis. So in addition to administering the individual MAS servers, you administer the MM System composed of multiple MAS servers.

SES is deployed in a network of one or more SES hosts, one or more Communication Manager communication manager servers, and one or more MM systems. Each of these three systems may be composed of multiple servers. The SES administrative system is designed to accommodate network topologies of many hosts with varied relationships, as well as the single-box solution where a single SES communicates with a single Communication Manager communication manager server and a single MM adjunct system.

To ease administrative tasks, a single point of administration allows for management of all user information in the SIP network. This single point of administration is named the Administration

Interface subsystem. The recommended deployment is for the master administration subsystem to be installed on the edge server in a SIP network. On each node in the SIP network there is also a web interface available for system maintenance, however the functionality is limited to host-specific actions and highly tailored towards serviceability. Administrators can only administer SES users on the master administration system.

A command line interface is available for maintenance and serviceability purposes for the convenience of service technicians.

Local redundant server feature

An optional feature in SIP Enablement Services is local failover as implemented by a pair of duplicated servers. This feature supports replicating the database and server software for any system node (home, edge, or combination home/edge). To take advantage of local failover, the servers must have a duplicated architecture. Read these sections:

- Duplicated and single server configurations on page 26
- Server-level details of failover on page 27
- Local failover design on page 28
- Failover scenarios on page 28
- Causes for failover on page 29
- Server interconnections and routing on page 30

Duplicated and single server configurations

The local failover feature requires a duplicated server configuration. For example, in a duplicated configuration of edge servers, EdgeA has a backup server, EdgeB. Server Home1A has a backup of Home1B. EdgeB and Home1B are servers that take over should the A counterpart fail.

Duplication is an optional feature that provides a backup server that provides service if the primary server fails. For example, EdgeA has a backup server EdgeB and Home1A has a backup server Home1B.

Duplicating of servers consists of a backup server for a stand-alone SES host, either home servers, edge servers, or a combined home/edge. Duplicating requires the addition of dual NIC modules in both the primary and the backup server. S8500C, S8510, S8800 and HP servers come with dual NICs installed. S8500B comes with dual NICs installed only if a duplicated system has been ordered.

Except for connection cables, no other optional hardware is necessary.

Not all the nodes in an enterprise's SES system need to be duplicated. You might choose one of the following architectures:

- Home/edge combined single
- Home/edge combined duplicated
- Edge single, and one or more home(s) single
- Edge single, and one of more home(s) duplicated
- Edge duplicated, and one or more home(s) single
- Edge duplicated, and one or more home(s) duplicated

Timely system backups of servers are mandatory for all these various architectures.

Important:
If you want to run a full backup on a cable duplicated SES server, you must execute the backup on the active server and not on the backup server. Running the full backup on the redundant server will result in failure.

Network Duplication

Network Duplication enables the physical separation of duplicated SES servers. This feature allows you to set up Edge and Home duplicated servers in separate geographic locations. This configuration ensures business continuity and disaster recovery.

The supported server and platform types are the HP, S8800, S8510, S8500 Servers.

Servers in a single cluster should be of the same server platform and consist of homogenous server types, that is, Home, Edge, or Home and Edge combos.

The SES 5.2.1 duplicated configuration for co-located servers continues to be offered as an option.

This solution is not applicable to the Communication Manager/SES co-residency solution on the S8300 server.

Server-level details of failover

A server may be single or duplicated. In an SES system, a home and edge server may reside on two boxes, whose separate power, disk, and communications components make simultaneous failure unlikely. One box is the primary and provides service, while the other one (the backup or B server) monitors the primary server and takes over if it fails. The primary server performs extensive self-diagnostics as it recedes from service, voluntarily relinquishing control to the backup server in case it finds trouble. After giving up control (whether voluntarily or not), the primary server attempts to restore itself to a state in which it can provide service. Once this has been accomplished, either automatically or with manual intervention, the former

primary server then assumes the role of the new backup sever. In this way, the duplicated-server configuration is maintained even after a local failover has occurred.

Local failover design

Elements within the design of Avaya's primary and backup servers and database local failover feature include:

- Health self-monitoring of the primary server
- Monitoring of the primary server by its backup server
- Mirroring on the servers of persistent data
- Recovering after failure of the primary server
- Monitoring of the control components so they do not contribute unduly to failures
- Restarting a failed processor, resynchronizing its database, and bringing it back into service as the backup server

Failover scenarios

Typically, there are four scenarios in which an SES host may fail to process requests and provoke interchange:

- A primary server detects its own failure or a system administrator takes it out of service. A primary server will failover to the backup server, which becomes the primary server. This exchange of roles is called interchange. The server that was originally primary tries to become the backup server, restarting if necessary.
- A backup server fails or an administrator takes it out of service. In this scenario, no interchange between the two servers occurs. The primary server maintains normal operation without service interruption. The backup server may or may not successfully restart itself. if it does, it remains in the backup role.
- A primary server detects a communication problem with its request link. Communication data are shared by the two servers, and if the backup server detects no problem with its request link, then an interchange takes place. The server that had been primary restarts as the backup server.
- A backup server detects the loss of the primary server. It interchanges with the primary server, then tries to force the other server to restart as the new backup server.

Causes for failover

There are a number of reasons that a primary server might interchange with its backup server:

- The primary server cannot communicate with backup server using dedicated cable.

  Failover will occur if the primary server cannot communicate over the dedicated crossover cable, which carries the heartbeat, to the backup server, but *can* communicate with the backup server using the main network IP LAN port. If the backup server can communicate back to the primary server, the backup server makes the interchange and become the new primary server.
- Data disk space is 90 percent full.
- One or more of the following server processes on the primary server is down:
  - Alarm process
  - Watchdog daemon
  - Heartbeat service
  - PostgreSQL service
- Logical IP addressing fails to operate.
- Any required system process on the primary server fails to respond to **mon** (monitor health).
- System cannot execute drbd (distributed redundant block device) for database replication.
- **`ipfail`**, a tool on the servers used to monitor IP network connectivity to their clients, reports an error on the local, primary machine but no error on its partner, the backup server.

TLS links used for failover

There are 16 available TLS links in SES and Communication Manager. For each SIP signaling group administered, when active, it will utilize 1 link on each system (near-end and far-end). In duplicated home server configurations, reserve some TLS links to support failover.

If your configuration is a duplicated SES home server, and some fault occurs that causes a failover to the standby home server, the newly active home server sets up TLS link to the communication manager server running Communication Manager. It might take 15 minutes to bring down the TLS link to the previously active SES Home).

TLS link utilization is real-time. SES and Communication Manager set up TLS links for SIP when they send the very first SIP request, such as INVITE, or SUBSCRIBE/NOTIFY. The link remains active as long as there is SIP message traffic.

Note that the limit of 16 TLS links is a restriction of the Communications Manager.

For example, if you have 10 SIP trunk groups, you have the possibility of a maximum of 10 TLS links in use at one time.

You can have multiple C-LANs associated with an SES. With multiple C-LANs, you can administer them for load sharing purposes. The Avaya SIP solution does not support alternate C-LANs to handle C-LAN failure scenarios.

From the SES administrator's perspective, each SIP endpoint is administered so that it uses one of the available C-LANs. If there is an SES home with 3,000 users, and you administer two C-LANs to support that SES home, administer 1,500 SIP endpoints to use C-LAN #1 and the other 1,500 to use C-LAN #2. If C-LAN#1 goes down, then those 1,500 SIP endpoints would not be able to make calls. Currently, there is no mechanism to administer an alternate C-LAN on the SES administration screens.

Server interconnections and routing

This section discusses several types of connections between the servers in SES systems:

- Physical and logical connections on page 30
- Address maps for Communication Manager and SES hosts on page 30

Physical and logical connections

The most important aspect of interconnecting the servers is to have a clear idea of which server is the primary and the backup, and if the home and edge servers are combined or distributed.

When you install, check the instructions. Diagrams are provided for all network and power connections, which can differ by hardware and whether servers are single or duplicated.

Address maps for Communication Manager and SES hosts

Address maps for hosts and communication manager servers are an optional but useful feature. In SES R5.1, host address maps are needed if the SES edge or host does not have a public address associated with the called address, or if a specific address is to be routed to a specific address. When SES extensions are administered, they receive a public address and communication manager server contact. No address or host map is needed.

Because of the introduction of visiting user, you must have an address map to complete the call to the PSAP.

Communication Manager server address maps should only be administered to match those extensions that are not local to the SES configuration. Similarly, host address maps should only be administered for those extensions/addresses that are to be routed to a specific proxy, most likely out of the SES configuration, for example, a SIP service provider.

Normal SIP call flow

Recall how a call is setup to fully understand scenarios for which address maps may be needed.

- When a call is originated from a SIP / OPS telephone, the call will initially be directed back to Communication Manager over the communication manager server that phone is associated with. When a call is initiated from a non-SIP phone to another phone over a SIP trunk, the call itself also is initiated from the associated communication manager server running Communication Manager.
- Communication Manager will compare the incoming call to its dial plan and attempt to find a trunk or line over which to direct that call.
- If none are available, or if the extension is not in the dial plan, then the call is rejected. The Proxy Route Selection Pattern in Communication Manager is used to direct calls back to SES servers when SIP messages' REQUEST-URI host portions do not match the domain administered on the Communication Manager Network Region screen, or the user portion is a handle, not digits.
- At this point, the SES system examines the various address maps to determine the best SIP trunk to route the call to next.
- If there is no applicable address map, then SES will not know where to direct the call and will return an appropriate error message to the calling phone or device.

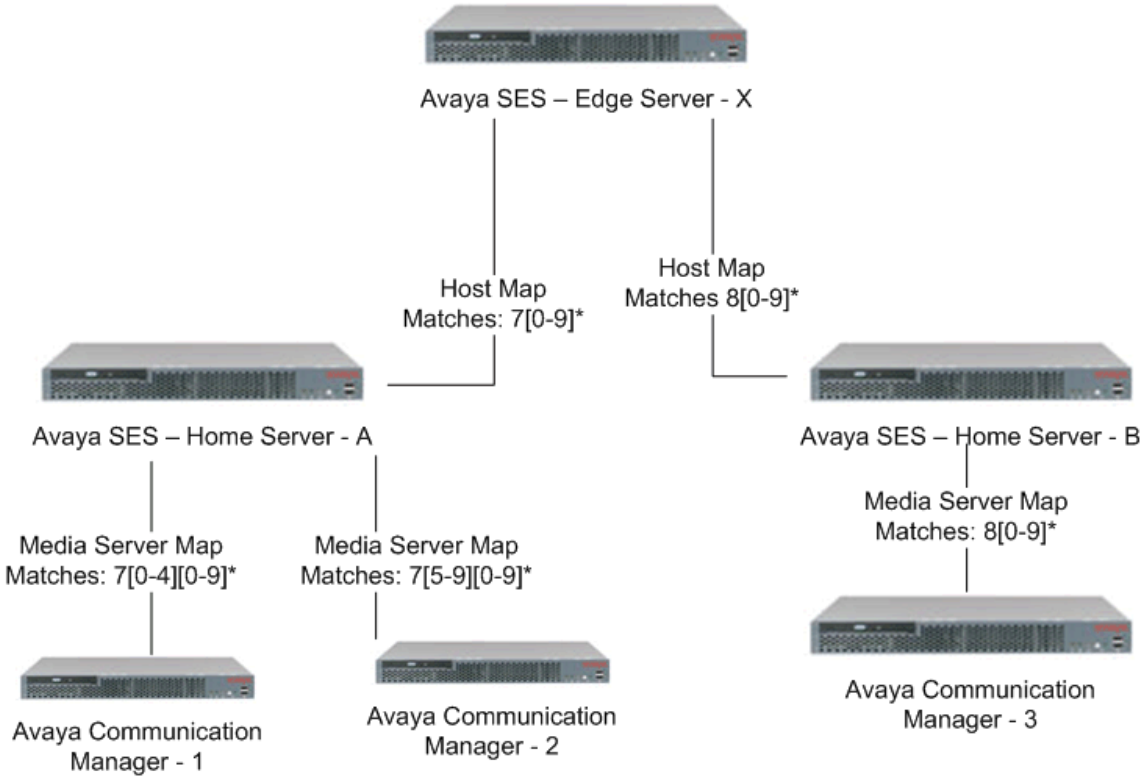
What are address maps and why are they used?

Address maps are a feature in SIP Enablement Services used to route SIP messages to the appropriate SIP hosts based on the destination address in the INVITE message. Address maps are based upon two important concepts:

- A pattern matching a specific destination address (or range of addresses)
- A host contact address indicating where the SIP message should be forwarded.

For example, if there is an SES edge server with multiple SES home servers, and each home has a specific communication manager server running Communication Manager configured, then host address maps need to be configured to route the correct digits to the correct homes, and communication manager server maps need to be configured to route extensions to correct communication manager servers. See Figure 3.

Figure 3: Example of SES network using address maps



For the Example of SES network using address maps, the edge server- X needs to know SIP addresses starting with the digit 7, followed by any number of other digits, are associated with the home server - A. The SES host, home server - A, then needs to know that extension ranges 70 through 74, followed by any number of digits, are associated with Communication Manager - 1, as well as that addresses starting with 75-79, followed by any number of digits, are associated with Communication Manager - 2. Likewise, the edge needs to know that home server - B owns digits starting with 8, followed by any number of digits, and the host, home server - B itself, needs a map to route those calls to Communication Manager - 3.

Important:
Address maps should not conflict. Use the Address Map Priorities screen to prioritize address maps that use the Address Maps link.

Beyond the enterprise ranges, address maps are commonly used when connecting an SES network to a SIP service provider.

Some other sample scenarios for address maps

The following are additional common scenarios of when to use address maps:

- To map incoming DID numbers provided by a service provider to the appropriate server running Communication Manager

- Where the enterprise employs multiple service providers, then maps are used to direct traffic to the correct service provider
- To route calls to a local edge router that also has a PSTN interface

Note:

Routing to a foreign domain (that is, other than the SES domain) can be achieved several ways. The easiest and most preferred method is to configure DNS SRV records for the foreign domains. When the SES SIP proxy receives a message to a foreign domain, it will check for a DNS record to route to. Any SES server can also configure an outbound proxy for foreign domain calls. Finally, a host map can be used though this is not recommended unless there are specific digit ranges that need to be directed to different foreign hosts or there is no DNS service present in the network.

Maps in SES

There are two types of address maps used by SES:

- Communication Manager server Maps
- Host Maps

Communication Manager server maps help route SIP messages to Communication Manager Servers running Communication Manager on one (or more) Linux-based communication manager server interfaces when the called extension is not an administered user in the SES configuration.

Host maps help route SIP messages to SIP proxies or destination that are not in the SES configuration.

These SES administration screens can be used in the process of setting up address maps:

- List Host Address Map screen on page 235
- Edit Host Contact screen on page 241
- List Communication Manager Server Extensions screen on page 216
- List Communication Manager Server Address Map screen on page 246
- Add Communication Manager Server Address Map screen on page 249
- Edit Communication Manager Server Contact screen on page 254

Become familiar with the fields and uses of the screens listed above. You should also be accustomed to using regular expressions for pattern matching, and the effect of wild cards.

Address map pattern matching

Usual pattern for Contact in a communication manager server address map

This contact is for a communication manager server to match calls of any handle and send them to the communication manager server IP address shown after the at sign (@). This contact is automatically provided when a communication manager server address map is administered.

```
^sip:$(user)@123.4.56.78:5061;transport=tls
```

In the example contact above,

^	matches the beginning of a line in the SIP message
sip:	denotes the protocol. This could be `sip:` and `sips:` protocols.
$`(user)`	variable substituting the user portion of the SIP message
@	means a communication manager server IP address is next
123.4.56.78	is the IP address of the communication manager server
5061:	is typically the port number for TLS, although others may be used.
transport = tls	indicates transport method. For most customers' use, this must be set to **tls**.

Usual pattern for a map in a communication manager server address map

This pattern matches any calls having 231 as the first 3 digits, then any number of other digits.

```
^sip:231[0-9]*@customer.com
```

So in the preceding example:

- ^ matches the beginning of a line
- for any first 3 digits of 231
- ending with any other sequence of digits (including no other digits, matching 231 itself)
- in the **`customer.com`** domain

And in the example contact,

^	matches the beginning of a line in the SIP message
sip:	denotes the protocol. This could be `sip:` and `sips:` protocols.
nnn	specific digits
{nnn}	length of match digits
*	any length
@	means a communication manager server IP address is next
123.4.56.78	is the IP address of the home host or edge host that takes the call because of a successful match.

This pattern matches seven-digit calls starting with 303 for the customer.com domain:

```
^sip:303[0-9]{7}@customer.com
```

This pattern matches any calls for customerdomain.com that begin with the digit 7:

```
^sip:7[0-9]*@customerdomain.com
```

This pattern matches any calls for the customer.com domain from Australia, country code 61, and the city of Sydney, city code 2:

```
^sip:612[0-9]*@customer.com
```

Pattern

This is a Linux regular expression that will match the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s). (NOTE: You must match the characters in SIP's INVITE message exactly. You do not need to match characters not present in the invite message, such as the marks of punctuation like dashes, periods or parentheses which may sometimes be used to enhance the readability of telephone extensions.) For example, [0-9] represents any single digit and * represents any number of digits or characters. So the example in the preceding illustration **`^sip:231[0-9]*@customer.com`**
would match a SIP invite message (^ matches the start of a line) for any set of 3 or more digits, beginning with the digits 231, and ending with any other digits, in the customer.com domain.

An example of a pattern useful for matching messages would be
`^sip:[0-9]*@customer.com`
which would match a SIP invite message for any length of dial string beginning with the digit 9.

Square brackets contain a selection of characters to be matched, with a hyphen indicating a range; so in our example,[0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Curly brackets, which contain a whole number, match that number of instances of the preceding item. So for example, 231[0-9]{4} matches any seven digits that begin with 231 and end with any four digits of zero through nine. Note that the braces may require escape characters: \{4\}

Another helpful metacharacter is dot (period), which matches any single character; for example, the regular expression **`.*`** matches any quantity of any character(s).

See "*SIP Support in Avaya Aura® Communication Manager*", doc ID 555-245-206, for more details.

Requirements for the SIP solution

These sections specify the required elements of the SIP Enablement Services solution:

- Hardware and Equipment on page 36
- Software requirements on page 38

Hardware and Equipment

This is the equipment list for installing and running SIP Enablement Services:

- Avaya S8800 and HP servers—for use as SES edge and home hosts. They employ a BMC module for remote servicing.
- Avaya S8300C and Avaya S8300D—for communication manager servers that run Communication Manager. SES can be co-resident with Communication Manager on this server. You cannot install Avaya Communication Manager Branch Edition, which uses SES, on an S8300 co-resident with Communication Manager.
- Avaya S8500- Series Servers—for use as SES edge and home hosts. The S8500B, S8500C and S8510 employ a SAMP module for remote servicing.
- PC or laptop
- Keyboard and monitor
- Null modem cable
- CAT 5e (or better) Ethernet crossover cable for connecting duplicated-server hardware
- S8500B comes with a dual NIC installed only if a duplicated system has been ordered.

SES Hardware

The server hardware required for an SES server can be one of these:

- HP DL360 G7 Server
- Avaya S8800 Server
- Avaya S8300C or S8300D Server
- Avaya S8500 or S8510 Server

If your network uses SES on an S8300C or S8300D Server, it shares this server with Communication Manager. It is co-resident.

For the HP DL360 G7 Server, Avaya S8800 Server, and S8500-Series Servers, you must use the SIP Enablement Services setup and install CD.

Visit the Support site: http://www.avaya.com/support for more information and instructions on installing these components:

- Dual in-line memory module (DIMM). ***This memory must be added to S8500 Servers before use.***
- Server Availability Management Processor (SAMP) remote maintenance board in S8500 and S8510 Servers.

Any home server that supports up to 3,500 users requires a total installed RAM of 1 GB.

An home server that supports up to 6,000 end users requires a total of 3 GB of memory. Because one edge can link to as many as 1000 home servers, the edge server requires 3 GB of memory.

S8510 Server does not require additional RAM as it comes with standard 4 GB RAM.

For S8500B or S8500C Server, 1 GB or 3 GB RAM is required because the RAM modules are deployed in pairs in either of these servers, as follows:

- 1 GB = two 512 MB DIMMs installed in slots 1 and 3
- 3 GB = two 512 MB DIMMs + two 1 GB DIMMs installed in slots 2 and 4

Avaya requires that one universal serial bus (USB) modem be connected to each server (one for each of the duplicated servers) for remote access.

On HP DL360 G7 and S8800 Servers, a modem is connected to the USB port on the server. On the S8500-Series, a modem is connected to the USB port on the SAMP card. Multiple modems may be configured to share one analog telephone line (each answering after a different number of rings). Implementation and maintenance services require remote access in this way.

The servers come with a blank, unpartitioned hard-disk drive, and without an operating system or any Avaya server software files installed. These components must be installed and configured properly before using SES.

In addition, IP connectivity must be configured correctly on all Communication Manager servers running Communication Manager. For more details on configuring your IP system, refer to *Administering Network Connectivity on Avaya Aura® Communication Manager,* Doc ID 555-233-504*.*

Supported Phone Types for SES

- Toshiba SP-1020A
- Avaya one-X™ Deskphone, 9620, 9630, 9630G, 9640, or 9640G, with SIP firmware R 2 or later
- SIP Softphone / Avaya one-X™ Deskphone Edition
- 4600 series telephones except 4610 with SIP firmware
- Visiting User requires a Avaya one-X™ Deskphone with R 2 or later of SIP firmware

- Call Center requires Avaya 16CC telephones

Software requirements

These software components are installed from the Avaya installation CD:

- Linux operating system
- WebLM, for managing licensing
- Proxy, IM Logger and TraceLogger services provided by Avaya
- PostgreSQL database
- Apache web server (for providing access to the Administration and Maintenance web interfaces)

You will also need this, available on the web:

- PuTTY client, a type of SSH client

Chapter 3: Installing SES on the server

This section contains the procedures for installing, configuring, and administering SIP Enablement Services (SES) software on servers in various configurations. The configurations include

- Combined single edge/home server.
- Combined duplicated edge/home server.
- Distributed single edge with single or duplicated homes.
- Distributed duplicated edge with single or duplicated homes.

Before the installation, determine the following information:

- Type of configuration you are installing.
  - Separate edge and home or combined edge/home
  - If duplicated servers, cabled duplicated (collocated) or network duplicated (physically separated).
- If duplicated servers, be clear on the names and roles of which server is A and which is B. The designation A and B does not indicate which machine is primary and which is backup.
- A filled-out Installation Worksheet.

These installation procedures include

- Completing pre-installation checklist.
- Physically installing the server(s).
- Physically connecting duplicated servers.
- Installing the SES software on the server(s).
- Configuring SES on the server(s).
- Installing licenses on the server(s).
- Administering SIP and SIP endpoints on the servers and on the server running Communication Manager.
- Testing the installation.

When installing multiple servers, install, configure, and administer edge servers first, then the home servers. Administer SES on the server running Communication Manager last. See *SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers* (555-245-206) for details.

Server Availability Management Processor (SAMP) firmware and operations

When performing a fresh new installation of SIP Enablement Services on the S8510, S8500B, or S8500C servers, the initial_setup script will install the proper version of the Server Availability Management Processor (SAMP) firmware. It is recommended for proper operation of the Avaya SIP Enablement Services server that you do not upgrade the SAMP firmware independently of the SIP Enablement Services software, even if a newer version is available. SIP Enablement Services software includes the SAMP firmware for its operations.

The installation, configuration, and administration use telnet, Secure Shell, the Maintenance Web Interface, and the SES Administration Interface.

Pre-installation checklist

Use this checklist to make sure that you are prepared for the installation.

✓	**Task**
	Determine the configuration being installed on your SES network and specifically where your edge server will be running the Master Administration web interface.
	Verify that a server running Communication Manager R3.1 or later is installed and functioning properly.
	Verify that the server running Communication Manager has the latest firmware installed for the TN799D C-LAN and TN 2302BP Media Processor or TN2602AP Media Resource 320 circuit packs.
	Ensure that the customer site has the racks installed and is setup for the installation.
	Ensure that all the equipment and cables are on site. Verify the contents against the list provided by the project manager.
	Determine whether you are installing the HP Server(s), S8800 Server(s), S8500 Server(s) or S8510 Server(s). Rack installation and connectivity is different.
	Verify that you have the documentation for physically installing the server(s) with you. It no longer ships with the server.
	Decide the functional type of your server(s): home, edge, or combined edge/home

✓	Task
	If duplicated configuration, determine whether cabled duplication (collocated) or network duplication (separated).
	Verify that you have the filled-out Installation Worksheet (see Appendix A for a blank form) to help you fill in the configuration and administration fields.
	Verify that you have the CD with the SES software; it ships with the server.
	Verify that you have a keyboard and monitor and appropriate cables.
	Verify that you have a services laptop with CAT5 Ethernet crossover cable. Have laptop configured for direct access to the server.
	Verify that you have a CAT 5 Ethernet crossover cables for connecting duplicated servers.
	Verify that you have a null modem cable for connecting cabled duplicated servers.

Installation checklist

Use this checklist to install, configure, and administer SIP Enablement Services.

✓	Task
Pre-Installation tasks	
	Configuring the network settings on the computer
	Configuring Telnet for Windows 2000 and Windows XP
	Connecting to the server directly
	Clearing the ARP cache on the laptop
	Server physical installation and connection
	If the ARP cache does not contain the specified IP address, the message The specified entry was not found appears. You can ignore this message.

✓	Task
	Rebooting S8800 or the HP Server
	Changing the BIOS settings on the S8510 Server
	Rebooting the S8510 Server
Installation tasks	
	SES installation
	Powering up the server
	Accessing the server
	Installing SIP Enablement Services
Configuration tasks	
	Configuring SES
	Verifying the start of SES
	Accessing the System Management Interface
	Setting the date and time
	Rebooting the server
	Configuring the time server
	Verifying the configuration
	Copying files to the server
	Creating a super-user login
	Server license installation
	Configuring the network settings on the computer
	Accessing RFA
	Launching the SES Administration Interface
	Installing WebLM license file
	Installing the Avaya authentication file
Administration tasks	
	Administering setup
	Setting up hosts

✓	Task
	Initial administration on an edge server
	Setting up SIP domains
	Setting up default user profiles (optional)
	Setting up servers
	Adding trusted hosts
	Configuring SNMP
	Configuring Communication Manager endpoints

Preinstallation tasks

Before starting the installation, make sure that you have the following equipment:

- Keyboard and monitor and appropriate cables
- Services laptop with CAT5 Ethernet crossover cable. Have laptop configured for direct access to the server.
- CAT 5 Ethernet crossover cable for connecting cabled (collocated) duplicated servers.
- Null modem cable for connecting cabled (collocated) duplicated servers.

Configuring the network settings on the computer

You need to configure your computer's network settings to access the server directly.

Important:
Write down the original settings for use in case you need to revert to the original configuration.

These procedures are for computers using Windows 2000/XP.

1. On the computer, right-click **My Network Places** and left-click **Properties** to display the Network Connections window.

   Windows 2000 or Windows XP should automatically detect the Ethernet card in your system and create a LAN connection. More than one connection might appear.

2. Right-click on the correct **Local Area Connection** and left-click **Properties** to display the Local Area Connection Properties dialog box.

3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties** to display the Internet Protocol (TCP/IP) Properties dialog box.
5. On the General tab, select **Use the following IP address**.
6. Make a note of any IP addresses or other entries that you have to clear. You might need to restore them later to connect to another network.

   Enter the following:

   - IP address: `192.11.13.5`
   - Subnet mask: `255.255.255.252`
7. Select **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
8. Click **Advanced** at the bottom of the dialog box to display the Advanced TCP/IP Settings dialog box.
9. Click the **DNS** tab. Ensure no DNS server is administered. The address field should be blank.
10. Click **OK** and **Close** to close all the windows.

Configuring Telnet for Windows 2000 and Windows XP

The Microsoft Telnet application might be set to send a carriage return (CR) and a line feed (LF) whenever you press **Enter**. The installation program sees this as two separate key presses. If you are running Windows 2000/XP, you must correct this setting before you copy the script to the hard disk drive.

1. Click **Start** > **Run** to open the Run dialog box.
2. Type `telnet` and press **Enter** to open a Microsoft Telnet session.
3. Type `unset crlf` and press **Enter**.
4. Type `display` and press **Enter** to verify that you see the message **Line feed mode - Causes return key to send CR**.
5. Type **q** and press **Enter** to exit the telnet session.

Server physical installation and connection

See the *Installing the Avaya S8800 Server for Avaya Aura® SIP Enablement Services* (03-603447) for procedures on physically installing the Avaya S8800 Server in a rack. See *Installing the HP DL360 G7 Server* (03-603799) for procedures on physically installing HP

ProLiant DL360 G7 Server. See the *Installing the Avaya S8510 Server Family and Its Components* (03-602918) for procedures on physically installing the Avaya *S8510 Server* in a rack.

Before beginning the installation procedure, check all connections and ensure that the physical connections are correct. See Connection schema for duplicated servers on page 65 for connecting duplicated servers in either a cabled duplication (collocated) or network duplication (separated) schema.

Connecting to the server directly

Make sure your laptop is configured for direct access. See Configuring the network settings on the computer on page 43.

To connect to the server directly:

1. Plug one end of the CAT5 cable into the Services access port on the back of the server.
2. Plug the other end of the CAT5 cross-over cable into the NIC on your computer. Use a NIC adapter if necessary.

Clearing the ARP cache on the laptop

Depending on the operating system of your Services laptop computer, you might need to clear the Address Resolution Protocol (ARP) cache before you enter a new IP address. If you enter an IP address and your computer cannot connect, perform the following procedure to clear the cache.

1. On your computer, click **Start** > **Run** to open the Run dialog box.
2. Type **command** and press **Enter** to open an MS-DOS command line window.
3. Type **arp -d 192.11.13.6** and press **Enter** to clear the ARP cache in the laptop.

   If the ARP cache does not contain the specified IP address, the message **The specified entry was not found** appears. You can ignore this message.

Accessing the uEFI and firmware updates for S8800 Server

To access downloads and instructions for the uEFI and firmware updates for S8800 Server:

4. Log on to the Avaya support website at http://support.avaya.com
5. On the left navigation panel, click **Downloads**. A product pop-up window appears.
6. Type **S8800** in the product pop-up window. **S8800 Server** appears as an option.

7. Select **S8800 Server**. The system displays download links for **S8800 Server**.
8. From the release drop-down menu at the top of the screen, select **5.2x**
9. Click **S8800 Server uEFI Setting Tool**

Rebooting S8800 or the HP Server

You need to reboot the server for the uEFI changes to take affect.

To reboot the server:

1. Push and hold the power button on the front of the server.
2. Release the button when the server shuts down.
3. Press the power button to restart the server.

You can now disconnect keyboard and monitor from the server.

Go to SES installation on page 48 to start the installation process.

Disabling Remote Console on an S8800

Use a monitor and keyboard for this procedure.

1. Power on the server and observe boot messages on the monitor. The system displays Integrated Management Module (IMM) messages followed by uEFI initialization messages. An **IBM System X** splash appears and the system displays the message about hardware initialization. The screen temporarily blanks out for 15 seconds approximately and then prompts you to press **F1** to enter setup.
2. Press **F1** quickly. use the arrow keys to move up and down in the **System Configuration** selection screens.
3. Move down and highlight **System Settings** and press **Enter**
4. On the next screen, highlight **Devices and I/O Ports** and press **Enter**
5. System displays **Console Redirection Settings** screen. Highlight **Remote Console** and press **Enter**
6. Change the **Remote Console** setting to **Disable** and press **Enter**

The **Remote Console** is now set to **Disabled**.

7. Press **Esc** four times to return to the top setup menu
8. Select **Y** and press **Enter** to save and exit the setup menu. The system will now reboot.

Disabling Remote Console on an HP DL360 G7

Use a monitor and USB keyboard for this procedure.

1. Power on the server and observe boot messages on monitor. The system displays **HP Proliant Splash** screen. After the splash screen fully populates in the bottom left corner of the display, the user is prompted to press **F9** to enter Setup
2. Press **F9** quickly. The system displays'**F9 Pressed**' message. Use the arrow keys to move up and down in the **Setup Utility** selection screens
3. Move down and highlight **BIOS Serial Console & EMS** and press **Enter**
4. On the next screen, highlight **BIOS Serial Console Port** and press **Enter**
5. Select **Disable**. Press **Enter**

The **BIOS Serial Console Port** is now set to **Disabled**.

6. Press **Esc** two times to return to the top **Setup Utility** menu.
7. Press **F10** to save and exit the **Setup Utility** menu. The system will now reboot.

Changing the BIOS settings on the S8510 Server

Use a monitor and keyboard for this procedure.

1. Power on the server and observe the boot messages on the monitor.

   The system immediately prompts for BIOS information.
2. Press **F1** quickly.
3. When prompted for the **Configuration/Setup Utility** press **F1** again.
4. Select **Start Options > Power** management.
5. Set **Automatic Power On** to **Enabled**.
6. Select **Advanced Setup > Console Redirection.**
7. Set the **Com Port Address** to **Disabled**.
8. Select **Save Settings** and confirm by pressing **Enter**.
9. Select **Exit Setup** and confirm by pressing **Enter**.

Rebooting the S8510 Server

To reboot the server:

1. If you are presented with an **SES Software Install Selection screen**, use the arrow keys to highlight the **Reboot** option.
2. Press the space bar to select **Reboot**. The server reboots.

   Observe the kernel loading and any Ethernet port messages that are displayed.
3. Type **exit** and press **Enter** to close the command line window.

You can now disconnect keyboard and monitor from the server.

Go to SES installation on page 48 to start the installation process.

SES installation

The following tasks install the SES software on the server(s). The same installation process is used whether the server is an edge, home, or edge/home combination.

Powering up the server

Note:

In this procedure, the software CD-ROM is placed into the CD-ROM drive on the server immediately after you turn on the power to the server.

To power up the server:

1. Connect the AC power cord to the server and to the UPS or a nonswitched electrical outlet.
2. If the server does not turn on, press the power button on the front of the server.
3. Immediately place the software CD-ROM into the DVD/CD-ROM drive on the server.

Accessing the server

To access the server:

1. Use a cross-over cable to connect the laptop computer to the Services port on the back of the server.

2. Wait at least 3 minutes after you turn on the server before you start a Telnet session to access the information on the CD-ROM.

Installing SIP Enablement Services

Use a Telnet session to access the information on the CD-ROM.

1. On the laptop computer, click **Start** > **Run** to open the Run dialog box.
2. Type **`telnet 192.11.13.6`** and press **Enter** to view the first screen.

   Note:

   To navigate on these screens, use the arrow keys to move to an option, and then press the spacebar to select the option. Press **Enter** to submit the information on the screen.

3. On the first screen, select **- Install or Upgrade SES Software**. Ensure that **<OK>** is highlighted, and press **Enter**.
4. On the second screen, select **- Select Release Version: SES software build number**.

   Wait about 10 seconds for this to complete.

5. Press **Enter** to accept each of the default settings.

   Accept these defaults to install a new release on this server.

6. Select **y** or **Enter** to proceed.

   The server copies software packages and package managers to the appropriate partition.

   Once the drive is properly configured, the program starts the installation process and reports the progress.

   These processes can take up to 20 minutes to complete.

7. When the server is ready to reboot, the drawer of the CD-ROM drive opens. Remove the CD.
8. The reboot can take up to 4 minutes. The Telnet session drops automatically when the reboot starts.

   If the CD does not eject, restart the installation procedures.

   If either member of a duplicated-server pair does not reboot, then the software likely was not properly installed.

Installing SES Service Packs on HP DL360 G7 Server

The HP DL360 G7 Server supports SES 5.2.1 SP 4 and later releases only. The common installer does not support the HP DL360 G7 Server. Therefore, version upgrades through Web pages are locked unless you deactivate the service pack. To install from a CD, use the procedure below:

Note:

The below instructions apply to HP Servers only. For instructions on how to install SP 4 or later releases on other server types, see Service Pack release notes.

1. Install the HP DL360 G7 Server with the SES 5.2.1 GA CD. Choose IBMX3550 as the hardware type.
2. Run initial setup. Choose a simplex configuration, and define the IP address.
3. Ensure that SES is out of service during the service pack installation. At the prompt to start the SES services during the initial setup, select **No**.
4. Reboot the server.
5. When the server is functional, make sure the servers are out of service, download the SP and activate it.
6. In a simplex configuration - reboot the server.
7. In a duplex configuration - perform the following steps on both the servers:
   a. Run the initial setup. Choose a duplex configuration
   b. Turn off the servers
   c. Remove the AC cable for at least 20 seconds, then reconnect
   d. Turn on the servers
   e. Wait for the two servers to synchronize their databases (DRBD)
   f. Place both servers in service
   g. If required, perform a system restore operation on the primary server as the server only the "SES_files" option.

Note:

Make sure that, when in service, both servers in a duplex setup have the same service pack installed at all times.

Configuring SES

When configuring SES on a server, you get different screens and prompts, depending on whether you are configuring a single server or duplicated server pair. Use the Installation Worksheet (Appendix A) to help you fill in the fields in this section.

For configuring a server in a single configuration, see Configuring a single server on page 51. For configuring a server that is part of a server pair, seeConfiguring a redundant server on page 52.

Configuring a single server

To configure the server:

1. Connect to the services port on the server.
2. Log in as **craft**.
3. At the prompt, enter **`initial_setup`** to run the initial configuration script.
4. The script checks the SAMP firmware version and indicates the current firmware version of SAMP and what the correct version should be. It then upgrades the firmware if necessary. This takes about 10 minutes.
5. On the first screen fill in the information for the following fields then click **OK**:
   - Host name
   - DNS domain name
   - IP address
   - Netmask
   - Gateway
   - Primary (and optionally Secondary and Tertiary) DNS IP address(es)
6. On the **Redundancy Configuration** screen, select **single** then click **OK**:
7. Click **Finish** to complete the configuration.
8. When asked if the watchdog must be stopped before installing SES, type **y**.
9. At the prompt **Are you initializing a Master Administrator on this machine?** enter one of the following options then click **OK**:

   Enter **y** if this is a single edge or edge/home. If more than one edge server, enter **y** for the first one only.

   Enter **n** if this is a single home.

   The system initializes the SES Master Database.

10. At the prompt **Start Services**, enter **y**.

Configuring a redundant server

You want to configure Server A first, then configure Server B.

To configure the server:

1. Connect to the services port on the server.
2. Log in as **craft**.
3. At the prompt, enter **`initial_setup`** to run the initial configuration script.

   The script checks the SAMP firmware version and indicates the current firmware version of SAMP and what the correct version should be. It then upgrades the firmware if necessary. This takes about 10 minutes.
4. On the first screen fill in the information for the following fields then click **OK**:
   - Host name
   - DNS domain name
   - IP address
   - Netmask
   - Gateway
   - Primary (and optionally Secondary and Tertiary) DNS IP address(es)
5. On the **Redundancy Configuration** screen, select one of these options then click **OK**:

   If this is a cabled duplicated (collocated) edge/home server or duplicated edge or duplicated home, select **Cabled Duplicated**.

   If this is a network duplicated (separated) edge/home server or duplicated edge or duplicated home, select **Network Duplicated**.
6. Click **Finish** to complete the configuration.
7. On the **Redundancy Role** screen, select one of two options then click **OK**:

   If this server is the active server, select **A**.

   If this server is the backup server, select **B**.
8. On the **Redundancy Configuration** screen, fill in the information for the following fields then select **OK**.
   - Logical Host name:
   - Logical IP address:
   - Host Name of Server (A or B):
   - IP address of Server (A or B):

9. On the **Redundancy Initial_setup type** screen, select one of two options then click **OK**:

   New install to create a new redundant pair.

   Reinstall or reconfigure server in an existing redundant pair.

10. Click **Finish** to complete the configuration.
11. When asked if the watchdog must be stopped before installing SES, type **y**.
12. At the prompt **Are you initializing a Master Administrator on this machine?** enter one of the following options then click **OK**:

    Enter **y** if the duplicated server is an edge server.

    Enter **n** if the duplicated server is a home server.

    The system initializes the SES Master Database.

13. Repeat these steps on the second server (Server B).
14. At the prompt **Start Services**, enter **y**.

Note:

SipServer is partially up until the data service and SES host configuration is completed.

Important:

Problem: During the configuration of a Network Duplicated SES you may come across the following problem: The backup server is reporting its SIP Roll as **Unknown** when checking server state. Takeover and interchanges are successful for both servers. SIP endpoints will not register to the backup server when it is Active Primary. All other routing through SES works.

Solution: The secondary SES does not know its roll, so it will not register SIP endpoints. It needs to be administered as the Master Administrator through the **initial_setup** and in the Administration web interface.

Verifying the start of SES

You must run the initial_setup script before performing this procedure. This procedure is for the whole site. If you have more servers to install, for example more home servers, install SES on and configure them before performing these steps for the whole site.

These steps verify that the software can run. Later, you or another person might do a more complete installation check before the customer performs their own customer acceptance testing. You are connected to the Avaya Services port.

1. Connect to the Services port on the server.
2. Start a telnet session.

3. Log in as **craft**.
4. Enter **statapp**.
5. The status should show the following results for the active server:

```
Watchdog                UP
ModemMtty               UP
TraceLogger             UP
SME                     UP
INADSAlarmAgen          UP
GMM                     UP
SNMPManager             UP
ImLogger                UP
SipServer               partially UP 2/45
CCSTrapAgent            UP
mon                     UP
MtceMgr                 UP
```

You can check the System Status screen in the Administrative interface at any time to monitor the progress of the processes starting up.

You can also look at current alarms to see what process alarms are coming in.

Accessing the System Management Interface

Use Internet Explorer Web browser to access the System Management Interface.

1. In the **Address** field, type **192.11.13.6**.

   Note:

   The first time that you log in, you see a message that asks you to install a security certificate. Follow the instructions for your particular browser to accept the certificate. You can also install the certificate on your computer with the instructions in the online Help for your browser.

2. When prompted, log in as **craft**.
3. When you see **Do you want to suppress alarms?**, select **Yes**.
4. The system displays the System Management Interface.

Setting the date and time

Use the System Management Interface for this procedure.

To set the date and time:

1. Under Server, select **Server Date/Time**.

2. In the **Server Date/Time** window, verify the date and time are correct. If the date and time are incorrect:
   a. Enter the date
   b. Enter the time
   c. Enter the time zone
   d. Click **Submit**

Resetting the time zone requires a reboot. See Rebooting the server on page 55

Rebooting the server

Use the System Management Interface for this procedure.

To reboot the server:

1. Under Server, select **Shutdown Server**.
2. Select **Delayed Shutdown and Restart server after shutdown**.
3. Click **Shutdown**.

   You will be logged off the server when it reboots. You can ping the server to verify when the server is accessible again.

Configuring the time server

Use the System Management Interface for this procedure.

To configure the time server

1. Under Server Configuration select **Configure Server**.
2. From the menu select **Configure Time Server**.
3. Select **Use these Network Time Servers:** field and fill in the DNS or FQDN host name or IP address for the external time source being used.

Verifying the configuration

Use the System Management Interface for this procedure.

To verify the configuration:

1. Under Server Configuration select **Configure Server**.

2. View all the screens to verify that the fields show the correct data for your site. Ensure that the IP address is populated with the information contained in the installation script received from ART.

Copying files to the server

Use the System Management Interface for this procedure.

To copy files to the server:

1. From the Maintenance Web Interface, under **Miscellaneous**, click **Download Files**.
2. Select **File(s) to download from the machine I'm using to connect to the server**.
3. Click **Browse** next to the top field to open the Choose File window on your computer. Find the files that you need to copy to the server.
4. Click **Download** to copy the files to the server.

   The files are automatically copied to the default file location /var/home/ftp/pub.

Creating a super-user login

Note:

A craft level login can create the super-user login.

Use the superuser login name and password that the customer provided.

Use the System Management Interface for this procedure.

Note:

Make sure the customer can change this login, its password, or its permissions later.

1. Under Security, click **Administrator Accounts**.
2. Select **Add Login** and **Privileged Administrator** and click **Submit**.
3. In the **Login name:** field type a login name for the account. The following information displays:
   - In the **Primary group** field: `susers`.
   - In the **Additional groups (profile)** field: `prof18` (`prof18` is the code for the customer superuser).
   - **In the Linux shell** field: /bin/bash
   - In the **Home directory field**: /var/home/login name. ***`login name`*** is the name you chose in step 3.

4. Skip the **Lock this account** and **Date on which account is disabled-blank to ignore** fields.
5. In the **Select type of authentication section**: field select **Password**.

   Note:

   Do not lock the account or set the password to be disabled.
6. In the **Enter key or password** and **Re-enter key or password** fields, enter the password.
7. In the **Force password/key change on next login section** field, leave the default to no.
8. Click **Submit**.

Server license installation

If a single SES solution, you need only one license for the entire SES solution. If duplicated SES edges, you need two licenses. The licenses are based on the edge servers' MAC addresses.

These three licenses are included in the single license file:

- Home proxy license
- Edge proxy license
- Home seat licenses

Terminology differs between the Master Administration interface License screen and the WebLM > Licensed Products > IMPRESS screen. See License Terminology on page 57.

Table 1: License Terminology

Administration Web Interface	WebLM screen
Edge proxy	Edge proxy license (EDGE_proxy)
Basic proxy	Home proxy license (BASIC_proxy)
Home seats	Home seat licenses (HOME_seats)
one-X Deskphone Edition	Softclient

The WebLM server is installed in one location only, on the primary edge or combined edge/home server.

Obtaining the MAC address

You need the MAC address of the server that will be configured as the edge or combined edge/home to get the license file from RFA.

To obtain the MAC address:

1. Type **`get-mac-address`**.

Accessing RFA

You must have the MAC address before accessing RFA.

Use the established RFA procedures for obtaining licenses for Avaya servers.

1. In a Web browser, type **http://rfa.avaya.com** in the Location field.
2. Download the license file to a location that can be accessed later, typically to a location on a laptop used by services personnel.

   Note:

   To obtain RFA licenses needed to install the entire SES solution, you must have required manager approval for three product families: Communication Manager, SES, and Softclients.

Launching the SES Administration Interface

To launch the SES Administration Web Interface:

1. On the Standard Management Solutions page, click **Launch SES Administration Interface**.

   You receive a warning about License Error Mode. Ignore it until after completing the server configuration.

Installing WebLM license file

Note:

When installing a WebLM license using the Internet Explorer web browser on a PC with a non-U.S. version of Microsoft Windows (for example, Japanese Windows), the full path name to the license file should contain only ASCII characters and not international or special characters.

Use the SES Administration Interface for this procedure.

To install WebLM license file on the server:

1. Under Server Configuration select **License**.
2. Select **Access Web LM** to view the WebLM License Administration page.

Note:

If the WebLM browser screen does not launch, disable pop-ups on your browser.

3. From the WebLM screen, select **License Administration** and enter the WebLM default administrative password.
4. After the initial login to WebLM, the system prompts you to change the password then logs you out.
5. Log back in with the new password.
6. Select **Install license**.
7. Select **Browse** and navigate to the location where you saved the license file.
8. Select **Install**.

   The proxy server renews acquired licenses every 5 minutes. However, initially it has not acquired any licenses (none are installed), so the proxy server tries every 60 seconds. After it has acquired them all, it renews them every 5 minutes.

Installing the Avaya authentication file

Use the System Management Interface for this procedure.

To install the password file on the server:

1. Under Security select **Authentication File**.
2. Select **Install the Authentication file I previously downloaded** and click **Install**.

   The system tells you the authentication is installed successfully.

Once the authentication (password) file is loaded, root is disabled, and craft and sroot are ASG challenged, even on the Services port.

Administering SES

The following tasks are the initial administration tasks done at installation.

Administering setup

Use the SES Administration Interface for this procedure.

To administer SES:

1. Select each link on the **Top** screen to complete the initial host administration screens if you are installing an edge or edge/home server.
2. Under Server Configuration select **Admin Setup**.
3. Select one of the following options, then click **Setup**.

   If configuring an edge or edge/home server, select "This server is the SES Master Administration System for the SES Network."

   If configuring a home server, select "This server is configured to use another SES Administration System with the following address:"

   In the Master Administration IP Address field, type in the IP address of the single edge server. If the edge is duplicated, type in the virtual IP address of the edge server.

Setting up hosts

Use the SES Administration Interface for this procedure.

To set up hosts:

1. From the menu, select **Hosts > Lists**.
2. Click **Edit** to display the Edit Hosts page.
3. In the **Host IP Address** field, enter the IP address of this server.
4. In the **Profile Service Password** field, enter the password for the server.

   The Profile Service Password is not used by users or administrators. Rather, it is a password that internal software components use for secure communication between SES servers and the master administration system. The Profile Service Password must be unique for each administered host.
5. In the **Host Type** field, select the appropriate type for this server from the from the drop-down list**.**
6. Set the **Listen Protocols** and **Link Protocols**.

   The link protocols for SIP trunking in Communication Manager are TCP and TLS. By default, the system shows all listen protocols and one link protocol (TLS for SES host-to-server communication). You may select your own link protocol as long as it is also selected as a listen protocol.

   For example, if you are using a 4600-series or 9600-series SIP telephone, then you should check all three listen protocols. If you are using only the IM client in IP Softphone R5.1 or later or SIP Softphone R2.1 within your enterprise, then the TLS Listen Protocol is sufficient.
7. (Optional) In the **Minimum Registration** field, if you want to change the default value of 900 seconds, enter a new, whole integer, 900 through 59940.

8. (Optional) Accept the defaults for the following fields:
    - Access Control Policy
    - Emergency Contacts Policy
    - Minimum Registration and Registration/Subscription Expiration timer (seconds)
    - Line Reservation Timer (seconds)
    - Outbound Routing Allowed From
    - Outbound Proxy and Port
    - Outbound Direct Domains
    - Default Ringer Volume and Cadence
    - Default Receiver/Speaker Volume
    - VMM Server Address
    - VMM Server Port and Report Period
9. Select **Update**.

Initial administration on an edge server

The following installation administration is done on an edge or edge/home combo server only.

Setting up SIP domains

Use the SES Administration Interface for this procedure.

To set up SIP domains:

1. Under Server Configuration select **System Properties** to display the View System Properties page.
2. In the **SIP Domain** field, enter the domain name of the enterprise you want to use for SIP communications.

    Note:

    Avaya does not recommend entering an IP address in this field, but it is possible if you want to address SIP users via the syntax of userhandle@<IP-address-of-domain>
3. In the **SIP License Host** field, enter the IP address of this server.

    This address refers to the host name or fully qualified domain name of the server. If this is a combined edge/home single host, use localhost for the domain name.
4. In the **Call Control PHB Value** and **Priority Value** fields, keep the defaults.

5. In the **Management System Access Login** and the **Management System Access Password** fields, enter the login ID and password.

   If you are setting up for branch-to-core access, use the login ID and password exactly as you used for Avaya Distributed Office.

6. Select **Update** to effect the changes.
7. Select **Continue**.

Setting up default user profiles (optional)

Use the SES Administration Interface for this procedure.

To set up default user profiles:

1. From the menu, select **Users**.
2. Select **Edit Default User Profile** to display the Edit Default User Profile page.
3. In the **Host** field, verify the IP address of the server. In the other fields, enter the address data that will be used most frequently when accessing users on this server.

Setting up servers

Use the SES Administration Interface for this procedure.

You must do this task before any server extensions are administered.

To set up servers:

1. From the menu, select **Communication Manager Servers** to display the Manage Communication Manager Server Interfaces page.
2. Click **Add Communication Manager Server** to display the **Add Communication Manager Server** Interface page. Use the descriptions associated with this page to fill in the following fields:
   - In the **Communication Manager Server Interface Name** field, enter the network node name for the server's interface.
   - In the **Host** field, select the IP address of the home server for whose users the server specified above is the default.
   - In the **SIP Trunk Link Type** field, select TLS to specify a secure transfer layer between the server and this host.
   - In the **SIP Trunk IP Address** field, enter the IP address for the C-LAN circuit pack or processor ethernet interface that terminates the SIP link from SES.

- In the **SIP Trunk Port** field, enter the same trunk port that is used to configure the signaling group on Communication Manager.

  In standalone installations, this value should be 5061.

  In co-resident installations, this value defaults to 6001. Verify that this field matches the 6001 value.
- For the **Communication Manager Server Admin Address** field, enter the IP address that allows SAT access to the server.
- For the **Communication Manager Server Admin Port** field, enter the port number of the server you are using to get dial plan and button download data from the server, which is used by SES to configure AST (SIP) phones.
- For the **Communication Manager Server Admin Login** field, enter the login used to access the server's administration service.
- For the **Communication Manager Server Admin Password** field, enter the password used to access the server's administration service, and then confirm your entry.
- For the **SMS Connection Type** field, select SSH for a secure connection.

3. Select **Add** to effect the changes.

After these associated screens are completed, **Setup** disappears from the left-hand menu of choices.

Adding trusted hosts

Use the SES Administration Interface for this procedure.

To add trusted hosts:

1. From the menu, select **Trusted Hosts** to display the Manage Trusted Hosts page.
2. Click **Add Trusted Hosts** to display the **Add Trusted Hosts** page. Fill in the following fields:
   - For the **IP address** field, enter the IP address of the server designated as the trusted host.
   - For the **Host** field, select the IP address of the home or edge server that accepts or rejects the SIP request from the IP address you specified.
   - To configure the host as Trusted Origination Host, select the **Perform Originating Processing** check box.
3. Select **Add** to effect the changes

Configuring SNMP

Use the SES Administration Interface for this procedure.

To configure SNMP:

1. From the menu, select **Server Configuration** to display the Server Configuration page.
2. Click **SNMP Configuration** to display the SNMP Configuration page.
3. Enter the name of the community string your site uses.
4. Select **Set** to effect the changes.

Configuring Communication Manager endpoints

Endpoints for Communication Manager include a variety of devices, terminals or stations, such as:

- Avaya SIP telephones (the 9600 phones and the 4600-series phones).
- Third-party SIP phones
- Wireless, digital, and analog endpoints
- Avaya Softphones:
  - Avaya one-X Deskphone Edition
  - SIP Softphone R2.1 or later
  - IP Softphone R5.1 or later with instant messaging

Before the installation is complete, you must administer Communication Manager running on an Avaya S8xxx Server. See *SIP Support in Avaya Aura® Communication Manager* (555-245-206). Use the administration tasks in the section titled Administering Communication Manager for SIP. These tasks include adding users of all SIP telephones and Avaya SIP Softphones, adding extensions for each SIP user, and updating proxy route patterns, as appropriate.

SIP-enabled stations, such as the Avaya one-X Deskphone Edition and the Avaya 4600-series telephones, must be administered in Communication Manager as Outboard Proxy SIP (OPS). See the *Avaya Aura® Communication Manager Feature Description and Implementation* guide (555-245-205), Extension to Cellular feature, and the *Administration Guide for Communication Manager* (03-300509), all Off-PBX administration screens.

Complete the following tasks

- Administer Avaya Communication Manager to work with SIP devices.

  The fields that differentiate SIP from non-SIP Communication Manager administration are detailed in the document *SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers* (555-245-206).

  The document includes entries for Signaling Group and Trunk Group setup that are specific to SIP. After you have completed setup in Communication Manager, you must save the translations to save the additions and changes you have made.

- Set up the telephones and endpoint devices.

  After setting up Avaya SIP Softphone users in Communication Manager as SIP Softphones, ensure each client PC has the proper release of Avaya Softphone software installed, licensed and configured to use SIP for Instant Messaging (IM). Refer to online help in the SIP Softphone application for more information, as well as the documentation or user assistance for each of the types of supported endpoints. You also may want to verify that softphones can register with the home or combined edge/home server and test that they can send and receive instant messages and update their contact lists.

- Check the endpoint devices.

  After administering SIP telephones in Communication Manager, make sure that each telephone has a version of firmware that can support SIP.

  The Avaya 4600-series SIP telephone requires that you enter a domain name on its SIP Settings page.

  You may wish to verify that you can make and receive test calls.

For application notes on which third-party SIP endpoints are supported, go to this web site:

http://www.avaya.com/gcm/master-usa/en-us/corporate/alliances/devconnect/index.htm and select **Application Notes** from the menu on the left.

Connection schema for duplicated servers

The following graphic shows the connection schema for an HP ProLiant DL360 G7 cable duplicated server pair.

Figure 4: Schema for HP ProLiant DL 360 G7 cable duplicated server

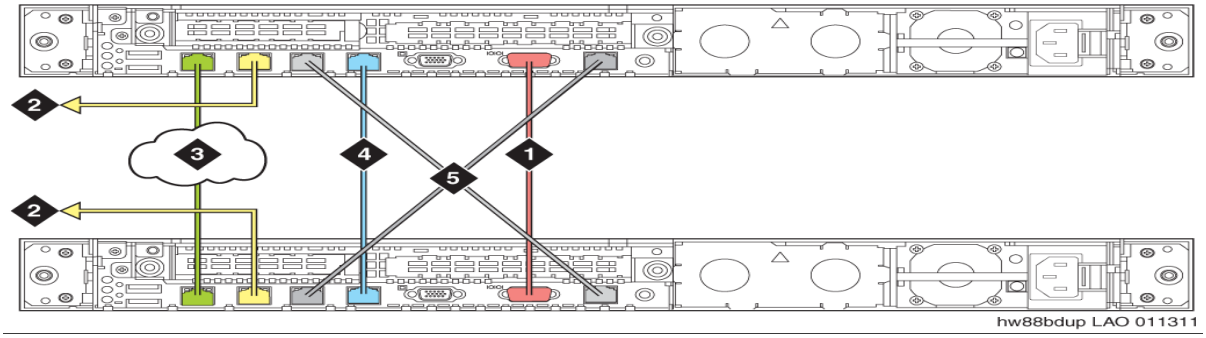


Figure notes:

1. **Null modem cable connecting the servers through RS-323 serial port.**
2. **Ethernet cable connecting the servers to the services port (Eth01)**
3. **Ethernet cable connecting the servers to the customer network through the customer network port (Eth0)**
4. **Ethernet cable connecting through the dual NIC port (Eth3)**
5. **The cable connects the ILO port of one server to NIC port 3 (eth2) of the other**

The following graphic shows the connection schema for an HP ProLiant DL 360 G7 network duplicated server.

Figure 5: Schema for HP ProLiant DL 360 G7 simplex and network duplicated server

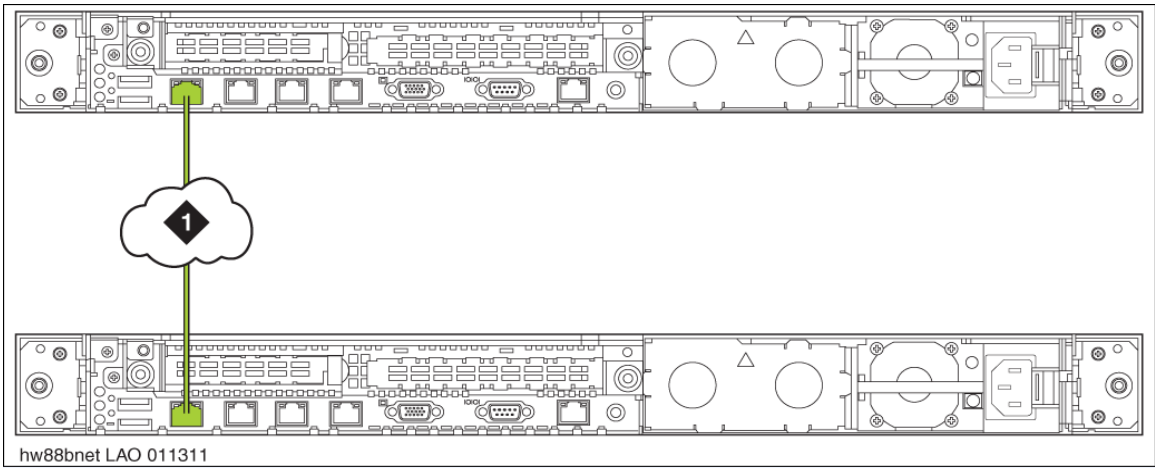


Figure notes:

1. **Straight through Ethernet cable connecting the servers to the customer network through the customer network port (Eth0)**

The following graphics show the connection schema for a S8800 cable duplicated and network duplicated server pair.

Figure 6: Schema for S8800 cable duplicated server

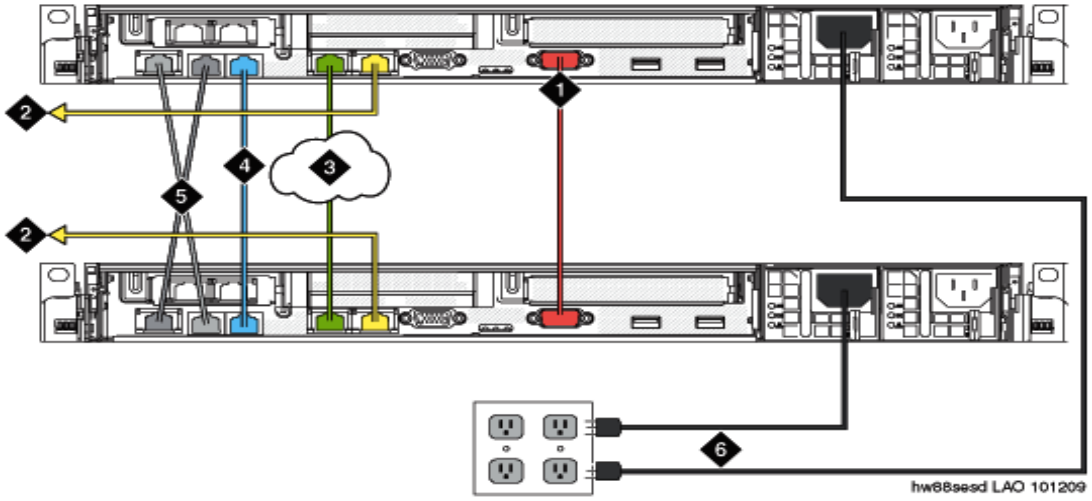


Figure notes:

1. **Null modem cable connecting the services through the RS-232 serial port.**
2. **Ethernet cable connecting LAN (Eth1).**
3. **Ethernet cable connecting the servers to the customer network through the customer network port (Eth0).**
4. **Ethernet cable connecting the servers through the dual NIC port.**
5. **The cable connects the IMM port of one server to Eth2 of the other.**
6. **Power cords of the servers connected to the electrical outlet.**

Figure 7: Schema for S8800 simplex and network duplicated server

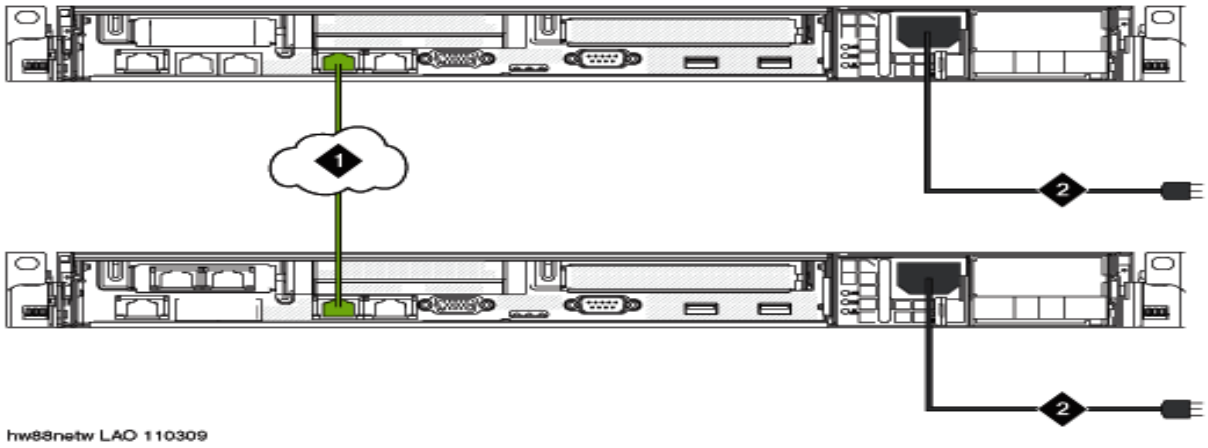


Figure notes:

1. **Straight-through Ethernet cable connecting the servers to the customer network through the customer network port (Eth0).**
2. **Power cords for servers connecting to electrical outlet.**

The following graphic shows the connection schema for S8510 cable duplicated and network duplicated server pair.

Figure 8: Schema for S8510 cable duplicated server

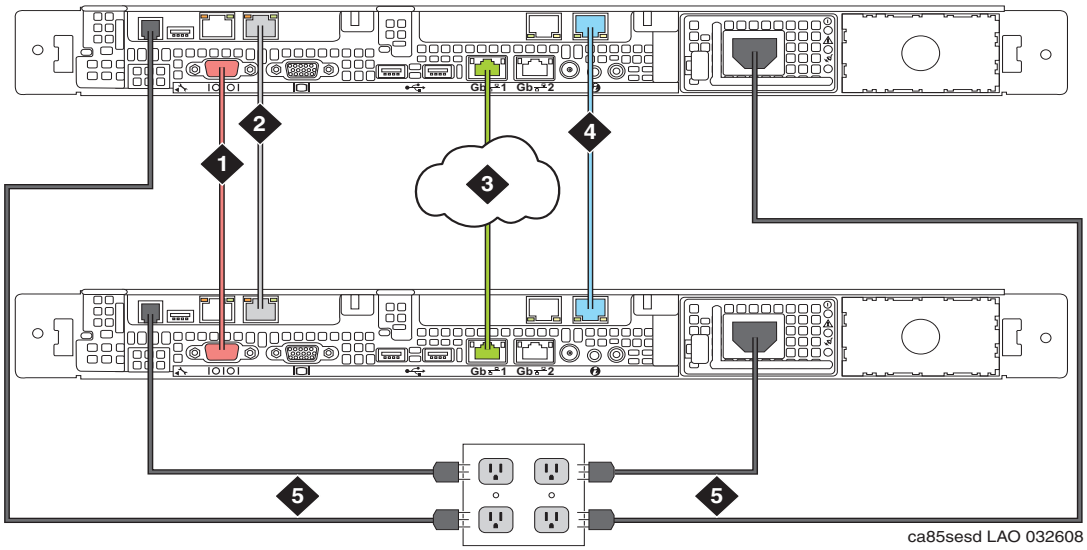


Figure notes:

1. **Null modem cable connecting the servers through the RS-232 serial port**
2. **Crossover ethernet cable connecting SAMPs through the SAMP Services port (Eth2)**
3. **Straight -through Ethernet cable connecting the servers to the customer network through customer port (Eth0)**
4. **Crossover ethernet cable connecting the servers through the dual NIC port (Eth3).**
5. **Power cords for servers and SAMP boards connecting to electrical outlet. The power cord of SAMP card should have an AC/DC adaptor between AC power outlet and the SAMP card RJ-11 jack.**

Note:

Avaya does not recommend connecting both S8510 servers and its SAMPs to the same AC power source for a cabled duplicated SES server, to prevent failures.

Figure 9: Schema for S8510 simplex and network duplicated server

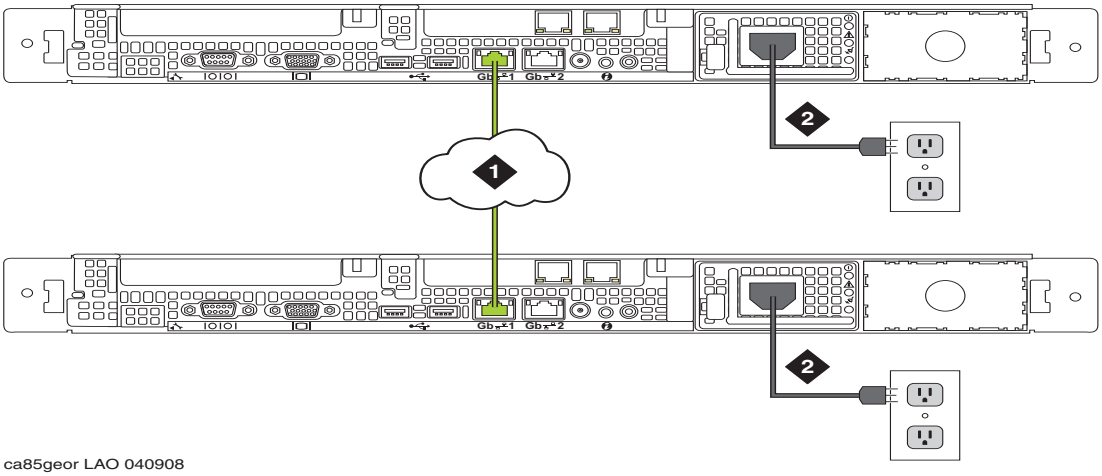


Figure notes:

1. **Straight-through Ethernet cable connecting the servers to the customer network through the customer network port (Eth0)**
2. **Power cords for servers connecting to electrical outlet**

Chapter 4: Upgrading SIP Enablement Services

This section guides you to upgrade an existing S8500-Series Server from Avaya SIP Enablement Services (SES) Release 3.x, 4.x, 5.0, 5.1 and 5.2 to Release 5.2.1. This chapter also guides you to upgrade a cable duplicated pair. The procedures for upgrades use the **Manage Software** link on the **System Management Interface (SMI)**.

Important:

The procedure for upgrading a cable duplicated pair of servers has changed from previous releases. Please follow the instruction in the Upgrading a Cable Duplicated Server Pair on page 82 section for the correct steps.

Important:

S8500A servers cannot upgrade to SES 5.x or later releases. You must migrate from the S8500A Server to an S8500B, S8500C, S8510, S8800 SESv2 Server or HP DL360 G7 server to run SES 5.x or later. SES 5.2.1 and SES S8800 or an HP DL360 G7 server are the only SES software and hardware currently sold by Avaya.

If you are an existing customer with S8500-based deployments of SIP Enablement Services 3.1.1 or later, you can directly upgrade to release 5.2. But if your software release is earlier than 3.1.1, you must upgrade to minimum release 3.1.1, before upgrading to SIP Enablement Services 5.2. You can download the SES 3.1.1 software from the Avaya SAFE download site.

Upgrading from release 5.2 to release 5.2.1 requires less time then upgrading from previous versions. You must upgrade SIP Enablement Services servers in an enterprise starting with the edge server. For release 5.2.1, home servers can be on either release 5.2 or release 5.2.1.

When upgrading from release 4.0 or earlier to release 5.2.1, a required update to the database and initial data replication must occur after the system reboot when the upgrade is complete. You can monitor the progress of these activities by using the **Status Summary** Web page or by a new command **`sds-monitor`**.

Important:

You must complete these activities before proceeding to upgrade the next SIP Enablement Services server in the enterprise.

When upgrading a duplicated SIP Enablement Services server pairs, these activities also must occur, when the first upgraded server in the pair becomes the primary server of the pair. Wait for these activities to be completed on the primary server before upgrading the backup server of the duplicated pair.

Important:

These activities are performed only once when upgrading a duplicated pair, so you do not have to monitor after the upgrade of the second server.

After you reboot the server successfully using the new release, use Status Summary or the "sds-monitor" command to monitor the progress and wait until initial replication is completed before proceeding to the next Home server. If the server is part of a duplex pair, the upgrade of the backup server in the duplex pair cannot be started until Status Summary or the "sds-monitor" command indicates that the initial replication is completed.

These activities are not required when upgrading from release 5.0 or later to release 5.2. However, it is recommended that you check the status of the "sds-monitor" before proceeding to upgrade the next server (if applicable).

After upgrading all home servers in the enterprise, backup the data on the edge 5.2.1 server.

The approximate time required for upgrading from release 5.2 or earlier to release 5.2.1 is as follows:

Server	**Time (R5.2 to R5.2.1**	**Time (R5.0 and R5.1 to R5.2)**	**Time (Pre-R5.0 to R5.2)**
Duplicated edge pair – 12K users	1.5 hours	1.5 hours	3 hours
Duplicated home pair – 4K users	1 hour	1 hour	2 hours (edge upgrade must be completed first)
Simple edge – 12K users	1 hour	1 hour	2.5 hours
Simple Home – 4K users	1 hour	1 hour	1.5 hours (edge upgrade must be completed first)
Duplicated edge or duplicated combined home/edge – 4K users	1.5 hours	1.5 hours	2 hours

Preupgrade tasks

Connecting to the server

Perform one of the following options:

- If you are on site, connect to the services port.
- If you are off site, use the IP address of the server to log on to the server.

Accessing the System Management Interface

To access the server:

1. Start the Web browser.
2. In the **Address** field, type `192.11.13.6` and press **Enter** to open the login Web page.
3. Log in as **craft**
4. Click **yes** to suppress alarms

   The system displays the **System Management Interface**.
5. Click the **Manage Software** link under the **Upgrade** menu to go to **Manage Software** web page.

To upgrade remotely:

1. Start the Web browser.
2. In the **Address** field, type the hostname or IP Address of the target SES server.
3. Select the required option in the **Manage Software** web page in the **System Management Interface** and load the software.
4. Follow the steps as required.

Copying files to the server

To copy files to the server:

Copy the following files, as appropriate, from the computer to the server:

- License file and Avaya Authentication file
- Postupgrade service pack files, if required

- Security update files (used post-upgrade, if required)

To copy files to the server:

1. On the Maintenance Web Interface, under Miscellaneous, click **Download Files**.
2. Select **File(s) to download from the machine used to connect to the server**.

   Note:

   Do not select the check box, “Install this file on the local server.”
3. Click **Browse** next to the top field to open the **Choose File** window on your computer. Find the files that you need to copy to the server.
4. Click **Download** to copy the files to the server.

   The system copies the files automatically to the default file location.
5. Repeat steps 1 through 4 for each server that will be upgraded.

Resolving alarms

To clear alarms:

1. On the Maintenance Web interface, under **Alarms**, click **Current Alarms** to examine the alarm log.
2. Select the server alarms that you want to clear and click **Clear**, or click **Clear All**.

Backing up recovery system files

To back up the system configuration files:

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Select the SES files. Do *not* select **Full Backup** because this option does not save data files.

   Note:

   If you back up to a flashcard, Avaya recommends that you use a different flashcard from the one with the prior release data files. You might need these data files if you need to back out of the upgrade procedure.
3. Select the backup method.
4. Click **Start Backup** to start the back up process.

Verifying the backup

To verify that the backup was successful:

1. Under **Data Backup/Restore**, click **Backup History**.
2. Select the backup that you want to verify, and click **Check Status**.

   The system displays the status of the backup.
3. Verify that **Backup Successful** appears for each data set in the backup.

Suppressing alarming

CAUTION:

Ensure that you suppress alarming during the upgrade. If you do not do so, the system can generate alarms, resulting in unnecessary trouble tickets.

To suppress alarming:

1. Access the command line interface of the server with telnet or an SSH client like PuTTY and an IP address of **192.11.13.6**.
2. Log in as **craft**.
3. Type **almsuppress -t *time*,** where ***time*** is the length of time that the alarms are suppressed up to 120 minutes (2 hours). Press **Enter** to suppress both dial-out and SNMP alarms.

   The system displays the following message:

   Alarm is suppressed. 120 minutes left.
4. Log off and close the dialog box.

Disabling the boot timeout of the SAMP board

Note:

You can also disable the boot timeout of the SAMP board by connecting to the SAMP services port and using the SAMP's Web pages. For more information, see "Disabling the boot timeout on Release 3.1 using the SAMP Web page" in the *Using the Avaya Server Availability Management Processor (SAMP),* 03-300322.

Note:

This process is applicable only to S8500 Series-Server.

To disable the boot timeout of the SAMP:

1. At the command line on the S8500 Server, enter **sampcmd**.

   The Welcome banner appears, followed by the SAMP command line.

2. At the SAMP command line, enter **serverctrl boot timer disable**.

   The system responds with **OK**.

3. At the SAMP command line, enter **serverctrl**.

   The system responds with the following output:

```
Power On
Server Operational
Reset Deasserted
Boot Time Disabled
```

4. Enter **Exit** to return to the server command line.

   When you have completed the upgrade and the server reboots, the SAMP boot timeout is automatically enabled again.

Upgrade tasks

Inserting the SES CD into the server

Insert the CD that contains SES into the CD-ROM drive on the server. Close the tray.

Note:

You can copy SES software from an http or tftp server onto the server. In this case, skip this step.

Upgrading SES

To start the upgrade:

1. Under **Upgrade**, select **Manage Software**.

Important:
If three releases already reside on the hard disk, you must delete one release to make room for the new release.

2. Perform one of the following tasks:

- If three releases already reside on the hard disk

1. Select **Delete one of the above releases from the local hard drive**. Click **Continue** to view the releases available.
2. Select the software release that you want to delete and click **Delete**.

   When complete, the system displays the following message:

   Deletion Complete
3. Click **Continue** to return to the initial **Manage Software** page.

- If less than 3 releases reside on the hard disk

1. Select one of the following:

- Copy a release to the local hard drive, but do not install it
- Copy from TFTP server at this IP address
- Copy from URL

and click **Continue** to view the options for copying the software to the hard drive.

2. Select **Copy from this server's CD-ROM drive:** and click **Continue**.
   The **Choose Software** page appears, which you use to copy files from the source you selected.
3. Select the release to be copied and click **Continue**.
   The system displays the **Copy in Progress** page.
4. View the progress screen as the software is copied to the hard drive.
   When complete, the system displays the following message:
   Success
5. Click **Continue** to return to the initial **Manage Software** page.

Installing a new release of SES from the local hard drive

If you selected **Install one of the following releases currently resident on the local hard drive** in the previous step, then follow these steps:

1. Select the software release you want, and click **Continue**.
2. If you have copied the license and authentication files to the server, select the following options:
   - If a super-user login already existed prior to the upgrade, select:

- I will supply the license files myself when prompted later in this process.
- Update authentication information as well as license information.

- If a super-user login did not exist prior to the upgrade, select:
  - I will supply the license files myself when prompted later in this process.
  - Do not update authentication information.

3. Click **Continue**.
4. For a new installation, or if you previously ran a backup, you do not need to run a backup at this time.
5. Click **Continue**.
   The system displays the **Review Notices** page.
6. Click **Continue**.

   The system displays the **Begin Installation** page. The page summarizes the request you have made.
7. Click **Continue**.

   The installation takes approximately 10 to 20 minutes.

   The system refreshes the **Install in Progress** window every 10 seconds or when you click **Refresh**. When complete, the system displays the **Reboot Server** page.

Rebooting the server

To reboot the server.

Note:

When you reboot the server, it can no longer communicate with the Web interface. The **Reboot in Progress** Web page displays during the reboot. Although the **Continue** button is visible, do not click **Continue** yet.

1. Click **Reboot**.

   The system displays the **Reboot in Progress** window. The tray of the CD-ROM drive opens automatically.
2. Remove the CD-ROM from the CD-ROM drive.

CAUTION:

If you do not remove the CD-ROM and the tray of the CD-ROM drive closes again, the system might try to reboot from the software on the CD-ROM.

Note:

The reboot takes approximately 3 minutes. The system does not automatically report when the reboot is complete.

3. Wait for 3 minutes and then click **Continue**.

   If you click **Continue** before the reboot is finished, the browser displays **Expired Page**. If you see the **Expired Page** message, refresh the browser. If the system displays **Page cannot be displayed**, use the browser Back button to return to the **Reboot in progress** screen. If the **Session Timeout** screen appears, close the screen, logoff, and log on again. Select **Manage Software**, select the option **Join this upgrade session in progress and monitor its activity**. Click **Pickup**.

   CAUTION:

   Do not click **Cancel** after this point. Be patient. If the installation fails, a message displays on the **Reboot in Progress** window.

   Note:

   This Web session will be interrupted by the reboot which occurs during the upgrade of the server. After the reboot, you can continue to use the **Manage Software** window without logging in.

4. When the reboot is complete, click **Continue**.

   The system displays the **Update Tripwire Database** Web page. If your planning documents instruct you to enable Tripwire, follow the instructions to reset the signature database.

   If your planning documents instruct you to enable Tripwire, follow the instructions to reset the signature database.
   You can also Verifying reboot progress at this stage.

5. Click **Continue**.

   The system displays the **Install License Files** Web page.

6. Click **Continue**.

   The system installs the license file and authentication file if you selected this action in step 5 on Rebooting the server.

   The system displays the **Installation Complete** screen.

7. Click **Close**.

   The **Manage Software** window closes and returns you to the main menu.

   Note:

   This Web session will be interrupted by the reboot that occurs during the server upgrade. After the reboot, the links in the main menu of the Web interface will not function. Therefore, you must close and reopen the Web browser to continue with the upgrade procedure.

8. Close the Web browser.
9. Reopen the Web browser and log in.
10. Use the **Status Summary** web page to monitor the progress and wait until initial replication is completed before proceeding to the next home server.

If the server is part of a duplicated pair, you cannot start the upgrade of the backup server in the duplicated pair until the **Status Summary** web page indicates that the initial replication is completed.

Note:

You do not have to perform these activities if you are upgrading from release 5.0 to release 5.2. However, it is recommended that you check the status before proceeding to upgrade the next server (if applicable).

Verifying reboot progress

To check the reboot process.

1. Click **Start > Run** to open the **Run** dialog box.
2. Type **command** and press **Enter** to open an MS-DOS window.
3. Type **arp -d 192.11.13.6** and press **Enter** to clear the ARP cache in the laptop. This command responds with one of the following responses:
   - The command line prompt when the cache is cleared.
   - The following message is when the specified IP address does not currently contain an entry in the ARP cache:

     The specified entry was not found.
4. Type **ping -t 192.11.13.6** to access the server. The **-t** causes the ping to repeat until you get a response. When you get a response, in about 3 minutes, wait an additional 30 seconds before you go back to the Web interface.
5. Type **ctrl c** to stop the ping.
6. Close the MS-DOS window.

Verifying software operation

To verify the software version.

1. Under Server, click **Software Version**.
2. Verify the details in the **Software Version** web page to ensure that the new software is present.

Checking system status

To check the system status:

1. Under **Server**, click **Status Summary** to verify that the server mode is active.
2. Click **Process Status**.
3. Select **Summary** and **Display once**. Click **View** to access the View Process Status Results screen.
4. Verify that all the processes are **UP**.

Making the upgrade permanent on the server

CAUTION:

You must make the upgrade permanent. Otherwise, the next time when you reboot the server, the server might run the previous version of the software. You might lose any new translations you might have made, and you must install the new software again. If you do not make the upgrade permanent within 2 hours of the upgrade, an alarm is raised.

To make the upgrade permanent.

1. Under **Server Upgrades**, click **Make Upgrade Permanent**.
2. Click **Submit** to make the partition with the new software version the permanent partition.
3. Under Server Upgrades, click **Boot Partition** to confirm that the new software release is selected for the boot partition and the active partition.

Downloading security and SES service packs, if any

1. Go to http://support.avaya.com and click **Downloads**
2. Select **Avaya Aura SIP Enablement Services**
3. Click **Avaya Aura SIP Enablement Services 5.2.1 Service Pack** or click **Avaya Aura® Communication Manager 5.2.1 / SIP Enablement Services 5.2.1 Security Service Pack 1** to download security pack and follow the instructions on screen.

Installing security and SES service packs

1. Under Server Upgrades, select **Manage Updates**.
2. If an update file you want to activate shows **packed** in the **Status** column, select update ID and click **Unpack**.
3. The window shows the status of the update.
4. Wait until the system displays the message **Finished unpacking...**and click **Continue**.
5. The system displays the **Manage Updates** screen.
6. If the update ID you want to activate shows **unpacked** in the **Status** column, select the update ID and click **Activate**.
7. The window shows the status of activating the update. If a reboot is required, the system automatically reboots.
8. Click **Yes**.

Wait until the system displays the Continue button.

9. Click **Continue**.

Installing the authentication file

To install the authentication file on the server:

1. Under Security, click **License File**.
2. Select **Install the license I previously downloaded** and click **Submit** to install the license file.
3. Under Security, click **Authentication File**.
4. Click **Install the Authentication file I previously downloaded** and click **Install**.

Upgrading a Cable Duplicated Server Pair

A redundant pair consists of a primary server and a backup server. In the following steps, it is assumed that Server A is the primary server and Server B is the backup server.

1. Run the CLI Command **`out-of-service`** on server B. Do not use the **Busy-out Server** web page of the **System Management Interface**.
2. Wait for one minute and then run the CLI command **`out-of-service`** on Server A. Do not use the **Busy-Out Server** Web page of the **System Management Interface**.

3. Upgrade both Server A and Server B in the redundant pair using the software upgrade process. Start by upgrading Server B first, and then upgrade Server A.
4. Reboot each server when the system displays the reboot instruction.

   Note:

   If `session has expired` message appears, close all browser windows, start a new browser session with the server. Select `Join the existing upgrade` option in the **Manage Software** web page to complete the upgrade.
5. After completing the upgrades, ensure to perform the **Make Upgrade Permanent** step on both the servers.
6. Run the CLI command **`in-service`** on server A.

   Note:

   If SAMP cards (S85xx servers) or BMC modules (S8800 and HP DL360 G7servers) are interconnected, it will cause server B to reboot. Wait for the rebooting to be complete.
7. Wait for 5 minutes and then run the CLI command **`in-service`** on Server B.

   Note:

   Avaya recommends the wait time, as there could be a full replication of the database partition from Server A to Server B in progress in the background. You cannot place Server B into service until the replication is completed.
8. Confirm that both servers are in-service and that Server A is the primary server and Server B is the backup server, using the **Status Summary** Web page.
9. If Server A is either a home server or a combined home/edge server, then make a test call to verify that Server A is working properly. If Server A is an edge server, access master admin to verify operation.

   Note:

   When upgrading a cable duplicated server pair to Release 5.2.1, there will be a downtime in the availability of the system, as both servers will be out of service simultaneously.

Upgrading a Network Duplicated Server Pair

A redundant pair consists of a primary server and a backup server. In the following steps, it is assumed that Server A is the primary server and Server B is the backup server.

1. **`Busy-out Server`** B, so it is out of service.
2. Upgrade Server B using the software upgrade process.
3. Reboot the server when the system displays the reboot instruction.
4. After completing the upgrades, make sure to perform the **Make Upgrade Permanent** step.

5. (Optional) Apply service packs to Server B, if applicable.
6. Release Server B, so it is back in service.
7. Confirm that Server B is in-service and that it is the backup server, using the **Status Summary** web page.
8. Perform an interchange between the servers.
9. Confirm that both servers are in-service and that Server A is the backup server and Server B is the primary server, using the **Status Summary** Web page.
10. Repeat steps 1 to 7 for Server A.

Post-Upgrade tasks

Resolving alarms

1. To clear alarms:
2. On the Maintenance Web interface, under **Alarms**, click **Current Alarms** to examine the alarm log.
3. Select the server alarms that you want to clear and click **Clear**, or click **Clear All**.

Backing up recovery system files

1. Under **Data Backup/Restore**, click **Backup Now**.
2. Select the required data sets.

   Do *not* select **Full Backup** because this option does not save data files.
3. Select the backup method.
4. Click **Start Backup** to start the backup process.
5. Click **Check Status** to observe the status of the backup.

Releasing alarm suppression (optional)

If you complete the upgrade well before the time set when you suppressed alarming, you might want to release alarm suppression manually rather than wait for the system to release alarm suppression.

To release alarm suppression:

1. Access the command line interface of the server with an SSH client like PuTTY and an IP address of **192.11.13.6**.
2. Log in as **craft**.
3. Type **almsuppress -s n** and press **Enter** to release alarm suppression.
4. Log off.

Logging off all administration applications

When you complete all the administration, log off all the applications that you used.

Chapter 5: Migrations to new servers

This section describes the migration paths supported in Release 5.2.1 of SIP Enablement Services.

- S8800 Server to HP DL360 G7 server in a single and duplcated edge, home, or combined edge/home configuration
- S8500 Server to S8800 Server or HP DL360 G7 server in a single and duplcated edge, home, or combined edge/home configuration
- S8510 Server to S8800 Server or HP DL360 G7 server in a single and duplicated edge, home, or combined edge/home configuration
- S8500 Server to S8510 Server in a single and duplicated edge, home, or combined edge/home configuration
- S8500 Server in a single combined edge/home configuration only to S8300C Server in a single combined edge/home configuration
- S8300C/D Servers with Communication Manager/SES coresident in a combined edge/home or home configuration to S8800 Server in a single combined edge/home or home configuration. Migration to an edge configuration is not supported.
- S8500 Server in a single edge, home, or combined edge/home configuration to either cabled (collocated) or network (separated) duplicated edge, home, or combined edge/home configuration.
- S8500 Server in a combined edge/home configuration to an edge server and adding a new S8500-Series Server in a home configuration.
- cabled duplex (collocated) servers to network duplex (separated) servers.

Most of these migrations require installing and configuring one or more new servers. See Installing SES on the server on page 39 for information on installing and configuring SES on a new server.

Most of them also require a new or updated license file. Adding a new server requires an updated license. An additional license is required when going from a single server to duplicated servers or going from a cabled duplex configuration to a network duplex configuration. No new license is required when going from a single server to a cabled duplex configuration.

All of the migrations cause an interruption in service.

Prerequisites

Before you start the migration, verify that:

- Have all the hardware and cables if installing a new server.
- You have the IP addresses and the unique names for the server(s). You can gather this information from the existing server(s) or fill out the Installation Worksheet; a blank worksheet is in Appendix A.
- You have a new license file and a password file.

Best practices

It is best practice to backup all the files before starting the migration. When attempting a full restore or an OS dataset restore, you must ensure to restore only to a server with the same hostname as the server where the backup was created.

The migration scenarios that are supported are shown in Migration paths on page.

Table 2: Migration paths

	Migrate to:					
Migrate from:	***S8300C/ S8300D***	***S8500B***	***S8500C***	***S8510***	***S8800***	***HP DL360 G7***
S8800 single or duplicated edge	NA	NA	NA	NA	NA	single or duplicated edge
S8500A single or duplicated edge	NA	single or duplicated edge	single or duplicated edge	single or duplicated edge	single or duplicated edge	single or duplicated edge
S8500A single or duplicated home	single home	single or duplicated home	single or duplicated home	single or duplicated home	single or duplicated edge	single or duplicated edge
S8500A single or duplicated combined edge/ home	single combined edge/ home	single or duplicated combined edge/home	single or duplicated combined edge/home	single or duplicated combined edge/home	single or duplicated edge	single or duplicated edge
S8500B single or duplicated edge	NA	NA	single or duplicated edge	single or duplicated edge	single or duplicated edge	single or duplicated edge
S8500B single or duplicated home	single home	NA	single or duplicated home	single or duplicated home	single or duplicated edge	single or duplicated edge

Table 2: Migration paths

S8500B single or duplicated combined edge/ home	single combine d edge/ home	NA	single or duplicated combined edge/home	single or duplicated combined edge/home	single or duplicated edge	single or duplicated edge
S8500C single or duplicated edge	NA	NA	NA	single or duplicated edge	single or duplicated edge	single or duplicated edge
S8500C single or duplicated home	single home	NA	NA	single or duplicated home	single or duplicated edge	single or duplicated edge
S8500C single or duplicated combined edge/ home	single combine d edge/ home	NA	NA	single or duplicated combined edge/home	single or duplicated edge	single or duplicated edge
S8300C with Communication Manager/SES co-resident combined edge/ home	NA	single combined edge/home	single combined edge/home	single combined edge/home	single combined edge/ home	NA
S8300C with Communication Manager/SES co-resident home	NA	single home	single home	single home	single home	NA

Premigration tasks

Each migration path has standard tasks that you do before starting the migration. These include noting the configuration information on the existing server and backing up the files.

Configuration information

Note:

When migrating, you cannot use **View/Restore Data** to restore the server and system files, security files, or all data sets. All configuration data must be obtained from the existing server and recorded for later use.

The configuration information found in the **System Management Interface** on the old server is used to configure the new server. You cannot complete the migration without this information.

You can manually copy the information in each screen (not recommended), copy and save each screen to your computer, or print each screen.

Copying the configuration screens

Use the following steps to copy each configuration screen. Each screen can be stored as a separate file on your computer.

1. Create a new folder on your computer to store the configuration files that you copy. Storing the files in a new folder makes them easier to find.
2. Copy the screens to Word, Wordpad, or Paint. Decide which application you are going to use and open it on your computer.
3. When the configuration screen is displayed on your computer, press **Alt** + **PrintScrn** on your keyboard. The captured screen is copied into the Windows clipboard.
4. Within the application to which you are copying the screens:
   a. Right click on your mouse and select **Paste**. The configuration screen appears in your application.
   b. Click **File** and select **Save As**. Select the folder you created in step 1. In the **File Name** field, change the name of the file to match the configuration screen that you copied. Click **Save**.

   You can also copy all the screens into one file.

Viewing the configuration screens to copy or print

Use the **System Management Interface** for these procedures.

1. Under **Server Configuration**, click **Configure Server**.
2. Print or copy the information from the following screens:
   - **Set Static Routes**
   - **Configure Time Server**
   - Set Modem Interface
   - **Configure RMB**: You use the SAMP settings when you configure the RMB on the S8510 Server.
3. After copying or printing the Configure Server screens, click **Cancel**. ***Do not*** click **Submit**.
4. Under **Alarms** click SNMP Traps and look for data. If the screen is administered, copy the information or print it.

Note:

The SNMPV3 authentication password and privacy password does not display on the screen.

Backing up files

Use the **System Management Interface** for this procedure.

To back up the files:

1. Connect your backup location to the server.

   Note:

   Backup location can be a locally attached USB compact flash device, or a network location using SFTP, SCP, or FTP.

2. Under **Data Backup/Restore**, click **Backup Now**.
3. Under **Data Sets**, select one of the following options:

   SES Files if not remastering the hard drive. Do not select any other data sets.

   All Data Sets if remastering the hard drive.
4. Under **Backup Method**, select your backup location.
5. Click **Start Backup** to start the backup process.
6. Under **Data Backup/Restore** click **Backup History** to view the progress of the backup process.
7. When the backup is finished, disconnect the backup location from the server.

S8500-Series Server to S8800 Server or HP DL360 G7 Server

This section addresses migrating an S8500 Server and S8510 Server to an S8800 Server or HP DL360 G7 Server. The migration also requires migrating like to like, meaning if the existing server is an edge configuration, then the new server is also an edge configuration.

Migrating an existing server to an S8800 or an HP Server requires:

- Physically installing the new server
- Installing the SES software on the server
- Configuring SES on the server
- Reinstalling the user database on the new server.

If migrating to an S8800 or HP server and the servers are duplicated, both servers must be migrated to S8800 Servers.

For information on physically installing the server in a rack, see *Installing the Avaya S8800 Server for Avaya Aura® SIP Enablement Services* (03-603447). For information on physically installing the server in a rack, see *Installing the HP ProLiant DL360 G7 for Avaya Aura® SIP Enablement Services* (03-603799).

Installing SES on the server on page for information on installing and configuring the new server.

Premigration tasks

Before starting the migration, you must

- Note the configuration information on the existing server. See
  - Configuration information on page 89
  - Copying the configuration screens on page 90
  - Viewing the configuration screens to copy or print on page 90.
- Back up the SES files only. See Backing up files on page 91

Install the server in the rack

To physically install the S8800 Server, see *Installing the Avaya S8800 Server for Avaya Aura® SIP Enablement Services* (03-603447). To physically install the HP Server, see *Installing the HP ProLiant DL360 G7 for Avaya Aura® SIP Enablement Services* (03-603799).

Installing SES

You need to do all the tasks through Installing SIP Enablement Services because you are installing a new server. You also need an updated license file.

Configuring SES (initial_setup)

If migrating a single server, configure SES on the new server as a single server. If converting a single server to a duplicated server, configure the SES on the new server as either a cable or network duplex server, depending on the configuration.

Restoring SES files

Use the **System Management Interface** for this procedure.

To restore the files:

1. Connect the drive to the backup location with the SES files.

   Note:

   A backup location can be a locally attached USB compact flash device or a network location using SFTP, SCP, or FTP.

2. On the main menu, under **Data Backup/Restore** click **View/Restore Data**.
3. Under **View current backup contents in**, select your backup location.
4. Click **View** to access the second page.
5. Under Data Sets, select **SES Files**.
6. Click **Restore** to restore the files to the new server. The following message appears:

   Restoring . . . The restore has started. From the main menu, click Restore Status. For complete restore status, click Check Status.

When the restore is finished, disconnect the backup location from the server.

Verifying service

Make a test call on a SIP phone to verify that you have service and that the migration was successful.

Shutting down S8500-Series Server

To shut down the S8500-Series Server:

CAUTION:
Do not unplug a functioning server unless you first stop all processes. If you unplug a functioning server but do not stop all processes first, you can corrupt the hard disk drive.

1. Under Server, click **Shutdown Server**.
2. Select **Delayed shutdown.**
3. Deselect **Restart server after shutdown**.
4. Click **Shutdown**.
5. Wait about 30 seconds.

CAUTION:
Do not press the power button for more than a second. If you hold it down too long, the server reboots.

6. Press and release the power-control button on the front of the server.

   The internal fan shuts off.

Disconnecting the cables from the old server

Label and disconnect the following cables from the back of the S8500-Series Server.

- The laptop from the Services port.
- The power cord from server.
- The power cord from the SAMP or RSA board.
- The modem from the RS-232 or USB port on the SAMP or RSA board.
- The CAT 5 cable(s) from the Ethernet port on the server.
- If duplicated, the CAT 5 cables from the Ethernet port on the SAMP or RSA board and the dual NIC.

If duplicated, the null modem cable from the RS-232 port.

Connecting the cables to the new server

Connect the following cables to the back of the S8800 Server.

- The power cord to the server.
- The CAT 5 cable(s) to the Ethernet port on the server.
- If duplicated, the CAT 5 cables to the Ethernet port and the dual NIC.
- If duplicated, the null modem cable to the RS-232 port on the server.

Removing the S8500- Series Server from the rack

Use the *Installing the Avaya S8800 Server for Avaya Aura® SIP Enablement Services* (03-603447) as a reference.

1. Slide the S8500 or S8510 Server from the rack.
2. Remove the side rails from the rack.

S8500 Server to S8300C/D Server with Communication Manager/SES coresident

The only supported configuration for this migration path is single combination edge/home only. The S8300 Server must run Communication Manager Release 5.0 or higher to be able to enable SES.

Important:
Because SES on the S8300C/D Server handles fewer users than SES on an S8500 Server, do not migrate if the number of users exceeds the capacity on the S8300C/D Server.

Migrating an existing Avaya S8500 Server to an Avaya S8300 Server requires either

- Enabling SES on an existing S8300 Server with Communication Manager, Release 5.0 or higher.
- Physically installing a new S8300 Server in an existing media gateway.
- Physically installing a new media gateway, installing Communication Manager on it, enabling and configuring SES, and reinstalling the user database on the S8300 Server.

The S8300 Server can only be configured as a combination single edge/home only.

Follow the instructions in the *Installing and Upgrading the Avaya S8300 Server with the Avaya G700 Media Gateway* (555-234-100) to install and configure the new S8300 Server.

Premigration tasks

Before starting the migration, you must

- Note the configuration information on the existing server. See
  - Configuration information on page
  - Copying the configuration screens on page
  - Viewing the configuration screens to copy or print on page.
- Back up the SES files only. See Backing up files on page

Installing the S8300 Server

If an S8300 Server exists with Communication Manager, Release 5.0 or higher, go to Enabling SES on S8300.

To physically install an S8300 Server in an existing H.232 media gateway (G250, G350, G450, or G700), use one of the following books:

- *Quick Start for Hardware Installation: Avaya G250 Media Gateway* (03-300433)
- *Quick Start for Hardware Installation: Avaya G350 Media Gateway* (03-300148)
- *Quick Start for Hardware Installation: Avaya G450 Media Gateway* (03-602053)
- *Quick Start for Hardware Installation: Avaya G700 Media Gateway* (555-233-150)

To install Communication Manager and configure the S8300, use the *Installing and Upgrading the Avaya S8300 Server with the Avaya G700 Media Gateway* (555-234-100).

Enabling SES on S8300

Use the **System Management Interface** for these procedures.

To enable SES

1. Under Miscellaneous, click **SES Software**.
2. Click **Enable SES**.
3. Wait about 30 seconds then click the refresh button on your browser.

   The SES Software page shows **SES is enabled**.
4. To verify that SES is enabled, return to the Standard Management Solutions page, and refresh your browser.
5. Verify that the **Launch SES Administration Interface** option is now available.

Restoring SES files

Use the **System Management Interface** for this procedure.

To restore the files:

1. Connect the drive to the backup location with the SES files.

   Note:

   A backup location can be a locally attached USB compact flash device or a network location using SFTP, SCP, or FTP.
2. On the main menu, under **Data Backup/Restore** click **View/Restore Data**.
3. Under **View current backup contents in**, select your backup location.
4. Click **View** to access the second page.
5. Under Data Sets, select **SES Files**.

6. Click **Restore** to restore the files to the new server. The following message appears:

   Restoring . . . The restore has started. From the main menu, click Restore Status. For complete restore status, click Check Status.

When the restore is finished, disconnect the backup location from the server.

Administering Communication Manager

Because SES and Communication Manager are co-resident on the S8300C/D Server, the S8300C/D served as the Communication Manager server.

Use the SAT command line interface on the server running Communication Manager for these procedures.

You need to retranslate some of the SAT screens on the server running Communication Manager. See *SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers* (555-245-206) for information on which SAT screens to modify.

Verifying service

Make a test call on a SIP phone to verify that you have service and that the migration was successful.

Shutting down the S8500 Server

To shut down the S8500 Server:

CAUTION:

Do not unplug a functioning server unless you first stop all processes. If you unplug a functioning server but do not stop all processes first, you can corrupt the hard disk drive.

1. Under Server, click **Shutdown Server**.
2. Select **Delayed shutdown**
3. Deselect **Restart server after shutdown**.
4. Click **Shutdown**.
5. Wait about 30 seconds.

CAUTION:

Do not press the power button for more than a second. If you hold it down too long, the server reboots.

6. Press and release the power-control button on the front of the server.

   The internal fan shuts off.

Disconnecting the cables

Label and disconnect the following cables from the back of the S8500 Server.

- The laptop from the Services port.
- The power cord from server.
- The power cord from the SAMP or RSA board.
- The modem from the RS-232 or USB port on the SAMP or RSA board.
- The CAT 5 cable(s) from the Ethernet port on the server.
- If duplicated, the CAT 5 cables from the Ethernet port on the SAMP or RSA board and the dual NIC.
- If duplicated, the null modem cable from the RS-232 port.

Removing the S8500 from the rack

Use the *Quick Start for Hardware Installation: Avaya S8500 Server* (555-245-701) as a reference.

1. Slide the S8500 Server from the rack.
2. Remove the side rails from the rack.

S8300 Server with Communication Manager/SES coresident to S8800 Server or HP ProLiant DL360 G7 Server

Migrating an existing S8300 Server with Communication Manager/SES coresident to an S8800 Server or the HP Server requires:

- Physically installing a new Avaya S8880 Server
- Installing the SES software on the server
- Configuring SES on the server
- Restoring the SES files on the new server.

The S8800 Server can be configured as either a home or a combination edge/home server in either a single or duplicated configuration. It cannot be configured as a distributed edge.

Follow the instructions in Installing SES on the server on page 39 to install and configure the new server.

Premigration tasks

Before starting the migration, you must

- Note the configuration information on the existing server. See
  - Configuration information on page
  - Copying the configuration screens on page
  - Viewing the configuration screens to copy or print on page.
- Back up the SES files only. See Backing up files on page

Installing the S8800 or HP DL 360 G7Server in the rack

To physically install the S8800 Server, see *Installing the Avaya S8800 Server for Avaya Aura® SIP Enablement Services* (03-603447). To physically install the HP Server, see *Installing the HP ProLiant 360 G7 Server for Avaya Aura® SIP Enablement Services (03-603799)*

Installing SES

You need to do all the tasks through Installing SIP Enablement Services because you are installing a new server. You also need an updated license file.

Configuring SES (initial_setup)

If migrating a single server, configure SES on the new server as a single server. If converting a single server to a duplicated server, configure the SES on the new server as either a cable or network duplex server, depending on the configuration.

Restoring SES files

Use the **System Management Interface** for this procedure.

To restore the files:

1. Connect the drive to the backup location with the SES files.

   Note:

   A backup location can be a locally attached USB compact flash device or a network location using SFTP, SCP, or FTP.

2. On the main menu, under **Data Backup/Restore** click **View/Restore Data**.
3. Under **View current backup contents in**, select your backup location.
4. Click **View** to access the second page.
5. Under Data Sets, select **SES Files**.
6. Click **Restore** to restore the files to the new server. The following message appears:

   Restoring . . . The restore has started. From the main menu, click Restore Status. For complete restore status, click Check Status.

When the restore is finished, disconnect the backup location from the server.

Disabling SES on S8300

Use the **System Management Interface** for these procedures.

To disable SES:

1. Under Miscellaneous, click **SES Software**.

2. Click **Disable SES**.
3. Wait about 30 seconds then click the refresh button on your browser.

   The SES Software page shows **SES is disabled**.
4. To verify that SES is disabled, return to the Standard Management Solutions page, and refresh your browser.
5. Verify that the **Launch SES Administration Interface** option no longer shows.

Administering SES on the S8800 Server and HP ProLiant DL360 G7 Server

You must administer SES on the new S8800 Server and HP DL360 G7 Server. See particularly

- Administering setup on page 59
- Setting up servers on page 61

Administering Communication Manager

Because SES and Communication Manager are co-resident on the S8300C/D Server, the S8300C/D serves as the Communication Manager server.

Use the SAT command line interface on the server running Communication Manager for these procedures.

You need to retranslate some of the SAT screens on the server running Communication Manager. See *SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers* (555-245-206) for information on which SAT screens to modify.

Verifying service

Make a test call on a SIP phone to verify that you have service and that the migration was successful.

S8500 Server single to duplicated configuration

To add redundancy to an SES system, a customer must add a second server. The redundant pairs can be either cabled duplication or network duplication.

Migrating an existing S8500 Server in a single configuration to a duplicated configuration requires

- Copying the configuration screens
- Backing up the SES files
- Remastering the existing S8500 Server to SES Release 5.2 and configuring it as a duplicated server
- Physically installing a second Avaya S8500 Server
- Installing the SES Release 5.2 software on the new server and configuring it as a duplicated server
- Restoring the SES files on the primary server.

If migrating to an S8800 or an HP Server, then the existing S8500 Server must also be migrated to an S8800 Server. You cannot pair an S8500 Server with an S8800 or an HP Server.

Premigration tasks

Before starting the migration, you must

- Note the configuration information on the existing server. See
  - Configuration information on page
  - Copying the configuration screens on page
  - Viewing the configuration screens to copy or print on page.
- Back up the SES files only. See Backing up files on page

Install a second server in the rack

If the servers are to be cable duplicated (collocated), then install the second server in the same rack as the existing server or in a rack close by so that the cables can reach it. If the servers are to be network duplex (separated), one server in another building, then install the server in a rack in another location. Both servers can be either in a LAN or WAN environment but must be within the same subnet.

Important:

You can pair an S8500 Server with an existing S8500B or S8500C Server; however, you cannot pair an S8510 Server with an existing S8500B or S8500C Server. If using an S8510 Server, then both servers must be S8510 Servers. See S8500 Server to S8300C/D Server with Communication Manager/SES coresident for information on migrating an S8500 Server to an S8510 Server.

To install the S8500 Server, see *Quick Start for Hardware Installation: Avaya S8500 Server (555-245-701)*

To install the S8510 Server, see *Installing the Avaya S8510 Server Family and Its Components* (03-602918).

Note:

Do not apply power to the server in this step.

Connection schema for duplicated servers

Before beginning the installation procedure, check all connections and ensure that the physical connections are correct. See Connection schema for duplicated servers on page for the two duplicated connection schemas.

Installing SES

You need to do all the tasks through Installing SIP Enablement Services because you are installing a new server.

If cabled duplication, you do not need a new license. If network duplication, you need an additional license for the second server.

Configuring SES (initial_setup)

If migrating a single server, configure SES on the new server as a single server. If converting a single server to a duplicated server, configure the SES on the new server as either a cable or network duplex server, depending on the configuration.

Select either cabled duplex or network duplex, depending on the configuration. Use the IP address for the existing server as the virtual address for the duplicated pair.

Restoring SES files

Use the **System Management Interface** for this procedure.

To restore the files:

1. Connect the drive to the backup location with the SES files.

   Note:

   A backup location can be a locally attached USB compact flash device or a network location using SFTP, SCP, or FTP.

2. On the main menu, under **Data Backup/Restore** click **View/Restore Data**.
3. Under **View current backup contents in**, select your backup location.
4. Click **View** to access the second page.
5. Under Data Sets, select **SES Files**.
6. Click **Restore** to restore the files to the new server. The following message appears:

   Restoring . . . The restore has started. From the main menu, click Restore Status. For complete restore status, click Check Status.

When the restore is finished, disconnect the backup location from the server.

Shutting down the S8500 Server

To shut down the S8500 Server:

CAUTION:

Do not unplug a functioning server unless you first stop all processes. If you unplug a functioning server but do not stop all processes first, you can corrupt the hard disk drive.

1. Under Server, click **Shutdown Server**.
2. Select **Delayed shutdown**
3. Deselect **Restart server after shutdown**.
4. Click **Shutdown**.
5. Wait about 30 seconds.

CAUTION:

Do not press the power button for more than a second. If you hold it down too long, the server reboots.

6. Press and release the power-control button on the front of the server.

   The internal fan shuts off.

Installing SES

Important:

When installing the software, choose the remaster option on the first screen. This wipes out all the data on the hard drive before reinstalling the software.

You need to do all the tasks through Installing SIP Enablement Services because you are installing a new server.

If cabled duplication, you do not need a new license. If network duplication, you need an additional license for the second server.

Configuring SES (initial_setup)

Note:

The physical IP address of the existing server *must* be the logical IP address. If not, the entire database becomes corrupt and unusable.

If migrating a single server, configure SES on the new server as a single server. If converting a single server to a duplicated server, configure the SES on the new server as either a cable or network duplex server, depending on the configuration.

Select either cabled duplex or network duplex, depending on the configuration. Use the IP address for the existing server as the virtual address for the duplicated pair.

Verifying service

Make a test call on a SIP phone to verify that you have service and that the migration was successful.

Converting a combination edge/home to an edge

You can convert an existing combination edge/home server to a edge server, but you then must install a second server to act as the home server. The existing combination edge/home server

must be upgraded to Release 5.2 of SIP Enablement Services before the conversion. See the chapter on SES Upgrades for the upgrade procedure.

Converting a combination edge/home server to an edge server requires

- Upgrading the server to SES Release 5.2
- Copying the configuration screens
- Backing up the SES files
- Reconfiguring the existing S8500 Server to be an edge server.
- Physically installing a second S8500-Series Server to be the home server. You cannont use an S8300 Server as a home server.
- Installing SES Release 5.0 or higher on the new second server and configuring it as a home.
- Stop services on the existing and new server
- Administer SES to migrate
- Administer Communication Manager
- Start services on new server(s)
- Change the PPM address on all the supported SIP endpoints

If the combo is duplicated, you must add additional servers to act as the duplicated edge or home.

Premigration tasks

Before starting the migration, you must

- Note the configuration information on the existing server. See
  - Configuration information on page
  - Copying the configuration screens on page
  - Viewing the configuration screens to copy or print on page.
- Back up the complete data set. See Backing up files on page

Install a second server in the rack

If the servers are to be cable duplicated (collocated), then install the second server in the same rack as the existing server or in a rack close by so that the cables can reach it. If the servers are to be network duplex (separated), one server in another building, then install the server in a rack in another location. Both servers can be either in a LAN or WAN but must be within the same

subnet. If one of the servers is installed across a WAN connection, note the following additional details:

- Network Duplication over WAN requires guaranteed bandwidth and reliable WAN service for SIP signaling. It requires service level agreements with the customer to ensure a reliable WAN environment.
- Bandwidth: Minimum of 100 MB for data replication traffic. Event states are not replicated as they change frequently.
- Packet loss: Must not be greater than 3%.
- Jitter: Average one-way jitter must be less than 30 milliseconds.
- Delay: One-way delay must be no more than 150 milliseconds.
- QOS policy parameters appropriate for SIP signaling is required. DSCP36 (Assured Forwarding 42) is recommended. Other DSCP values can be assigned but must guarantee bandwidth to minimize packet loss.

Important:

An S8500 Server can be duplicated with an existing S8500B or S8500C Server; however, an S8510 Server cannot be duplicated with an existing S8500B or S8500C Server. If using an S8510 Server, then both servers must be S8510 Servers. See S8500 Server to S8300C/D Server with Communication Manager/ SES coresident for information on migrating an S8500 Server to an S8510 Server.

To install the S8500 Server, see *Quick Start for Hardware Installation: Avaya S8500 Server (555-245-701)*

To install the S8510 Server, see *Installing the Avaya S8510 Server Family and Its Components* (03-602918).

Note:

Do not apply power to the server in this step.

Installing SES

You need to do all the tasks through Installing SIP Enablement Services because you are installing a new server. You also need an updated license file.

Configuring SES (initial_setup)

If migrating a single server, configure SES on the new server as a single server. If converting a single server to a duplicated server, configure the SES on the new server as either a cable or network duplex server, depending on the configuration.

Select either cabled duplex or network duplex, depending on the configuration.

Restoring SES files

Use the **System Management Interface** for this procedure.

To restore the files:

1. Connect the drive to the backup location with the SES files.

   Note:

   A backup location can be a locally attached USB compact flash device or a network location using SFTP, SCP, or FTP.

2. On the main menu, under **Data Backup/Restore** click **View/Restore Data**.
3. Under **View current backup contents in**, select your backup location.
4. Click **View** to access the second page.
5. Under Data Sets, select **SES Files**.
6. Click **Restore** to restore the files to the new server. The following message appears:

   Restoring . . . The restore has started. From the main menu, click Restore Status. For complete restore status, click Check Status.

When the restore is finished, disconnect the backup location from the server.

Administering SES

Use the SES Administration Interface for these procedures.

To administer xxx:

1. Using the **List Hosts** screen in the Administrator interface, select **Migrate Home/Edge**.
2. Enter the IP address of the new home server.
3. Enter the database password.
4. Select **Submit** to start the process.

   The former combined home/edge server becomes the edge. The user data from the edge server is moved to the new home server that was set up earlier.

5. On the new edge server, using the Master Administration interface, recreate the non-standard system administrator accounts and the WebLM license file on the SES R3.0.

Administering Communication Manager

Use the SAT command line interface on the server running Communication Manager for these procedures.

You need to retranslate some of the SAT screens on the server running Communication Manager. See *SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers* (555-245-206) for information on which SAT screens to modify.

You need to point to the new home server.

Administering SES

Use the SES Administration Interface for these procedures.

To administer SES:

1. Start the services proxy and imlogger on the edge and the new home:
   a. On a single server (start -a)
   b. On a duplicated server, start the services as follows:
      - On the primary server (start -a)
      - HTTP to the backup server's Maintenance web page, and release the backup system.
2. Change the PPM address on all the supported SIP endpoints.

   If the endpoints were registered previously, they register automatically to the new home server and can make calls.
3. Choose a license source.
4. Add more home servers to the configuration if desired.
5. Reboot the servers if this is a duplicated configuration.

Verifying service

Make a test call on a SIP phone to verify that you have service and that the migration was successful.

Converting cable duplicated to network duplex

A customer who has a cable duplicated pair may want to move one server to another location.

Converting a cable duplicated server to a network duplex server requires

- Backing up all the files on one server in the pair.
- Remastering the server and upgrading it to SES Release 5.2.1.
- Reconfiguring the server as a network duplex server.
- Restoring the files.
- Repeat remastering and reconfiguring tasks on second server.
- Powering down one of the servers and disconnecting it from the other server and move to new location.
- Install the server in its new location.

If one of the servers is installed across a WAN connection, note the following additional details:

- Network Duplication over WAN requires guaranteed bandwidth and reliable WAN service for SIP signaling. It requires service level agreements with the customer to ensure a reliable WAN environment.
- Bandwidth: Minimum of 100 MB for data replication traffic. Event states are not replicated as they change frequently.
- Packet loss: Must not be greater than 3%.
- Jitter: Average one-way jitter must be less than 30 milliseconds.
- Delay: One-way delay must be no more than 150 milliseconds.
- QOS policy parameters appropriate for SIP signaling is required. DSCP36 (Assured Forwarding 42) is recommended. Other DSCP values can be assigned but must guarantee bandwidth to minimize packet loss.

Premigration tasks

Before starting the migration, you must

- Note the configuration information on the existing server. See:
  - Configuration information on page 89
  - Copying the configuration screens on page 90
  - Viewing the configuration screens to copy or print on page 90.
- Back up the SES data files on Server A. See Backing up files on page 91.

Migration checklist

- Making Server A the primary server
- Removing the crossover cables
- Installing SES
- Configuring SES (initial_setup)
- Reboot the servers
- Restoring SES files
- Administering Communication Manager
- Installing the server in the rack
- Connecting the server to network

Making Server A the primary server

Important:
If it isn't already, make Server A the primary (active) server.

Use the **System Management Interface** for this procedure.

To make Server A the primary server

1. Under Server select **Status Summary**
2. In the **Mode** field, verify that it says Active (In service Primary).
3. If it says Standby, under Server select **Interchange Servers**.
4. Click **Interchange** to make Server A the primary (active) server.

Removing the crossover cables

Remove the crossover cables connecting the two server pairs.

Label and disconnect the following cables from the back of the S8500 Server.

- The modem from the RS-232 or USB port on the SAMP or RSA board.
- The CAT 5 cable(s) from the Ethernet port on the server.
- If duplicated, the CAT 5 cables from the Ethernet port on the SAMP or RSA board and the dual NIC.
- If duplicated, the null modem cable from the RS-232 port.

Installing SES

Important:

When installing the software, choose the remaster option on the first screen. This wipes out all the data on the hard drive before reinstalling the software.

You need to do all the tasks through Installing SIP Enablement Services because you are installing a new server. You also need an updated license file.

Configuring SES (initial_setup)

Note:

The “old” physical IP address *must* be the “new” logical IP address. If not, the entire database becomes corrupt and unusable.

If migrating a single server, configure SES on the new server as a single server. If converting a single server to a duplicated server, configure the SES on the new server as either a cable or network duplex server, depending on the configuration.

When prompted, select network duplex.

After the second server is configured, put both servers in service.

Reboot the servers

Use the **System Management Interface** for this procedure.

To reboot the server:

1. Under Server, select **Shutdown Server**.
2. Select **Delayed Shutdown and Restart server after shutdown**.
3. Click **Shutdown**.

   You will be logged off the server when it reboots. You can ping the server to verify when the server is accessible again.

Restoring SES files

Use the **System Management Interface** for this procedure.

To restore the files:

1. Connect the drive to the backup location with the SES files.

   Note:

   A backup location can be a locally attached USB compact flash device or a network location using SFTP, SCP, or FTP.

2. On the main menu, under **Data Backup/Restore** click **View/Restore Data**.
3. Under **View current backup contents in**, select your backup location.
4. Click **View** to access the second page.
5. Under Data Sets, select **SES Files**.
6. Click **Restore** to restore the files to the new server. The following message appears:

   Restoring . . . The restore has started. From the main menu, click Restore Status. For complete restore status, click Check Status.

When the restore is finished, disconnect the backup location from the server.

Administering Communication Manager

See *SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers* (555-245-206) for information on administering Communication Manager for SES.

Installing the server in the rack

To physically install the S8500 Server, see *Quick Start for Hardware Installation: Avaya S8500 Server (555-245-701)*

Connecting the server to network

The following graphic shows the connection schema for an S8800 network duplex server pair.

Figure 10: Schema for S8800 simplex and network duplex servers

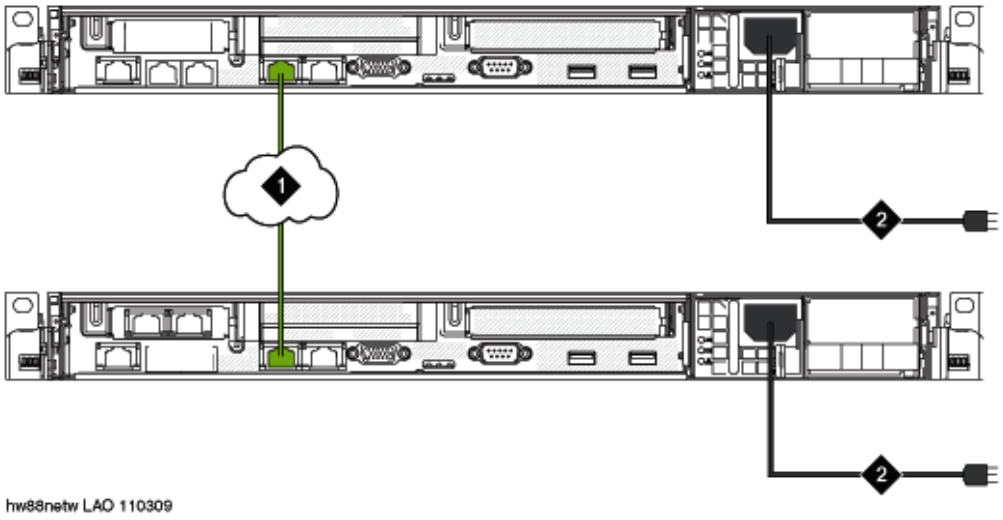


Figure notes:

1. **Straight-through Ethernet cable connecting the servers to the customer network through the customer network port (Eth0)**

Figure 11: Schema for S8800 cable duplicated server

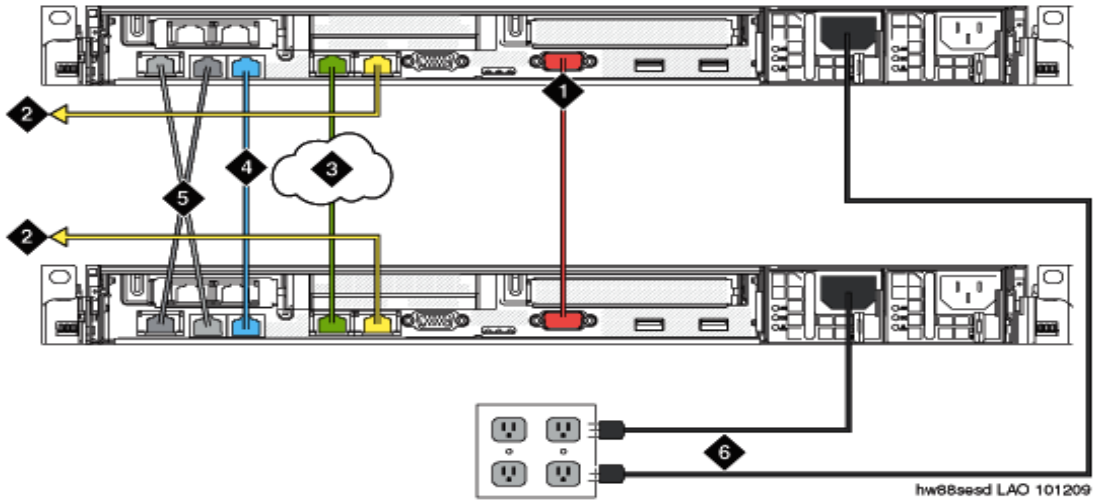


Figure notes:

1. **Null modem cable connecting the services through the RS-232 serial port.**
2. **Ethernet cable connecting LAN (Eth1).**
3. **Ethernet cable connecting the servers to the customer network through the customer network port (Eth0).**
4. **Ethernet cable connecting the servers through the dual NIC port.**
5. **The cable connects the IMM port of one server to Eth2 of the other.**
6. **Power cords of the servers connected to the electrical outlet.**

The following graphic shows the connection schema for an Avaya S8510 network duplex server pair:

Figure 12: Schema for S8510 simplex and network duplex servers

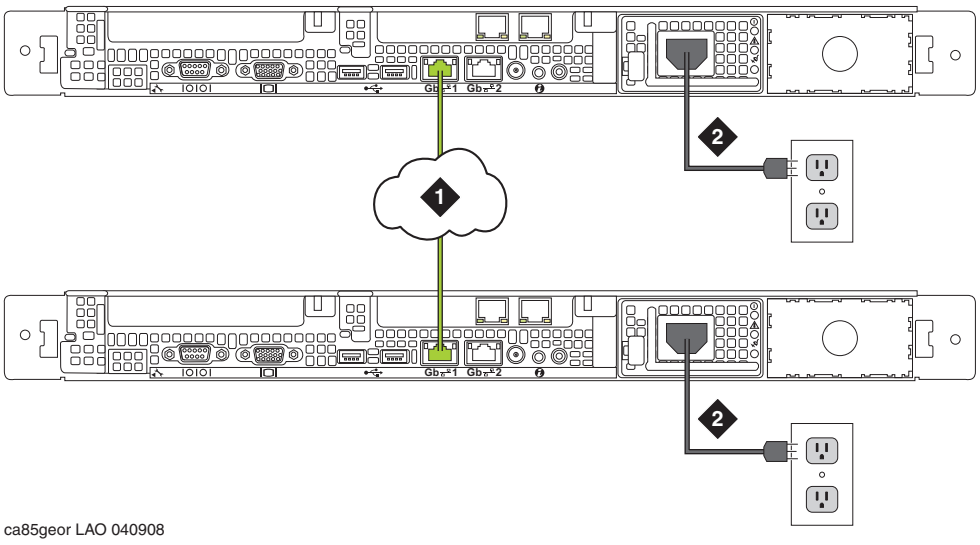


Figure notes:

1. **Straight-through Ethernet cable connecting the servers to the customer network through the customer network port (Eth0)**
2. **Power cords for servers connecting to electrical outlet.**

The following graphic shows the connection schema for S8510 cable duplicated and network duplicated server pair.

Figure 13: Schema for S8510 cable duplicated server

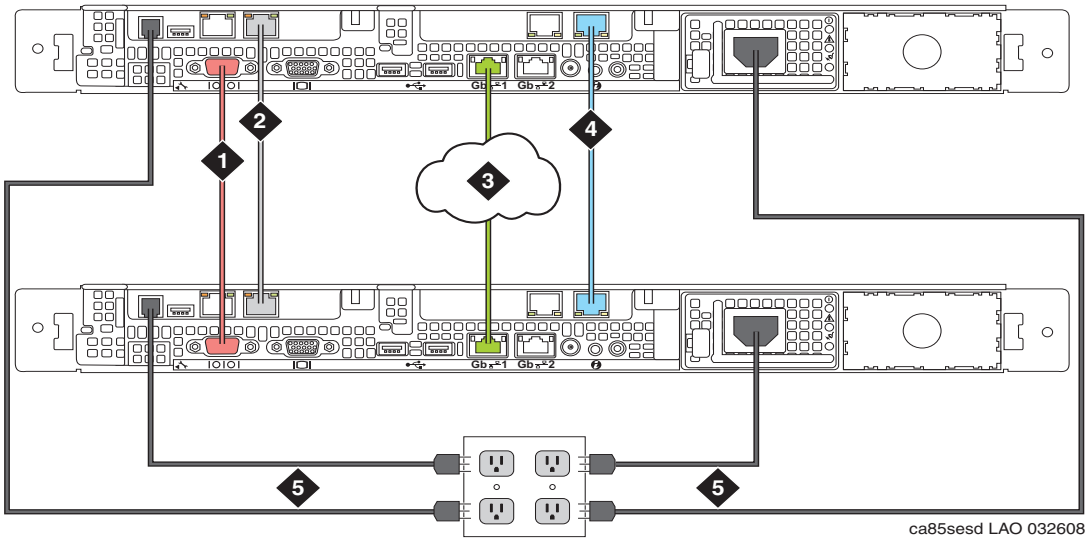


Figure notes:

1. **Null modem cable connecting the servers through the RS-232 serial port**
2. **Crossover ethernet cable connecting SAMPs through the SAMP Services port (Eth2)**
3. **Straight -through Ethernet cable connecting the servers to the customer network through customer port (Eth0)**
4. **Crossover ethernet cable connecting the servers through the dual NIC port (Eth3).**
5. **Power cords for servers and SAMP boards connecting to electrical outlet. The power cord of SAMP card should have an AC/DC adaptor between AC power outlet and the SAMP card RJ-11 jack.**

Note:

Avaya does not recommend connecting both S8510 servers and its SAMPs to the same AC power source for a cabled duplicated SES server, to prevent failures.

Following graphic shows the connection schema for an HP cable duplicated server pair:

Figure 14: Schema for HP DL360 G7 cable duplicated server

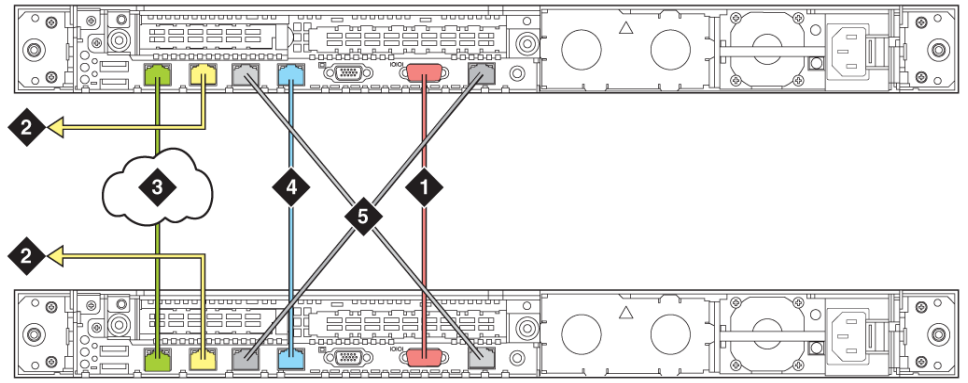


Figure notes:

1. **Null modem cable connecting the servers through the RS-232 serial port.**
2. **Ethernet cable connecting to the services port (eth1)**
3. **Ethernet cable connecting the servers to the customer network through the customer network port (Eth0)**
4. **Ethernet cable connecting through the dual NIC port (eth3)**
5. **The cable connects the ILO port of one server to NIC port 3 (eth2) of the other**

The following graphic shows the connection schema for an HP network duplicated server pair:

Figure 15: Schema for HP DL360 G7 simplex and network duplicated server

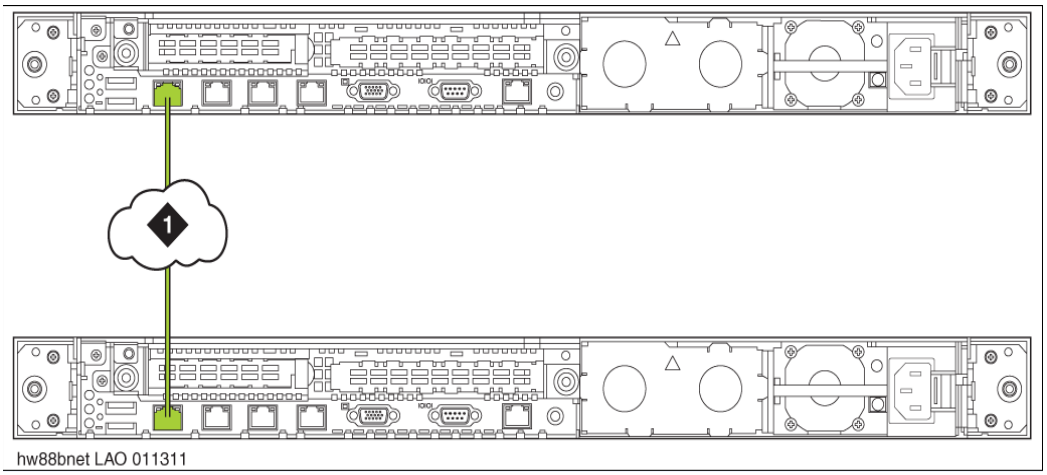


Figure notes:

1. **Straight through Ethernet cable connecting the servers to the customer network through the customer network port (eth0)**

Modem support

The Avaya S8800 Server supports only the US-Robotics modem, while the HP DL360 G7 Server supports all the three modem types listed in the table below:

Terminology	Description	Manufacturer's Product Name
Old MultiTech	USB MODEM v.92 56k RHS	MT5634 USB (discontinued)
New MultiTech	USB MODEM MT9234ZBA v.92 56k RHS	MT9234ZBA-USB
USR Modem	USB MODEM USR5637-OEM 56k ROHS 6	USR5637-OEM

Chapter 6: Administering web interface

This section describes in detail the use and meaning of the screens in the SES Administration Interface. This topic is divided into groups, based on the main headings in the menu at the left of the main window.

Publication note about figures

Most of the screen examples in this document were taken from a distributed configuration with a single edge and two single home servers. If your installation is any other type of configuration, the screens may differ slightly. Figures taken from other hardware configurations are noted in the discussion.

Logon screen

To display the SES Logon screen, enter this URL:

- http://*_IP address of SES server_/*admin
- http**s**://*_IP address of SES server_/*admin

The URL for the SIP PIM application that an end user sees is this:

- http://*_IP address of SES server_*/user

Logon screen field descriptions

Logon ID

Enter the user name for your administrative account. After you enter this and press the Enter key or select **Logon**, the screen refreshes to display the **Password** field. Initially, the **craft** account should be used for initial setup and after remastering.

Password

Enter the password, at least 6 to 12 characters in length, at least 1 of which is alphabetic and at least 1 numeric.

After completing both fields, select **Logon** or press Enter.

System Management Interface

The system displays the **System Management Interface** after you log in to the web interface.

Do one of the following depending on what functions you need to perform on the server:

- To access the **SIP Enablement Services** web page:
  On the **System Management Interface**, select **Administration > SIP Enablement Services**.
- To access the **Server (Maintenance)** web page
  On the **System Management Interface**, select **Administration > Server (Maintenance)**

System Management Interface field details

SIP Enablement Services

The **SIP Enablement Services** interface from the **Administration** menu provides screens for initial server setup, user contact database changes, and communication manager server-related activities.

Server (Maintenance)

The **Server (Maintenance)** interface from the **Administration** menu provides maintenance activities including server status and diagnostics, alarms and traps, and remote access security.

Setup screens

When installing or updating, the setup screens provide the needed interface. Once the system is set up, these screens are available individually, but not displayed by the system as a setup task. The setup screens consist of these:

- Setup Master Admin screen
- Admin Setup screen
- Edit System Properties screen
- Add Host screen
- Edit Default User Properties screen
- Add Communication Manager server Interface screen

The **Setup** screens contain links to the screens necessary to initially configure servers. This screen provides different choices depending on which required tasks have been completed.

Before filling in the Setup screens, you need to know IP addresses, machine names, and answers to the prompts in the install script. See Installation Worksheets on page 323 for a list of the things you will need to know.

Setup Master Admin screen

This screen lets you specify if the machine you are setting up is an SES edge server or and SES home server.

Select the top radio button for an edge server, primary or backup.

Select the second radio button if you are setting up a home server, either primary or backup. The IP address you type here is the IP address of the edge server that acts as parent to this home server. If you have a duplicated edge server, use the logical IP address.

Setup SIP Domain

Select this link to go to the Edit System Properties screen. You must use this screen to specify the domain to assign to this SES configuration before you may proceed with any other setup options. After specifying the SIP domain, you must restart the proxy service on each SIP proxy Host computer in your enterprise before any newly specified domains are recognized system-wide.

The next Setup screen lets you set up your host.

Setup Hosts

After setting up the domain, select this link to create a host computer entry for the first edge or home/edge server in your enterprise. Recall that a host is either a home, an edge, or a combined home/edge. The link on this screen directs you to the Add Host screen.

Note:

You will not be able to continue with administration and configuration until the Set Up Host and Setup SIP Domain options both have been completed.

Setup Default User Profile and Communication Manager servers

The next **Setup** screen typically provide two other choices. Completing these screens is optional but recommended before continuing with administering SIP endpoints or associated telephone numbers (extensions on communication manager servers).

Be aware that you may not add user information or communication manager server extensions until the next two setup options are completed.

Setup Default User Profile

The system displays this link after you have added one edge or home/edge server with **Setup Hosts**. Now, you may select this link to go to the Edit Default User Profile screen or you may first choose to set up your system's communication manager servers running Communication Manager.

Information for user profiles now accepts UTF-8 encodings to accommodate multibyte languages. You may input Shift_JIS (SJIS) as well. Whether the user's browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

Setup Communication Manager Servers

This system makes this link available after you have added any type of host using the **Setup Hosts** link. Select this link to go to the Add Communication Manager server Interface screen where you create one or more entries for your network's communication manager servers running Communication Manager.

Media gateways must also be up-to-date.

Tip:

Note that you may not add user information such as end user contacts, or communication manager server extensions, for example, telephone numbers or handles, to the database until these setup options have been completed.

Edit System Properties screen field descriptions

SES Version

This field displays the major and minor release number, R4.0.0.0, and the current load and build number, -027. 0, of the Avaya software that is running on this SES server.

System Configuration

Identifies this SES server as being a single, standalone machines, or as duplicated, redundant machines. This read-only field does not indicate the server's role of primary or backup.

Host Type

Identifies this SES server as a home, edge, or home/edge type. This read-only field does not indicate the server's role of primary or backup.

SIP Domain

Enter a domain name to assign to this SIP Enablement Services configuration.

Name your domain with lowercase alphanumeric characters and dashes. Do not use any upper case or special characters with the exception of the dash.

Note:

Updates to system-wide properties like the **SIP Domain** field require you to restart the proxy service on each SES host computer in the system. Otherwise, the domain name updates are not recognized.

SIP License Host

Enter the host name, the fully qualified domain name, or IP address of the SES server that is running the WebLM application and has the associated license file installed.

This entry shows the IP address of the licence host in this field. Note that, for duplicated-server configurations, this is the physical, fully qualified domain name or IP address of the SES system running WebLM, *not* the virtual address of the duplicated pair.

DiffServ/TOS Parameters

Call Control PHB Value—The Call Control PHB Value defines the per hop behavior value for signaling used by the intermediary routers in the network order. These values are used to expedite the message flow through the network. Improved flow reduces unnecessary delays and time outs. The default value for this field is '46' which is the 'expedite forwarding' value, normally used for real-time RTP traffic. The range is 0-63.

802.1 Parameters

Priority Value—The Priority Value is associated with the priority tag in the ethernet header and is used to prioritize ethernet layer messages.

Avaya default is 6. Range is 0-7.

Management System Access Login

This is the login for the server that performs core-routing functions for Communication Manager Branch Edition network.

In an Avaya Communication Manager Branch Edition solution, first specify the login for Communication Manager Branch Edition Central Manager in Communication Manager Branch Edition on SES Edge server, then specify it here in SES. The login must match exactly.

Management System Access Password

This is the password for the server that performs core-routing functions for Communication Manager Branch Edition network.

You must first specify the password for Communication Manager Branch Edition Central Manager in Communication Manager Branch Edition on SES Edge server, then specify it here in SES. The passwords must match exactly.

DB Log Level

Setting the DB Log Level lets the administrator set a preference for database access logging.

The information will be provided in /var/log/ecs/commandhistory.

Logging levels will be added to the System Properties form. Logging levels will be a pull down menu with the following choices:

Choice	Stored in data base	What is logged
Disabled	off	No logging of database access. This is the default.
Log Both Before And After Values	both	Log both the original values in the database and new or changed values.
Log After Values Only	new	Log the new or changed values only.
Log No Values	none	Log the database access but, no values.

Network Properties

Lists the Local IP address and Local Name for this physical server, as well as the Logical IP and Logical Name for the node.

In a single configuration, Local and Logical properties are the same.

On a server that is one of a duplicated pair, its Local properties differ from its Logical ones. However, the Logical properties are the same for both of the servers of a duplicated pair.

The information displayed was provided at install time.

The Gateway IP Address field shows the IP address of the gateway that supports this domain.

Redundant Properties

The **Management Device** field reflects the SAMP module that provides access to the machine. In this screen, redundant properties have nothing to do with redundant, backup, duplicated, high availability, or failover meanings.

The remote maintenance board is a SAMP on S8500B, S8500C, and S8510 server hardware.

Select **Update** to submit the updated information on this host. Then, all the hosts should be updated.

Add Host screen

A host is an SES home or edge server, or a combined home/edge server.

If your system architecture is a home/edge, use this screen to add the home/edge server. If your system architecture uses a single home/edge architecture, you cannot add a host of any kind in addition to the home/edge server, and are denied access to this screen.

If your system architecture is a single edge server with one or more home servers, use this screen to add the edge server at install time, and then add each home server. Specify the type, edge or home, in the **Host Type** field.

Add Host screen field descriptions

Host IP Address

Enter the IP address for this host server, either home, edge, or home/edge. Use the dotted decimal notation to enter IP addresses (for example, 123.45.67.89).

Profile Service Password

This password is for permissions between SES hosts, that is, home server(s) and edge.

Note that the Profile Service Password is not used by users or administrators. Rather, it is a password that is used by internal software components for secure communication between SES servers and the master administration system. The Profile Service Password must be unique for each administered host.

Host Type

Select one of the following from the drop-down list:

- Edge—if this will be an edge proxy server for the SIP traffic of all domains.
- Home —This option appears only after an edge proxy has been added. If this will be a Home proxy to manage the SIP traffic of a specific domain.
- Home/edge—if this server functions as both your enterprise's edge and home proxies. Note that no additional proxy servers may exist within this architecture.

If the server type is an S8300C running SES co-resident with Communication Manager, the Host Type drop down contains the following:

- Communication Manager combined home-edge—this server functions as both your enterprise's edge and home proxies and communication manager server. Note that no additional proxy servers or communication manager servers may exist within this architecture.
- Communication Manager home—This option appears only after an edge proxy has been added. Select this option if the server you are adding is a co-resident SES and Communication Manager server.

Parent

Select one of the following from the drop-down list to indicate the communication manager server this host uses:

- Select NONE if you selected edge or home/edge for the server's Host Type above. An edge server has no parent.
- Select HOST NAME or IP if you selected home for the server's Host Type above. The name of the edge servers for all your enterprise's domains are listed. Select the correct edge server as Parent.

Listen Protocols

At a minimum, select TLS for the **Listen Protocol**. You may select UDP or TCP for other uses. Communication Manager supports the TLS and TCP link protocols for SIP trunking.

Note that the protocol you select for linking must also be selected here for listening. At a minimum, you must select the protocol you selected as the **Link Protocol**, below, although you may want to select additional protocols only for listening but not for linking.

When you add a host, all three protocols are selected for listening. There is little reason to change this default.

Link Protocols

This field refers to the trunk signaling between SES and Communication Manager. Typically, the selection here matches the Signal Group value on Communication Manager.

The link protocols for SIP trunking in Communication Manager are TCP and TLS. For third-party proxy servers, you may select to link to SES with TLS, TCP, or UDP. You must also select the Link Protocol as a Listen Protocol, above. You may want to select additional listen protocols.

There is no special reason to change the default.

Access Control Policy

This setting correlates to the Watcher feature on the end user's SIP PIM web interface.

Accept the default policy of **Deny All**, or select **Allow All** to change this default policy and show the presence of SIP users on this server. The system displays the presence of SIP users on the Watchers screen in the SIP PIM web interface to PPM.

The administrator may set a system policy to specify that all users on the system default to a blocked state, where users must authorize each other to view each other's presence. The end SIP user may override this setting.

This administration policy is on a per-node basis and may be administered for each home node in the network.

Emergency Contacts Policy

Enable this field to allow unauthenticated calls for the emergency contact named for this host.

If you allow emergency contacts, emergency calls can come to this host. If you disable this field, unauthenticated calls to the emergency URI will be dropped.

Set up emergency URIs for the end user with the Add Emergency Contact screen.

This feature is supported on configurations using a single communication manager server.

Minimum Registration (seconds)

Enter a whole number of seconds, 900 through 59,940, that the SIP server should consider as the minimum acceptable duration when a SIP client registers. If no value is entered, the default of 900 seconds will be used.

Line Reservation Timer

This value configures the maximum amount of time that an end user is allotted to dial a number after going off-hook. The default for this field is 30 seconds. The range is 30 to 240 seconds.

Registration Expiration Timer (seconds)

The value for Registration Expiration Timer determines how long a SIP endpoint should register for and renew its registration.

This value is not enforced by the registrar, but downloaded by an endpoint through PPM if they support it. The value for Minimum Registration (seconds) is enforced by the SIP registrar and it will not allow new registrations prior to that minimum registration time.The minimum registration timer is a SIP protocol feature that prevents endpoints from registering too quickly. Such a registration may be in error.

The default is 3,600 seconds, or 60 minutes.

This field affects all the users on this host.

Outbound Routing Allowed From

Select **Internal** or **External** or both to specify whether SIP traffic can be routed only from endpoints internal to this server's domain, or also from those external to it.

Outbound Proxy

Enter the host name of the server within your enterprise that should manage SIP traffic bound for domains external to this server's domain.

For example, on a home/edge server, this would be the host name of the edge named as Parent of that home. On a combined home/edge or an edge proxy server, this entry might be a remote host, a service provider, ar an alternate edge server.

For a home server, define an outbound proxy only if a host other than the edge will route outbound calls.

Outbound Port

Enter the number of the port (1-65535) on the outbound proxy server specified above that should manage SIP traffic bound for domains external to this server's domain. Use port **5060** if the entry for Outbound Transport is UDP or TCP, and port number **5061** if it is TLS.

Select the transport protocol of the outbound proxy server that should manage SIP traffic bound for domains external to this server's domain. Use TLS as a best practice.

Outbound Direct Domains

Users do not need to be under the same edge server to take advantage of hairpinning/shuffling and the absence of map addresses. For example, a user in New York can call another user in Paris, and the call is directly routed to the trusted domain in Paris. Set those trusted domains for the host, home, edge, or home/edge, here.

Use this area to list those domains for which traffic may completely bypass the Outbound Proxy server specified above. Separate entries in the list with commas, or with a white space followed by a new line, after each domain.

Select the **Add** button to add a host with the properties you've entered. If you have added an edge proxy, then selecting **Continue** at the next screen returns you to the Add Host screen until you add at least one home proxy server as well. If you add a combined home/edge proxy, then you return to the Setup screen if you are initially installing hosts.

Default Ringer Volume

This field sets the ringer setting for the stations bridged appearance buttons. The values in this field are not related to the ringer setting configuration in Communications Manager, nor does it reflect the Communication Manager's settings.

The default is 5. The range is 1 to 10. This field affects supported SIP endpoint users on this host, such as the Toshiba SP-1020A and Avaya Sparc.

Default Ringer Cadence

The value in this field sets the speed of the default ring tone for supported SIP endpoints, such as the SP-1020A. The default is 2, and the range is 1 (slowest cadence) to 3 (fastest cadence).

Default Receiver Volume

This field sets the volume in the handset, rather than the speaker, for supported SIP endpoints, such as the Toshiba SP-1020A. The default is 5, and the range is 1 (lowest) to 10 (highest).

Default Speaker Volume

This field sets the volume on the speaker, rather than the handset, for supported SIP endpoints, such as the Toshiba SP-1020A. The default is 5, and the range is 1 (lowest) to 10 (highest).

VMM

Voice Over IP Monitoring Manager (VMM) is a voice over IP (VoIP) quality of service (QoS) monitoring tool. This feature is available only on endpoint SIP phones, model SP-1020A.

VMM information is taken from the VMM server. SES requires the server name, port address, and how frequently an end point should report back to the VMM Server. See the VMM document titled *Voice Over IP Monitoring Manager User Guide*, 555-233-510.

This field is specific to the Toshiba solution and only work with supported phone types.

VMM Server Address

Address of the VMM server.

This field is specific to the Toshiba solution and only work with supported phone types.

VMM Server Port

Port number for the VMM server’s address.The range is 1 through 65,535, and the default is 5005.

This field is specific to the Toshiba solution and only work with supported phone types.

VMM Report Period

The report period is in seconds, and reflects how often an endpoint should report back to the VMM server. Reports show jitter, round trip time, and packet loss. This may help in solving troubles on the IP network. The default value is 5 seconds, and the range is 5-30 seconds.

This field is specific to the Toshiba solution and only work with supported phone types.

Edit Default User Profile screen

This screen lets you enter a common address for all user profiles on the SIP system. You will not have to type it in repeatedly for each user later. The system displays the data you enter here on an individual user’s profile. You can change it there to be more specific.

There is exactly one default user profile on the entire system. The default user profile data resides on the edge server.A specific user's profile is then pushed to their specific home.

Information for user profiles now accepts UTF-8 encodings to accommodate multibyte languages such as Japanese. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser’s language setting.

Edit Default User Profile screen field descriptions

Host

From the alphabetized drop-down list of names, select the home server for whose users this location information will become the default entries. The host name selected by default in the list is either the first home server alphabetically or the single home/edge server.

Address 1, Address 2

This is the first line and second line of the default address for users. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS depends upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

City

Enter the name of the city or town of the default address for users. You may use alphanumeric characters.

State

Enter the name of the state or province of the default address for. You may use alphanumeric characters.

Country

Enter the name of the country of the default address for users. You may use alphanumeric characters.

ZIP

Enter the ZIP or postal code of the default address for users. You may use only numeric characters.

Edit Default User Profile screen commands

Update

Select **Update** to submit the information on this screen to the server's database.

Add Communication Manager server Interface screen

Use this screen to add additional communication manager server interfaces to your SES network.

This section also discusses the Edit Communication Manager server Interface screen.

Depending on configuration and features used, SES may employ two links to a communication manager server:

- SIP trunk—this is a SIP signaling link between SES and the communication manager server.
- Administration interface—If SES needs to obtain configuration information from the communication manager server, it will use the link to the specified Communication Manager server Admin Address.

These two links may be to the same IP address. If so, the communication manager server services the two different protocols on different ports.

Select **Add** to submit the communication manager server with the properties entered to this database for this home host. On the Edit version of this screen, select Update.

Add Communication Manager server Interface screen field descriptions

Communication Manager server Interface Name

Enter the network node name in alphanumeric characters for the communication manager server's C-LAN or processor C-LAN IP interface, PE. You may want to use the same name you used for this communication manager server on the ***IP Node Names*** screen in Communication Manager. Each communication manager server's name must be unique within the SIP domain. Refer to *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

If the *communication manager server* has more than one C-LAN interface used for SIP trunking to this SES, then, you must add each C-LAN interface as a unique communication manager server.

Host

In this screen, The Host field lists the IP address of the home server for whose users the communication manager server specified above is the default.

SIP Trunk Link Type

Select TLS for the SIP link between the communication manager server and this host. This is the default protocol selected for all servers.

SIP Trunk IP Address

This field holds the IP address for the communication manager server's C-LAN or processor ethernet interface (PEO that terminates the SIP link from SES. The IP address must be specified as 'dotted IP notation', that is, a 32-bit address comprising four 8-bit octets in the form 'xxx.xxx.xxx.xxx' where xxx is a value in the range of 0-255. If DNS is available within the SIP domain, enter the fully qualified domain name of the communication manager server's C-LAN or processor C-LAN.

SIP Trunk Port

The SIP trunk is for SES/Communication Manager co-resident installations only.

The SIP Trunk Port field lets you configure SES with the same port number configured in the Communication Manager signaling group field.

When you configure the signaling group on Communication Manager, there is a Co-resident check box that defaults the port to 6001. This value must match on the SES. It is not critical that the matching ports are 6001, but that they match. The Communication Manager configuration of 6001 is the "near end port" on the signaling group form.

The signaling group that Communication Manager uses to talk to a co-resident SES cannot have a near-end port of 5061 because SES owns that port.

Communication Manager server Admin Address

This field holds the fully qualified domain name or IP address (in dotted notation) for access to the administration service on the communication manager server. For Communication Manager, this administration service is the System Access Terminal (SAT), so this address would be the address of procr or a C-LAN that allows SAT service.

If a C-LAN on Communication Manager is used, then SAT service on port 5023 must be enabled on that C-LAN. If any SES users have associated extensions on Communication Manager, SES obtains certain configuration information from Communication Manager over this interface.

Communication Manager server Admin Port

The Communication Manager server Admin Port is the port used by the SES Home or Home/Edge to get data over OSSI from the communication manager server, which is used by the SES to configure AST (SIP) phones.

Communication Manager server Admin Login

Enter the login used to access the communication manager server's administration service, for example, the Communication Manager's SAT. Your login on Communication Manager should be of type **customer** and service level **superuser** at a minimum.

Do not expect phones to work correctly unless your provision an Communication Manager login and password.

Communication Manager server Admin Password/ Password Confirm

This is the password for the Communication Manager server Admin Login described above, the password of SAT.

Do not expect phones to work correctly unless your provision an Communication Manager login and password.

SMS Connection Type

This field defines the connection type between an SES home server and communication manager server to obtain provisioned data from PPM.

Choose SSH for a secure connection, or choose telnet for unsecured connection.

Choose Not Available if you do not want to communicate with Communication Manager, perhaps for troubleshooting purposes.

Add or Edit Communication Manager server Interface screen command

Add

Commit the information on this screen to the database.

Update

Commit the information on this screen to the database.

Core Router screens

The Core Router screens menu option appears depending on your SES system. It is a component of a Communication Manager Branch Edition solution.

The core router feature enables a branch office to call another branch by going through the SES edge server. In order to use the core router feature of SES, the Management System Access Login field and Management System Access password field on the Edit System Properties page must be administered to match those administered for the edge server of the Communication Manager Branch Edition.

In SES, the screens used to set up the core router feature are these:

- List Prefix Maps screen
- List Handle Maps screen

Prefix maps are used with Communication Manager Branch Edition, and correlate branch office prefixes with server IP addresses.

Handle maps are used with Communication Manager Branch Edition, and show the IM handles of branch employees.

List Prefix Maps screen

The Prefix Maps screen shows, for Communication Manager Branch Edition, the correlation between branch office prefixes and the IP addresses of the servers at the branch office. The information here is a reflection administration performed in the Communication Manager Branch Edition. The List Prefix Maps screen is read only in SES.

List Prefix Maps screen field descriptions

Branch Prefix

Branch Prefix is the prefix used to uniquely identify each Communication Manager Branch Edition platform, including each optional SIP Server in the main or headquarters location.

Branch Address

Branch Address is the IP address of the Communication Manager Branch Edition platform at each location.

Core Router

Core Router is the IP address of the SES edge server performing branch to core routing.

Total Length

Total Length is the digit length of the assigned branch prefix *plus* extension.

List Handle Maps screen

This screen is a read-only summary page listing the current alphanumeric handles associated with users at Communication Manager Branch Edition branch locations.

This screen is provided to SES by Communication Manager Branch Edition Central Manager. Fields on this list screen are read-only; they may be edited using the appropriate screen(s) in Communication Manager Branch Edition Central Manager.

List Handle Maps screen field descriptions

Branch Prefix

Branch Prefix is the string of digits uniquely identifying each Communication Manager Branch Edition platform, including each optional SIP Server (home) in the main or headquarters location)

IM Handle

IM Handle is the alphanumeric IM handle for each branch user.

User screens

The User screens permit customizing aspects of the system for each user. Use the check boxes to apply a task in the pull-down menu to more than one user.

List Users screen

To use this screen, check a box next to a user ID, select an action from the task drop-down menu, select Submit.

This screen is viewed only from the edge server's Master Administrator interface.

Notice that if you are logged in to a home server, the Tasks drop-down menu is not available.

List Users screen field descriptions

User ID

Lists the IDs of administered users in the database.

Host

This is the name of the home server for this user. A user's host is a home server or a combined home/edge server.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

List Users screen commands

All of the tasks in this drop-down menu reflect data that the user sees on the SIP PIM interface.

You may select any of the tasks in the Task field.

Add User task

Use the Add User screen to add a new user to this home server. This command is the same as selecting **Users** > **Add** from the menu.

Contact List task

This series of screens relates to the sites and friends the end users want to contact. Create and edit the personal contact with whom this user may want to communicate with the My Contact List task screen.

Devices task

Manage the tones, volume, and cadence of certain SIP-enabled devices with the Device Settings screen. For you to view this screen, the end user must have a compatible device.

Delete All Displayed Users task

This task lets you delete all the users currently displayed without having to check the boxes to the left of the name. This is useful after a search has properly returned a group of users.

Delete Selected Users task

Delete more than one user at a time by checking several check boxes. You can check up to 68 check boxes to delete up to 68 users at one time. Select this and confirm your decision to delete one or more users.

Extensions task

Add, delete, and make available the communication manager server extensions assigned to a user with the Extensions task.

Handles task

The Handles task concerns how the end user wants to be contacted. Administer a user's personal points of contact, and user groups with the screen in Handle task.

A user may have more than one handle. For instance, one handle may be the user's communication manager server extension. Another handle maybe a team designation such as Head_Of_Payroll. Even though the number of contacts to a handle is limited to two, the number of handles for a user is *not* limited. A user must always log in to his or her SIP device using his or her primary handle as the user ID. A primary handle matches the User ID.

Memos task

Write short notes about the user for other administrators to read using the User Memos screen. Maximum size of the notes is 256 characters.

Move User

Move User occupies the screen only when there is more than one home server. Move User changes a user from one home server to another.

You can also move a user from one home server to another using the Edit Profile screen.

Permissions

Use this task to specify if other SIP users can detect a user's presence on the system. This is the Watchers feature of PPM. Selecting this task displays the Permissions screen.

Note that presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.

Profile

Edit the full profile of a user and customize it with the Edit User Profile screen.

Watchers for User

This task choice lets you select for the user who on the system may observe the user's presence. Selecting this task displays the screens for the Watcher's Task

Note that presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.

Submit

Check mark a user, or in limited instances, several users, select a task from the drop-down menu, then select Submit to proceed to the next screen.

Add User screen

Add users one at a time with this screen. The contents setup in the default user profile initially populate the fields Host, Address 1, Address 2, City, Country, and ZIP. You may change those entries here for this single user. Check the **Add Communication Manager server Extension** box to immediately assign a communication manager server extension, and a SIP address based on that extension, to the new user.

The fields for user profiles accept UTF-8 character encodings to accommodate multibyte character languages such as Japanese. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. Used with the SP-1020A, this alias string is in Kana characters, and is designed to help with contact sorting. (Contrast this with Name.)

Add User screen field descriptions

Primary Handle

A handle identifies the user on the SES system. Users' primary handles must be the same as their user IDs. Selecting this link displays the detailed user contact information for the SIP user. User handles must be unique within the SES system domain. Users may have multiple handles to accommodate more than one personal point of contact.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- handle_list
- presenceserver

In addition:

- All handles must be between 3 and 16 ASCII characters in length.
- If any of the preceding transformations produce handles already present, then they are dropped.

- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique.
- All handles must be alphanumeric with no special characters other than dash (-).

User ID

(Optional) This is an identifier of at least three alphanumeric characters in length. Each administered user has one unique User ID and it is used as their display name within SES administration. For example, the User ID is the name listed for the user on the List Users, Search User, Edit User and List Communication Manager server Extensions screens.

It is recommended that the User ID be the same as the Primary handle administered for the user. If the User ID is left blank when the user is added, it is defaulted to the Primary handle.

A User ID is administered as an alphanumeric string between 3-16 characters in length.

A user's User ID may be changed from their Edit User Profile screen. A user's Primary handle may only be changed from the Edit Handle screen (List Users -> Select A user -> Select Handles task).

Password, Confirm Password

Enter a password of 6 to 12 alphanumeric characters. Both field entries must match.

Host

From the drop-down list of names, select the home server for this user. The host name of the current server is selected by default.

This is the name of the SES host serving the domain for this user. An SES host is a home or edge server or a combined home/edge server.

First Name, Last Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser’s language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

Address 1, Address 2

(Optional) This is the first line and second line of the default address for users. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS depends upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

Office

Enter a designation for the user's office suite or perhaps floor, in alphanumeric characters.

City

Enter the name of the city or town of the user's address in alphanumeric characters.

State

Enter the name of the state or province of the user's address in alphanumeric characters.

Country

Enter the name of the country of the user's address in alphanumeric characters.

ZIP

Enter the number of the ZIP or postal code of the user in numeric characters.

Survivable Call Processor

The Survivable Call Processor field points to auxiliary call processor hardware if service from SES is lost. The list of SCPs on the drop down menu is empty until you add one or more SCPs using screens under Survivable Call Processor screen.

Ideally, administer your SCPs before you add or edit a user.

Note:

SIP Enablement Services will support Avaya Communication Manager Survivable SIP Gateway Solutions in a distributed network settings in a later release. For more information, visit the following website: https://enterpriseportal.avaya.com/ptlWeb/internal/support/CS20062289553889009 1/C20071121376669013/SN20063141134188610 75/SN20071151175317042

Add Communication Manager server Extension

You may select this box to assign a communication manager server extension now, or leave it unchecked to assign one later. If you check this box, the system displays the Add Communication Manager server Interface screen after this user's profile has been added. If you do not check this box, you can wait and associate extensions with the user later.

Add User screen commands

Add

After entering or updating entries, select **Add** to submit the user's profile to the database on this host.

Update

On the Edit User Profile screen, click Update after entering or updating information to submit the user's profile to the database.

My Contact List task screen

This series of screens displays the sites and friends an end user wants to contact. The contact address can be IP addresses, e-mail address, or web pages with which an end user would like to communicate.

If a SIP softphone user adds a contact for a non-sip user, then when the SIP user logs into SPIM, they will see a 'dummy' handle for the non-sip contact that looks like: "softphone_xxxxxxxxx@domain.com", where "xxxxx" is a unique string.

This screen is also available on the web page viewed by the end user of PPM, the SIP Personal Information Manager pages, but there it is rendered differently.

The maximum number of contacts an end user may have on this page depends on the device they have. If the device is an SP-R 5.2 or later, the maximum number of contacts is 50. For any other device, the maximum number of contacts is 250.

Contact List screen field descriptions

Handle

This is a valid name or User ID for the contact. Selecting this link displays the detailed user contact information for the contact. Handles must be unique contact URIs within the SES system domain, but contacts may have multiple valid handles.

Note:

The SES system automatically appends the *sip_domain.com* portion of the handle. This portion of the handle should not be entered as part of the handle field when adding or updating a handle.

If you select a user's option button, or select a group name by clicking on it, the system displays a Contact Details screen or Group Details screen. These two screens let you edit details about the contact or group, respectively.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

Alias

This field displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name.)

Telephone #1 / Telephone #2

Lists a telephone number or valid SIP user address. A valid SIP user address may be any Uniform Resource Identifiers (URIs) beginning with **sip:** or **sips:**. The SIP user address is associated with this handle in the contact database.

This field may contain a maximum of 256 ASCII characters.

My Contact List screen commands

Handle (link)

If you click directly on an underlined handle, the system displays Contact Details for that handle as a view only screen.

Group (link)

If you click directly on an underlined group name, the system displays the Group Details screen for that group. At this time, only one level of hierarchy for groups are supported.

View

View details about the contact or group.

Delete

Select a contact, then select Delete to remove that contact from the user's list. This does not delete the contact from the system.

Add Contact

Add another individual contact or group. At this time, only one level of hierarchy for groups are supported.

Add Group

Add a group name to which this contact belongs. At this time, only one level of hierarchy for groups are supported.

Speed Dial

Select this to view the speed dial telephone numbers and speed dial digit assignments for contacts this user may want to communicate with.

Reload Configuration

If you have made changes on this end user's list of contacts, select Reload Configuration to refresh the list.

For SIP users, you may wish to reload the configuration data for your telephone, like its Ringer Settings, its Speed Dial List entries (from My Contact List), and its One Touch Dial List entries. Select this link and then submit the reload request.

For system administrators, a variety of data affects the device:

- Changes to network node information
- Data regarding station aliasing
- Associated Dial Plan assignments

These data may have been updated and submitted on the communication manager server running Communication Manager. Submitting this request reloads this updated device configuration data.

Note:

Provisioned users who have been administered may not have logged on to their device, registering it with the SIP proxy server. Submitting the Reload Device Configuration (or executing the Reload Complete task) will take effect the next time they log on successfully to their SIP device.

When you are ready to reload your configuration for this device, including any station-affecting changes made in Communication Manager running on the communication manager server, then select the Submit button on this screen. Otherwise, select the Cancel button to ignore this request.

After you click Continue, the screen displays the My Contacts list again.

Contact Details screen

This system displays this screen when you select an item and then the View button on the My Contacts screen. This screen is read only. To make changes, select **Update Contact** to obtain an editable view.

With this information, SIP users can access each other at a variety of contact points.

All fields on this screen are view only.

Select **Update Contact** to make changes on the Update Contacts screen.

Select **Delete Contact** to remove this contact’s information from access by the user.

Update Contact screen

Change the contact information for the end user's contact with this screen. With this information SIP users can access each other at a variety of contact points.

SIP User dlaser, who wants to contact user Digi Minky, must put in all the contact information for DMinky via the PIM or Softphone. That way dlaser can choose to reach DMinky at a work telephone, cell telephone, web page, fax number, and so on.

Add Contact screen

From the SIP PIM interface an end user builds a list of friends, e-mail addresses, web pages and so on, with whom to communicate. As an administrator, with this screen, you may add a contact for the end user, with a group affiliation, and speed dial numbers.

With this information, that SIP users can access each other at a variety of contact points.

SIP User Dani Laser, who wants to contact user Digi Minky, must put in all the contact information for dminky via the PIM or Softphone. That way dlaser can choose to reach dminky at a work telephone, cell telephone, web page, fax number, and so on.

If a SIP softphone user adds a contact for a non-sip user, then when the SIP user logs into SPIM, they will see a 'dummy' handle for the non-sip contact that looks like: "softphone_xxxxxxxxx@domain.com", where "xxxxx" is a unique string.

Add Contact and Update Contact screen field descriptions

Address

On this screen, the Address field must contain the SIP address of the contact in this field, that is, the user's handle on the SIP domain.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

Alias

(Optional) This field displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name.)

Group Name

A valid name for the group with which the contact has been associated, as a selectable link. This field may contain a maximum of 32 UTF-8 characters. Select the link to view the details screen showing the contacts for this Group.

Tip:

If the contact list is lengthy, use your web browser's "Find in This Page" function to search the page for a particular entry.

You may select a contact to View or Delete using the radio button to the left of the name and/or handle. After you choose a contact, select the "View" button to display the Contact Details screen, or select the "Delete" button to display a warning message for you to confirm the deletion from the contact list.

Note:

Deleting a user contact from the contact list does not affect the associated provisioned user's information in the user database.

E-mail

Enter a string in this field as the e-mail address associated with this contact. It may contain as many as 256 ASCII characters. When displayed in the read-only fields, this becomes a selectable **mailto:** link on the web page.

Notes

Enter any informational notation to be associated with this contact in this field. It is free-form text, and may contain as many as 1,024 UTF-8 characters. You can input Shift_JIS (SJIS) as well. Whether the user's browser sends UTF-8 or SJIS is dependent upon your browser's language setting.

Track Availability

Check the box if the user named at the very top of the screen.

Note that presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.

Contact Phones

This group of fields lists up to six ways for a user to reach a contact.

- **Phone Type—**The drop-down menu for this field provides identification for the rest of the information in the row.
- **Phone Number—**SIP handle, e-mail, fax, or telephone number for this contact.
- **Label / Label—**a short description of the contact, perhaps a server or type of contact.
- **Speed Dial—**check this box to let the end user reach the contact with speed dial. The first contact is speed dial number 1, the second is number 2, and so on. Speed dial is a soft button on a SIP telephone
- **Prefix—**any outward dialing prefix, comma, or other sequence the end user may need to dial before they dial the telephone number.

Add Contact screen command

Add

Record this contact's information and it's association with a user in the database.

Add Group screen

This page enables you to create a new access-profile or a non-access profile Linux Group.

Add Group screen field descriptions

Select Action

Choose one of the following options:

- **Add a new access-profile group**—choose this selection and then select a desired profile from the drop-down menu to add a new access-profile group. Only a profile group that is unassigned is listed in the drop-down menu.
- **Add a new non-access-profile group**—choose this selection to add a non-access profile group.
    - **Group Name**—values are characters from the set a-z, A-Z, 0-9, and _ (underscore). Do not name the group in the form of profn or profnn, where n is 0 through 9 and nn is 10 through 69.

Note:

Multiple group names may be entered with a comma separating the group names. Each group name may not be longer than 31 characters. The group name must not already exist.

- **Group Number**—valid values are 500 through 60000. A group number must not already be assigned to another existing group.

Add Group screen command

Submit

Validate and create the group name.

Speed Dial List screen

This screen is view only. It reflects the settings made in Contact Details screen. You can quickly see what is assigned to speed dial 1, speed dial 2, and so on.

To make changes to the speed dial information of a contact, use the Update Contact screen. Entries on this list typically appear as soft button labels on the SIP user's device.

Handle

This is a valid name or User ID for the contact. Selecting this link displays the detailed user contact information for the contact. Handles must be unique contact URIs within the SES system domain, but contacts may have multiple valid handles.

Note:

The SES system automatically appends the *sip_domain.com* portion of the handle. This portion of the handle should not be entered as part of the handle field when adding or updating a handle.

Name

On this screen, Name is the label you assigned to the phone number for this contact.

Alias

This field displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name.)

Prefix

Lists the optional prefix digits associated with this user's extension (**Telephone #**) in the user database. An example of a prefix would be an AAR or ARS dial access code of 0-4 digits. This field blank may be blank if no such prefix code applies to this user contact.

Telephone

Lists a telephone number or valid SIP user address. A valid SIP user address may be any Uniform Resource Identifiers (URIs) beginning with **sip:** or **sips:**. The SIP user address is associated with this handle in the contact database.

This field may contain a maximum of 256 ASCII characters.

Select **Handle** to view the associated user's detailed contact information.

Delete Contact screen

As administrator, you may want to delete infrequently used contacts for a user. Deleting a contact will adjust the speed dial order. Deleting a contact does not delete the group of which the contact may be a member, nor does it delete the contact from the system.

Select OK to remove both the association from the end user and the contact from the database.

Select Cancel if you change your mind about the delete. Group Details screen

If a contact can be classified with a certain group, view and delete group members here. At this time, only one level of hierarchy for groups are supported.

Group Details screen field descriptions

Handle

This is a valid name or User ID for the contact. Selecting this link displays the detailed user contact information for the contact. Handles must be unique contact URIs within the SES system domain, but contacts may have multiple valid handles.

Note:

The SES system automatically appends the *sip_domain.com* portion of the handle. This portion of the handle should not be entered as part of the handle field when adding or updating a handle.

After viewing the details of this group, select the **Add Contact** link to go to the Add Host screen and associate a contact with this group in your list of user contacts. Select the **Delete Group** link to go the Delete Group screen and delete this group name from your contact list. Select the **Update Group** link to go to the Update Group screen and change the name of this group in your user contact list.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias.)

Alias

This field displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name.)

Telephone #1 and Telephone #2

Lists a telephone number or valid SIP user address. A valid SIP user address may be any Uniform Resource Identifiers (URIs) beginning with **sip:** or **sips:**. The SIP user address is associated with this handle in the contact database.

This field may contain a maximum of 256 ASCII characters.

Group Details screen commands

Back to My Contact List

Select this link to return to the My Contact List.

Add Contact

Select this to display the Add Contact screen and to add another contact to the group selected.

Delete Group

Select OK to delete the group from the database. Select Cancel if you change your mind about deleting the group.

Deleting a group does not remove the contacts in the group from use. The contacts automatically become members of the default group.

Update Group

Select this to display the Update Group screen and to change the group's name.

View

Select a contact for the user and click View to show a view-only screen of the contact's details.

Delete

Delete this contact from this particular group.

This command does not delete this contact from any other groups to which it belongs.

If a group is empty, View and Delete operate on the group, not members of the group. If a group is not empty, it has members, and View and Delete operate on the members, showing them in the group or deleting them from the group, respectively. **Delete** does not delete a contact group member from the user database.

Delete Group screen

Deleting a group generates the following results:

- Delete the group and all its members.
- Move the members to another group and then remove the original group.

Delete Group screen field descriptions

Delete all contacts

Select this radio button to remove the members from the group but keep the group itself. The contacts that are members of this group are not deleted from the database.

Move all contacts

Select this to move all the group’s members to another group. The original group is deleted.

Delete Group screen commands

Back to My Contact List

Select this link to return to the My Contact List screen.

Yes

Go ahead and invoke your selections.

No

Cancel the selections on the screen and do nothing. The system displays the My Contacts screen.

Update Group screen

Modify the group name here. All contacts associated with the original group name now are associated with the new group name.

Update Group screen field descriptions

Old Group Name

Displays the name of the existing group that you are about to change.

Group Name

Enter a new name for the existing group, of as many as 32 UTF-8 characters in length. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

Used with SP-1020A, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name.)

When finished entering data, select **Submit** to rename the group in your contact list.

Update Group screen commands

Back to My Contact List

Select this link to return to the Contact List

Submit Update

Select this to apply the group name change to the database.

Device Settings screen

The Devices screen allows the users of certain supported SIP devices to view, change, and reload certain configuration settings. Note that the example screens shown in this section apply to the Toshiba Business Phones (SP-1020A).

One Touch Dial List screen

This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

One Touch Dial List screen field descriptions

Button

The number designating the button which is assigned to this auto-dial list entry in Communication Manager running on the communication manager server. The maximum button number is 66.

Address

May be blank, in which case SIP contact Uniform Resource Identifiers (URIs) for the auto-dial list entry may be entered here, or it may display the non-blank auto-dial list entry or entries made in Communication Manager running on the communication manager server for the associated button. In the latter case, if the entry is edited in this SIP PIM web interface, any changes made to these entries here will ***not*** be reflected in Communication Manager on the communication manager server(s). The maximum length of any Address field entry is 256 ASCII characters.

Label

May be blank, in which case a label for the auto-dial entry may be entered here, or it may display (read-only) the non-blank auto-dial entry label made in Communication Manager running on the communication manager server for the associated button. In the latter case, the entry may not be edited here. The maximum length of any Label field entry is 20 UTF-8 characters. Note that UTF-8 characters can include ASCII, Kanji and Kana characters. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser’s language setting.

Used with SP-1020A, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name.)

Note:

The Toshiba Business Phone (SP-1020A) does not display half-width, Han Kaku Kana characters.

One Touch Dial List screen commands

Save

Commit the one touch dial information to the database.

Ringer Settings screen

This screen lets you turn the ringer on and off for the user, and shows information about the telephone's bridged appearance. This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

Ringer Settings screen field description

Button

This field shows one or more numbers designating the bridged appearance buttons on a telephone for which you may turn the ringer on or off (and independent of and not reflecting the OPS settings for the station in Communication Manager running on a communication manager server).

Setting the ringer settings is for the station's bridge appearance buttons. This is not related to ringer settings configured on Communications Manager.

Bridged Appearance

Lists the communication manager server extension associated with this telephone button in the user database. This field may contain a maximum of 256 alphanumeric characters.

Ringer ON/OFF

If the ringer of any available button is set to off, you may select the radio button under On to enable its ringer. Likewise, if it is set to On, you may select the button under Off to disable it.

Ringer Settings screen command

Save

Commit the ringer settings to the database.

Tone and Volume screen

This screen is view only for the administrator, and provides a list of how the tones, volumes and speed of the user's telephone device were set by the user.

This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

Ringer Cadence

Displays the default Ringer Cadence (default is 2) for the device administered for end users in the database. This number represents the speed of the telephone's ringing (1 through 3).

Ringer Volume

Displays the default Ringer Volume (default is 5) for a device administered by end users in the database. This number represents how loudly the telephone will ring. The range is 1 through 10.

Receiver Volume

Displays the default Receiver Volume (default is 5) for a device administered by end users in the database. This number represents handset loudness (1 through 10).

Speaker Volume

Displays the default Speaker Volume (default is 5) for a device administered by end users in the database. This number represents speakerphone loudness (1 through 10).

Delete All Displayed Users task

This task lets you delete all the users currently displayed without having to check the boxes to the left of the name. This is useful after a search has properly returned a group of users.

After carefully checking the list of names on the List User's screen, select either OK or Cancel.

Click Delete All Displayed Users, then the Submit button to delete all the users listed. When asked to delete the extensions also, check that box if you want to prevent that extension from being used later.

You may also select individual users' check boxes, and then highlight Delete Selected Users.

Delete Selected Users task

Delete more than one user at a time by checking several check boxes. You can mark many check boxes and delete up to 68 users at one time. Select and confirm your decision to delete a user.

When asked to delete the extensions also, check that box if you want to prevent that extension from being used later.

Extensions task

This section describes administering a specific user's extension.

Tip:

You can refer to List Communication Manager Server Extensions screen to look up information about extensions on the Communication Manager communication manager server, perhaps to make more extensions available.

With the screen described here, you can associate an extension with a user, remove an extension from a user, or free an extension for use by any other user with this screen series. List Communication Manager server Extensions screen field descriptions

Extension

The numeric telephone extension in the database.

This is the extension for the user named at the top of the screen.

User

This is the User ID assigned when the user was added to the system.

See User ID on page 145.

Communication Manager server

The name of the communication manager server the extension was assigned to.

Host

This is the name of the home server for this user.

List Communication Manager server Extensions screen commands

Free

This command removes an extension from the user named at the top of the screen, but keeps it available on the communication manager server for reassignment. Select this to show an OK or Cancel screen.

Edit User

For the convenience of the administrator, this selection lets you display this user as the only user in the list. Pick a task from the drop-down list.

Delete

This command deletes an extension from the user in the database. The user remains, but no longer has this extension associated with him or her.

Select this to show an OK or Cancel screen.

List Communication Manager server Extensions when user has none

Sometimes, when asking to see the communication manager server extension for a user, there is none. That is, a user may not have yet been assigned an extension, or may have had the extension removed for some reason.

If a user has no assigned extension, the system displays the List Communication Manager server Extensions screen.

Tip:

If you want to look up information about extensions on the Communication Manager communication manager server, perhaps to make more extensions available, see the menu for the Communication Manager screen.

Add Another Communication Manager server Extension

This link takes you to the Add Communication Manager server Extension screen, so that you may create an extension and assign to the user.

Assign Free Communication Manager server Extension

This link takes you to the Select Free Extension screen.

There, click on the pull-down list and select an extension that is already created and assigned to a communication manager server on the user's home. That extension is assigned to the user displayed here.

Add Another Communication Manager server Extension screen

Create a communication manager server extension for a user who does not have one. This screen only sets up the extension in SES. Administer that extension on the Communications Manager soon.

Tip:

If you want to look up information about extensions on the Communication Manager communication manager server, perhaps to make more extensions available, see the menu for the Communication Manager Server screen.

Add Communication Manager server Extension screen field descriptions

Extension

The numeric telephone extension in the database.

Enter the numeric telephone extension you want to create as an extension.

The entered extension must be administered on the communication manager server running Communication Manager before the extension becomes functional.

Communication Manager server

Select the network name for the extension's communication manager server interface from the drop-down list.

The node name in alphanumeric characters associated with the communication manager server's C-LAN (or processor C-LAN) IP interface. For more information on IP node names, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Add Communication Manager server Extension command

Add

Select **Add** to create a new entry for this communication manager server extension in this SIP proxy server's database.

Note:

This will not create any extensions or change any existing administration performed directly through Communication Manager on the associated communication manager server. You have to do that manually from the Communication Manager interface.

Select Free Extension screen

You may want to check on Communication Manager to make sure that the extension is administered there.

Select **Assign a Free Communication Manager server Extension**.

This screen lets you choose an unused extension from the available extensions for the communication manager server. When you first add a user, you are not required to assign a media extension. To provide one later, use this screen.

Extension

Click this drop-down list to see what extensions are currently available for assignment. Select an extension from this list.

Select

Make your selection permanent.

Handles task

The Handles task concerns the contact points at which the end user can be contacted.

One way to get to this screen is to select List Users, find the user you want, and click the check box. From the task drop-down list select **Handles**. Click **Submit**.

Handles may be:

- Totally numeric, as in a telephone number
- Totally characters, as in a name
- A mix of alphanumeric characters, but no special characters other than dash.

Handles must be unique across the SIP domain.

IDo not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- handle_list
- presenceserver

In addition:

- All handles must be between 3 and 16 ASCII characters in length.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.

- All handles must be entered in lower case.
- All handles must be unique.
- All handles must be alphanumeric with no special characters other than dash (-).

Edit User Handles screen field descriptions

User ID

This is an identifier of at least three alphanumeric characters in length. Each administered user has one unique User ID and it is used as their display name within SES administration. For example, the User ID is the name listed for the user on the List Users, Search User, Edit User and List Communication Manager server Extensions screens.

It is recommended that the User ID be the same as the Primary handle administered for the user. If the User ID is left blank when the user is added, it is defaulted to the Primary handle.

A User ID is administered as an alphanumeric string between 3-16 characters in length.

A user's User ID may be changed from their Edit User Profile screen. A user's Primary handle may only be changed from the Edit Handle screen (List Users -> Select A user -> Select Handles task).

Handle

A handle identifies the user on the SES system. Users' primary handles must be the same as their user IDs. Selecting this link displays the detailed user contact information for the SIP user. User handles must be unique within the SES system domain. Users may have multiple handles to accommodate more than one personal point of contact.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Contact

In this screen, the information in the Contact column is the SIP address of the user, which is created based on the user's telephone extension and the IP address of the communication manager server this user is assigned to.

Edit User Handles screen commands

Edit (Handle)

Go to the Edit Handle Detail screen for that user's handle for the associated user Contact.

Delete (Handle)

Display the **Confirm Delete Handle** screen for that user's handle. The handle that has no Delete command next to it is the primary handle for the user and cannot be deleted.

Add Another Handle

You may select **Add Another Handle** to provide another handle for the user ID named at the top of the screen. Users may have several handles, but each must be unique within the SIP domain to which they belong.

Edit (Contact)

Select Edit next to the contact information to change the information about this user's personal point of contact.

Delete (Contact)

Display the **Confirm Delete Contact** screen to delete a personal point of contact for the user named at the top of this screen.

Add Another Contact

Select this link to add another point of contact for the SIP user named at the top of the screen.

Add Handle in New Group

A group is a set of handles that resolves to a set of contacts. At this time, the SES system supports only one level of hierarchy for groups.

Select **Add Handle In New Group** to go to the Add Handle in a New Group screen. There, you can create a new group to add a handle to.

Delete Group

Select **Delete Group** to display the **Confirm Delete Group** screen. When viewing the confirmation screen, you may choose to delete the group and all of its members, or to delete only the group association of the members, and leave the member user contacts available.

Edit Handle detail screen

Change the users handle at with this screen.

Edit Handle detail screen field description

User ID

This is an identifier of at least three alphanumeric characters in length. Each administered user has one unique User ID and it is used as their display name within SES administration. For example, the User ID is the name listed for the user on the List Users, Search User, Edit User and List Communication Manager server Extensions screens.

It is recommended that the User ID be the same as the Primary handle administered for the user. If the User ID is left blank when the user is added, it is defaulted to the Primary handle.

A User ID is administered as an alphanumeric string between 3-16 characters in length.

A user's User ID may be changed from their Edit User Profile screen. A user's Primary handle may only be changed from the Edit Handle screen (List Users -> Select A user -> Select Handles task).

With this screen, you can change the handle for this User ID.

Handle

A handle identifies the user on the SES system. Users' primary handles must be the same as their user IDs. Selecting this link displays the detailed user contact information for the SIP user. User handles must be unique within the SES system domain. Users may have multiple handles to accommodate more than one personal point of contact.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- handle_list
- presenceserver

In addition:

- All handles must be between 3 and 16 ASCII characters in length.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique.
- All handles must be alphanumeric with no special characters other than dash (-).

Edit Handle detail screen command

Update

Select Update to commit the information to the database.

Edit Host Contact screen

This screen lets you change the contact associated with a specific handle. Do not use this screen to change contacts assigned to the user by the SES system. Use this screen to edit communication manager server contacts associated with a user's extension.

Edit Host Contact screen field descriptions

User ID

The user ID for whom you want to name a new host contact to redirect calls to.

Contact

Enter a point of contact for the selected user's handle. This contact is usually a fixed destination.

The **Communication Manager server contact type** is for all handles that should be resolved to contacts that are routed directly to a communication manager server. This only includes handles that are also extensions, because communication manager servers only recognize extensions, not alphanumeric handles.

If you select the communication manager server contact type, the entered Contact pattern should be a contact that includes a communication manager server IP address.

If you select the Communication Manager server contact radio button, the system is expecting that the corresponding contact is a communication manager server contact. If you select the Communication Manager server contact type, and the corresponding contact is *not* a pattern recognized by the communication manager server, then calls may not get routed.

The **User contact type** is used for all handles that should be resolved to contacts that are directly routed to addresses that are *not* communication manager servers. This includes other home servers, or devices that are not connected to a communication manager server.

If you select the User contact type, the entered Contact on the page should be a contact that is *not* a communication manager server IP address.

If you select User contact type, and the corresponding contact is a communication manager server, then calls may get routed to the communication manager server but not complete.

Contact Type

Communication Manager server or User

Edit Host Contact screen commands

Communication Manager server option

Specify that the information in the Contact field is a users primary SIP contact address that is recognizable by the communication manager server. The call will route successfully through the communication manager server.

User option

Indicate that the information in the Contact field is not a user's primary SIP contact address, and should not be routed through the communication manager server.

Update

Commit your changes to the database.

Add Handle screen

This displays when you select Add Another Handle command on the Edit User Handles screen. Use this screen to provide a SIP user with an additional handle that routes calls differently.

Add Another Handle screen field descriptions

User ID

An identifier of at least three alphanumeric characters in length, used to authenticate a user.

Handle

A handle identifies the user on the SES system. Users' primary handles must be the same as their user IDs. Selecting this link displays the detailed user contact information for the SIP user. User handles must be unique within the SES system domain. Users may have multiple handles to accommodate more than one personal point of contact.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

This is never the primary handle, which is defined in the Add User screen.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- handle_list
- presenceserver

In addition:

- All handles must be between 3 and 16 ASCII characters in length.

- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique.
- All handles must be alphanumeric with no special characters other than dash (-).

Add Another Handle screen command

Add

Commit this additional information to the user database.

Add Host Contact screen

The Add Host Contact screen allows an additional point of contact to be added for the selected handle. For user contacts that are not extensions, the Contact Type should be User.

Add Host Contact screen field descriptions

User ID

An identifier of at least three alphanumeric characters in length, used to authenticate a user.

Handle

A handle identifies the user on the SES system. Users' primary handles must be the same as their user IDs. Selecting this link displays the detailed user contact information for the SIP user. User handles must be unique within the SES system domain. Users may have multiple handles to accommodate more than one personal point of contact.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Contact and Contact Type

Enter a point of contact for the selected user's handle. This contact is usually a fixed destination.

The **Communication Manager server contact type** is for all handles that should be resolved to contacts that are routed directly to a communication manager server. This only includes handles that are also extensions, because communication manager servers only recognize extensions, not alphanumeric handles.

If you select the Communication Manager server contact type, the entered Contact pattern should be a contact that includes a communication manager server IP address.

If you select the Communication Manager server contact radio button, the system is expecting that the corresponding contact is a communication manager server contact. If you select the Communication Manager server contact type, and the corresponding contact is *not* a pattern recognized by the communication manager server, then calls may not get routed.

The **User contact type** is used for all handles that should be resolved to contacts that are directly routed to addresses that are *not* communication manager servers. This includes other home servers, or devices that are not connected to a communication manager server.

If you select the User contact type, the entered Contact on the page should be a contact that is *not* a communication manager server IP address.

If you select User contact type, and the corresponding contact is a communication manager server, then calls may get routed to the communication manager server but not complete.

Add Host Contact screen commands

Communication Manager server option

Specify that the information in the Contact field is a user's primary SIP contact address that is recognizable by the communication manager server. The call will route successfully through the communication manager server.

User option

Indicate that the information in the Contact field is not a user's primary SIP contact address, and should not be routed through the communication manager server.

Add

Confirm to add the new host contact you have set up.

Add Handle in a New Group screen

Add Handle in New Group displays an Add Group screen that is specifically for groups of handles that resolve to the same User Contact in the database. Stated another way, use this screen to start a new group and add a new line for handles and contacts to resolve to.

A group is a set of handles that resolves to a set of contacts. At this time, only one level of hierarchy for groups is supported.

Even though the screen title says Add Group, you are adding the handle in the required field to the group you selected previously.

Add Group screen field descriptions

User ID

An identifier of at least three alphanumeric characters in length, used to authenticate.

Handle

In this screen, enter a handle of any end user to include them in this group.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- handle_list
- presenceserver

In addition:

- All handles must be between 3 and 16 ASCII characters in length.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique.

- All handles must be alphanumeric with no special characters other than dash (-).

Add Group screen commands

Add

Add the handle to the database in the new group of handles that you specified.

User Memos screen

This screen lets administrators write memos about a user. The memos are available only to another administrator looking at this screen. End users do not see this information.

User Memo screen field descriptions

User ID

An identifier of at least three alphanumeric characters in length, used to authenticate a user.

List of memos

The available memos display in chronological order, most recent at the top.

Add Memo box

Write a new memo about the user inside this text box.

Delete

Remove the memo to the left.

Add Memo button

Select this button to store the memo in the area above.

Move User Task

The Move User task lets you easily select and move a single user to a different home server if one is available in your architecture.

Select the user to move with the check box, select Move User in the Task pull-down list, and click submit. The pull-down list for the New Host field lets you see what home servers are available to move to.

Select the new home and click OK.

After moving a user, you may have to go to the communication manager server and log in there. Then, using the `off-pbx-telephone station-mapping` form, check the moved user's SIP trunk. Change the form if necessary.

The system displays a confirmation to allows you to cancel the move.

Moving a user to another home server

In this procedure, the destination home server must be fully functional.

If you are moving a user to another home server, and that home server is associated with two or more communication manager server interfaces, you will be prompted to select one of those interfaces.

If the user has a communication manager server extension and the destination home does *not* have an administered communication manager server, the Move User operation cannot be completed. The move may only be completed if a communication manager server is added to the destination home or the user's extension is removed or freed.

1. From the Administrator interface, go to the **List Users** screen.
2. Select the **check box** next to the user you want to move.
3. Click the **Move User** task in the pull down menu.

   The system displays a Move User page.

   Select the new home server using the **New Host** drop-down box.

   Only those homes that the user can be moved to are displayed in this box. All home servers that exist are not shown. The **New Host** drop-down box does not contain the user's current home.

   If a home server connects to a communication manager server that contains more than one communication manager server interface, the drop-down menu displays both interfaces for you to choose from.
4. Press OK or Cancel.

   The update procedure is performed by the system.

5. On Communication Manager, change the SIP trunk for the extension of the user with the form off-pbx-telephone station-mapping form.
6. On the Toshiba Business Phone SP-1020A, log out and log in. Other telephones in your system may require additional procedures.

Permissions screen

The Permissions page manages a user's control over presence, who they permit to see them on the system. This page has four versions, depending on the current setting, and every page allows the setting to be changed to the other type.

- Unblocked watchers are not updated until after the telephone user logs off and logs back in.
- Presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.

Permissions screen field descriptions

Current Permissions Type

Note the type of Permissions that now are set for the user. The types of Permissions are **Allow All**, **Block All**, and **Contact List Only**. **Block All** is the default permission type for any user unless you specify a different type of permissions or modify the user's permissions. To modify the current Permissions type that is displayed for this user, you may use Permissions screen.

Change Permissions Type

The drop-down list provides three levels of permissions:

- Allow All—Select **Allow All** if you want all administered SIP users to be able to watch this user's presence and availability in the system, using any presence-enabled SIP client like Avaya IP Softphone.
- Block All—Select **Block All** if you want no administered SIP users to be able to watch this user's presence and availability in the system.
- Contact List Only—Select **Contact List Only** if you want only those administered SIP users that you have added to your contact list to be able to watch this user's presence and availability in the system.

After selecting the appropriate permissions type, select the Change button to commit the entry to the user contact database.

Note that unblocked watchers are not updated until after the telephone user logs off and logs back in.

Handle

This is a selectable link, a valid handle for the blocked or allowed caller. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique contact Uniform Resource Identifiers (URIs) within the SIP domain, but users may have several.

Note:

If entering or changing the Handle, only provide characters for the portion in front of the `@` sign. The system automatically appends the `@systemdomain.com` portion of the handle.

Permissions screen commands

Change Permissions Type

Choose from the drop-down list of user-contact permissions:

Allow All — permits all administered SIP users to note your presence in the system.

Block All — permits *no* administered SIP users to note your presence in the system.

Contact List Only — lets only those administered SIP users on the user's contact list to be able to observe your presence in the system.

Note that unblocked watchers are not updated until after the telephone user logs off and logs back in.

Allow List/Block List

Lists any users for whom there are discrete entries to Allow permission or Block permission to watch this user's presence and availability on the system. If the Current Permissions Type is set to **Contact List Only**, then the Allow List/Block List does not display. Instead, you may select the link to view the members who are allowed to watch this user's presence and availability in the system. If you wish to delete the **Block** (or **Allow**) permission type entry for a specific person on the list, then select the Remove link.

Note:

If you didn't specify a domain for a user on either list, then the SIP system *domain.com* will be appended automatically to the user contact entry.

Add Entry

Use this area to add a valid user handle to one of the two permissions lists, Allow or Block. To remove a permission entry, select from the **Allow List/Block List** field.

Note that unblocked watchers are not updated until after the telephone user logs off and logs back in.

Edit User Profile screen

For specific details about this screen, see the Add User screen.

The User Profile screen contains specific demographic information about this user. This screen is originally populated by the default user profile data.

This screen supports UTF-8 encoding. You may input Shift_JIS (SJIS) characters as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

Watchers Task

The Watchers screen quickly relays the level of watch permissions this user has set. Then, with the command buttons, you can adjust that level using either the Permissions screen or the Contacts list.

Note that unblocked watchers are not updated until after the telephone user logs off and logs back in.

Watchers screen field descriptions

Current Permissions Type

Note the type of Permissions that now are set for the current user. The types of Permissions are **Allow All**, **Block All**, and **Contact List Only**. **Block All** is the default permission type for any user unless you or the user specify a different type of permission, or modify the user's permissions. To modify the current Permissions type displayed for this user, you may use **Change Permissions Type** field on the Permissions screen.

Tip:

Changing the Current Permissions Type does not interactively add or delete existing exception entries made on the Allow List/Block List. That is, if you change from Block All to Allow All, then any exceptions on the Block List remain in effect. Likewise, if you change from Allow All to Block All, then any exceptions on the Allow List remain in effect.

Contact List Members

This area of the screen lists members of the end user's contact list who are aware of the end user's presence, that is, who have subscribed to be updated on your presence and availability in the system. If no such users exist and are subscribed, then this field does not appear on this page.

Note that presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.

Select the associated link to the right to **Block** a **Contact List Member** from being able to watch your presence and availability in this system.

Unknown (SIP Users)

Lists any SIP users not on the contact list, but provisioned in this system, and for whom you have added discrete entries to **Allow** permission to watch your presence. If no such entries have been made, this field does not appear on this page. If you wish to **Block** permission for a specific unknown SIP user from being able to watch your presence and availability in this system, then select the link to the right of the list entry. To change the default permissions for all SIP users, then select the **Go To Permissions** link and use the **Change Permissions Type** field on the Permissions screen. If you want to add any of the SIP users who are unknown to this system to your list of (known) user contacts, for example to watch their presence and availability, then you may select the **Add to Contact List** link to the right of any **Unknown** list member.

Note that presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.

Watchers screen commands

Go to Permissions

Select this to change the current level of permissions for the user. The system displays the Permissions screen.

Go to Contact List

Select this to add more contacts to the users contact list. Doing so makes the permission type of Contact List Only more inclusive.

Search User screen

Locate any user on the system by searching on any of the fields in this screen.

On the left, open up the **Users** menu and select **Search** from the sub-menus.

Fill in any of the fields to try and match. If any matches are found, the List Users screen that displays next shows only the matches.

Search Users screen field command

Search

After you've entered the information on which you want to match in the database, select **Search**.

The system displays the List Users screen.

Select User screen

The Select User screen is available from the Users menu and three of its submenus:

- Users>Edit
- Users>Delete
- Users>Password

This click path provides a quick way to select a user for the tasks above when you are certain of the user's ID.

Select User screen field description

User ID

This is an identifier of at least three alphanumeric characters in length. Each administered user has one unique User ID and it is used as their display name within SES administration. For example, the User ID is the name listed for the user on the List Users, Search User, Edit User and List Communication Manager server Extensions screens.

It is recommended that the User ID be the same as the Primary handle administered for the user. If the User ID is left blank when the user is added, it is defaulted to the Primary handle.

A User ID is administered as an alphanumeric string between 3-16 characters in length.

A user's User ID may be changed from their Edit User Profile screen. A user's Primary handle may only be changed from the Edit Handle screen (List Users -> Select A user -> Select Handles task).

Select User screen commands

Edit User

Select Edit User to edit the user’s profile.

Update Password screen

This is the screen on which you change a user’s password for them. This screen is preceded by a the Select User screen that requires the user ID.

Update Password screen field descriptions

User ID

An identifier of at least three alphanumeric characters in length, used to authenticate a user to the system.

Password, Admin_Password_Confirm

Enter a password of at least 6 and at most 12 alphanumeric characters. Both field entries must match exactly.

Update Password screen command

Update

After entering and confirming the new password, select **Update** to submit it to the database.

Default Profile

Use of this screen usually occurs when the system is first installed and configured.

Moving a user to another home server from Edit Profile screen

In this procedure, first verify that the home server that is the destination for the move is fully functional.

If the user has a communication manager server extension and the destination home server does not have an administered communication manager server, the Move User operation cannot be completed. The move may only be completed if a communication manager server is added to the destination home or the user's extension is removed or freed.

If your are moving a user to a home that links to a communication manager server with more than one C-LAN interface, you will be prompted to select one.

Move user can also be done from the List Users screen.

1. From the Master Administration interface go to the Edit User Profile screen.
2. Select the Host field to display a drop-down menu of all home servers.

   The drop-down defaults to highlight the user's current home server.
3. Select another home server from the drop-down.

   If a home server connects to a communication manager server that contains more than one communication manager server interface, the drop-down menu displays both interfaces for you to choose from.
4. Select **Update**.
5. The system displays a Move User confirmation screen.

6. Press Accept or decline. OK or Cancel.
7. The system performs an update.
8. In Communication Manager on the administered communication manager server, change the SIP trunk for the extension of the user using the **off-pbx-telephone station-mapping** screen.
9. On the Toshiba Business Phone SP-1020A, log out and log in. Other telephones in your system may require additional procedures.

Confirm Delete User screen

This screen is preceded by a Select User screen that requires the user ID of the user you want to delete.

Confirm Delete User screen field descriptions

Confirm Delete

Informs you of which user you have selected for deletion from the database.

Delete Extensions Also

Check this box to delete the communication manager server extensions associated with this user. This user's extensions are deleted from the database as well. Leave the box unchecked, the default, to leave the unassociated extensions free for future use.

Confirm Delete User screen commands

OK

Select **OK** to delete the user (and associated extensions, if applicable).

Cancel

Select **Cancel** to ignore your delete choices, keeping the user and associated extensions in the database unchanged.

Search Registered Users

This screen is available only from a home server.

On the home server, you can search and find registered and provisioned users on the home server you are logged in to.

Search Registered Users screen field descriptions

Handle

The handle identifies the user uniquely within the SES system. The user's handle is the same as the user's ID.

First Name, Last Name, Address

This is the demographic data of the user. Because an exact match is required on these fields, use them carefully.

Include Registered Users

Select this check box to find users who match the criteria above and who are currently registered on the system.

Be sure to check either this check box or the one for Include Provisioned Users.

Include Provisioned Users

Select this check box to find any users matching the criteria in the fields that are set up on your system, even though they may not be currently registered with their home server.

Be sure to check either this check box or the one for Include Registered Users.

Search Registered Users screen commands

Search

Click this button to start the search.

Registered and Provisioned Users Search Results screen

After using the Search Registered Users screen, the search results are displayed in this screen.

Notice in the search results screen, some users are provisioned, and some are both provisioned and registered. Provisioned users are administered as users on the system, but are not currently logged in to their phone. Registered users are logged in with a user name and password from their phone.

If a provisioned user is not registered, you cannot perform any actions from the task list, such as reload, or reboot, on that phone.

The commands at the top of this screen further refine your search results. Based on the results of your original search, you can see just registered users, just provisioned users, or both.

By selecting the check box next to the handle of a registered user, you can perform action from the task list to just the selected user.

By selecting the check box at the bottom, you can perform actions in the task list to all users on the home server or on the current page.

Registered and Provisioned Users Search screen field descriptions

Handle and Name

This is the handle, first name and last name found in the user’s profile.

Address

This is the contact address of the user.

Type

The Type column shows if the user is provisioned, registered, or both.

Expires

If the user is registered, this column shows when the session will expire.

Registered and Provisioned Users Search screen commands

Registered and Provisioned Users

Click this to re-display your original search results to show both registered and provisioned users.

Registered Users

Click this to re-display your original search results to show only registered users.

Provisioned Users

Click this to redisplay your original search results to show only provisioned users.

Search

Click this to redisplay the Search Registered Users screen and begin a new search.

Refresh

Click this button to re-search and see any alterations in the previous result.

Apply to all registered users with compatible devices on this home.

Select this check box to perform an action from the task list to all the registered users with compatible devices on this home.

Apply to all registered users with compatible devices on the page.

Select this check box to perform an action from the task list to all the registered users with compatible devices on this page.

Reload - complete

Select this to completely reload software from the server to the device of all rows selected.

Reload - configuration

Select this to reconfigure the users' device for all selected.

Reload configuration can also be done from the edge server’s administration interface by clicking Users > List > select a user > Contact List > Reload Configuration.

Reload - maintenance

Select this to reload only maintenance data to the phone. Personal data of the user will not be affected.

Reboot

Select this to instruct the users’ device to reboot itself, that is, to reload its firmware for all selected users.

The user will have to log in again with a user name and password.

Status

This action is valid only when a single user is selected. This action is not available if you select the "Apply to all …" check boxes.

Select this to instruct the user's device to report its current status to the server.

Manage All Registered Users screen

This screen is available only from a home server.

This screen lets you perform reloads and reboot the all the users’ phones on the home server you are logged in to. This screen covers the situation when a user is administered without hardware.

Manage All Registered Users screen commands

Reload-complete

Select this to completely reload software from the server to the device of all rows selected.

Reload-configuration

Select this to reconfigure the users' device for all selected.

Reload configuration can also be done from the edge server's administration interface by clicking Users > List > select a user > Contact List > Reload Configuration.

Reload-maintenance

Select this to reload only maintenance data to the phone. Personal data of the user will not be affected.

Reboot

Select this to instruct the users' device to reboot itself, that is, to reload its firmware for all selected users.

The user will have to log in again with a user name and password.

Submit

Perform the tasks selected above.

Search Registered Devices

This screen is available only from a home server.

This screen searches for devices on the home server you are logged in to. When you find a device or several devices, you can perform reload and reboot procedures to just those devices, or a subgroup of those devices.

The results screen for shows you the device's firmware version, the type of hardware, the MAC address of the device, and the user of the device, and whether the device is provisioned or registered.

Search Registered Devices screen field descriptions

Handle

This is the handle found in the user's profile.

Program Version

This is the firmware version of the user's device.

Phone Type

The type of phone or the model number of the users' device.

Registered Users Only

Select this check box to find only those users who match the criteria above *and* who are currently registered on the system.

Search Registered Devices screen commands

Search

Click this button to start your search.

Search Registered Devices Results screen

This is the screen displays when you have searched for devices on this home using the Search Registered Devices screen.

Notice in the search results screen, some devices are provisioned, and some are both provisioned and registered. Provisioned devices are administered on the system, but are not currently logged in.

The commands at the top of this screen further refine these search results. Based on the results of your original search, you can see just registered devices, just provisioned devices, or both.

By selecting the check box next to the handle of a registered device, you can perform actions from the task list to just the selected device.

By selecting the check box at the bottom, you can perform actions in the task list to all devices on the home server or on the current page.

Search Registered Devices Results screen field descriptions

Handle

This column shows the handle of the user of this device.

Program Version

This column shows the version of software or firmware the endpoint or device uses. This information is taken from the phone. That is, it is not entered in the user record.

MAC Address

This column shows the MAC address of the endpoint or phone.

Phone Type

This column shows the kind of phone hardware. This information is taken from the phone. That is, it is not entered in the user record.

Type

This column shows if the phone is provisioned, registered and in use, or both.

Search Registered Devices Results screen commands

Registered and Provisioned Users (Devices)

Click this to redisplay your original search results to show both registered and provisioned devices.

Registered Users (Devices)

Click this to redisplay your original search results to show only registered devices.

Provisioned Users (Devices)

Click this to redisplay your original search results to show only provisioned devices.

Search

Click this to redisplay the Search Registered Devices screen and begin a new search.

Refresh

Click this button to re-search and see any alterations in the previous result.

Apply to all registered users (devices) on the home.

Apply to all registered users (devices) on this page.

Reload-complete.

Select this to completely reload software from the server to the device of all rows selected.

Reload-configuration

Select this to reconfigure the users' device for all selected.

Reload configuration can also be done from the edge server's administration interface by clicking Users > List > select a user > Contact List > Reload Configuration.

Reload-maintenance

Select this to reload only maintenance data to the phone. Personal data of the user will not be affected.

Reboot

Select this to instruct the users' device to reboot itself, that is, to reload its firmware for all selected users.

The user will have to log in again with a user name and password.

Status

This action is valid only when a single user is selected. This action is not available if you select the "Apply to all …" check boxes.

Select this to instruct the user's device5 to report its current status to the server.

Submit

Perform the tasks selected above. Select this to completely reload software from the server to the device of all rows selected.

Select this to reconfigure the users' device for all selected.

Reload configuration can also be done from the edge server's administration interface by clicking Users > List > select a user > Contact List > Reload Configuration.

Select this to reload only maintenance data to the phone. Personal data of the user will not be affected.

Select this to instruct the users' device to reboot itself, that is, to reload its firmware for all selected users.

The user will have to log in again with a user name and password.

SIP Phone Settings screens

SIP phone users with an Avaya one-X Deskphone R2. 0 can log in to any phone in the enterprise and receive their own individualized services and menus, contacts, buddy list and so on.

When a user is visiting, they may or may not be accessing their usual SES home server. If they are not, the visited home server receives data from the usual home server to provide menus, contact, permissions, and other individualized aspects of the user's phone.

For phones designated a visiting, an inactivity timer notifies the user before a visiting session expires, even if the timer is set to null.

An overview of this architecture is available for reading on SES visiting user on page 16.

- Visiting user on page 198
- List Default Settings screens on page 199
- List Group Settings screen on page 206
- Download Maintenance Data screen on page 209

You must restart an 96xx Avaya one-X Deskphone to download the latest values from the settings file. After making any changes at all, use the Download Maintenance Data screen.

Order of precedence for SIP settings

The are two values, active and persistent, saved for each phone parameter. The active value is what the phone is currently using and the persistent value is the value that is currently administered.

When you change the Visiting User mode or Quick Login Status values in the Master Admin screens, and download them to the phone, these values appear as the persistent value. They are not copied into the active value until the phone does its next logout. This also means the MIB will not display the most recently downloaded value of VU_MODE and QKLOGINSTAT until the next phone logoff.

Also understand that there is an order of precedence between the settings.txt file, the master administration interface, and the phone firmware.

- Server settings override settings.txt file
- Settings.txt file overrides the phone firmware

The order of precedence, from lowest to highest, for determining all SIP phone data, is this:

1. Phone firmware defaults
2. settings.txt file
3. SNMP On/Off Master Admin data
4. Manual setting on the phone

Visiting user

There is no need to change the settings.txt file. Do these tasks in any order:

- Use the screens in this section to set parameters for individuals and groups that want to have a visiting user attributes.
  - List and edit common parameters
  - List and edit group parameters
  - Download data to the phone
- Administer Communication Manager using the Feature Related System Parameters screen, page 3, and set the EMU field to 1 for a one hour visiting user session, 2 for a 2 hour session, and so on.
- Using the SIP PIM interface:
  - Administer which device is active for visiting user sessions
  - Set other visiting user parameters, such as visiting user mode and quick login status.
  - Refer the user to their user guide for that interface, *SES Personal Information Manager*, doc ID 03-300441.

List Default Settings screens

Displays the settings administered for the SIP phones on your system. You can use this screen to administer the following settings:

- •IP addresses for SNMP Queries
- •SNMP community string
- •Station administration password
- •Visiting user mode
- •Quick login status
- •Reactive monitoring interval
- •Timer B
- •Failback policy
- Registration policy

This screen displays only the settings that have been configured. You may use all or some of the parameters available. To configure a setting that is not displayed, click Add Settings.

Edit and remove the parameters listed one at a time. For example, to edit the visiting user mode, click the Edit link on the right. You are presented with a screen to change that parameter only.

Removing a parameter turns it off *and* removes it from this screen. To re-enable the parameter, click the Add Settings button. On the ensuing screen, you are permitted to add any of the other remaining parameters.

You must restart a 96xx phone to download the latest values from the settings file.

List Default Settings screen field descriptions

Parameter Name

IP Address for SNMP Queries—This is the IP address of a server, that has the correct community string, that can query the phone for SNMP messages. If this field is blank, any server can query the phone.

SNMP community string—This string is both a challenge and a response for the server named in the IP address above and the phone. If a server IP address is named, both the server and the phone must have the same community name administered.

Visiting user mode—Off, Optional, or Forced.

Off —Never ask about visiting when the user logs in.

Optional—Have the phone display a prompt to ask if the user is a visiting user or is the primary user.

Forced—Always make this device a visiting phone.

Before a visiting user session is terminated, the phone provides a message.

Quick login status:

Password Entry Required -- No quick log in. Users must always type in an ID and password.

Quick log in Allowed -- Phone users just press the Continue button on the phone.

Station admin password—The Station Admin password is the code that an administrator enters on a SIP phone. This allows the administrator to log into the actual phone to administer it.

This is the PROCPASSWD in the 46xxsettings.txt file.

Reactive Monitoring Interval— Specifies how often (in seconds) the phone will attempt to REGISTER with a proxy server when it is not reachable/available. Range is **10** to **3600** seconds. The default is **60** seconds. This parameter is only used by phones that support survivability features, such as the Avaya one-X Deskphone SIP R2.1 or later 9600 series phones.

Timer B— Specifies whether a phone will automatically revert to using a higher priority proxy server whenever one becomes available. Valid entries are **Auto** and **Admin**. The default is **Admin**. This parameter is only used by phones that support survivability features, such as the Avaya one-X Deskphone SIP R2.1 or later 9600 series phones.

Failback Policy— Specifies how long (in seconds) the phone will wait for a provisional response after transmitting a SIP INVITE to a proxy server before assuming that proxy is unavailable/ unreachable and proceeding to another proxy. The range is **0** to **32** seconds. (**0** disables this feature.) The default is **2**. This parameter is only used by phones that support survivability features, such as the Avaya one-X Deskphone SIP R2.1 or later 9600 series phones.

Registration Policy—Specifies how the phone registers. Choices are **Alternate** and **Simultaneous**.

Parameter Value

This column shows the values you have chosen for the parameter.

List Common Parameters screen field commands

Add Settings

If you have not selected to employ all of the visiting user parameters available, this link displays. Click this to add another parameter to the list.

Edit

Click on the Edit button to the right of the parameter to display the Edit Parameter screen. You can only edit the parameter you select, but you will see all the parameters you have previously selected.

Remove

Click Remove to disable a parameter and remove it from display in the list.

Add Settings screen

This screen lets you add, modify, or remove the selected phone attributes. Your choices are reflected in the List Phone Settings screen.

You must restart the 96xx phone to download the latest values from the settings file.

Add Settings screen field descriptions

Group ID

A group ID lets you collect 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. The values you specify here apply to all phones in the group.

Edit and remove the group parameters listed one at a time. For example, to edit the visiting user mode, click the Edit link on the right. You are presented with a screen to change that parameter only.

Changing the group ID for a 96xx phone causes the phone to restart and reboot. In addition, you must send a reload command as well when changing group data.

To include a phone in a SIP phone group, see Adding a phone to a group on page 209.

SNMP Community String

This string is both a challenge and a response for the server named in the IP address 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.

Note:

If a value is put into the SNMP string in the settings file for the phones, you will be unable to disable SNMP queries.

Visiting User Mode

Lets you specify whether the phone will prompt users about the Visiting User feature during login. Choices are:

Off —The phone will not prompt the user about the Visiting User feature when the user logs in to the phone.

Optional—The phone will prompt the user to specify whether the user is a visiting user or the primary user when the user logs in to the phone.

Forced—The phone will prompt the user to log in as a visiting user. The user must log into the phone as a visiting user.

Before a visiting user session is terminated, the phone provides a message.

Quick Login Status

Password Entry Required -- No quick log in. Users must always type in an ID and password.

Quick log in Allowed -- Phone users just press the Continue button on the phone.

IP Addresses for SNMP Queries

This is the IP address of a server, that has the correct community string, that can query the phone for SNMP messages. If this field is blank, any server can query the phone.

Station Admin Password

The Station Admin password is the code that an administrator enters on a SIP phone. This allows the administrator to log into the actual phone to administer it.

This is the PROCPASSWD in the 46xxsettings.txt file.

Reactive Monitoring Interval

Lets you specify how often (in seconds) the phone will attempt to REGISTER with a proxy server when it is not reachable/available. Enter a setting from **10** to **3600** seconds. The default is **60** seconds. This parameter is only used by phones that support survivability features, such as the Avaya one-X Deskphone SIP R2.1 or later 9600 series phones.

Timer B

Lets you specify whether a phone will automatically revert to using a higher priority proxy server whenever one becomes available. Valid entries are **Auto** and **Admin**. The default is **Admin**.

This parameter is only used by phones that support survivability features, such as the Avaya one-X Deskphone SIP R2.1 or later 9600 series phones.

Failback Policy

Lets you specify how long (in seconds) the phone will wait for a provisional response after transmitting a SIP INVITE to a proxy server before assuming that proxy is unavailable/ unreachable and proceeding to another proxy. Enter a setting from 0 to 32 seconds. (0 disables this feature.) The default is 2. This parameter is only used by phones that support survivability features, such as the Avaya one-X Deskphone SIP R2.1 or later 9600 series phones.

Registration Policy

Lets you specify how the phone will register. Choices are **Alternate** and **Simultaneous**.

Click **Add** to add this setting to your SES system.

Add Settings screen commands

Add

Submit your changes.

Edit Parameter screen

This screen lets you edit the value of the parameter you selected on the List Phone Settings screen.

You must restart the 96xx phone to download the latest values from the settings file.

Edit Parameter screen field descriptions

Group ID

A group ID lets you collect different phones on your network for ease of administration.

To include a phone in a SIP phone group, see Adding a phone to a group on page 209.

Param Name

Parameter Name is the name of the parameter or attributes that are administrable on this phone.

The possible parameters are

- Group ID
- IP Address for SNMP Queries
- SNMP Community String
- Station Admin Password
- Visiting User Mode
- Quick Login Status
- Reactive Monitoring Interval
- Timer B:
- Failback Policy

Param Value

Param Value is the current setting of the phone’s parameter.

Edit Parameter screen command

Submit

Submit your changes to the database.

Remove Parameter screen

You must restart the 96xx phone to download the latest values from the settings file.

Press Continue to return to the list screen.

List Group Settings screen

If you go on to make changes to any of the values listed here, you must restart the 96xx phone so it can download the latest values from the settings file.

List Group Settings screen field descriptions

Parameter Name

Parameter Name is the name of the parameter or attributes that are administrable on this phone.

The possible parameters are

- Group ID
- IP Address for SNMP Queries
- SNMP Community String
- Station Admin Password
- Visiting User Mode
- Quick Login Status
- Reactive Monitoring Interval
- Timer B:
- Failback Policy

Parameter Value

Parameter Value is the current setting of the phone's parameter.

List Group Settings screen commands

Edit

Click this link to make changes to the groups of phones in your network.

Remove

Click this link to delete a phone group.

Add Group

Click this link to display the Add Group screen to define a new group. Assign an endpoint to a group with the instructions on Adding a Phone to a Group screen.

Add Group screen

This screen lets you add and define a group of SIP phones that you want to manage in the same way. Assign phones to this group with Adding a phone tp a group screen.

You must restart the 96xx phone to download the latest values from the settings file.

Add Group screen field descriptions

Group ID

A group ID lets you collect 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. The values you specify here apply to all phones in the group.

Edit and remove the group parameters listed one at a time. For example, to edit the visiting user mode, click the Edit link on the right. You are presented with a screen to change that parameter only.

Changing the group ID for a 96xx phone causes the phone to restart and reboot. In addition, you must send a reload command as well when changing group data.

SNMP Community String

This string is both a challenge and a response for the server named in the IP address above and the phone. If a server IP address is named, both the server and the phone must have the same community name administered.

Note:

If a value is put into the SNMP string in the settings file for the phones, you will be unable to disable SNMP queries.

Visiting User Mode

Off —Never ask about visiting when the user logs in.

Optional—Have the phone display a prompt to ask if the user is a visiting user or is the primary user.

Forced—Always make this device a visiting phone.

Before a visiting user session is terminated, the phone provides a message.

Quick Login Status

Password Entry Required -- No quick log in. Users must always type in an ID and password.

Quick log in Allowed -- Phone users just press the Continue button on the phone.

IP Addresses for SNMP Queries

This is the IP address of a server, that has the correct community string, that can query the phone for SNMP messages. If this field is blank, any server can query the phone.

Station Admin Password

The Station Admin password is the code that an administrator enters on a SIP phone. This allows the administrator to log into the actual phone to administer it.

This is the PROCPASSWD in the 46xxsettings.txt file.

Reactive Monitoring Interval

Specify how often (in seconds) the phone will attempt to REGISTER with a proxy server when it is unreachable/unavailable. Enter a setting from **10** to **3600** seconds. The default is **60** seconds.

Timer B

Specify whether a phone will automatically revert to using a higher priority proxy server whenever one becomes available. Valid entries are **Auto** and **Admin**. The default is **Admin**.

Failback Policy

Specify how long (in seconds) the phone will wait for a provisional response after transmitting a SIP INVITE to a proxy server before assuming that proxy is unreachable/unavailable and proceeding to another proxy. Enter a setting from **0** to **32** seconds. (**0** disables this feature.) The default is **2**.

Registration Policy

Specify how the phone registers. Valid entries are **Alternate** and **Simultaneous**. The default is **Alternate**.

Click **Submit** to add this group to your SES system.

Adding a phone to a group

Use the SES administration interface to create a group definition with a group ID. Then you may add an individual phone to the group.

1. Go to the phone.
2. Press Mute and enter the craft password and then pound sign.
3. Scroll down to the group.
4. Enter the new group number.
5. Save the changes.
6. Exit the craft menu.

Download Maintenance Data screen

After you make any changes to the SIP settings values, use this screen and push those changes to the phone.

Click OK to proceed with the down load, or cancel to avoid it.

Conferences screens

The Conferences screens let you add and delete communication manager server extensions that act as conference bridges. These extensions should not be given to end users, and should not be used for any other purpose.

This release supports 6-party conferences only.

The Conferences screens are these:

- List Conference Extension screen
- Add Conference Extension screen
- Conference Status

The SIP Conferencing feature allows SIP users to create multi-party conference calls. This feature works with SIP Softphone R2.1 only.

- On the edge server, the administrator can add, delete, edit, and list all conferences on all Homes servers that edge is a Parent of.
- On a home server, the administrator can list the conferences associated with that Home server, and view their status.
- If your Communication Manager installation uses Meet Me conferencing, the Meet Me conferencing vector directory numbers, or VDNs, should be administered before you administer conference extensions in SES.

List Conference Extension screen

This screen shows the pool of conference extensions of the communication manager servers in your system. From this screen you can add and delete specific extensions.

With the Administration interface on the edge server, you can add, delete, edit, and list all conferences on all home servers associated with that edge.

On the home server's limited administrative interface, you can see the conferences associated with that home server, and their status.

List Conference Extensions screen field descriptions

Extension

The number of the conferenceable extensions on all communication manager servers in your system.

Type

The type of extension. Right now, the only type available supports six participants or less.

Communication Manager Server

The name of the communication manager server that provides the conferenceable extension.

Host (home)

The name of the SES Host computer that is supported by the Communication Manager Server listed to the left.

List Conference Extensions screen commands

Move Conf

Click on this command to display the Select Communication Manager Server Interface for Conference Extension screen on page 214. With this screen, you can change the conference extension to a different communication manager server.

Reset All Conferences

Resetting the extension in the conference pool releases it back to the free pool so that it can be allocated for new conferences.

Conference extension numbers that are administered on both the communication manager server running Communication Manager and on SES are meant to be used with the Click to Conference feature. These conferences are dynamically allocated by SES when the conference is begins.

If a user manually dials a conference extension number in the pool when it is not currently associated with a conference, SES perceives this operation as invalid. The Conference Server running on SES gets a NOTIFY from Communication Manager regarding the membership update, and marks the conference number as INVALID, in this case. An SES alarm is raised.

When a conference number is marked as INVALID, it does not get used for further conferences until you click the Reset button and it is returned to an IDLE state.

Add Another Conference Extension

Select this to display the Add Conference Extension screen.

Add Conference Extension screen

Each communication manager server has a pool of extensions available for use as conference bridges. Use this screen to add another extension to that pool.

Add Conference Extension screen field description

Extension

Type in a number of an extension or SIP ID. This extension will be added to the pool of conference bridge numbers on the Communication Manager.

Communication Manager Server

From this pull-down list, select the communication manager server that will support the conference extension.

Type

The type of extension. At this time, the only type available supports six participants or less.

Add Conference Extension screen command

Add

Adds the extension you specify as a conference number in SES. Later on, create this extension on the communication manager server running Communication Manager, if it does not already exist there.

Select Communication Manager Server Interface for Conference Extension screen

Display this screen to move a user's extension for support by a different communication manager server interface. For example, the prefix group of a user may be on one C-LAN, but the user may need to be supported by a different communication manager server because of the features provided by Communication Manager running on that server. This screen lets you administer that move.

Select Communication Manager Server Interface for Extension screen field descriptions

Extension

This is the conference extension you want to move to a different C-LAN or PROCR communication manager server interface.

Communication Manager Server Interface

This pull-down list contains the communication manager server interfaces available to you. Select one.

Select Communication Manager Server Interface for Extension screen command

Submit

Click this button to make the change.

Communication Manager Server Extensions screens

This section describes administering telephone extensions provided by the Communication Manager communication manager server.

Administering Communication Manager extensions uses the edge server's Master Administrator interface. If you would like to manage a specific user's extension, see Extensions task on page 163. Access the Extensions screens through the Master Administration interface.

Conference extension numbers that are administered on both the communication manager server running Communication Manager and on SES are meant to be used with the Click to Conference feature.

These conferences are automatically allocated by SES when the conference begins.

Manage Communication Manager Server Extensions screen

This menu has several links to take you to the screens that list, add, and search for extensions on the communication manager server.

Administering Multiple C-LANs for a Communication Manager

A Communication Manager SIP trunk group allows for 255 trunk members. If you have more than one home server to connect to your Communication Manager, you may want to have a separate trunk group to each home, although this is not required. Your decision should be based on these considerations:

- How many trunk members are or will be needed
- How many home servers are needed
- Failover or routing techniques, to some degree

If you desire to have multiple SIP trunks across multiple C-LANs to one home server, the issue of "partitioning users" requires much more discussion and insight than what can be presented here. Please contact Avaya Services or your Avaya representative for more details.

Follow these steps:

1. You must administer a communication manager server interface for each C-LAN that you use for SIP trunking.
2. Select the **Communication Manager Server** link on the menu and add a communication manager server interface for each C-LAN board associated with the Communication Manager.
3. On the **Add Communication Manager Server** screen, the **Communication Manager Server Interface** field should contain a name to describe the C-LAN, for example **C-LAN1**.

4. Enter the IP address of the C-LAN board in the **SIP Trunk IP Address** field.
5. Partition extensions across C-LANs by assigning a unique set of extensions to each communication manager server interface, logically distributing those extensions across users on that home server.

   Partitioning extensions across C-LANs balances users, not traffic.

List Communication Manager Server Extensions screen

Use this screen to manage the communication manager server extension of an existing user. You can create an extension here with the SES interface, or use a free one that already exists on the communication manager server. If you create a new extension with this screen, you must go to the communication manager server running Communication Manager and administer it there as well.

Tip:

Another screen with the same name is discussed in Extensions task on page 163. Go there if you want to look up information about the extensions for a single end user.

List Communication Manager Server Extensions screen field descriptions

Extension

The numeric telephone extension in the database.

User

The name of the user associated with this telephone extension, if any. Blank if free.

Communication Manager Server

The name of the communication manager server running Communication Manager that supports this extension.

Host

The home server managed by the communication manager server named to the right.

List Communication Manager Server Extensions screen commands

Move Ext

Click this command to go to the Select Communication Manager server Interface screen. Once there, use the screen to move this extension to another communication manager server.

Free

The system displays this link only when extensions are already associated with a user. Select this to disassociate this extension from the user but leave the extension available so that it can be reused in the future.

Assign

Select Assign if a user has no extension and you want to provide one. You can use the Assign screen for this purpose.

Edit User

This field provides a convenient way to correct any errors in the user's profile. Selecting this displays the List Users screen and let's you access all the user-related tasks in the pull-down menu there.

Delete

Select this to go to the **Confirm Delete Extension screen**. This will delete the extension from the communication manager server.

Add Another Communication Manager Server Extension

Select this link to display the Add Communication Manager Server Extension screen and assign extensions on the home to a communication manager server.

Assign Communication Manager Server Free Extensions screen

This screen allows you to select a user and assign them a specific extension. The list of User IDs shown in the drop down are administered users associated with the home server where the free extension and associated communication manager server reside.

See Select Free Extension screen for the converse task, that is, choosing from a list of available extensions to assign to a specific user.

User ID

This is the unique identifier of the user. The User ID may look like a name or extension number.

Select

Click this button to make the change.

Select Communication Manager server Interface for Extension screen

Display this screen to move a user's extension for support by a different communication manager server interface. For example, the prefix group of a user may be on one C-LAN, but the user may need to be supported by a different communication manager server because of the features provided by Communication Manager running on that server. This screen lets you administer that move.

Select Communication Manager Server Interface for Extension screen field descriptions

Extension

This is the extension you want to move to a different C-LAN or PROCR communication manager server interface.

Communication Manager Server Interface

This pull-down list contains the communication manager server interfaces available to you. Select one.

Select Communication Manager Server Interface for Extension screen command

Submit

Click this button to make the change.

Add Communication Manager Server Extension screen

This screen lets you add an extension to a specific communication manager server, helpful when it is necessary to combine two communication manager servers, or change a user from one communication manager server to another and not change the user's extension.

After adding an extension with the SES interface, log into Communication Manager and create and administer the newly created extension there.

Extensions may be associated with users at the time they are created, or they may be created as free, and then associated with users in the future. Observe the following tips when creating extensions for users.

Tip:

Avaya highly recommends the following general user administration guidelines:

Each SIP-enabled endpoint is administered as an off-premise station in Communication Manager.

- Verify that the SIP Signaling Group screen administered on the communication manager server interface for this OPS station correctly names this SES home host computer.
- Verify on the Communication Manager, for this extension, that there is an entry in the **`off-pbx-telephone station-mapping`** screen.
- Also, verify that the entry has the correct trunk selection for this SES system.

- Extensions for all users of Avaya SIP Softphone clients that are set up in Communication Manager must be added to SIP Enablement Services explicitly and associated with their User IDs. The Administration Without Hardware (AWOH) extension administered on the communication manager server must match the extension administered in SIP Enablement Services. A match is required so that the users' SIP contact address, for example,
  `SIP:123456@mediaserver.domain.com`

  may be used as their handle as well.
- Extensions for all other users can be administered more easily using the patterns comprising address maps, the syntax of which is described in Pattern on page 249.

  For example, endpoints in your SES system currently use the prefix 543. The prefix of all users on the system must be changed to 987. Address maps advise the servers that any call directed to 543-0000 should be rerouted to 987-000.

Add Communication Manager Server Extension screen field descriptions

Extension

The numeric telephone extension in the database.

Enter the numeric telephone extension you want to create in the database.

Communication Manager Server

Select the name of the extension's communication manager server interface from the drop-down list.

The node name in alphanumeric characters associated with the communication manager server's C-LAN (or processor C-LAN) IP interface. For more information on IP node names, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

List Communication Manager Server Extension screen command

Add

Select **Add** to create a new entry for this communication manager server extension in this SES host's database.

Note:

This will not create any extensions or change any existing administration performed directly through Communication Manager on the associated communication manager server.

Add Another Communication Manager Server Extension screen

This screen allows you to create a communication manager server extension associated with a specific communication manager server. You then administer that extension on the selected Communication Manager.

This screen allows you to create a communication manager server extension through the SES Administration interface. You then administer that extension on the Communication Manager side later.

This screen is displayed after you click the **Add Another Communication Manager Server Extension** button.

This screen functions the same as the Add Communication Manager Server Extension screen.

Search Communication Manager Server Extension screen

With this screen, you can search for extensions on a specific communication manager server and find out which user is assigned to it. The results screen shows the user's User ID, communication manager server interface, and home host.

Search Communication Manager Server Extension screen field descriptions

Communication Manager Server

The node name in alphanumeric characters associated with the communication manager server's C-LAN (or processor C-LAN) IP interface. For more information on IP node names, see *Administering Network Connectivity on Avaya Aura® Communication Manager,* 555-233-504.

Select the name of the communication manager server you want to search from the drop-down list of communication manager servers. If you select the default **any**, the search checks all administered communication manager servers.

Extension

The numeric telephone extension in the database.

Enter only a portion of the number, and the results of your search will be all extensions that match the entered digits.

Search Communication Manager Server Extension screen command

Search

After you've entered your pattern criteria, select **Search** to initiate your database query.

Emergency Contacts screens

Emergency endpoints, for example, 911 or 999, are designated by the screens in this section as emergency contacts. In your SES system, create a user extension of 911@*yourcompany*.com to handle calls from users that need assistance.

Endpoints originating emergency calls are never authenticated.

The emergency contact screens are useful in the following scenarios.

Scenario 1

- Endpoint is registered to the SES server.
- Endpoint is registered to Communication Manager, and are OPS/OPTIM.
- 911 routing is set up on Communication Manager.

  In this scenario, the situation is optimum. There is no need for either a map or an emergency contact entry.

Scenario 2

- Endpoint is registered to the SES server.
- Endpoint is NOT registered to Communication Manager. The endpoint has no Communication Manager extension, and is not identifies as OPS/OPTIM.
- 911 routing is set up on Communication Manager.

  In this scenario, for emergency calls to route correctly,

  -- You must have a communication manager server map for the SES host with which the endpoint is registered. To create this map, see Creating an Emergency call address maps on page 251.

  -- No emergency contact handle is necessary.

Scenario 3

- The endpoint is not registered with SES.
- The endpoint is not administered in Communication Manager, and so is not identified as OPS/OPTIM, and has no Communication Manager extension.
- The endpoint is in a non-authenticated state.

In this scenario, for emergency calls to route correctly, you must have the following administered for calls to route correctly:

-- 911 routing on Communication Manager

-- a communication manager server map of 911@yourcompany.com on the SES server

--an emergency contact handle in the Emergency Contact screen

List Emergency Contacts screen

Calls to the SES home/edge or home server in the Host column do not require registration and will not be authenticated.

This screen shows emergency contact IP addresses for the home servers in your SES system.

List Emergency Contacts screen field descriptions

Contact

The emergency **Contact** is a handle, or extension that users dial in an emergency. This field can be pre-populated or administered. SES appends the domain portion.

Host

The **Host** field is the home/edge or home server with which the emergency URI is associated.

Host accepts a full SIP contact address or a partial URI, for example, just ***handle*** as in `handle@domain`.

List Emergency Contacts screen commands

Edit

Select the Edit command to display the Edit Emergency Contact screen. After edits are complete, the system displays the **List Emergency Contacts** screen.

Delete

After deleting, the system displays the **List Emergency Contacts** screen.

Add Another Emergency Contact

Select this to display the Add Emergency Contact screen.

Add Emergency Contact screen

This screen lets you add emergency contacts to an SES host. If a user makes a call to this contact, the host waives registration and authentication.

Edit Emergency Contact screen

You may change the emergency contact for the host at any time. If a user makes a call to this contact, the host waives registration and authentication.

Add/Edit Emergency Contact screen descriptions

Contact

The emergency **Contact** is a handle, or extension that users dial in an emergency. This field can be pre-populated or administered. SES appends the domain portion.

Host

The IP address for a home/edge or home server.

Add/Edit Emergency Contact screen commands

Add

On the Add version of this screen, click Add to submit this contact to the database.

Update

On the Edit version of this screen, click Update to commit your changes to the database.

Host screens

Host screens list, edit and add hosts and attributes of their functionality to the SES system.

Specifically, a host is an S8300C, S8300D, S8500B, or S8500C hardware, that performs as an edge server, home/edge server, or home server.

This set of screens also allows administration of host address maps. Host address maps let you redirect calls between home servers, and between edge servers.

Contrast this with List Communication Manager Server Adress Map screen. Communication Manager server address maps redirect calls between extensions on communication manager servers.

List Hosts screen

The List Host screen shows all the host proxies, home, edge, and home/edge, in the SIP domain.

If information has been changed on one of the hosts, the status column indicates that the change needs to be pushed to the other hosts in the domain.

List Hosts screen field descriptions

Host

The name or IP address of the edge, home, or home/edge server. This screen displays all SES hosts in the domain.

Type

Describes the host’s type as either a home/edge, home, or edge server.

SES Version

This is the version and build number of the software on this server.

List Hosts screen commands

Edit

Select **Edit** to manage the attributes of the host with the Edit Hosts screen.

Map

Select **Map** to go to the List Host Address Map screen, for that server. There you can manage the address maps this home server uses to redirect calls to other servers or to foreign domains.

For example, host address maps can direct calls between home servers, in order to reduce traffic on the edge server and edge address maps can redirect calls to a foreign edge proxy.

Host address maps have no correlation to communication manager server address maps. Maps in general have no relation to local failover or duplicated configurations.

Go To

Select **Go-To** to open a separate window that displays the target server's administrative web interface. This creates a session on that host to perform administrative tasks.

Test Link

Selecting **Test-Link** opens a window with a message indicating the host's response to a ping.

Delete

Select **Delete** to delete the host. This will fail if, for example, one or more communication manager server(s) use this host exclusively, or if the deleted host is an edge server that is the Parent of home servers.

Add Another Host

You may add a home host server as needed.

Only at install time can you add the edge server as a host. Once an edge server (or combined home/edge server) has been created, you may not add another edge.

Migrate Home/Edge

The Administration interface displays this link only if the hardware configuration is a home/edge.

Select this to change the current server from a combined home/edge configuration to distributed edge and a new, additional home server.

Migrate Home/Edge Host screen

Use this screen to change the current combined home/edge server to a distributed edge and home servers. With this screen, the current home/edge remains the edge, and new hardware you have brought in becomes the home.

The system's hardware configuration must be a home/edge for this option to display.

Migrate Home/Edge Host screen field descriptions

Edge Host Name

This is the name of the machine that will assume the functionality of edge.

Home Host Name

Type the name or IP address for the new home server, the one you want to move off the combined machine. The edge functionality stays on the old machine; the home functionality goes to the new machine you specify here.

Home DB Password

Type the name of the database password for the new host.

Migrate Home/Edge Host screen commands

Submit

Click this link to make the change.

Edit Hosts screen

With this screen, you can edit attributes of the host, including protocols, passwords, and system-wide rings and tones. Edit Host screen field descriptions

Host IP Address

Enter the IP address for this host server, either home, edge, or home/edge. Use the dotted decimal notation to enter IP addresses (for example, 123.45.67.89).

If your host is duplicated, use the logical IP address, not the physical address.

Profile Service Password

This password is for permissions between SES hosts, that is, home server(s) and edge.

Note that the Profile Service Password is not used by users or administrators. Rather, it is a password that is used by internal software components for secure communication between SES servers and the master administration system. The Profile Service Password must be unique for each administered host.

Host Type

Select one of the following from the drop-down list:

- Edge—if this will be an edge proxy server for the SIP traffic of all domains.
- Home —This option appears only after an edge proxy has been added. If this will be a Home proxy to manage the SIP traffic of a specific domain.
- Home/edge—if this server functions as both your enterprise's edge and home proxies. Note that no additional proxy servers may exist within this architecture.

Parent

Select one of the following from the drop-down list to indicate the communication manager server this host uses:

- Select NONE if you selected edge or home/edge for the server's Type above. An edge server has no parent.
- Select HOST NAME or IP if you selected home for the server's Type above. The name of the edge servers for all your enterprise's domains are listed. Select the correct edge server as Parent.

Listen Protocols

At a minimum, select TLS for the **Listen Protocol**. You may select UDP or TCP for other uses. Communication Manager supports the TLS and TCP link protocols for SIP trunking.

Note that the protocol you select for linking must also be selected here for listening. At a minimum, you must select the protocol you selected as the **Link Protocol**, below, although you may want to select additional protocols only for listening but not for linking.

When you add a host, all three protocols are selected for listening. There is little reason to change this default.

Link Protocols

This field refers to the trunk signaling between SES and Communication Manager. Typically, the selection here matches the Signal Group value on Communication Manager.

The link protocols for SIP trunking in Communication Manager are TCP and TLS. For third-party proxy servers, you may select to link to SES with TLS, TCP, or UDP.

You must also select the Link Protocol as a Listen Protocol, above. You may want to select additional listen protocols.

There is no special reason to change the default.

Access Control Policy

This setting correlates to the Watcher feature on the end user's SIP PIM web interface.

Accept the default policy of **Deny All**, or select **Allow All** to change this default policy and show the presence of SIP users on this server. The system displays the presence of SIP users on the Watchers screen in the SIP PIM web interface to PPM.

The administrator may set a system policy to specify that all users on the system default to a blocked state, where users must authorize each other to view each other's presence. The end SIP user may override this setting.

This administration policy is on a per-node basis and may be administered for each home node in the network.

Emergency Contacts Policy

Enable this field to allow unauthenticated calls for the emergency contact named for this host.

If you allow emergency contacts, emergency calls can come to this host. If you disable this field, unauthenticated calls to the emergency URI will be dropped.

Set up emergency URIs for the end user with the Add Emergency Contact screen.

Minimum Registration

The minimum registration timer is a SIP protocol feature that prevents endpoints from registering too quickly. Such a registration may be in error.

Enter a whole number of seconds, 900 through 59,940, that the SIP server should consider as the minimum acceptable duration when a SIP client registers. If no value is entered, the default of 900 seconds will be used.

Registration Expiration Timer

The value for Registration Expiration Timer determines how long a SIP endpoint should register for and renew its registration.

This value is not enforced by the registrar server, but downloaded by an endpoint through PPM if they support it. The minimum registration time is enforced by the SIP registrar and it will not allow new registrations prior to that minimum registration time.The minimum registration timer is a SIP protocol feature that prevents endpoints from registering too quickly. Such a registration may be in error.

The default is 3, 600 seconds or 60 minutes.

This field affects all the users on this host.

Line Reservation Timer

Outbound Routing Allowed From

Select **Internal** or **External** or both to specify whether SIP traffic can be routed only from endpoints internal to this server’s domain, or also from those external to it.

Outbound Proxy

Enter the host name of the server within your enterprise that should manage SIP traffic bound for domains external to this server’s domain.

For example, on a home/edge server, this would be the host name of the edge named as Parent of that home. On a combined home/edge or an edge proxy server, this entry might be a remote host, a service provider, ar an alternate edge server.

For a home server, define an outbound proxy only if a host other than the edge will route outbound calls.

Outbound Port

Enter the number of the port (1-65535) on the outbound proxy server specified above that should manage SIP traffic bound for domains external to this server's domain. Use port **5060** if the entry for Outbound Transport is UDP or TCP, and port number **5061** if it is TLS.

Select the transport protocol of the outbound proxy server that should manage SIP traffic bound for domains external to this server's domain.

Outbound Direct Domains

Users do not need to be under the same edge server to take advantage of hairpinning/shuffling and the absence of map addresses. For example, a user in New York can call another user in Paris, and the call is directly routed to the trusted domain in Paris. Set those trusted domains for the host, home, edge, or home/edge, here.

Use this area to list those domains for which traffic may completely bypass the Outbound Proxy server specified above. Separate entries in the list with commas, or with a white space followed by a new line, after each domain.

Select the **Add** button to add a host with the properties you've entered. If you have added an edge proxy, then selecting **Continue** at the next screen returns you to the Add Host screen.

until you add at least one home proxy server as well. If you add a combined home/edge proxy, then you return to the Setup screen if you are initially installing hosts.

Default Ringer Volume

This field sets the ringer setting for the stations bridged appearance buttons. The values in this field are not related to the ringer setting configuration in Communications Manager, nor does it reflect the Communication Manager's settings.

The default is 5, and the range is 1 to 10. This field affects all users of the specifically supported SIP phone types, such as the Toshiba SP-1020A, on this host.

Default Ringer Cadence

The value in this field sets the speed of the default ring tone for specifically supported SIP endpoints, such as the Toshiba SP-1020A.

The default is 2, the range for this field is 1 (slowest cadence) to 3 (fastest cadence).

This field affects all users of the supported phones type(s) on this host, but can be adjusted by the individual user of a telephone.

Default Receiver Volume

This field sets the volume in the handset, rather than the speaker. The default is 5, and the range is 1 (lowest) to 10 (highest). This field affects all users of the specifically supported phone types, such as the Toshiba SP-1020A, on this host.

Default Speaker Volume

This field sets the volume on the speaker rather than the handset. The default is 5. The range is 1 (lowest) to 10 (highest). This field affects all users of the specifically supported phone types, such as the Toshiba SP-1020A, on this host.

VMM

Voice Over IP Monitoring Manager (VMM) is a voice over IP (VoIP) quality of service (QoS) monitoring tool. This feature is available only on TSP SIP phones, model SP-1020A.

VMM information is taken from the VMM server. SES requires the server name, port address, and how frequently an end point should report back to the VMM Server. See the VMM document titled *Voice Over IP Monitoring Manager User Guide*, 555-233-510.

This field is specific to the Toshiba solution and only work with supported phone types.

VMM Server Address

Address of the VMM server.

This field is specific to the Toshiba solution and only work with supported phone types.

VMM Server Port

Port number for the VMM server’s address.The range is 1 through 65,535, and the default is 5005.

This field is specific to the Toshiba solution and only work with supported phone types.

VMM Report Period

The report period is in seconds, and reflects how often an endpoint should report back to the VMM server. Reports show jitter, round trip time, and packet loss. This may help in solving troubles on the IP network. The default value is 5 seconds, and the range is 5-30 seconds.

This field is specific to the Toshiba solution and only work with supported phone types.

Edit Hosts screen commands

Update

Select **Update** to submit your new or changed information to the server's database.

Host Address Map screens

The Host Address Map screens consist of these:

- List Host Address Map screen
- Add Host Address Map screen
- Edit Host Mao Entry screen

List Host Address Map screen

Use this screen to view and change the address maps used by an SES host.

Host address maps enable an SES server to redirect calls out of the current configuration or to a specific server or endpoint.

The address map strategy provides additional functionality to the local failover, high availability, duplicated-server hardware configuration.

The map names are in the Name column, and the details of a map are the map name, AbilineHostMap, invented by an administrator, and the pattern on which to match the incoming call.

Within each map, there are fields to specify the map name, and the incoming pattern to match on.

For all the match patterns in all the map names in a group, the matched call will be redirected to the first contact associated with the group, shown on the right side of the screen under the Contact heading. If that home server cannot resolve the call, AND if there is a second contact, the call will be redirected sequentially down the Contact list until the call is resolved or rejected.

List Host Address Map screen field descriptions

Host

The network name or IP address of the home server that uses the maps shown below.

Name (of the map)

This is a friendly name of the map created by an administrator. When creating the map, the administrator provided this name and the pattern to match for redirection.

Contact

This is the IP address or fully qualified domain name of another home server that you want to redirect calls to. If a call comes to the home host shown above, and is not listed in the database, the home server shown above evaluates the call for the regular expression provided in the pattern field for any in the map group. If it finds a match, the original home redirects the call to the first home host computer named in the Contact field.

To obtain better traffic balance, you may want to put high volume users on a different home server.

SES provides sequential routing, not parallel forking. The calls that match the patterns of a map will be redirected to the first home server in the Contact field. If you provide a second contact, the call will be redirected to the next contact on the list. If the last contact in the list cannot resolve the call, the call is marked with an *Unknown* caller response and sent to the PSTN.

List Host Address Map screen commands

Edit (name)

Edit the name of the address map or the pattern used for matching against. Use the Edit Host Map Entry screen.

Delete (name)

Delete this specific address map and the map’s pattern for matching from use by the host named at the top of the screen.

Edit (Contact)

Change the IP address or the friendly name of the host to which calls matching the map's pattern will be directed.

All the maps listed on the left in the map group use the contacts listed on the right, in a sequential fashion.

Add Another Map

Select this link to add another map, with a different name or a different pattern for matching, to a map group already present. Next, create the home server contact for the call to be redirected to.

Delete (contact)

Deletes a home server from the Contact list so that it will not be used to resolve calls.

Add Another Contact

Provide additional home servers to try sequentially to resolve a call.

SES provides sequential routing, not parallel forking. The calls that match the patterns of a map will be redirected to the first home server in the Contact field. If you provide a second contact, the call will be redirected to the next contact on the list. If the last contact in the list cannot resolve the call, the call is marked with an *Unknown* caller response and sent to the PSTN.

Delete Group

Select Delete Group to delete all of the map names and contacts listed above this link.

Add Map In New Group

Select this link to create a new map group and place a new map in it.

When you complete the Add Host Address Map screen, and select the Add command, a new group with one map is created for the host computer named at the top of the screen. Next, create the home server contact for the call to be redirected to.

Add Host Address Map screen

Display this screen by selecting this path:

Hosts-> Map-> Add Another Map

Hosts-> Map-> Add Map in New Group

Use this screen to create an address map for use by an SES server. On a home server, an address map redirects a call to another home server. On an edge server, the address map redirects a call to another, foreign-to-this-domain edge server.

This screen defines the match pattern. Send the call to another home in the next step. Go on to create a host contact for this host to turn to with the Add Host Contact screen.

Add Host Address Map screen field descriptions

Host

The network name or IP address for the home server that receives unknown calls.

Name

Enter an alphanumeric name for the address map you want this home server to use.

Pattern

Enter a Linux regular expression on which to match an incoming call.

After creating a map name and matching pattern with this screen, go on to name the host computer that can resolve the routing of the call.

Add Host Address Map screen commands

Replace URI

The **Replace URI** field is enabled by default because that is the correct selection in almost every circumstance. Select **Replace URI** to indicate that the pattern above should be resolved and forwarded by the host shown. This is the default, for this proxy to resolve and forward.

Deselect **Replace URI** if SIP requests are to be forwarded to a *different* edge proxy server for resolution and routing.

Put another way, if the contact information must jump from edge proxy to edge proxy, Replace URI must *not* be checked. If the information only traverses within the local SIP-CM domain, Replace URI must be checked.

In case the pattern information in this map is that of an endpoint, for example, a SIP phone or a user on a communication manager server running Communication Manager, then this box should be checked. The box is checked by default, because the SIP proxy on a Converged Communications Server will overwrite the URI of the SIP request for these cases. If, however, you wish to configure this SES proxy to forward requests to another entity, that is, another SIP proxy server, for that entity to resolve the contact and route the request, then uncheck the **Replace URI** box.

Add

On the Add version of this screen, click Add to submit your map to the database.

Update

On the Edit version of this screen, click Update to submit your changes to the database.

Edit Host Map Entry screen

Change the name of the map, or the pattern used for matching the incoming call with this screen.

Host Contact screens

Host Contact screens consist of these:

- Add Host Contact screen
- Edit Host Contact screen

Add Host Contact screen

Display this screen by selecting this path:

Hosts-> Map->Edit (Contact)

Host -> Map -> Add new

In this screen, **Contact** is the contact information of a home server to which you want to direct a call. You may also direct calls from an edge to another edge.

This screen populates the right side of the List Host Address Map screen. When you have created a map name and a pattern, use this screen to indicate where the call should be redirected.

Add Host Contact screen field descriptions

Host

The SES home server from which calls are being taken. This is the original home server that cannot resolve the call and wants to map the call to another home.

Handle

On this screen, **Handle** means the name of a host address map created with the Add Host Address Map screen.

Contact

In this field, enter the IP address or FQDN of another home server that can resolve the call redirected to it.

SES provides sequential routing, not parallel forking. The calls that match the patterns of a map will be redirected to the first home server in the Contact field. If you provide a second contact,

the call will be redirected to the next contact on the list. If the last contact in the list cannot resolve the call, the call is marked with an *Unknown* caller response and sent to the PSTN.

Add Host Contact screen commands

Add

On the Add Host Contact screen, this button adds the new host contact information to the database.

Update

On the Edit Host Contact screen, this button adds the changed host contact information to the database.

Edit Host Contact screen

This screen lets you change the information about the home server that will try to resolve an unknown call.

Communication Manager Server screens

The Communication Manager Server screen series lets you administer aspects of the communication manager server running Communication Manager.

Communication Manager communication manager server address maps are not required if all of the endpoints in the system reside on the Communication Manager communication manager server. Because all endpoints are known by the system, the SIP message is correctly routed to the correct endpoint.

Use this screen to view and change the address maps used by a communication manager server running Communication Manager. Communication Manager Server address maps let the Communication Manager communication manager serverserver direct calls that may be unfamiliar to them to other communication manager servers. The address map strategy is in addition to the local failover, high availability, duplicated server hardware configuration. Redirecting incoming calls with maps is also a strategy for use in disaster planning, maintenance schedules, and in planning for organizational growth.

Also see TLS links used for failover on page 29 for more information on how to set up communication manager servers.

List Communication Manager Servers screen

This screen shows all of the communication manager server interfaces running Communication Manager in the SIP domain.

Tip:

If you want to look up information about the extensions used by a specific user, see the menu for the Extensions task on page 163.

To redirect calls from 135.8.113.130 to a communication manager server OTHER than the one assigned on that home, select **Map**.

List Communication Manager Servers screen field descriptions

Interface

Name of the communication manager server running Communication Manager’s processor C-LAN that serves the home hosts listed.

Host

The alphanumeric, friendly name or IP address for a home server.

To administer a new communication manager server in the proxy host's database, select **Add Another Communication Manager Server**.

List Communication Manager Server screen commands

Edit

Select **Edit** to display the Edit Communication Manager server Interface. The **Edit communication manager server** screen allows changes to the server name, host, passwords, IP addresses, and more.

Extensions

This command relates to the telephone extensions on the communication manager server. Select **Extensions** to view the List Communication Manager server Extension screen for this communication manager server. With this screen, you can free, delete entirely, or change what user is assigned to a particular extension on the communication manager server.

This screen is not a substitute for manually administering extensions on the Communication Manager side.

Map

Select **Map** to display the List Communication Manager server Address Map screen for that communication manager server.

Communication Manager server maps resolve and route unknown incoming calls to alternative communication manager servers, using extensions. They have no correlation to host address maps.

An important type of communication manager server map is the one that directs the call to the public service access point or PSAP. Procedures for creating an emergency call map are on Creating an Emergency call address maps on page 251.

Test Link

Select **Test Link** to open a window with a message indicating the status of the communication manager server, trunk address, and communication manager server admin address (clan or procr). The status is either in service, UP, or not. Select Close when finished viewing the status.
Delete

Select **Delete** to go to the **Confirm Delete Communication Manager Server** screen. Verify that you want to delete the communication manager server from use by the SIP domain.

Add Another Communication Manager Server

Add another communication manager server running Communication Manager. Recall that all communication manager servers in a SIP domain must use the same Communication Manager software version and provide the same feature set. Add Communication Manager Servers screen

The first communication manager servers were added at install time. That screen is provided there for the installers.

See Add Communication Manager server Interface screen on page 135 for a discussion of this screen.

Tip:

If you want to look up information about the extensions used by a specific user, see the menu for the Extensions task on page 163.

Edit Communication Manager server Interface screen

use this screen to edit communication manager server properties. If the SES host associated with the communication manager server changes, then the communication manager server needs to be deleted first then re-added.

Tip:

If you want to look up information about the extensions used by a specific user, see the menu for the Extensions task on page 163.

Communication Manager server Address Map screens

There are three screens for administering the communication manager server address maps, List, Add, and Edit.

- List Communication Manager server Address Map screen
- Add Communication Manager server Address Map screen
- Edit Communication Manager server Map Entry screen

List Communication Manager Server Address Map screen

Use this screen to view and change the address maps used by communication manager servers running Communication Manager.

Communication Manager Server address maps check unknown extensions and route calls between communication manager servers.

Communication Manager Server address maps do not relate to host address maps. Host address maps use another home or edge server as a ’map to’ endpoint. Communication Manager Servers use a SIP user’s handle as a ’map to’ endpoint.

If all endpoints in your SIP domain are Avaya soft phones with OPTIM/OPS administered on the Communication Manager, a communication manager server map is not needed.

The address map strategy is in addition to the local failover, high availability, duplicated server hardware configuration.

Redirecting incoming calls with maps is also a strategy for use in disaster planning, maintenance schedules, and in organizational growth.

The map names are in the Name column, and the details of a map are the map name, 123map, invented by an administrator, and the pattern with which to match the call.

For all the patterns in all the map names in the group, the matched call will be redirected to the first contact on the right of the screen. If that contact cannot resolve the call, AND if there is a second contact, the call will be redirected sequentially down the Contact list until the call is resolved. If after redirecting to all listed contacts, the call still cannot be resolved, then the call is given an **Unknown** response line and sent to the attendant.

So, any pattern matched in 123map, 456map, or 789map will be redirected to the communication manager server 176.21.20.126 first, and if not resolved there, to communication manager server 176.21.20.128.

List Communication Manager Server Address Map screen field descriptions

Name

The name of the address map.

Contact

Contact entries may be fixed (constant data you enter after selected **Edit**) or dynamically constructed by the system. In the example shown, the host has constructed a Contact dynamically by substituting `sip` as the protocol, `$(user)` to represent the user name or extension in the original request URI, the IP address of the communication manager server to try next, and the port number and name of the transport method to be used.

For example, you may want to map calls from certain extensions to a communication manager server that uses TLS.

You may want to map calls from a certain extension to a secure sip server that provides sips: protocol.

List Address Map screen commands

Edit (Address Map)

Edit the name of the address map or the pattern used for matching against.

Edit the contact for the communication manager server. Use the Edit Communication Manager server Contact screen.

Delete (Addr Map)

To confirm your deletion, go to the **Confirm Delete Map** screen for that map or the **Confirm Delete Contact** screen for that Contact in the database.

Edit (Contact)

This displays and permits changing the address of the host, that is, the address of the machine to which the call will be routed.

Delete (Contact)

Delete this specific address map from use by the original communication manager server.

Add Another Map

Select the **Add Another Map** to add another address map, with possibly another name or another pattern to this group.

Add Another Contact

Provide additional communication manager server to try sequentially for resolution of the call.

At this time, SES provides sequential routing, not parallel forking. If you have one contact for the patterns in the maps in this group, the calls that match those patterns will be redirected to the IP address or friendly name of the home server you provide in the Contact field. If you provide a second contact, the call will be redirected to the first contact first, and if unsuccessfully completed, will go to the next contact on the list. If the last contact in the list cannot resolve the call, the call is marked with an **Unknown** caller response and cannot be completed.

Delete Group

Select Delete Group to delete all of the map names and contacts listed above this link.

Add Map in New Group

Select this link to create a new map group and place a new map in it.

When you complete the Add Communication Manager Server Address Map screen, and click Add, a new group with one map is created for the communication manager server named at the top. Go on to create the communication manager server contact for the call to be redirected to with Add Communication Manager server Contact screen.

Add Communication Manager Server Address Map screen

Use this screen to create an address map with an alphanumeric name and a call matching pattern.

If all endpoints in your SIP domain are Avaya soft phones with OPTIM/OPS administered on the Communication Manager, then communication manager server maps are not needed.

When you have created a map name and a pattern, select Edit (Contact) and use the Add Communication Manager server Contact screen to indicate where the call should be redirected.

After creating an address map with this screen, create the contact for the next communication manager server that will try to resolve the call. Add/Edit Communication Manager Server Address Map screen field descriptions

Note:

An address map identifies the relationship between the host servers and the communication manager servers. These messages travel over the SIP trunk administered in Communication Manager. Devise map patterns to specify the allowed messages clearly. If a map does not clearly identify the allowed message string, especially when the map uses wild-card metacharacters, then unnecessary data may flow to Communication Manager.

For example, an address map pattern of **`^sip:13*`** may match many IP addresses in the network, resulting in much unintended messaging traffic over that SIP trunk. If presence isn't working properly in your IM client, check that the patterns in your address maps are clear and correct.

Name

The name of the address map.

Enter an alphanumeric name to identify the address map you are adding to this Communication Manager communication manager server. This is not a network name, but might be a way of identifying which set of extensions on which Communication Manager communication manager server the map applies to.

Pattern

Enter a Linux regular expression on which to match an incoming call.

Replace URI

The **Replace URI** field is enabled by default because that is the correct selection in almost every circumstance. Select **Replace URI** to indicate that the pattern above should be resolved and forwarded by the host shown. This is the default, for this proxy to resolve and forward.

Deselect **Replace URI** if SIP requests are to be forwarded to a *different* edge proxy server for resolution and routing.

Put another way, if the contact information must jump from edge proxy to edge proxy, Replace URI must *not* be checked. If the information only traverses within the local SIP-CM domain, Replace URI must be checked.

In case the pattern information in this map is that of an endpoint, for example, a SIP phone or a user on a communication manager server running Communication Manager, then this box should be checked. The box is checked by default, because the SIP proxy on a Converged Communications Server will overwrite the URI of the SIP request for these cases. If, however, you wish to configure this SES proxy to forward requests to another entity, that is, another SIP proxy server, for that entity to resolve the contact and route the request, then uncheck the **Replace URI** box.

Add/Edit Communication Manager server Address Map screen commands

Add

In the Add version of this screen, this link commits the change to the database.

Update

This button is in the Edit version of this screen. After reviewing and changing the entries in one or more of the fields, select **Update** to submit the address map entry to the database on this host.

Edit Communication Manager Server Map Entry screen

You may need to edit the name of a communication manager server's map entry or change the pattern for that map.

If all endpoints in your SIP domain are Avaya soft phones with OPTIM/OPS administered on the Communication Manager, communication manager server maps are not needed.

Creating an Emergency call address maps

To make emergency calls you must have two communication manager server address maps set up to take the call from the SIP phone through the communication manager server and on to the public service access point (PSAP).

- You need two maps for every home or home/edge in your SES installation to correctly communicate with the communication manager server that finishes the emergency call to the PSAP.
- An edge server does not need a map for emergency calls because it does not communicate with the communication manager server.
- Each map must be a member of different map group as described in the instructions here.

Do this on each home:

1. Create an emergency contact using the SES Admin screens. Go to the Emergency Contacts link in the administration menu on the edge and use the Add Emergency Contact screen.

   The **Contact Handle** is the number the user would dial to make an emergency call, for example, 911.

   The **Host** is the IP address for the home/**edge** or **edge** server that is the parent of this home server.

2. Go to Communication Manager Servers > List to display the List Communication Manager server screen.

3. On the row for the edge server, click the **Map** link to display the List Communication Manager server Address Map screen.

   You may reuse map groups already present, or you can set up your two required groups. We will discuss the latter.

4. Add a new group to administer a map for unsecured SIP. Click **Add Map in New Group** and display Edit Communication Manager server Edit Communication Manager server Map Entry screen.

5. For the **Name** field, invent a name for this emergency calling map for unsecured SIP, perhaps EmergencyUnsec.

6. For the **Pattern** field, use regular expression rules. Make sure that your regular expression specifies the number a user would dial to make an emergency call.

   When creating the mapping for unsecured SIP, your pattern should look like this:

   ^sip:911@sipdomain.com

   When creating the second instance of mapping for secured SIP, your pattern should look like this:

   ^sip**s**:911@sipdomain.com

7. For the **Replace URI** check box, make sure it is unselected.
8. Click **Add** when you are satisfied.

Communication Manager Server Contact screens

The Communication Manager Server Contact screens let you create and change the way you route traffic to a different communication manager server interface.

- Add Comminication Manager server screen
- Edit Communication Manager server Contact screen

Add Communication Manager Server Contact screen

Use this screen to redirect calls to a communication manager server interface.

In this screen, **Contact** is the IP address of a communication manager server to which you want to direct calls.

When you have created a map name and a pattern, use this screen to indicate where the call should be redirected.

Add Communication Manager Server Contact screen descriptions

Handle (name of address map)

In this screen, this is the name of the address map.

Contact

In this field, type the name of the communication manager server that should next try to resolve the call, the communication manager server you want to direct the call to.

Add Communication Manager Server Contact screen commands

Add

Select this link on the Add version of this screen to commit the new data to the database.

Update

After reviewing and perhaps changing it, select the Update button on the Edit version of this screen to submit the entry to the host's database.

Edit Communication Manager Server Contact screen

This screen enables you to change the contact information for a Communication Manager Server.

However, it is not recommended to edit the communication manager server contact information directly. It is better practice to change attributes of the communication manager server contact by editing those attributes on the communication manager server interface form in Communication Manager. Once changed, the communication manager server contact will be updated automatically by SES to reflect the change.

Address Map Priorities screen

This screen lists all address maps currently administered for both Hosts and communication manager servers. Maps are originally administered with these screens:

- Host Address Map screen
- Communication Manager server Address Map screen

With the Address Map Priorities screen, assign a priority to each address map. This priority determines the order in which the proxy tries to match an incoming call pattern to an address map pattern.

For example, if an incoming call pattern (extension) matched 2 address map patterns, the proxy would route the call to the address map with the higher priority.

Address Map Priorities screen field descriptions

Map Handle

Map Handle is the address map name assigned when the address map was added.

Pattern

Pattern is the Linux regular expression entered when the map was added.

Map Type

Map Type is either Host or Communication Manager Server.

Map Owner

Map Owner identifies what entity the map is associated with. For a communication manager server address map, the Map Owner will be the communication manager server interface name where the map is assigned. For a Host address map, the Map Owner will be the IP address of the Host where the map is assigned.

Host

Host is the server IP address where the map resides.

Priority

Priority determines the order in which the proxy tries to match an incoming call pattern to an address map pattern. The highest priority that can be assigned to an address map is 1 and collectively represent an order of precedence.

Priorities must be a positive integer from 1-10000, and duplicate priorities are allowed. That is, any one, a subset or all address maps may have the same priority.

Address Map Priorities screen command

Update

After completing the Priority field, select **Update** to submit the change to the database.

Adjunct Systems screens

A system that functions as an adjunct to the SIP system is one that has one or more of its own servers and is integrated with SES via SIP.

SES supports multiple servers on an adjunct system, and those servers can co-exist under one or more systems.

In SES R5.1, servers support multiple applications, and so more than one application ID can be assigned to a system. In previous versions of SES, only one application ID was associated with a system.

- Examples of adjunct systems are Avaya Modular Messaging, for voice mail, and Avaya Voice Portal, for speech applications.
- Different types of adjuncts are set up and administered the same way. There is no special SES administration for different adjuncts.
- Physically, an adjunct connects to a home or combined home/edge server. It never connects to an edge server. Put another way, an adjunct system resides on a home and the adjunct server under the system points to the home where its system lives.
- Take care to associate the correct adjunct servers with the applications they are meant to provide. For example, administer MM adjunct server on adjunct systems meant for voice mail. Provision voice portal adjunct servers on adjunct system for speech applications. Do not attach application IDs unless they truly need to be invoked.
- Call routing through an adjunct uses a round-robin strategy. Round robin causes load balancing among the servers in the adjunct system.
- If the proxy does not receive a final response before a 2-second timer expires, the proxy routs the INVITE to the next adjunct in the adjunct system's adjunct server list.
- SES tries all the servers in that system before SES send a final response to the INVITE.
- You may have 30 servers per adjunct system and 300 adjunct systems per SES host.

  In certain cases, this restriction of 30 servers per adjunct system is lifted. Voice Portal servers, when administered on SES under an adjunct system are called adjunct servers, are different than a modular messaging server. These servers differ in the number of applications they can support. A Voice Portal server can support multiple applications, but modular messaging servers support one application, specifically, voice mail.
- Adjunct systems in this release of SIP Enablement Services are not applicable to Multivantage Concert.
- Adjunct servers need their own mechanism to generate, sign, and distribute server certificates, whether unique or common.

Adding and Removing Adjunct Systems

When SES is installed, use these instructions to provision adjunct systems that provide applications to SES that are outside its innate function, such as voice mail or speech applications.

These instructions are general enough to provide a high level strategy of how to implement any adjunct system. Information such as IP addressees, host names, application IDs and so on will depend on your specific site requirements.

- Adding an Adjunct System
- Removing an Adjunct System

Adding an Adjunct System

To begin, plan for the adjunct system:

- System name
- Application ID
- Host IP address, that is, the home server of the adjunct system.

Plan for the adjunct server:

- Server name
- Server ID
- Link type, TCP or TLS
- Server IP address

These steps describe how to add an adjunct system to your SES site using the master administration interface of SES.

1. Add the system first.

   Click Adjunct Systems > Add and fill in the Add Adjunct System screen. Identify the home server that will connect with this adjunct as the host. Click Add.

   The List Adjunct Systems screen shows the newly added adjunct system. T.

2. Add an adjunct server to the system.

   a. Display the List Adjunct Systems screen and click List Adjunct Servers.

      The List Adjunct Servers screen displays, showing the number of servers on this system.

   b. Click Add Another Adjunct Server to System.

      The screen displays the Add Adjunct Server screen.

c. Fill in this screen.

3. Click Add.

   The screen returns to the List Adjunct Server screen.

   Note the newly added server.

Removing an Adjunct System

These steps describe how to safely remove an adjunct system from your SES site.

1. First, delete the servers within the system.
   a. From the master Admin interface, click Adjunct Systems > List > List Adjunct Servers.
   b. Click Delete for every server in the list, clicking OK and Continue, to progress through the screens.
2. Remove the system next.
   a. Click Adjunct Systems > List > List Adjunct Servers.
   b. Click Delete to remove the correct Adjunct System.

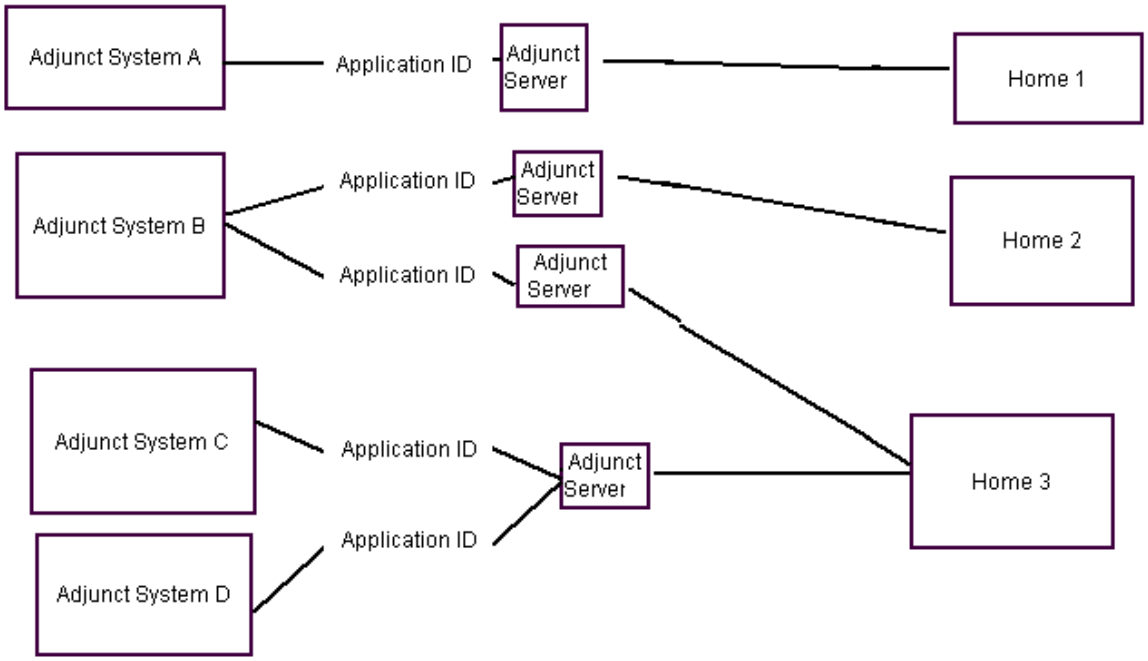
Variable administration scenarios

An adjunct server can belong to one or several adjunct systems.

An adjunct can be administered on SES in different ways, depending on the application and its needs:

- An adjunct system may have only one adjunct server, and so one Application ID
- An adjunct system may have multiple adjunct servers, and so multiple Application IDs

Figure 16: Logic of Adjunct Systems and Servers



List Adjunct System screen

Display this screen to view and edit the adjunct systems that work with your SES system.

The number in parentheses is the number of administered servers for each system.

You may have up to 300 adjunct systems communicating via SIP with your SES system.

List Adjunct Systems screen field descriptions

System

This column shows the names of the adjunct systems service.

Host

This column shows what home and edge servers are being serviced by the adjunct system named in the System column.

List Adjunct Systems screen commands

Edit

Select this link to use the Edit Adjunct Ssyetm screen to change the information for the adjunct system you selected.

Delete

Select Delete to remove an adjunct system from the SES system. Click OK or Cancel to be sure.

Remove an adjunct system after removing the servers in the system. Be careful not to delete any adjunct servers belonging to other adjunct systems.

You can delete an adjunct system even though it has adjunct servers administered to it. If the adjunct servers exists in multiple adjunct systems, and in the system you want to delete, adjunct servers' entries corresponding to that system are deleted. The adjunct server itself is not deleted completely.

List Adjunct Servers

Select this link to use the List Adjunct Servers screen to see what servers belong to this adjunct system.

List Application IDs

Select this link to use the List Application IDs screen to see what application IDs are used by this adjunct system.

Application IDs are administrable using Edit Application ID screen. Application IDs are alphanumeric values, such as 20042 or Voice. Application IDs are unique throughout the system.

Add Another Adjunct System

Select this link to add another adjunct system to the SES system.

Add Adjunct System screen

Use this screen to provision an adjunct system such as Modular Messaging for your SES system.

Add Adjunct System screen field descriptions

System Name

More properly, the Adjunct System Name, this is a convenient name you can invent to reference the adjunct system.

The administration of an adjunct system results in a linkage to each adjunct server that is part of that system.

Host

This column shows what home and edge servers are being serviced by the adjunct system named just above.

Add Adjunct System screen commands

Add

On the Add screen select the Add button to commit this adjunct system to your SES system.

Submit

The Submit button is on the Edit Adjunct System screen. Select the Submit button to make the change in the database. List Application IDs screen

Every List Application screen is associated with an adjunct system. Multiple application IDs can be added to a system. This screen lists all the application IDs associated with the system and provides a link to add another application ID to the system.

List Application IDs screen field descriptions

Application IDs

This column shows all the application IDs used by this system.

Application IDs screen commands

Edit

Select Edit to go to the Edit Application ID screen. On that screen, change the Application ID. The Host IP address cannot be changed for an Application ID under a system. It can only be changed for the adjunct system.

Delete

Delete an application ID to prevent its further use.

Add an Application ID

Select this link to go to the Add Application ID screen. With that screen, add another application ID to use another application, such as a computerized calling program. Edit Application ID screen

This screen provides a field for application ID, an alphanumeric handle. This handle is used by Communication Manager to route the call to the SES. SES then uses this handle to connect to the adjunct servers administered on the system to route the call to a particular application on the server.

Edit Application IDs screen field descriptions

Application ID

This field contains an alphanumeric identifier that indicates which application on the adjunct server to use. There may be several applications on a server, and these may be used by several systems.

Host

This pull-down list shows the IP addresses of the home or home/edge servers. Select the home server that will use the adjunct application.

Edit and Add Application IDs screen commands

Add

On the Add Application IDs screen, this button commits the new information to the database.

Submit

The Submit button is on the Edit Application IDs screen. Select the Submit button to make the change in the database.

Delete

Delete an application ID to prevent its further use.

Cancel

Select Cancel to exit without making any change.

List Adjunct Servers screen

This screen shows the servers in the adjunct system named at the top.

List Adjunct Servers screen field descriptions

Server

This friendly name of the server that runs the adjunct software. This field is alphanumeric. You can have 30 application IDs for one adjunct system.

Extension

An extension lets you dial directly into the adjunct system. This is used for maintenance only

Host

The IP address of the home server that uses the adjunct server's application.

List Adjunct Server screen commands

Edit

Select Edit to correct or change a server's information in your adjunct system.

Test Link

Select Test-Link to open a window with a message indicating the adjunct system's response to a ping.

Delete

Delete a server from the adjunct system named above. This prevents the adjunct server from communicating with the SES system.

A server can be deleted that exists under another system. When such a server is deleted, the associating entry of server and system is deleted. The whole information of the server is not deleted. Only when a server that does not exist on any other system is deleted, its all information is deleted.

Add Another Adjunct Server to...

Select this to add another server into the adjunct system named in this screen.

Add Adjunct Server screen

Use this screen to add a server to an adjunct system that works with the SES system.

Add Adjunct Server screen field descriptions

Host

The home server in the SES system with which this adjunct server will communicate. This information is populated from the adjunct system you selected in order to display this screen.

System

The friendly name of the adjunct system to which this server belongs. This screen is populated from the adjunct system you selected in order to display this screen.

Server Name

This server's name. The name of the server you want to add to the adjunct system named above. This name must be unique in the SES system.

Server ID

This is the server's handle or extension that can be used to directly call this adjunct server, rather than being routed via the adjunct system handle or extension.

Link Type

Select one of the listed protocols to be used for the SIP link between the adjunct system and the SES host:

- TCP (Transport Control Protocol)—if this protocol is not an option for your system, then the Link Type field may not appear on this screen.
- TLS (Transport Link Security)—this is the default protocol that is selected for all servers.

Server IP Address

This field is the IP Address of the server that contains the application, for example, a voice mail application that messages customers of car for maintenance. It is most probably a separate server. This address must be unique on a system, but can exist across multiple systems, for

example, in a system that has a server with some IP address can't have another server with the same IP address; but the same IP address can be added as a system on another system.

Add Adjunct Server screen command

Add

On the Add Adjunct Server screen, click Add to commit this information to the database.

Submit

On the Edit Adjunct Server screen, click Submit to commit this change to the database.

Aggregator screens

The Aggregator sceens enables you to configure SES to send user presence information to Avaya presence aggregation service (APAS) servers.

Add Event Aggregator screen / Edit Event Aggregator screen

These screens enables you to add and modify an event aggregator server. This server will receive user presence information from SES.

Add Event Aggregator screen field descriptions

APAS Server Name

(Required) Enter the name for this event aggregation server.

Host

Select the home for this event aggregation server.

APAS Transport Type

Select the option button for the transport type this event aggregation server uses.

APAS Port No

Enter the port number of the event aggregation server.

APAS Server Address

(Required) Enter the IP address of the event aggregation server.

Bulk Throttling Interval (Seconds)

Enter the interval (in seconds) at which the SES will send presence information to the event aggregation server. The minimum interval is 60 seconds. If no value is entered, the default of 60 seconds will be used.

Presentities Per Batch

Enter the number of users whose presence information will be sent per batch to the event aggregation server. The minimum number of users per batch is 5.

From Handle

(Required) Enter the handle you want to assign to the SES. Do not include the domain in this handle.

To Handle

(Required) Enter the handle you want to assign to the event aggregation server. Do not include the domain in this handle.

Select the Add button to add this event aggregator server to your SES system.

List Event Aggregators screen

This screen displays the administered event aggregation servers. From this page, you can:

- modify the settings for an event aggregation server
- delete an event aggregation server
- add an event aggregation server

List Event Aggregators screen field descriptions

Commands

You may select any of the following links in the Commands field next to the name of an event aggregation server:

- Edit -- to modify the settings for the associated event aggregation server.
- Delete -- to delete the associated aggregation server.

Interface

(Read Only) Displays the name of the event aggregation server.

Host

(Read Only) Displays the home for the event aggregation server.

Add Another Event Aggregatot

Enables you to add an event aggregation server.

Trusted Hosts screens

The Trusted Hosts screens increase security by authenticating incoming SIP requests. If the SIP request comes from a host you specify as trusted, SES does not authenticate requests from that host.

List Trusted Hosts screen

The List Trusted Host screen shows the IP addresses of hosts, either inside or outside you SIP domain, that can make SIP requests but not have those requests authenticated. This screen shows the edge or home server that will accept or deny the SIP request, and also any comments about it.

In configurations where the SES server communicates with a third-party SIP proxy, do not configure SES to recognize that third-party proxy as a trusted host. If you do, SES assumes that the trusted third-party proxy has already authenticated SIP requests it sends to SES.

Note:

Foreign domain proxy servers are not authenticated and so should not be configured as trusted hosts.

After adding or deleting a trusted host, use UPDATE in the Master Admin web interface to propagate the change to the affected home servers. Changes to trusted host administration are not effective until UPDATE has been done.

List Trusted Hosts screen field descriptions

IP Address

This field contains the IP address of the trusted host.

Host

From this pull down list, choose the home or edge server that will accept or reject the SIP request from the IP address above.

Comment

Use this area to make any important notes you may want other administrators to know about the use or nature of this host.

List Trusted Hosts screen commands

Edit

Make changes about the IP address, the edge or home server that receives the request, or to the comments about the trusted host.

Delete

Delete a host from trust. SIP requests from this host will begin to be authenticated.

Add Another Trusted Host

Click this to display the Add Trusted Host screen and place another trusted host into your system.

Perform Origination Processing

The field shows whether a host is configured as a Trusted Origination Host or not.

Add Trusted Host screen

The Add Trusted Host screen lets you specify a new server that may make unauthenticated SIP requests to a home or edge server in your SIP system.

Note:

After adding or deleting a trusted host, use UPDATE in the Master Admin web interface to propagate the change to the affected home servers. Changes to trusted host administration are not effective until UPDATE has been done.

Edit Trusted Hosts screen

After adding or deleting a trusted host, use UPDATE in the Master Admin web interface to propagate the change to the affected home servers. Changes to trusted host administration are not effective until UPDATE has been done.

Edit Trusted Host screen field descriptions

IP Address

This field contains the IP address of the trusted host.

Host

From this pull down list, choose the home or edge server that will accept or reject the SIP request from the IP address above.

Comment

Use this area to make any important notes you may want other administrators to know about the use or nature of this host.

Perform Origination Processing

Select the checkbox to mark the host as a Trusted Origination Host.

Note:

By default the checkbox is disabled.

Edit Trusted Host screen commands

Add

On the Add Trusted Host screen, click to enter a new trusted host into the database.

Update

On the Edit Trusted Host screen, click this button to commit changes to the database.

Survivable Call Processors screens

The survivable call processor (SCP) is a server that accepts and routes SIP calls in a limited fashion. With the SCPs in place, backup SIP service is maintained if your SES network goes down.

Administer your SCP hardware before you add or edit users.

Note:

SIP Enablement Services will support Survivable SIP Gateway Solutions in a distributed network settings in a later release. For more information, visit the following website: https://enterpriseportal.avaya.com/ptlWeb/internal/support/CS20062289553889009 1/C20071121376669013/SN20063141134188610 75/SN20071151175317042

List Survivable Call Processors screen

This screen shows what backup call processors have been set up and administered. These call processors are then assigned to individual users on the add and edit users screens. If SES goes down, these servers provided limited SIP call handling.

List Survivable Call Processor screen field descriptions

Processor Name

This is the name of the hardware.

IP Address

In this field, enter the IP address of the hardware that hosts the call processing software.

List Survivable Call Processor screen commands

Edit

Make changes to the SCP on this row. This displays the Edit Survivable Call Processor screen.

Delete

Delete an SCP from the administration. The physical box is still available.

You do not have to shut down or quiesce the SCP before removing this administration.

Add Another Survivable Call Processor

Click this to display the Add Survivable Call Processor screen and add another SCP to your system.

Add Survivable Call Processor screen

After you have the hardware installed and provisioned, use this screen to attach it to the SES system.

Add Survivable Call Processor screen field descriptions

Processor Name

This is the name of the hardware.

IP Address

In this field, enter the IP address of the hardware that hosts the call processing software.

Protocols

Enter the number of the port (1-65535) on the SCP specified above that should handle SIP traffic if SES goes down. Use port **5060** for UDP or TCP, and port number **5061** if it is TLS.

Add Survivable Call Processor screen commands

Add

After entering or updating entries, select **Add** to submit the information to the database on this host.

Update

On the Survivable Call Processor screen, click Update after entering or updating information to submit the information to the database.

IM Logs screen

IM logs report on the instant messaging by users in the system. You may want to download instant messaging log files to your local computer to review the reports. You can download IM log files from each SES server.

IM Logs screen field descriptions

Filename

Each IM log file is named with its creation date (YYYY-MMDD) and timestamp (HHMMSS). A new file is not automatically created at any specific time or interval, but when the existing file reaches the maximum size for an IM log file, administered in kilobytes (KB) on the IM Log Setting screen.

IM Logs screen Commands

Download

Select **Download** to the right of the log filename you wish to download.

Back to IM Log Files

Click this link if you want to go back to the IM Log screen.

Server Configuration screens

The Server Configuration screens enable you to administer system properties, administrators, licenses, and logs.

Admin Setup screens

This screen lets you specify if the current server is an edge server or a home server. It is used primarily at installation time.

If you should ever need to restart the SES Data Service, click the Setup button on this screen.

Setup Master Administration screen field descriptions

The radio buttons let you choose if the server you are currently logged into and looking at is the edge or the home server.

If you are setting up a home server, select the second radio button. In the field, enter the IP address of the edge server that is the parent to the home server. If the parental edge server is a duplicated pair, enter the logical IP address of the pair.

Setup Master Administration screen commands

Setup

Click Setup to invoke your selection and restart the SES Data Service.

Edit System Properties screen

Refer to the Edit System Properties screen and read about tasks such as how to setup the server’s domain, typically done during the initial install.

Licenses screen

If you need to check the licensing on any of the SES host computers, then use this screen. You may also refer to the procedure Server license installation on page 78, for example, for more detail on this topic.

List Licenses screen field descriptions

Proxy Name

Shows the names for each of the configured proxies authorized on this host.

Name

Shows the names for each of the proxies that are licensed for this Avaya SES server. Duplicated server configurations are licensed as one primary host. The licensed proxies include:

- Basic Proxy — each host, whether it be an edge, home, or a combined home/edge server, requires a Basic Proxy license. An edge or combined server also requires an edge proxy license.
- Edge Proxy —there is one edge server, and exactly one edge proxy license, for each SES system.
- Home Seats—Each administered user in the system requires a Home Seat license. Note that licenses are not acquired or released based on user registrations, but rather on administration. Do not administer more users than you have available Home Seats.

Message

Displays an indicator if there is an issue with acquiring licenses at startup for the proxy software that is running on this server. The possible messages are:

- Blank—if this proxy is configured properly on this host
- Expired—if this proxy is no longer authorized on this host

Note:

If licenses cannot be acquired when the proxy server first starts or is restarted, then the server continues to check the specified licensing host computer for the license(s) every 5 minutes until the licenses are acquired successfully, or until the no-license mode times out. Grace periods for license files may range in duration from 10 to 30 days.

List Licenses screen commands

Show

Select **Show** to view the License Information screen. This screen lists the information about the licenses on the server.

Access WebLM

To activate an existing license on this server, select **Access WebLM**. You will start the WebLM application.

The default login/password is:

Login: admin

Password: See Maestro.

After your first log in, you will be prompted to change the password. You may change it back to the old password of **password** if you wish. WebLM will then log you out and expect you to log back in with your new password.

IM Log Settings screen

IM log settings are configured centrally on the edge server for all SES servers. The setting from the edge are then applied to all SES servers that the edge parents.

Tip:

The following tips will help you administer the IM Logger service.

- A new IM Log file is created whenever IM Logger starts.
- This file logs messages until it reaches the maximum size for an IM log file, administered in kilobytes (KB).
- A record is placed in the log file whenever logging is enabled and disabled from this administration screen.
- The maximum log space administered (also in KB) must be higher than the maximum log file size.
- Each log file name includes the date and timestamp of when that file was created. Note that a new file is not automatically created at any specific time or interval.
- The default values for Max Log Size and Max Log Space are 10K bytes and 100K bytes respectively, which are designed to be appropriate for lightly loaded instant-messaging systems, and should be adjusted according to a customer's IM volume.

IM Log Settings screen field descriptions

IM Logger State

(This field shows the current state of the IM Logger service as OFF or ON. If this field is set as OFF, the system creates no log files.

When you set this field on the edge server, it applies to all other SESservers in the configuration.

New State

Select the state you want to set the IM Logger as ON or OFF. By default, the current state is selected. By default, a new IM log file is created whenever IM Logger starts.

When you set this field on the edge server, it applies to all other SESservers in the configuration.

Directory Path

Enter a full path name to the directory to where the IM logger files should go. By default, the value of the path entered for you is /var/log/sip-server.

When you set this field on the edge server, it applies to all other SESservers in the configuration.

Max Log Size (K)

Enter a whole number of kilobytes as the maximum size you want to allow for each IM log file. The default value is 10 KB, which is 0.1 of the maximum log space specified by default. You can change this ratio of logs to available space, so long as the number entered here is smaller that the number entered in the **Max Log Space** field, described below.

When you set this field on the edge server, it applies to all other SESservers in the configuration.

Max Log Space (K)

Enter a whole number of kilobytes as the maximum space you want to allow for all log files, The default value is 100 KB, or approximately 10 of the maximum sized IM log files specified by default.

You can change this ratio, as long as the number here is larger that the number for the **Max Log Size** field, described above.

When you set this field on the edge server, it applies to all other SESservers in the configuration.

IM Log Settings screen command

Set

Enter the properties for IM Logger and select **Set** to submit your changes to all servers in the configuration.

SNMP Configuration screen

This version of SES can use SNMPv3 for traps, but not for browsing standard mibs.

SNMPv3 supports standard MIB browsing and sending SES custom traps. In SES R3.1 and R5.1, v3 traps can be sent.

Set the SNMP community string after a new install. Note that your SNMP manager, for example HP OpenView, must be set to use the same value for community string.

Community strings are set on SNMP agents to authenticate SNMP managers or other clients that wish to browse or modify MIB objects. Entities wishing to do so must present the community string for authentication purposes. Default community strings, such as **public**, present a security gap since they are commonly known.

SNMP Configuration screen field description

SNMP v2c Community name

This is the name of the community string your site uses.

Community strings are set on SNMP agents to authenticate SNMP managers, or other agents that wish to browse or modify MIB objects, such as SNMP Trap Agent and INADS Alarm Agent.

Entities wishing to browse or modify MIB objects must present the community string for authentication. Default community strings, such as **`public`**, present a security hole because they are commonly known.

SNMP Configuration screen commands

Set

Make the name change permanent.

View AV-CCS-MIB Data

Click on this link to view a full copy of the MIB description for this product.

WebLM Software screen

Use this screen to view whether WebLM is currently enabled on this server and to enable or disable it.

WebLM does not automatically download license files from an RFA server. At installation, the installer accesses the RFA web site with the laptop, downloads a license file, and then installs it on the server.

WebLM Software screen field descriptions

WebLM License File

Before you enable a communication manager server, a valid master enterprise license file is required, which is generated by the Remote Feature Activation (RFA). WebLM Software enforces and defines the capacity limits of the server and sends them to the master enterprise license file.

Understand that the license expiration date is verified when installing WebLM software. The date generated by the license file must not be pre-dated to the current date of the WebLM server. This can happen due to time-zone differences between the RFA server and the WebLM server.

System Status screen

This screen is informational only. View this screen to see if processes and connectivity are working properly.

- Admin Connectivity -- Displays one of the following values:
  - Connected-DataServices has already been setup
  - Setup -DataServices needs to be setup
- Master Administration IP Address--Displays the IP address that the SES Data Services has been configured to use for incoming connections.
- Host Type -- Identifies this SES server as a home, edge, or home/edge type. This does not indicate the server's role of primary or backup.
- SIP Server -- Displays the current status of the SipServer application on the local server. Will display either:
  - SipServer 0/34 OFF
  - SipServer 45/45 UP
- Initilal Data Replication--Displays the number of outstanding replication requests.
- Packets Received/Sent--Displays the number of data service packets received/sent.
- PPM Status -- Displays the current status of PPM service on the local server. Will display either:
  - Request denied
  - PPM is running
- SES Data Service—Displays the current status of SES Data Service on the local server. Will display either:
  - SES Data Service is running
  - SES Data Service is stopped
- Redundancy--Displays the information for the redundant server (if configured).

Certificate Management screens

An SES proxy server contains two server certificates:

- The SIP server certificate, found on both home and edge servers. This default certificate is pre-installed on all SES servers and is signed by the Avaya SIP Certificate Authority.
- A web server certificate to be used for web connections.

Under the Certificate Management menu, these screens are available:

- Generate Web Certificate Signing Request screen
- Install Web Certificate screen
- Generate SIP Certificate Signing Request
- Install SIP Certificate

The Generate and Install screens listed above let the administrator generate and install a web certificate and a SIP certificate. The system comes with default certificates for the web and SIP servers, but unique certificates are recommended for the web and SIP servers on every SES.

A daily audit checks the expiration status of the external certificate for both the SIP server and the Apache web server. For each of these servers alarms are issued as follows:

- Starting ten days before web certificate expiration, a warning is sent daily via SNMP.
- On the certificate expiration date, an alarm is sent via SNMP. If the expired certificate is the SIP certificate, an INADS alarm will be sent as well because SIP communication will fail.

The SNMP traps for the SIP server and the Apache server are described in Certificate expiration traps on page 746.

Best practices

- Generate, sign, and install unique certificates for each server.
- When your configuration features a duplicated-server pair, download and install certificates for each of the servers. The common name for each certificate should contain the logical name and logical IP address for the duplicated pair.
- Microsoft Internet Explorer 7 (IE7) differs from Internet Explorer 6 in how it presents certificate warnings to end users. In addition to a harsher sounding popup message, IE7 adds a Security Status Bar that will read “Certificate Error” with the default SES web certificate. Following the steps below to install a unique web certificate will allow SES administrators and SES PIM interface users to access SES System Web pages without seeing the popup warning or “Certificate Error” message.

Generate Web Certificate Signing Request screen

Use this page to generate a certificate signing to the CA for a certificate. The request generated here is sent to the CA with the monies necessary.

As soon as possible after installation, replaced the default web certificate with a unique web server certificate. If you use the default web certificate, every time you or an endpoint user starts a web application from the server, you receive a security alert from the browser.

When you use this screen to make a signing request, the screen displays a link to the CSR file so that you may download it.

This page is the WEB counter part to the SIP CSR described in the section Generate SIP Certificate Signing Request on page 292.

Generate Web Certificate Signing Request screen field descriptions

All the fields in this screen contribute to the subject name and become part of the certificate.

The common name is the most important part. This must be the host name of the server or server pair, if duplicated. If it is not, then the user connecting to the server will get a security dialog box that the certificate's server name does not match the server's name. This will not prevent you from connecting to the server, but is a warning that something may be incorrect.

When you view a certificate you see the following parts.

Country Name

The name of the country the server is in. The country name is a 2-letter code.

State or Province Name

The name of the state or province the server is in. Spell this out fully.

Locality Name

The city the server is in.

Organization Name

The name of the company that owns the server.

Organization Unit

The name of the company or business unit.

Common Name

This field must contain the host name of the server or of the server pair, if duplicated. If it does not, the user connecting to the server will get a security dialog box that the certificate's server name does not match the server's name. This mismatch does not prevent you from connecting to the server, but is a warning that something may be incorrect.

RSA Key Size

The RSA key size refers to the size of the private key. To break a key 1024 bytes long would take today's fastest computer, on average, many, many years. To break a key 2048 bytes long, it would take the same computer, on average, thousands of years.

Generate Certificate Signing Request screen command

Generate Request

This button invokes the script that generates a link to a signing request that is sent to a CA. A link to the signing request will appear on the screen. The place you choose to store the certificate is used in the Install Web Certificate screen that you access next.

- To use these pages:
  - Generate a signing request with the Generate Certificate Signing Request screen. It will ask you where on the PC to put the file.
  - Take that request file and send it to a CA with monies necessary to get it signed. The CA sends it back signed and possibly with a certificate chain of trust.
  - The Install Web Certificate page will get the files from the PC and install them in the correct location.

  Note:

  Separate server certificates are used for TLS authentication for SIP applications, and for Apache secure HTTPS.

Install Web Certificate screen

Use this screen to install a web certificate when your server's certificate signing request is signed.

Access this screen after generating a request with the Request screen.

When importing a root certificate, the file name must have the file extension .crt. If you use a different file extension, the hash file link is not created and the certificate is not recognized as a CA certificate.

This screen is the Web counterpart to the Install SIP certificate screen.

Install Web Certificate field descriptions

Web Certificate

Either type in the full path of the certificate of where it is on the PC or use the Browse button to find the location of the server's certificate in the file hierarchy.

Chain Certificate / Certificate Chain of Trust

Either type in the full path to the certificate on the server or use the Browse button to find the location of the server's chain certificate in the file hierarchy.

Note:

In the signaling path, TLS authenticates the two devices in the connection and encrypts the information they are exchanging. TLS exchanges the relevant information necessary to build the connection by exchanging certificates that contain this information. This means that each hop of the connection must produce a certificate and certificate chain acceptable to the next hop.

A certificate chain is a chain of certificates starting with the server's certificate used to sign the previous certificate and leads to a root certificate signed by a certificate authority (CA) such as Verisign or Avaya. The CA certificate must be acceptable to the client in order for the server to be authenticated.

Install Web Certificate commands

Install Web Certificate

Select this to install the previously downloaded certificate file.

View Current Web Certificate

Select this link to access the View Current Web Certificate screen.

This screen lets you view the contents of the certificate file you just installed.

Generate SIP Certificate Signing Request

Use this page to generate a certificate signing to the CA for a SIP certificate. The request generated here is sent to the CA with the monies necessary.

As soon as possible after installation, replaced the default SIP certificate with a unique SIP server certificate. If you use the default SIP certificate, every time you or an endpoint user starts a web application from the server, you receive a security alert from the browser.

When you use this screen to make a signing request, the screen displays a link to the CSR file so that you may download it.

.

Install SIP Certificate

Use this screen to install a SIP certificate when your server's certificate signing request is signed.

Access this screen after generating a request with the SIP Certificate Signing Request screen.

View Current Web Certificate screen

Viewing the certificate shows you what CA signed it and when it will expire.

This screen is representative of both Web certificates and SIP certificates.

Trace Logger screens

Trace Logger is a minimally intrusive means to trace SIP traffic on an operating, in service SES configuration.

Trace Logger provides a web-based interface that enables an SES administrator to selectively trace SIP messages across the entire SES configuration. Tracing is available for all of the network transport methods used.

Trace Logger provides a configurable SIP message filtering capability to limit output, filtering SIP messages by the specified SIP header parameters. When constructing filters for messages, limit the trace results with these criteria:

- SIP method (INVITE, ACK, BYE, SUBSCRIBE, NOTIFY, and so on)
- TO header
- FROM header

This section presents the trace logger screens:

- Configure Filters
- Edit Trace Logging Rule screen
- Add Trace Logging Rule screen
- Trace Logs File Download screen

You need to have at least an intermediate level of understanding of SIP messaging. Trace Logger is primarily for use by Avaya Tier III and above support services.

Using Trace Logger Filter

Trace Logger Filter is a tool which system administrators can use to analyze and troubleshoot Avaya Aura SIP Enablement Services and other SIP elements in the communication network deployment.

The following common scenarios require SIP traffic logging:

- When an endpoint or a user cannot register or make calls.
- When a specific service does not function properly. For example, MWI notification.

You can use the Trace logger to troubleshoot continuous conditions or problems that occur infrequently.

You must plan in advance regarding the type of traffic to capture because setting up tracing on a live system usually generates substantial amount of SIP data that is hard to analyze. Analyze the type of traffic that helps you understand or troubleshoot the behavior in question, and then describe the traffic based on a combination of the following attributes:

- The logical entity from where the traffic originates and uses the From or Contact header filter
- The logical entity that is the target of the traffic and uses the To header filter
- The type of device that is associated with the traffic and the User Agent header filter
- The type of SIP packet that uses Message Type and Method filters

The following examples represent typical filters:

Example 1

To analyze traffic from a specific user that cannot register or make calls, capture SIP messages with message type any and type the address of record (AOR) SIP address of this user in the From header filter. For example, sip:1234@domain.com.

Example 2

To analyze traffic from a specific type of device, find the value of the User Agent header that this device uses in outgoing requests and create a filter based on this value. For example, Avaya one-X Deskphone.

Example 3

To analyze all the registration traffic in the system, select messages marked as Request. Then from the methods list, select REGISTER.

Note:

The following are general recommendations on constructing filters:

- Capturing traffic can impact Avaya Aura SIP Enablement Services performance. Avaya recommends that you construct a trace filter to limit the amount of traffic captured.
- Consult an Avaya support representative to set the correct filter for troubleshooting a specific behavior.

Best practices

- You can run only one trace at a time.
- After creating or editing a trace, stop before starting the trace again to employ the changes.
- TraceLogger is a debugging tool. It is off by default. Do not leave it on indefinitely.
- Trace filters can be POSIX regular expressions. However, they should be as specific as possible, for example: From: userXYZ@domain.com. If they are too broad, they can degrade server perfornace because broad filters contain wildcard characters, such as *, or patterns that match all messages, such as sip.

Configure Filters

Use this screen to stipulate filter criteria to match against SIP messages on your system.

One filter is supported.

The filter is made more or less specific by rules. Rules are defined by the criteria selected.

You may have a maximum of 10 rules within one filter. The 'OR' between rules in a filter is an inclusive 'or', not an 'either or'. That is, the Trace Logger checks all rules in a filter to see if it can match a message. There is no order of precedence for the rules in a filter.

Within the rule, all specified criteria must be found in the SIP message in order to log the message to the log file. Within the rule, criteria are evaluated with a logical AND.

The contents of the Filter Configuration screen change, depending on what you have defined as rules and criteria.

Best practices

- Make sure all the servers in the SES domain are synchronized with a network time protocol server.
- Trace Logger works like `syslog` with respect to file naming.

In this example scenario, the user, Joe, incorrectly tries to register as 'joebloggs@jhsip.com'. Joe has entered the wrong domain. Additionally, Joe has typed in an incorrect password. By running Trace Logger with a filter set to log all messages with SIP **From** header containing the string 'joebloggs,' a SIP-savvy administrator can easily determine the cause of the problem.

The log from this trace and an explanation of the messages are available for study in Appendix D:Trace Log Files on page 369.

Configure Filters screen field descriptions

When you start logging, the entire SIP message is placed in the log file. The criteria you set using the fields on the Add or Edit TraceLogging Rule screens determine what SIP messages match, and what filter criteria display on this screen. See the field descriptions for Add Trace Logging Rule screen.

Configure Filters screen commands

Edit

Select this link to modify one of the rules in a filter you have already set up.

Delete

Select Delete to remove the rule from the filter. Stop and restart the filter if it is running to employ the changed filter. A new log file will be started.

Add New Rule to Filter

Adding a new rule makes the filter more granular and restricts the number of SIP message matches.

Add Trace Logging Rule screen

Use this screen to specify criteria for a single rule within a filter. A filter may have several rules. Then go to the Trace Manager screen to start tracing. If a trace is already running, stop it, then start to trace again in order to employ the newly added rule.

Trace Logging Rule screen field descriptions

The fields on this screen correspond to the headers in the SIP messages.

Rule Label

Invent a name to describe the combination of criteria that makes up the rule.

Methods

Click on one, several, or no check boxes to define the scope of the filter according to SIP REQUEST type messages.

From

The criteria you type here corresponds to the contents of the `From` line in the SIP message.

To

The criteria you type here corresponds to the contents of the `To` line in the SIP message.

Contact

The criteria you type here corresponds to the contents of the `Contact` line in the SIP message.

Request URI

Request-URI is the URI portion of a SIP Request-Line. It specifies the destination being requested. Example: sip:user@domain.com:5061;transport=tls

Response Line

Response line refers to the **Status-Line** of a SIP response. It contains the SIP version, a Status-Code, followed by a reason phrase. For example: SIP/2.0 200 OK.

User Agent

The criteria you type here corresponds to the contents of the `User-Agent` line in the SIP message, for example, Windows Messenger or CSCO/6.

Endpoints and communication manager servers both populate the SIP User-Agent header field.

Message Type

- Request—Only matching request messages will be logged. Response Line is disabled because it does not apply to requests.
- Response— Only matching response messages will be logged. Methods and Request URI are disabled because they do not apply to responses.
- Any—Any matching message will be logged. Methods, Request URI, & Response Line are disabled since they pertain to a specific message type.

Trace Logging Rule screen commands

Add

On the Add screen, select Add to create a new rule for the filter. Stop a running trace and restart it to employ the new filtering rule.

Update

On the Edit screen, select Update to save the changes you made. Stop a running trace and restart it to employ the changed filtering rule.

Edit Trace Logging Rule screen

Use this screen to modify criteria in a rule. If you make a change here, stop the trace and restart it to put the change into effect.

Trace Manager screen

Use this screen to start and stop tracing SIP messages on your system. You may run only one trace at a time. When the file **sipTraceLog** fills up to the 1 Mb maximum, the older messages are moved to a file named sipTraceLog.1. The most current traced messages are always in **sipTraceLog**.

Trace log messages include a time stamp based on the SES proxy it was captured from. In order to have sensible trace logs, make sure all the servers in the SES domain are synchronized with a network time protocol server.

Trace Manager screen field descriptions

This screen is purely informational and has no editable fields. The screen shows the start time of the trace, which SES servers are being traced, and the status of each host.

In the example above, an edge, and two home servers participate in the trace.

Status

The three types of status are:

- Active—the trace is proceeding on the SES host named to the right
- Idle—the trace has been stopped, as displayed at the top of the screen
- Error—This can either be Active-Error or Idle-Error.

  Active-Error means the trace was stopped, but a particular host has remained active.

  Idle-Error means a trace was started and a particular host has remained idle.

  In either error case, an "Attempt Recover" link will be displayed under the hosts in the "Host Tracing Audit" section. An error status can potentially occur when old data are restored onto a home or when a new home is added. Either restart (or stop) the trace or use the 'Attempt Recover' link to synchronize the individual host's status with the overall trace status.

Host

This shows the IP address of the SES host, either edge or home server, that is participating in the trace.

Stop Tracing

Select this link to stop the current trace. The messages matched by the trace are in the file `sipTraceLog` until `sipTraceLog` reaches its 10Mb size limit. Then the messages are moved to `sipTraceLog.1`.

Start Tracing

Select this link to start a trace. The messages that match the trace's filter are put into `sipTraceLog`. When `sipTraceLog` reaches its 10Mb size limit, the older messages are moved to `sipTraceLog.1`.

Trace Logs File Download screen

Use this screen to download trace logs for viewing and troubleshooting.

The system displays trace log files in chronological order of newest first, oldest last. The contents of trace logs contain the entire SIP message.

Trace Log behaves similarly to `syslog`. When 10 files exist, and a new one must be created, the system deletes the oldest file, `sipTraceLog.9`, and begins again with `sipTraceLog`, overwriting what was there. Traces that were in `sipTraceLog` before a rollover occurred are now in `sipTraceLog1`. The contents of `sipTraceLog1` are now in `sipTraceLog2`, and so on.

The system keeps a maximum of 10 trace logs.

The maximum size of a trace log is 10 megabytes.

Every time you start a trace, the newest matches go into a `sipTraceLog` file. Older messages are in `sipTraceLog.n` where n is an integer from 1 through 9.

Study an example of a portion of a trace log file in Appendix D:Trace Log Files on page 369.

Note that the SIP messages in a trace log file may not be in perfect order. For example, if one of the proxies has a higher traffic load, the traced messages to and from that proxy may not be in the expected place in the log file.

Trace log messages include a time stamp based on the SES proxy it was captured from. In order to have sensible trace logs, make sure all the servers in the SES domain are synchronized with a network time protocol server.

Trace Logs File Download screen field descriptions

Log Files Available

The number of log files available, some of which may be below the bottom border of the screen.

Filename

Trace logs are named by the system. When you download, you may assign a more meaningful name than `sesTraceLog.1`.

Trace Logs File Download screen commands

Download

Select Download to select a place in your file hierarchy to save the log. After download, view and edit the file with a text editor.

Delete

SES provides a mechanism to delete logs automatically. As new files are created, remember that the log file name rolls over, like the `syslog` utility. You may use **Delete** to delete a specific log file.

Export/Import with ProVision

This menu item imports and exports XML files for use with ProVision. Use this menu item for bulk loading of data. Refer to the documentation the comes with your ProVision software for details on how to set up and receive .XML files.

For general backup and restore procedures, go to the Maintenance interface and use the backup menu item there.

The Export/Import series of screens consists of these:

- Export screen
- Download screen
- Upload screen
- Import screen

Export—Data are placed in a file named `/tmp/mvss_admin.xml`. This is the only filename used. Once the database is captured in the .XML file, either rename the file or move it to another location so that it is not overwritten by a subsequent export operation.

Download —saves the .XML data to a user-specified location on a local drive. Move it to where it can be easily accessed from the ProVision software.

Upload— takes an .XML file from a user-selected local drive. Once uploaded, the file is imported automatically into the database.

Import—takes a ProVision .XML file from the `/tmp/mvss_admin.xml` location. The filename is specific, and no other filename can be used.

Export screen

The Export screen takes data from the database and converts it to an `mvss_admin.xml` file in the `/tmp` directory location on the SES server.

There is no opportunity to cancel the operation except to use the browser's Back button.

Download screen

The Download screen copies data from the SES database to a file that you save to a local drive. Once downloaded, the .XML file that you save can then be manipulated.

When you select the OK button, the system displays a dialog box to specify where to save the file. The download time interval depends on database size. Downloads may take a few minutes.

if your browser is Firefox, recall that you are unable to choose the location in which to store this download.

Upload screen

Select Upload to bring the ProVision .XML file from an external source into the SES system for use by the database.

The data are automatically inserted into the database after the import.

Import screen

Select Import to make the data in `/tmp/mvss_admin.xml` available for use by SES.

Chapter 7: System Management Interface

SES and Communication Manager share the System Management Interface. The System Management Interface comes with a help system embedded. For information about any screen that are not provided here, click the Help button on the screen.The screens in this chapter are SES screens that are additional to the Communication Manager screens.

- Authentication Protocol—specifies the authentication protocol in use.
- Privacy Protocol—specifies the privacy protocol in use.

Communication Manager Interchange Servers screen

This screen is seen only on duplicated pairs. Use the Interchange Servers page to make a primary server the backup, and the backup server to assume the role of the primary server. Interchange Servers screen field descriptions

Force Interchange

Click this check box to force the interchange between primary and standby regardless of the status of the server. If a server is out of service, it will be brought into service with this checked.

Busy-Out Server screen

This screen is seen only on duplicated pairs. Use the Busy Out Server page to remove a server from service. Having a server busied out prevents it from taking part in an interchange, a risky situation.

This screen operates on only one server in the duplicated pair. That server is identified in the upper right corner.

Release Server screen

This screen is seen only on duplicated pairs. Use the Release Server page to remove a server from a busy out operation.

The one server of the duplicated pair that you release from busy out is specified in the upper right corner. This screen does not affect both servers in the pair.

Types of Linux Groups

Access Profile Group

An access-profile group identifies a user profile that administers access to the SAT interface and the server Web pages.

Non-access Profile Group

A non-access profile group administers access to files and directories on the SES server.

Communication Manager

Chapter 8: Shutdown procedures

You may want to shut down the SES servers for the following reasons:

- To remaster the hard drive as part of a migratio
- To upgrade from R5.2 to R5.2.1

You cannot directly upgrade SES servers from R2.x to R3.x or R3.1.x. You must remaster from R2.1 to R3.x using the install CD, then use the web page to upgrade to newer builds of R3.1.x.

The graceful shutdown process here shuts down single and duplicated servers of any type, distributed or combined, and any hardware. Refer to the following sections:

- Best practices on page 317
- Shut down a co-resident server on page 318
- Shut down a single server on page 319
- Shut down both servers in a duplicated pair on page 319

Best practices

- To work on a specific machine, In the URL address line of a browser, log in to the server you want to shut down.
- Use the Manage software shutdown procedures to start and stop your servers. Never use the **`stop`** or **`start`** commands on duplicated servers.
- In general, use the **System Management Interface** and switch over servers from primary to backup, and then issue a shutdown from the **Server>Shutdown Server** screen.
- When shutting down a co-resident system, you may have to wait several minutes longer than for a standalone system.

Shut down a co-resident server

Use the usual procedures for shutting down Communication Manager. These are found in the document

Maintenance Alarms for Avaya Aura® Communication Manager, Media Gateways and Servers
Doc ID 03-300430

Shut down a single server

This procedure shuts down a single server, either a combined, home or an edge.

1. Go to the Maintenance page and select **Shutdown Server** from the menu on the left.
2. On the **Shutdown Server** web page, there is a check box for **Restart**.

   The check box is checked as the default.

   The SES software shuts down the server gracefully.

Shut down both servers in a duplicated pair

This procedure applies to home or edge duplicated-server pairs.

By design, the server shutdown of a duplicated SES system follows the similar procedures as those for communication manager servers running Communication Manager.

Be aware that the **Shutdown Server** selection is not **Shutdown Entire System**. Shutdown Server shuts down the server you name in Step 1. below.

1. Start a web session to the backup server, using its physical IP address or host name.
2. From the Maintenance interface, select **Busyout Server**.
3. Make sure the backup server in the duplicated pair is out-of-service now by checking the Maintenance Server Status web page.
4. Keep the primary server in service. Select **Status Summary** of the Maintenance web page for the information.

On the **backup server**, the Status Summary screen should look like this:

```
                              SERVER STATUS


                  sv11

           Mode: Out of service
   Major Alarms: yes
   Minor Alarms: yes
Server Hardware: okay
      Processes: okay


              sv12
           Mode: Active (Unknown)
```

The **primary server** shows the Status Summary as follows:

```
                              SERVER STATUS


                  sv12

           Mode: Active (In service Primary)
   Major Alarms: yes
   Minor Alarms: yes
Server Hardware: okay
      Processes: okay


              sv11
           Mode: Active (Out of Service)
```

5. Click **Shutdown Server** on the Maintenance web page.

   Shutdown Server has a check box for a restart option. To shut down the server and leave it down, leave the check box cleared.

   On the **primary server**, the Status Summary now displays the status as below:

```
                              SERVER STATUS

                  sv12

           Mode: Active (In service Primary)
   Major Alarms: yes
   Minor Alarms: yes
Server Hardware: okay
      Processes: okay


              sv11
           Mode: Inactive (Unknown)
```

6. If you want to shut down the remaining primary server, then start a new web session to the primary server and click **Shutdown Server**.
7. Manually restart the two servers by power cycling.

   The Status Summary page shows that the backup server is out of service because of the earlier busyout action.
8. To bring the duplicated servers back in service, manually restart both server A and server B by cycling their AC power off and back on.
9. Log in using a valid user ID and password.
10. To verify a successful reboot, run the **statapp** command on both duplicated servers.

The primary server should have all these services as shown:

```
root@sv12> statapp
Watchdog       16/16 UP
TraceLogger    04/04 UP
INADSAlarmAgen 01/01 UP
CCSTrapAgent   01/01 UP
GMM            05/05 UP
SNMPManager    01/01 UP
ImLogger       04/04 UP
SipServer      40/40 UP
MtceMgr        06/01 UP * 6
mon            06/01 UP * 6
SME            08/08 UP
```

The backup server should have these services up:

```
Watchdog       15/15 UP
TraceLogger    04/04 UP
INADSAlarmAgen 01/01 UP
CCSTrapAgent   01/01 UP
GMM            05/05 UP
SNMPManager    01/01 UP
ImLogger       00/04 DOWN
SipServer      00/40 DOWN
MtceMgr        06/01 UP
drbdEventSvc   06/01 UP
mon            06/01 UP
SME            08/08 UP
```

11. On the backupserver's Maintenance web page, select **Release** to set the backup server to be the primary server **(In Service Backup)**.

Appendix A: Installation Worksheets

This appendix contains the Installation Worksheets for configuring and administering SIP Enablement Services on a server. The worksheets do not cover fields that have standard default settings.

Use the worksheets to capture the information you need to enter in the various configuration and administration screens. Make a copy of these worksheets for each server in your SES network.

The worksheets are for the following applications:

- Information entered within initial_setup script on page 325
- Information entered within the SES Administration Interface on page 326
- Information entered within DHCP/46xxsettings.txt file or 96xxsettings.txt file on page 327.

Before you go on site

Determine the following information

- Server type--Whether home, edge, or edge/home combination. Standalone or coresident with Communication Manager.
- Type of redundancy--Whether single, cable duplicated (same location), or network duplicated (separate locations).
- If duplicated, the server's role--Whether A (primary) or B (backup).

You will need several logins and passwords to complete the configuration and administration:

- Superuser login and password
- Username WebLM login and password (customer-owned; entered on the license host)
- Management System Access login and password
- Communication Manager Server Admin login and password (minimum of 7 digits).

Important Notes

- If the customer has a maintenance contract with Avaya, then a phone line for remote connectivity is required.

- Passwords must be maintained by the customer. If lost, it is a Time and Materials (T&M) escalation.
- Please make sure that these worksheets are part of the permanent customer record (Maestro, EPROJECT, Rover, and so on).

Worksheets

Table 1: Information entered within initial_setup script

Field	Information to enter
Host Name (Do not use special characters or spaces.)	
DNS Domain Name (Do not use special characters or spaces.)	
IP Address	
Netmask	
Gateway	
Primary DNS IP Address	
Secondary DNS IP Address (optional)	
Tertiary DNS IP Address (optional)	
Redundancy Configuration (Single, Cabled Duplicated, Network Duplicated)	
Redundancy Role (A or B)	
Logical Host name of redundant system (only required on a duplicated server pair)	
Logical IP address of redundant system	
Host name of server (A or B)	
IP address of server (A or B)	
Are you initializing a Master Administrator on this machine? (y or n) (not prompted on B Server in Redundant configuration)	

Table 2: Information entered within System Management Interface

Field	Information to enter
DNS or FQDN host name (network time server)	
DNS or FQDN IP address	

Table 3: Information entered within the SES Administration Interface

Field	Information to enter
SES Master Administration System for the SES Network? If not, provide IP address for the edge server that is.	
Host IP Address (typically the physical address of the edge server if duplicated. Enable on only one server.)	
Profile Service Password (must be unique for each configured host)	
Host Type (selection on dropdown menu)	
SIP Domain	
SIP License Host	
Default User Profile Host	
Communication Manager Server Interface Name (node name for server interface - C-LAN)	
Host (IP address of home server associated with interface name)	
SIP Trunk IP Address (IP address of the C-LAN or processor Ethernet interface that terminates the SIP link from SES)	
SIP Trunk Port (5061 or 6001)	
Communication Manager Server Admin Address (IP address that allow SAT access)	
Communication Manager Server Admin Port (port number of the server used to configure SIP phones)	

Table 3: Information entered within the SES Administration Interface

Trusted host IP address (IP address of the server designated as the trusted host).	
SNMP v2c Community name (community string your site uses).	

Table 4: Information entered within DHCP/46xxsettings.txt file or 96xxsettings.txt file

Field	Information to enter
FTP Server IP Address (for backup of station profiles)	
TFTP/HTTP Server IP address (for station firmware and 46xx or 96xx settings file)	
SIP stations dial plan (dial string pattern as entered in 46xx or 96xx settings file to allow station dialing without using the Send key)	
DHCP option 176 or 242 option (See *4600 Series IP Telephone LAN Administrator Guide* (555-233-507) for more details)	

Appendix B: SNMP Alerts

What is in this appendix

Read about the SES R5.2 SNMP alerts presented in these sections:

- Managing traps on page 329
- Events on page 331, summarizing the trap, its cause, and resolution

To find SNMP traps by name and not by object ID, see the Index of SNMP traps on page 435. Click on the page number there to jump to a detailed description of the corresponding trap.

Viewing the AV-CCS_MIB file

The **AV-CCS-MIB** contains definition of all the supported SNMP Traps.

If you want a copy of the SNMP traps reported to the SNMP Trap Manager system, you can download the AV-CCS-MIB file from the SES R5.2 server.

To view the AV-CCS-MIB file:

- Click **View AV-CCS-MIB Data** link in either **Server Configuration** or **SNMP Configuration** page in the SES Administration Web Interface.
  The AV-CCS-MIB.asn1 file is displayed in the web page.

  Note:

  The AV-CCS-MIB file is for SNMP trap notification events only and does not support SNMP get or walk (browse) operations.

Managing traps

SNMP enables the SIP Enablement Services system to do the following things:

- Report the alarm events to the external manager entities such as Avaya INADS, Avaya Fault Performance Manager, Avaya Network Management System, and third party entities (for example, HP OpenView).
- Respond to the query requests from the external manager entities for the product configuration information. This only works on queries for MIB-II objects.

Network management using SNMP requires several components:

- Network manager or management station such as FPM or HP OpenView
- Managed network element's agent
- Management information base (MIB)

The customer supplies the network management station. The agent and MIBs are typically supplied by the network element vendor. The agent is co-resident with the managed element and is a subcomponent of the platform management system. MIBs are either standard or custom-built from the vendor. SIP Enablement Services supports certain groups of the IETF standard MIB-II as well as a custom Avaya SES MIB (for trap support only).

Remote maintenance boards

The SES hardware supports a remote maintenance boards (RMBs) called a Server Availability Management Processor or SAMP.

The extra reporting mechanism from the SAMP can be extremely helpful. If SES processes or the SES server itself is down, it cannot report its own condition. The SAMP provides the capability to restart and monitor processes on the SES server.

Events

This section discusses SNMP events into these sections:

- Administration system traps
- Standard MIB support

In the tables in all these sections, **RO** indicates Read Only and **NA** means Not Applicable.

Traps with a severity of **warning** are not sent as traps, but are logged in the syslog and the alarm log only:

avCCSApacheStartOK
avCCSConfCapacity
avCCSDBStartOK
avCCSDBUpgradeOK
avCCSVacuumOK
avCCSDiskWarning
avCCSEthfaultclear
avCCSUPSstatus
avCCSEvtSvrStartOK
avCCSEvtSvrPkNotSupported
avCCSEvtSvrCMSubRetry
avCCSEvtSvrCMResubscribe
avCCSEvtSvrSubsRej
avCCSProcessStop
avCCSRegRegAuthFailed
avCCSSerialLinkUp
avCCSIMLoggerStartOK
avCCSIMLoggerWarning
avCCSRegReqAuthFailed
avCCSProcessStartOK
avCCSProcessStop
avCCSAdminPSPwdUpdated
avCCSMemfaultclear

The exceptions are the following traps, which are not true traps but are defined as such in the MIB. These traps are logged in syslog, but *not* in the alarm log:

avCCSApacheStartOK
avCCSDBStartOK
avCCSEthFaultClear
avCCSProcessStartOK
avCCSSerialLinkUp
avCCSUpgradeOK
avCCSVacuumOK

Administration system traps

These traps monitor the administration system for events that indicate software problems.

OID	Object Type	Description	Variables
.47	avCCSAdminDBAccess major	The master administration database cannot be accessed by the administration subsystem.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The master administration database on a system is inaccessible. 1. Verify the `~postgres/data/pg_hba.conf` file for database file permissions. 2. If using DNS, verify that the host name is resolvable and authorized to access the DB as defined in the `pg_hba.conf` file. 3. Verify that Postgres is running. 4. Verify that the correct host name is administered in `/usr/impress/admin/share/impress.ini` under the [ImpressDb] section of the file on the system.			
.48	avCCSAdminRuntimeDBAccess major	The administration system cannot access the runtime database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostName avCCSAlarmType avCCSProductID
.49	avCCSAdminFailedLogin major	Administrator login has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
An administrator trying to log in has entered the incorrect password. Verify that the correct password for the administrative login is being used.			
.50	avCCSAdminError minor	An administration error has occurred	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
An administration function has raised an error. Examine the appropriate line number of the affected file as specified in the error log message for details.			

OID	Object Type	Description	Variables
.51	avCCSAdminPWCreateFailed major	A password create has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The system was unable to add or update a user's password. Verify that the installation of the administrative tools and shared libraries was successful by seeing if `/opt/ecsweb/admin/share/bin/epwd` exists, and if the `/opt/ecs/web/admin/share/lib` directory exists and is populated.			
.90	avCCSAdminDBnotCompatible major	The database schema between the edge and home servers are not compatible.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
On both servers, use the System Management Interface and check the version number of SES. Take one of the machines out of service and reinstall the version of SES that will make the two match. A **force all** or **update** to a home server has failed because the DB schema version of the master administration database does not match that of the runtime database on a home/edge or edge with homes. This can happen when a system is upgraded, a dbupgrade has occurred and the **import** command is used to restore the system data rather than the **restore** command. Although the system and database may contain the latest DB schema version, the imported data contain an old database schema that causes this error. Do not use the **import** command for a data restore following an upgrade. Restore data following an upgrade using the **restore** command only.			
.125	avCCSDBSchemaError major	SES system software does not support the schema version of SES database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This major error can occur when an upgrade occurs. Older version may use a different database schema than the upgraded version. This causes the database schemas to be mismatched. Most likely, you will have to back off any user data if possible, and wipe the hard drive clean, and then reinstall your upgrade version.			

Apache events traps

Both the Administration Web interface system and PPM (accessed via the SIP PIM) run on an Apache web server. This web server is monitored by the traps described in this section.

Although the trap `avCCSApacheStartOK` is an informational trap, the trap `avCCSApacheStop` is a major event.

OID	Object Type	Description	Variables
.43	avCCSApacheStartOK minor	The Apache web server has started.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. The Linux Service Apache service has started. This event is not sent as a trap, but is written to the syslog.			
.44	avCCSApacheStartFailed major	The Apache web server has failed to start.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The Apache web server service failed to start. The web service to the SES server is down.			
.45	avCCSApacheStop minor	The Apache web server has stopped.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The Apache web server service is stopped. Apache service is a critical component for SES server operation. Resolve: 1. Login as super user and enter **service httpd restart** at the command line. 2. If the httpd service still cannot be started, escalate the problem to Avaya Services.			
.96	avCCSApacheCertExpired major	The Apache web server certificate has expired.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The certificate used to authenticate the web server has expired. To replace this certificate, log onto this server's Web pages and generate a new certificate signing request. See Generate Web Certificate Signing Request screen on page 288. Have this request signed by the CA of your choice and install the resulting certificate.			

Certificate expiration traps

Without these certificates in place, SES services will fail. Take note if you see the warning that the system has entered the 10 day grace period.

OID	Object Type	Description	Variables
.93	avCCSCertExpWarn minor	The server certificate will expire in less than 10 days.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSCertCommonName
The certificate indicated in this trap (see avCCSCertCommonName) will expire in less than 10 days. This certificate needs to be replaced. Until this certificate is replaced, this trap will appear daily until the day before expiration. If the certificate indicated in this trap is the certificate used by Apache: Replace this certificate by the expiration date to properly authenticate the server and prevent web browser warning messages. To replace this certificate, log onto this server's System Management Interface and generate a new certificate signing request. See Generate Web Certificate Signing Request screen on page 288. Have this request signed by the CA of your choice and install the resulting certificate. If the certificate indicated in this trap is the certificate used for secure signaling: Please contact Avaya Services immediately to replace this certificate.			
.94	avCCSSIPCertExpired major	The SES proxy server certificate has expired.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSCertCommonName
The certificate used for SIP signaling has expired. Please contact Avaya Services immediately to replace this certificate.			

Presence server events traps

Traps generated by the presence server present as problems with instant messaging.

OID	Object Type	Description	Variables
.59	avCCSPresRegAccess major	The presence server cannot access the registrar.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Restart the SIP Server. Note that presence cannot be matched properly if the handle of the watched user does not match exactly, including its case.			

Conference server events traps

Traps generated by the conference server indicate software problems.

OID	Object Type	Description	Variables
.60	avCCSConfCapacity warning	The conference server has used up to 80% of its allotted conference extensions.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Allocate more conference extensions. The demand has outgrown the administered number of conference extensions, and soon, the requests to create click-to-conference sessions may start failing.			
.61	avCCSConfCapExceeded major	The conference server has exceeded its allotted number of conference extensions.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Allocate more conference extensions. The demand has outgrown the administered number of extensions and the requests to create click-to-conference sessions are failing.			

OID	Object Type	Description	Variables
.62	avCCSConfUnauthAccess major	An unauthorized user is using a conference extension.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSUserContact avCCSConferenceExtURI avCCSProductID
A user has dialed into a Meet Me number that is reserved as a conference extension, and is not allocated for any click-to-conference call. Make sure the Meet Me number has not been compromised. Delete and administer another one if compromised, otherwise reset it to make it available for use.			

Critical server events traps

The following traps are generated by critical events occurring on a home or edge server:

OID	Object Type	Description	Variables
.18	avCCSVIPFault major	The Virtual IP address is not operational on this server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The virtual IP address used for server redundancy is no longer operational. This can happen if someone configures another server with the same IP address. Find the erroneous, duplicate IP addresses and change one of them.			
.19	avCCSRAID1 major	The RAID 1 system is not operational.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			
.20	avCCSMONfault major	A required system process has stopped responding to MON.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
A required system process has stopped responding to MON. From the System Management Interface, view the Process Status screen to verify this. Reboot the server and verify that MON is running. If the situation persists, contact Avaya Services.			
.21	avCCSDRBDFault major	DRBD cannot be loaded or executed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
DRBD (distributed redundant block device) cannot be loaded or executed. The system is no longer redundant. See the avCCSHAFault error prior to this one. Call Avaya Services immediately.			
.22	avCCSIPfailFault major	IPfail cannot be loaded or executed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
IPfail cannot be loaded or executed. Reboot the server. If the situation persists, contact Avaya Services.			

Database events traps

The database events are monitored for the traps described here.

OID	Object Type	Description	Variables
.41	avCCSDBStartOK minor	The database process has started.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. The database process has started. This event is not sent as a trap, but is written to the syslog.			

OID	Object Type	Description	Variables
.40	avCCSDBStartFailed major	The database process has failed to start.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The database process has failed to start. Users will not receive services. Restart the server and verify that the database is running by checking for this condition on the Alarms screen of the System Management Interface. The the alarm generated is avCCSDBStartFailed. If the situation persists, contact Avaya Services immediately.			
.41	avCCSDBStop minor	The database process has stopped.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The database process has stopped. If this is due to administrator action, users will not receive service until the database is restarted. If this was not due to administrator action, reboot the server and verify that the database process has started. Look for the avCCSDBStartOK trap or use **ps -u postgres** to check. If the database will not restart, contact Avaya Services.			
.42	avCCSDBVacuumFailed minor	The database vacuum has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The database vacuum has failed. If the situation persists, please contact Avaya Services.			
.88	avCCSDBUpgradeFailed major	The database upgrade failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSDBUpgErrorMesg
Contact Avaya Services.			

OID	Object Type	Description	Variables
.88	avCCSDBUpgradeOK major	The database upgrade was successful.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational only. This event is not sent as a trap, but is written to the syslog.			
.91	avCCSVacuumOK warning	The database vacuum was successful.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational only. This event is not sent as a trap, but is written to the syslog.			

Disk error traps

Disk errors are significant to the health of the SES system. The following traps reflect disk errors:

OID	Object Type	Description	Variables
.10	avCCSDiskWarning* major	The data disk is 90% full	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSDiskPartition
The data disk is 90% full. Take immediate action to avoid a service outage. Back up any logs, temp files, and any superfluous data to another disk. If this error is due to log file accumulation, delete old logs, with approval, or move big logs to off-line storage. Depending on which disk partition is filling, the remedy can be different. This is a administration issue and resolution may be specific for your installation.			

OID	Object Type	Description	Variables
.11	avCCSNoDiskSpace** major	The data disk is 98% full.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSDiskPartition
The data disk is full. This error causes loss of service to if not corrected. Depending on which disk partition is filling, the remedy can be different. This is an administration issue and resolution may be specific for your installation.			

* Each disk partition is checked every 10 minutes. The database partition has a threshold of 60% full. Other partitions have a threshold of 90%. Once the threshold is crossed, the system sends the avCCSDiskWarning error.

**For the avCCSNoDiskSpace trap, the database partition has a threshold of 80% full. Other partitions have a threshold of 98%.

Duplicate server events traps

The traps in this section apply only when your system's configuration is duplicated, that is, has a backup server for either a home/edge, home, or edge server.

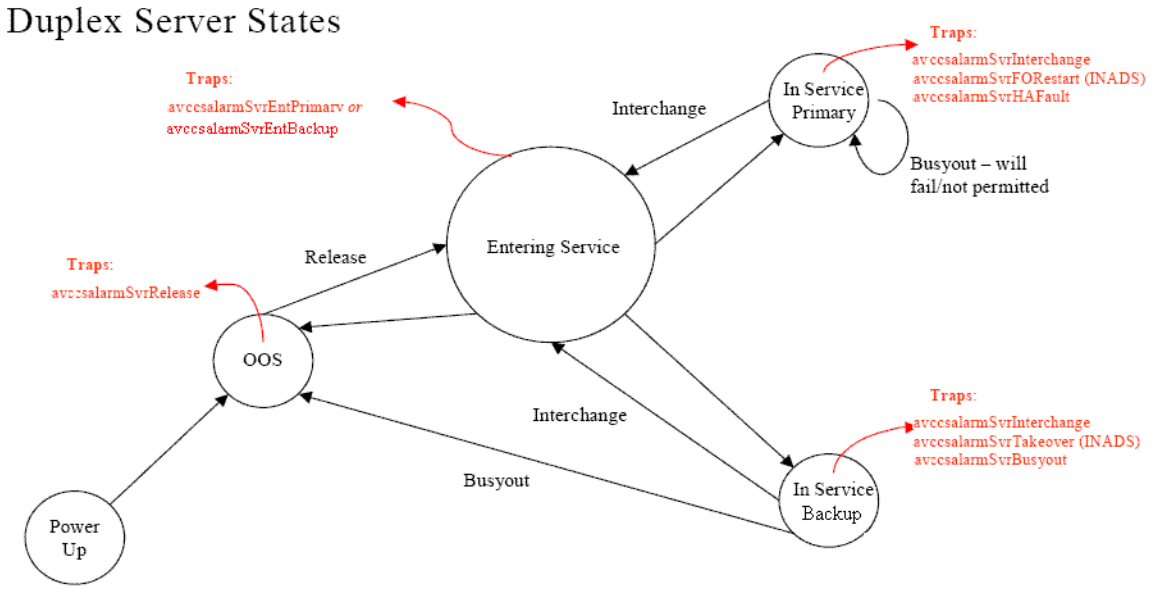
Figure 1 shows two important concepts:

- The direction and type of state changes that can occur for any server
- The changes of state a duplicated server may go through in the event of critical errors

A duplicated server *must* be aware of its role, either primary or backup. All duplicated traps are considered critical.

All administrative busyouts and releases are trapped and logged.

Figure 1: Duplicated Server State Changes



OID	Object Type	Description	Variables
.23	avCCSHAfault major	The server is no longer redundant.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
A fault of the redundant pair has been detected. The high availability operation is down. To resolve this alarm: 1. Check the system status by viewing the System Management Interface, Status Summary screen. 2. If the server has been busied out, then click the Release Server screen of System Management Interface to put the server back to service 3. If the alarm persists, escalate the problem to Avaya Services. If this error is not corrected, you might see avCCSDRBDFault. Call Avaya Services immediately.			
.24	avCCSFORestart major	The system has failed over to the backup system.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
The backup server has restarted as the primary server due to the failover. The original primary server may experience non-recoverable faults. To resolve this alarm: 1. View the Status Summary screen to verify the role of the duplicated server, which should be primary or backup. 2. If not, escalate the problem to Avaya Services.			
.81	avCCSSvrBusyout minor	The server has been administratively busied out.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server has been busied out manually. The redundant system cannot provide high availability operation. To resolve this alarm: 1. Check the system status by viewing the Status Summary screen of the System Management Interface. 2. If the server has been busied out, then click the Release Server screen of System Management Interface to restore the server back to service. 3. If the alarm persists, escalate the problem to Avaya Services.			
.82	avCCSSvrRelease minor	The server has been administratively released.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server has been manually released back to service. The redundant system is in transition to the high availability operation. To resolve this alarm: 1. Check the system status by viewing Status Summary screen of the System Management Interface. The Status Summary should show the role as primary or backup. 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services.			
.83	avCCSSvrInterchange major	The server has been administratively interchanged.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
A system administrator has initiated an interchange using the Interchange Server screen of the System Management Interface. 1. Check the system status by clicking Status Summary screen of System Management Interface. The Status Summary should show the state primary/ backup 2. If the server is not in primary or backup state, escalate the problem to Avaya Services.			
.84	avCCSSvrEntPrimary minor	The server is entering service as the primary server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server is entering the primary role. 1. Check the system status by clicking Status Summary screen of System Management Interface. The Status Summary should show the state primary/ backup. 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services.			
.85	avCCSSvrEntSecondary minor	The server is entering service as the secondary or backup server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server is interchanging to the backup role. 1. Check the system status by visiting Status Summary screen of the System Management Interface. The Status Summary should show the role as primary or backup. 2. If the server is not in the primary or backup state, escalate the problem to Avaya Services.			

OID	Object Type	Description	Variables
.86	avCCSSvrTakeover major	The server is taking over as primary server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The backup server is taking over as the primary. The existing primary server may experience faults. 1. Check the system status with the Status Summary screen of the System Management Interface. The Status Summary should show the role as primary or backup. 2. If the server is not in the primary or backup state, escalate the problem to Avaya Services.			

Ethernet links traps

Ethernet bus faults may result in complete loss of server functionality. The public link interfaces with clients; the private link is for duplication purposes. The services link is not monitored.

The following traps are generated by the Ethernet bus:

OID	Object Type	Description	Variables
.5	avCCSEthfaultPublic major	An Ethernet link fault has occurred on the public interface.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSproductID
The SES server's *public* Ethernet interface is no longer operational. Verify that there is a physical connection to this port and that network connectivity exists on other hosts on the same network. If this situation persists, contact Avaya Services.			
.6	avCCSEthfaultPrivate major	An Ethernet link fault has occurred on the private interface.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSproductID
The SES server's *private* Ethernet interface is no longer operational. Check the LAN cable and connection between the two servers. Verify the physical connection to this port and the connectivity on other hosts. If this situation persists, contact Avaya Services.			

OID	Object Type	Description	Variables
.7	avCCSEthfaultclear warning	The Ethernet bus fault has been cleared.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSproductID
The Ethernet fault previously identified is cleared now. avCCSEthfaultclear is not sent as a trap but is logged to syslog.			

UPS events traps

If a universal power supply (UPS) is used, these traps alert an administrator when it comes into service, and of any state changes.

Event Server event traps

OID	Object Type	Description	Variables
.52	avCCSEvtSvrStartOK warning	The event server process has started.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. Take no action. This is not sent as an error. In SES 5.2, the event server is eliminated. You should never see this error in release 5.2.			
.53	avCCSEvtSvrStartOK Major	The event server process has failed to start as expected.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. Take no action. This is not sent as an error. In SES 5.2, the event server is eliminated. You should never see this error in release 5.2.			
.54	avCCSEvtSvrStop Major	The event server process has stopped unexpectedly.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
In SES 5.2, the event server is eliminated. You should never see this error in release 5.2.			
.70	avCCSEvtSvrDBAccess major	The event server cannot access the database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
In SES 5.2, the event server is eliminated. You should never see this error in release 5.2. Generallly, check the status of the Postgres service using the **service postgresql status** command. Restart the Postgres service if it is stopped. Each of the following specific messages has a specific solution. • avCCSEvtSrvDBAccess: EventServer DB Error: database failure - addWatcher solution: Report this serious error to Avaya Services. • avCCSEvtSrvDBAccess: EventServer DB Error: database failure - getAliases: Report this serious error to Avaya Services. • avCCSEvtSrvDBAccess: EventServer DB Error: database failure - addwatcher: Report this serious error to Avaya Services.			
.71	avCCSEvtSvrSOAPinitFailed major	The event server failed to initialize the SOAP interface.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The PPM communication to endpoints must have the SOAP server. Restart the SES server if the SOAP server still fails to start.			
.72	avCCSEvtSvrSubsRej warning	An endpoint subscription was rejected by the event server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSEvtSvrReason avCCSEvtSvrPkj avCCSUserPrimHandle avCCSProductID
The event server rejected an endpoint subscription request. This could be simply a configuration issue, such as no communication manager server administered for this user, or a security problem where someone who is not allowed is trying to access resources. Check your communication manager servers against the data in the trap.			
.73	avCCSEvtSvrCMSubFailed major	The event server Communication Manager subscription has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMHostname avCCSCMHostname avCCSCMIPAddress avCCSalarmType avCCSEvtSvrPkgName avCCSEvtSvrReason avCCSProductID

OID	Object Type	Description	Variables
The event server subscription to Communication Manager has failed. This trap occurs because of some configuration problem, possibly these: • Communication Manager may not know about the SES host or has not been administered properly. • Domains are misconfigured. • Domain servers have incompatible versions of software loaded.			
.74	avCCSEvtSrvCMSubRetry warning	The event server is retrying a subscription to Communication Manager.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMHostname avCCSCMIPAddress avCCSEvtSvrPkj avCCSEvtSvrReason avCCSalarmType avCCSProductID
The event server is retrying a subscription to a communication manager server because the communication manager server has not been accessible. This could be because of the network problems or because the Communication Manager was rebooting. Check the network for outages. Wait for Communication Manager to fully reboot. If you get this specific message: avCCSEvtSrvCMSubRetry: EventServer is retrying a subscription to the Communication Manager			
.75	avCCSEvtSvrCMPkgNotSupported major	Communication Manager does not support this event package.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMHostname avCCSCMIPAddress avCCSEvtSvrPkj avCCSalarmType avCCSProductID
Communication Manager rejected a subscription request because it does not support that event package. Check for incompatible versions of software running on SES servers and Communication Manager.			
.76	avCCSEvtSvrMemError major	The event server does not have sufficient memory resources.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSUserPrimHandle avCCSProductID

OID	Object Type	Description	Variables
1. Check the total memory usage on the system using the **top** command and restart the system if the available physical memory is very low.			
.77	avCCSEvtSvrPkgNotSupported warning	The event server has received a subscription for a non-supported SIP protocol event package.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSUserPrimHandle avCCSProductID
.78	avCCSEvtSvrCMResubscribe warning	The event server has received a request from Communication Manager to recreate event server subscriptions to Communication Manager.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMIPAddress avCCSEvtSvrPkj avCCSalarmType avCCSProductID
The event server is trying to renew subscriptions to Communication Manager because of a Communication Manager reboot. When the Communication Manager is fully rebooted, the warnings stop.			

IM Logger events traps

The traps generated by the IM Logger indicate file/disk space problems regarding the logs.

OID	Object Type	Description	Variables
.63	avCCSIMLoggerStartOK Warning	The IM logger process has started	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. No action necessary.			

OID	Object Type	Description	Variables
.64	avCCSIMLoggerStartFailed Major	The IM logger process has failed to start as expected.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.65	avCCSIMLoggerStop Major	The IM logger process stopped.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.66	avCCSIMLoggerWarning major	80% of the maximum administered space for IM log files has been reached.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
80% of the maximum administered space for IM log files has been reached. If not corrected, expect to see the trap .67, discussed in the next row.			
.67	avCCSIMLoggerNoLogSpace major	The maximum administered space for IM log files has been reached.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The maximum administered space for IM log files has been reached. The system is deleting old log files to make space for newer ones.			

License-related events traps

If a server has a license error, it may impact service, perhaps several days later. Supporting details for these traps, such as not being able to connect to the WebLM server, are captured in the error log.

OID	Object Type	Description	Variables
.79	avCCSLicErrorMode major	The server is within the grace period for a license that could not be obtained. The server still provides service.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSLicErrorMessage
The grace period for the license has been exceeded and service will be suspended for one of the following: • basic license—no proxy service • home seats—the number of exceeded users will be disabled • edge—no edge routing will be performed (no routing out of the domain)			
.80	avCCSNoLicense major	The server is outside of the grace period for a license that could not be obtained and no longer provides service for that feature.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server could not get a license, but has service due to the grace period. The syslog message and the administration screen message states why the server could not get a license. Advise management to correct the license expiration within the grace period to avoid losing service.			
.87	avCCSLicSeatsExceeded minor	There are more provisioned users than there are licenses.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This trap indicates that the number of home seats has been exceeded. Advise management to purchase more home seat licenses.			

Personal Profile Manager events traps

The PPM (accessed via the SIP PIM) contributes information into the database. These traps indicate PPM access to the database.

Expect the trap `avCCSPPMInitError` to occur during initial installation only.

OID	Object Type	Description	Variables
.46	avCCSPPMDBAccess minor	PPM is not able to access the database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This event can occur for two reasons: 1. PPM is not able to connect to the database. A single event probably indicates that some element in the system was temporarily out of service, but able to restore itself. If this event repeats constantly, then a more serious problem exists. If PPM is the only element reporting an event indicating that the database is not accessible, try restarting tomcat using the **`service tomcat4 restart`** command from the Linux prompt. If the problem continues, a system error exists that requires additional services support. 2. PPM detected corruption in the database. If the event repeats, inspect the PPM log (`/var/log/sip-server/ppm.log` or `ppm.log.1`, `ppm.log.2`, and so on) for additional information. The problem might be fixed by using the Administration interface to remove the user, as identified by the information in `ppm.log`, and then add the user back. If not, this problem will likely require additional services support.			
.68	avCCSPPMResourceError minor	PPM is not able to access the indicated resource.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSPPMResource

OID	Object Type	Description	Variables
This event may occur for several reasons: 1. This error may be caused by incomplete information in the database. From the Administration interface, run the **Force All** command. If you recently performed a migration to a higher version level, make sure you have all the new fields completed. If the problem continues, additional services support is required. If you run Force All, expect a service outage. 2. PPM obtains a variety of information from associated Communication Manager communication manager servers, and the SES configuration for accessing Communication Manager might be incorrect. • Go to the Administration interface and check the data on the Edit communication manager server screen. • Go to the **Edit Communication Manager Server** screen and make sure that you have stipulated a valid password that is of type `Customer` and service level `superuser` at a minimum. Also, inspect the communication manager servers configurations. See Edit Communication Manager server Interface screen on page 245 and make sure all the values there are correct. • Try re-entering the login and password (these must match a SAT login and password on Communication Manager). • Note that in periods of heavy traffic, various elements in the system might shed load to support higher priority tasks. Alarms might reflect this behavior. • If you run **Force All**, expect a service outage. 1. The communication manager server running Communication Manager may be momentarily unavailable, perhaps performing reboot. If you get the specific error: avCCSPPMResourceError: nested exception is: ^lorg.xml.sax.SAXParseException: avCCSPPMResource Error: (0)null (avCCSPPMResource MAWS reports fault = (0)null) Do this to correct it: If the problem continues, request additional services support.			
.69	avCCSPPMInitError major	PPM initialization error has occurred	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSPPMError
This event is generated for these reasons: 1. This event indicates that PPM was not able to decrypt data, likely because of an internal software error. Additional services support is required. 2. This error indicates that PPM could not read the `ccs.conf` file during initialization, and therefore PPM is not running. Verify that the **ccsConf** parameter found in the `web.xml` file `/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml` points to the `ccs.conf` file, and that permissions on the file allow it to be read.			

OID	Object Type	Description	Variables
3. This event indicates that PPM was not able to determine the server's online status during initialization, so PPM is not running. Verify that the **statusCommand** parameter found in `web.xml` (`/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml`) fully qualifies the res-status command that can be executed from the shell to determine server status in a redundant system.			
4. This event indicates that PPM was not able to load the database driver during initialization, so PPM is not running. Verify that the **dbDriveName** parameter found in `/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml` specifies the fully-qualified Java class name of the JDBC driver (org.postgresql.Driver). 5. This event indicates that PPM did not obtain the location of its database during initialization, so PPM is not running. Verify that the **DbURL** parameter found in `web.xml` correctly identifies the location of the SES/PPM database (jdbc:postgresql:mvss).			
6. Inspect the `ppm.log` file and look for more information. This may depend on coding. Additional services support is required. 7. This event indicates that PPM was not able to connect to the database at initialization time, so initialization failed. Verify that postgres is running. Restart tomcat by running the **service tomcat4 restart** command from the Linux prompt.			
8. This event indicates that PPM encountered a fault getting data from the database. The error code was returned by postgres and should help explain the problem. 9. If an SES server restarted, this trap is expected. Otherwise, check `ppm.log` (`/var/log/sip-server/ppm.log`, or `ppm.log.1`, `ppm.log.2`, etc) for more information. Note that in a redundant system, PPM is restarted on the transition from backup to primary, so this event indicates the server switch over.			
10. This event indicates that PPM was not able to decrypt data, likely caused by an internal software error. Additional services support is required.			
.	avCCSlogResourceError	PPM xxx has occurred.	
	AxisFault remote exception from SMS - SMS Adapter	LOG_SMS_ERROR	
	AxisFault remote exception from SMS - SMSSessionAdapter	LOG_SMS_ERROR	

OID	Object Type	Description	Variables
PPM obtains a variety of information from associated Communication Managers. 1. Inspect the `PPM log` (`/var/log/sip-server/ppm.log`, or `ppm.log.1`, `ppm.log.2`, etc) and the syslog (`/var/log/messages`, or `messages.1`, `messages.2`, etc) for additional information, such as the address of the Communication Manager from which PPM was unable to obtain information. 2. From the Administration interface, inspect the communication manager servers' configurations. See the definitions for this page described in Edit Communication Manager server Interface screen on page 245. 3. Try re-entering the login and password (these must match a SAT login and password on Communication Manager). 4. If the PPM log shows socket read time outs, increase the `smsWaitTime` parameter in the `/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml` file and restart Tomcat (using the `service tomcat4 restart` command from the Linux prompt). 5. If the problem continues, additional Services support is required. Note that in periods of heavy traffic, various elements in the system might shed load to support higher priority tasks. The alarms might reflect this behavior.			
	Could not create master admin service port	LOG_MAWS_URI_ERR OR	
This error may be caused by incomplete information in the database. From the Master Administrator interface, try running the **force all** command. If the problem continues, additional services support is required.			
	malformed URI for master admin service	LOG_MAWS_URI_ERR OR	
This error may be caused by incomplete information in the database. From the Master Administrator interface, try running the **force all** command. If the problem continues, additional services support is required.			
	remote exception from master admin service	LOG_MAWS_ERROR	
This error indicates a problem communicating with the master administration service. 1. If the alarm repeats, inspect the PPM log (`/var/log/sip-server/ppm.log`, or `ppm.log.1`, `ppm.log.2`, etc) for additional information about the problem. 2. If the PPM log shows that the socket read timed out, increase the mawsWaitTime parameter in the `/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml` file and restart Tomcat (run the command `service tomcat4 restart` from the Linux prompt). 3. For other causes, try running the **force all** command. 4. If the problem continues, additional service support is required.			

OID	Object Type	Description	Variables
.95	avCCSPPMModifiedData warning	PPM has provided reduced or modified data.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
PPM has been forced to provide dial plan data that have been somehow reduced or modified. Depending on the truncation scheme configured, some dial plan data have been omitted, or each of the terms has been shortened, forcing the client to use an inter-digit timer to determine end of dialing. Use either of the following remedies: 1. Increase the maximum number of terms that PPM may provide. 2. Modify the AAR and ARS analysis tables on Communication Manager to define general rules with specific exceptions. A sample entry in the alarm log looks like this: `605 SES 95 MIN Y Wed Apr 20 12:43:32 EDT 2005 avCCSPPMModifiedData: Dialplan was truncated for handle 8896`			

Proxy events traps

These traps indicate proxy events of which an administrator should be aware. The first two, .34 and .38, below, are both event errors. The last two, .34 and .38, indicate software errors.

OID	Object Type	Description	Variables
.34	avCCSProxyDBAccess major Software error	The proxy cannot access the database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			
.37	avCCSProxyLinkAccess major Software error	The proxy cannot access the TLS link to Communication Manager or another proxy.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProxyHostname avCCSProductID

OID	Object Type	Description	Variables
Check all connections to another edge server or third-party proxy. Consider that access to third party proxies may occur through address maps. See Edit Communication Manager Server Map Entry screen on page 251.			
.38	avCCSProxyUserAuth major Software error	The proxy cannot authenticate a user.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSUserPrimHandle avCCSProductID
Contact Avaya Services.			
.92	avCCSProxyMMAccess Major	The proxy cannot access the TLS trunk to Modular Messaging due to authentication failure.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSMMHostname avCCSProductID
Contact Avaya Services.			

Registrar events traps

Traps generated from the registrar server indicate software problems.

Add a string detailing the username used during authentication failure events.

OID	Object Type	Description	Variables
.57	avCCSRegRegAuthfailed (note the letter G) warning	A registration authentication attempt failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This is not sent as an error, but is written to the syslog.			

OID	Object Type	Description	Variables
.58	avCCSRegRequestAuthFailed warning	An authentication request failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This is not sent as an error, but is written to the syslog.			

SES Data Service events traps

OID	Object Type	Description	Variables
.124	avCCSSDSStartFailed major	The SES data service tried to start but failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostName avCCSAlarmType avCCSProductID
Wait for the svc_mon to start the SES data service. This error is self-correcting by the system. If not, contact your Avaya support representative.			
.127	avCCSSDSRestartFailed major	Recovery of SES Data Services failed	sysUpTime, sysObjectID, avCCSIPAddress, avCCSHostName, avCCSAlarmType, avCCSProductID
.128	avCCSPPMhttpdStop MINOR	The PPM httpd service has stopped for some reason.	sysUpTime, sysObjectID, avCCSIPAddress, avCCSHostName, avCCSAlarmType, avCCSProductID
This warning notifies you that the PPM data push has not completed. Check the SES status screen first, then wait for self-correction. If the situation does not resolve itself automatically, call Avaya support.			

OID	Object Type	Description	Variables
.129	avCCSSDSReplicationFailed MINOR	The SES Data Service replication encountered an error.	sysUpTime, sysObjectID, avCCSIPAddress, avCCSHostName, avCCSAlarmType, avCCSProductID
This minor alert should self-correct. Check the SES status screen and wait. No action needed.			

Serial link events traps

In a duplicated configuration, a serial link connects the two duplicated servers.

OID	Object Type	Description	Variables
.25	avCCSSerialLinkUp warning	The serial link is up.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. Take no action. avCCSSerialLinkUp is not sent as a trap but will be logged to syslog.			
.26	avCCSSerialLinkDown major	The serial link is down.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The serial link between duplicated servers is down. Redundancy of servers is no longer possible, although the primary server may still be handling calls. Verify the serial cables and the physical connection to the Ethernet port. If the situation persists, contact Avaya Services.			

Watchdog event traps

Watchdog traps were formerly based on watchdog process events. Now, they reflect events of processes *monitored* by the watchdog.

The following traps are generated by the watchdog process about its watched events:

OID	Object Type	Description	Variables
.15 .29	avCCSProcessStartOK warning	The watchdog-monitored process has started.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProcess
avCCSProcessStartOK is not sent as a trap but is logged to syslog.			
.16 .30	avCCSProcessStartFailed major	The watchdog-monitored process has failed to start.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProcess
Contact Avaya Services.			
.17 .31	avCCSProcessStop minor	The watchdog-monitored process has stopped.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProcess
avCCSProcessStop is not sent as a trap but is logged to syslog.			

Core Router Notification traps

These traps relate to the core router used in Avaya Communication Manager Branch Edition.

The following traps are generated by the watchdog process about its watched events:

OID	Object Type	Description	Variables
.111	avCCSAdminPSPwdUpdated warning	Profile Service Password used for DECM (Distributed Enterprise Communication Manager) Manager login authentication has been updated at the SES Master Administration web service.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.112	avCCSMawsLoginFailed minor	DECM (Distributed Enterprise Communication Manager) logins to the Master Administration Web Service (MAWS) web service failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.113	avCCSMawsDBAccessError minor	MAWS (Master Administration web service) cannot access the SES database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			
.114	avCCSSipLinkTestFailed major	The SIP link test from the core router to a branch has failed. The IP address of the branch is provided in the error.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProxyIPAddress
Contact Avaya Services.			
.122	avCCSAMQStartFailed major	Starting SES ActiveMQ Services has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
Contact Avaya Services.			
.126	avCCSAMQRestartFailed major	Recovery of SES ActiveMQ failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			

Uncategorized traps

These traps are in the MIB but are as yet unassigned to a group discussion.

OID	Object Type	Description	Variables
.8	avCCSMemfault major	A fault has been detected in memory.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Receiving this error may indicate a hardware failure, or, it may mean that memory is insufficient or not being managed properly. Use your system utilities to track memory usage. Wait for the system to self-correct and look for event .9, Memfaultclear. Contact Avaya Services.			
.36	avCCSProxyCMAccess major Software error	The proxy cannot access the TLS trunk to Communication Manager.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSCMHostname avCCSProductID
.9	avCCSMemfaultclear Warning	The proxy cannot authenticate a user.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
This is notification that a memory fault has been cleared.			
. 32	avCCSProxyRegAccess Major	The proxy process cannot access the registrar.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			
. 33	avCCSProxyEvtSrvAccess Minor	The proxy process cannot access the event server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			
.35	avCCSProxyConfAccess Minor	The proxy process cannot access the conference server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This trap is sent when conference servers are unavailable for some reason. See Conferences screens on page 210. The result is no conference calls can ensue, but single calls go through.			

Standard MIB support

The SES system also supports the following groups within the IETF (RFC 1213) standard MIB-II:

- MIB-2 System Group
- MIB-2 IF Group
- MIB-2 IP Group
- SNMP Group

SNMP set traps or notifications are not supported for MIB-II.

The above MIB-II groups allow network management consoles to recognize each SES server individually as an Avaya IP network element. These groups contain the only MIB objects for which SES supports SNMP get or browse operations. The objects in SES custom MIB file AV-CCS-MIB are for SNMP trap notification events only.

INADS Support

This section discusses traps resulting in INADS calls.

The Global Alarm Manager monitors the following traps, which apply alarm rules to determine when to forward INADS alarm. Traps are sent at the time the event occurs, and again in an hour if the situation persists.

The MIB requires an object ID under the Avaya `sip-prod-mib` subtree. The MIB avCCS is placed in this branch of the Avaya sub-tree:

```
avaya 1.3.6.1.4.1.6889
     mibs (2)
          avSIPMibs (5)
               avCCSMib (1)
```

Appendix C: IM log example

The following text is an example of a log file from SES R5.0.

20051021:095311769:1:Proxy(5275):CRITICAL:[IMLogger Test 1, 10, 100]

20051021:163123984:2:Proxy(5495):CRITICAL:[[MESSAGE sip:sue@lzsip.com SIP/2.0

From: "joe" <sip:joe@lzsip.com>;tag=-36acf75b43594a0454203570_F10.10.10.55

To: sip:sue@lzsip.com

Call-ID: 7_10c6eb63-517d757b54203568_M@10.10.10.55

CSeq: 7 MESSAGE

Via: SIP/2.0/TLS 10.10.10.55:5061;branch=z9hG4bK7_10c6eb63-5f421f3f5420357e_M

Content-Length: 144

Max-Forwards: 70

Content-Type: text/html

User-Agent: Avaya SIP Softphone

Supported: replaces

hello sue!!

]]

20051021:163139817:3:Proxy(5495):CRITICAL:[[MESSAGE sip:joe@lzsip.com SIP/2.0

From: "sue" <sip:sue@lzsip.com>;tag=6ed93bb143594a36540612bf_F10.10.10.52

To: sip:joe@lzsip.com

Call-ID: 9_10acc888-befbfb540612bf_M@10.10.10.52

CSeq: 9 MESSAGE

Via: SIP/2.0/TLS 10.10.10.52:5061;branch=z9hG4bK9_10acc888-4477c42f540612c5_M

Content-Length: 144

Max-Forwards: 70

Content-Type: text/html

User-Agent: Avaya SIP Softphone

Supported: replaces

hello joe!!

]]

20051021:163150929:4:Proxy(5495):CRITICAL:[[MESSAGE sip:joe@lzsip.com SIP/2.0

From: "sue" <sip:sue@lzsip.com>;tag=6edcf65f43594a4154063e3f_F10.10.10.52

To: sip:joe@lzsip.com

Call-ID: a_10acf3ed-befa5954063e2f_M@10.10.10.52

CSeq: 10 MESSAGE

Via: SIP/2.0/TLS 10.10.10.52:5061;branch=z9hG4bKa_10acf3ed-4477c1c754063e45_M

Content-Length: 58

Max-Forwards: 70

Content-Type: text/html

User-Agent: Avaya SIP Softphone

Supported: replaces

good bye Sue!!

]]

20051021:163158955:5:Proxy(5495):CRITICAL:[[MESSAGE sip:sue@lzsip.com SIP/2.0

From: "joe" <sip:joe@lzsip.com>;tag=-36a6902f43594a275420be30_F10.10.10.55

To: sip:sue@lzsip.com

Call-ID: a_10c773fc-517d70f85420be24_M@10.10.10.55

CSeq: 10 MESSAGE

Via: SIP/2.0/TLS 10.10.10.55:5061;branch=z9hG4bKa_10c773fc-5f4218af5420be3a_M

Content-Length: 58

Max-Forwards: 70

Content-Type: text/html

User-Agent: Avaya SIP Softphone

Supported: replaces

good bye, Joe.

]]

Appendix D: Trace Log Files

The Trace log file shows all the messages in their entirety.

Whenever a host changes tracing status (Active or Idle), an entry is created in the log file. When a host becomes active, it logs a list of it's currently active rules. To see what was being matched, check the **start remote trace session** entries in the log file.

The system keeps a maximum of 10 trace logs.

The maximum size of a trace log is 1 megabyte.

Messages in the trace log may not be in chronological order.

Find details about the Trace Logger in the section titled Configure Filters on page 297.

Explanation

The log in this section contains 10 SIP messages. Each message contains the endpoint's REGISTER request followed by the SES response.

1) REGISTER request with incorrect domain 'lzsip.com' sent from endpoint to SES.

2) '403 foreign domain' response is sent to the endpoint. At this point, the administrator knows exactly what the problem is and tells the user to log in with the correct **usae.sushi.com** domain.

3) REGISTER with correct domain **usae.sushi.com** sent from endpoint to SES.

4) '401 Unauthorized' challenge response sent to endpoint.

5) REGISTER with correct domain usae.sushi.com but incorrect encrypted password in SIP Authorization header response sent from endpoint to SES.

6) '401 Unauthorized' challenge response again sent to endpoint. Since the endpoint was challenged again, the administrator should know that the user entered an incorrect password. The administrator tells Joe to correct his password. If the user has forgotten it, the administrator needs to reset it from the Administration Web interface's User Profile screen.

7) REGISTER sent from endpoint to SES.

8) '401 Unauthorized' challenge response sent to endpoint.

9) REGISTER w/ correct encrypted password in SIP Authorization header sent from endpoint to SES.

10) '200 OK' response sent to endpoint. The administrator now knows the user has successfully registered.

Trace log sample contents

Oct 6 11:40:16 2005 start remote trace session on ccsdeve.usae.sushi.com:

Using the following filters:

Field<from> Value<joebloggs>

Oct 6 12:21:48 2005 start remote trace session on ccsdevh1.usae.sushi.com:

Using the following filters:

Field<from> Value<joebloggs>

Oct 6 11:08:32 2005 start remote trace session on ccsdevh2.usae.sushi.com:

Using the following filters:

Field<from> Value<joebloggs>

Oct 6 12:24:05 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Recv Request]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

REGISTER sip:lzsip.com SIP/2.0

From: sip:joebloggs@lzsip.com;tag=56fd173243453d7f614c14be_F135.8.66.17

To: sip:joebloggs@lzsip.com

Call-ID: 1_1e06d71d-3b8df25614c14bf_R@135.8.66.17

CSeq: 1 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK1_1e06d71d-5954eb8614c14c4_R

Content-Length: 0

Max-Forwards: 70

Contact: <sip:joebloggs@135.8.66.17:5061;transport=tls>;q=1;expires=900

Allow: INVITE

Allow: CANCEL

Allow: BYE

Allow: ACK

Allow: SUBSCRIBE

Allow: NOTIFY

Allow: MESSAGE

Allow: INFO

Allow: REFER

User-Agent: Avaya SIP Softphone

Supported: replaces

Oct 6 12:24:05 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Send Response]

{connection: }

SIP/2.0 403 foreign domain

From: sip:joebloggs@lzsip.com;tag=56fd173243453d7f614c14be_F135.8.66.17

To: sip:joebloggs@lzsip.com;tag=56592AD313145B18AE8FCFB104712E9F11286158451158

Call-ID: 1_1e06d71d-3b8df25614c14bf_R@135.8.66.17

CSeq: 1 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK1_1e06d71d-5954eb8614c14c4_R

Content-Length: 0

Server: Avaya SIP Enablement Services

Oct 6 12:29:24 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Recv Request]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

REGISTER sip:usae.sushi.com SIP/2.0

From: sip:joebloggs@usae.sushi.com;tag=57b12da143453ebe6150f400_F135.8.66.17

To: sip:joebloggs@usae.sushi.com

Call-ID: 2_1e0bb520-3b8afcb6150f3ff_R@135.8.66.17

CSeq: 2 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK2_1e0bb520-59507b16150f406_R

Content-Length: 0

Max-Forwards: 70

Contact: <sip:joebloggs@135.8.66.17:5061;transport=tls>;q=1;expires=900

Allow: INVITE

Allow: CANCEL

Allow: BYE

Allow: ACK

Allow: SUBSCRIBE

Allow: NOTIFY

Allow: MESSAGE

Allow: INFO

Allow: REFER

User-Agent: Avaya SIP Softphone

Supported: replaces

Oct 6 12:29:24 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Send Response]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

SIP/2.0 401 Unauthorized

From: sip:joebloggs@usae.sushi.com;tag=57b12da143453ebe6150f400_F135.8.66.17

To: sip:joebloggs@usae.sushi.com;tag=56592AD313145B18AE8FCFB104712E9F11286161641160

Call-ID: 2_1e0bb520-3b8afcb6150f3ff_R@135.8.66.17

CSeq: 2 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK2_1e0bb520-59507b16150f406_R

Content-Length: 0

WWW-Authenticate: Digest realm="usae.sushi.com",domain="usae.sushi.com",nonce="MTEyODYxNjE2NDpTREZTZXJ2ZXJTZWNyZXRLZXk6MjAxNDg5OTY0OQ==",algorithm=MD5

Server: Avaya SIP Enablement Services

Oct 6 12:29:24 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Recv Request]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

REGISTER sip:usae.sushi.com SIP/2.0

From: sip:joebloggs@usae.sushi.com;tag=57b12da143453ebe6150f400_F135.8.66.17

To: sip:joebloggs@usae.sushi.com

Call-ID: 2_1e0bb520-3b8afcb6150f3ff_R@135.8.66.17

CSeq: 3 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK2_1e0bb520-59507b16150f406_R

Content-Length: 0

Max-Forwards: 70

Contact: <sip:joebloggs@135.8.66.17:5061;transport=tls>;q=1;expires=900

Allow: INVITE

Allow: CANCEL

Allow: BYE

Allow: ACK

Allow: SUBSCRIBE

Allow: NOTIFY

Allow: MESSAGE

Allow: INFO

Allow: REFER

User-Agent: Avaya SIP Softphone

Supported: replaces

Authorization: Digest
username="joebloggs",realm="usae.sushi.com",nonce="MTEyODYxNjE2NDpTREZTZXJ2ZXJ
TZWNyZXRLZXk6MjAxNDg5OTY0OQ==",uri="sip:usae.sushi.com",response="473951ffed0db
e6de73381b4f13b2778"

Oct 6 12:29:24 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com:
[Send Response]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

SIP/2.0 401 Unauthorized

From: sip:joebloggs@usae.sushi.com;tag=57b12da143453ebe6150f400_F135.8.66.17

To:
sip:joebloggs@usae.sushi.com;tag=56592AD313145B18AE8FCFB104712E9F112861616411
62

Call-ID: 2_1e0bb520-3b8afcb6150f3ff_R@135.8.66.17

CSeq: 3 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK2_1e0bb520-59507b16150f406_R

Content-Length: 0

WWW-Authenticate: Digest realm="usae.sushi.com",domain="usae.sushi.com",nonce="MTEyODYxNjE2NDpTREZTZXJ2ZXJTZWNyZXRLZXk6MjAxNDg5OTY0OQ==",algorithm=MD5

Server: Avaya SIP Enablement Services

Oct 6 12:30:44 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Recv Request]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

REGISTER sip:usae.sushi.com SIP/2.0

From: sip:joebloggs@usae.sushi.com;tag=57ded26743453f0f61522ffe_F135.8.66.17

To: sip:joebloggs@usae.sushi.com

Call-ID: 3_1e0cf0ee-3b8a3c561523000_R@135.8.66.17

CSeq: 3 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK3_1e0cf0ee-594f5a861523004_R

Content-Length: 0

Max-Forwards: 70

Contact: <sip:joebloggs@135.8.66.17:5061;transport=tls>;q=1;expires=900

Allow: INVITE

Allow: CANCEL

Allow: BYE

Allow: ACK

Allow: SUBSCRIBE

Allow: NOTIFY

Allow: MESSAGE

Allow: INFO

Allow: REFER

User-Agent: Avaya SIP Softphone

Supported: replaces

Oct 6 12:30:44 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Send Response]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

SIP/2.0 401 Unauthorized

From: sip:joebloggs@usae.sushi.com;tag=57ded26743453f0f61522ffe_F135.8.66.17

To: sip:joebloggs@usae.sushi.com;tag=56592AD313145B18AE8FCFB104712E9F11286162441164

Call-ID: 3_1e0cf0ee-3b8a3c561523000_R@135.8.66.17

CSeq: 3 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK3_1e0cf0ee-594f5a861523004_R

Content-Length: 0

WWW-Authenticate: Digest realm="usae.sushi.com",domain="usae.sushi.com",nonce="MTEyODYxNjI0NDpTREZTZXJ2ZXJTZWNyZXRLZXk6MTQ2OTMyODY1Mg==",algorithm=MD5

Server: Avaya SIP Enablement Services

Oct 6 12:30:44 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Recv Request]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

REGISTER sip:usae.sushi.com SIP/2.0

From: sip:joebloggs@usae.sushi.com;tag=57ded26743453f0f61522ffe_F135.8.66.17

To: sip:joebloggs@usae.sushi.com

Call-ID: 3_1e0cf0ee-3b8a3c561523000_R@135.8.66.17

CSeq: 4 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK3_1e0cf0ee-594f5a861523004_R

Content-Length: 0

Max-Forwards: 70

Contact: <sip:joebloggs@135.8.66.17:5061;transport=tls>;q=1;expires=900

Allow: INVITE

Allow: CANCEL

Allow: BYE

Allow: ACK

Allow: SUBSCRIBE

Allow: NOTIFY

Allow: MESSAGE

Allow: INFO

Allow: REFER

User-Agent: Avaya SIP Softphone

Supported: replaces

Authorization: Digest username="joebloggs",realm="usae.sushi.com",nonce="MTEyODYxNjI0NDpTREZTZXJ2ZXJTZWNyZXRLZXk6MTQ2OTMyODY1Mg==",uri="sip:usae.sushi.com",response="1b8f9ea2c5f72a4b6bee2f6b4612b800"

Oct 6 12:30:45 2005 matching filter label <joebloggs cannot login>: ccsdevh1.usae.sushi.com: [Send Response]

{connection: host=135.8.66.17 port=5061 protocol=TLS}

SIP/2.0 200 OK

From: sip:joebloggs@usae.sushi.com;tag=57ded26743453f0f61522ffe_F135.8.66.17

To: sip:joebloggs@usae.sushi.com

Call-ID: 3_1e0cf0ee-3b8a3c561523000_R@135.8.66.17

CSeq: 4 REGISTER

Via: SIP/2.0/TLS 135.8.66.17:5061;branch=z9hG4bK3_1e0cf0ee-594f5a861523004_R

Content-Length: 0

Contact: <sip:joebloggs@135.8.66.17:5061;transport=tls>;q=1;expires=900

Date: Thu, 06 Oct 2005 16:30:45 GMT

Appendix E: Configuring Avaya SIP Telephony Users on SIP Enablement Services and Communication Manager

Introduction

This appendix describe the configuration steps required to support Avaya SIP telephony users on a typical SIP Enablement Services and Communication Manager configuration. This includes the Avaya 46xx and 96xx-series IP Telephone configuration file parameter settings and the Avaya one-X Desktop Edition configuration screens required to support basic telephony and voice messaging. The steps pertain to SIP Enablement Services release 5.2.1 and Communication Manager release 5.2.1. They are applicable to other Linux-based Avaya Servers and Media Gateways running Communication Manager.

This document includes references to Avaya One-X Deskphone Edition. Avaya One-X Communicator is a replacement for Avaya One-X Deskphone Edition. For further details about Avaya One-X Communicator, see Avaya One-X Communicator documentation or contact Avaya Professional Services.

Background

This appendix provides the administrative steps for configuring SIP telephony users. They cover administration of the following Avaya products:

1. SIP Enablement Services (SES)

a. User

b. Communication Manager extension

c. Communication Manager server access information required to support Advanced SIP Telephony (AST) features[1]

2. Communication Manager

a. Station

b. Off-PBX-station-mapping

c. SES login configuration required to support AST

3. Avaya 46xx and 96xx-series IP Telephones[2]

a. `46xxsettings.txt` and 96xxxsettings.txt file parameters relative to 1 and 2 above

b. Firmware upgrade parameters

4. Avaya one-X Desktop Edition

a. Configuration screen settings relative to 1 and 2 above

Configuration

The sample configuration used in this appendix is shown in **Figure 1**. The diagram indicates logical signaling connections. Each Avaya telephone is configured to register to one of two SIP Enablement Services home servers and is administered as a station on an Avaya S8300 Server with G700 Media Gateway.[3] The Avaya Communication Manager Messaging Application resides on the Avaya S8300 Server and is used to support voice messaging. A PC supports an HTTP server accessed by the telephones as well as a web browser for administration of the Avaya servers. Avaya one-X Desktop Edition is installed on a second PC. Although specific Avaya IP Telephones are shown, the configuration steps in this appendix can be used with all Avaya 4600 Series (4602, 4602SW, 4610SW, 4620SW, 4621SW) and Avaya 9600 Series (9620, 9630, 9630G, 9640, 9640G) models.

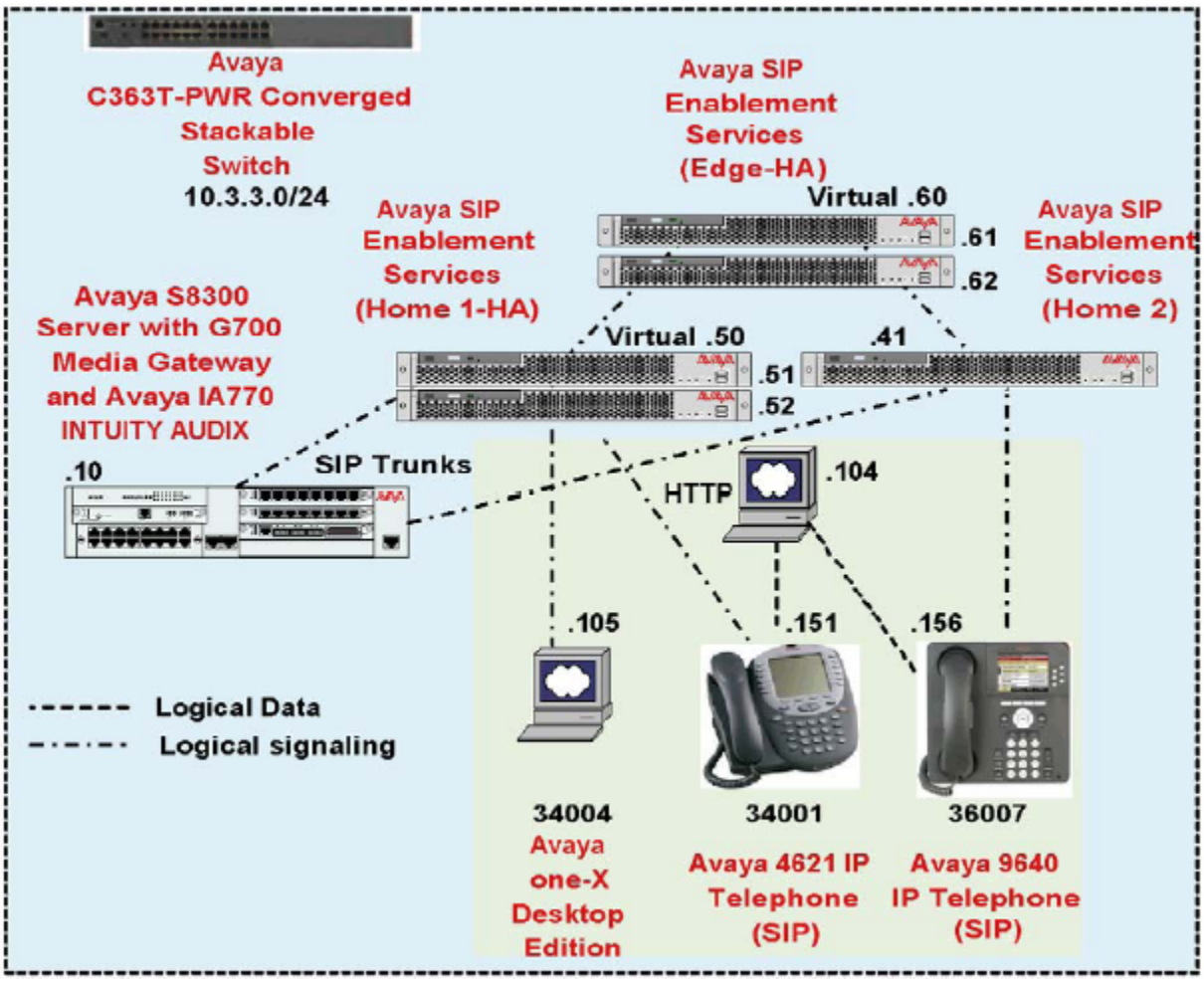


Figure 1: Avaya SIP Telephony Sample Configuration (HA = High Availability)

Equipment and Software Validated

The following equipment and software were used in the configuration.

Table 1: Equipment and Software Versions Used

Equipment	Software
SIP Enablement Services (SES) Server	5.1.1 (Load 415.1)

Avaya S8300 Server with G700 Media Gateway	Communication Manager 5.1.1
Avaya 4621 SIP Telephone	2.2.2
Avaya 9640 SIP Telephone (SIP)	2.0.4.0 (2)
Avaya one-X Desktop Edition	2.1 Service Pack 2 (Build 78)
PC's - Microsoft Windows 2000 Professional	5.00.2195, SP 4

Supported Features

Overview

Table 2 gives a summary of the features supported for Avaya SIP telephones. Notes on specific feature operations are included in Section 3.2. Some features are supported locally at the telephone, while others are only available with SES and Communication Manager. In addition to basic calling capabilities, the Internet Engineering Task Force (IETF) has defined a supplementary set of calling features, often referred to as the SIPPING service examples [1].

This provides a useful framework to describe and compare features supported by various equipment vendors. Communication Manager can support many of these features even though the telephone may not locally support them. Additional features beyond the SIPPING set can be extended to SIP telephones using Communication Manager.

Some Communication Manager features shown in **Table 2** can be invoked by using fixed local buttons (LB) on the telephone, or by dialing a Feature Name Extension (FNE). Or, a speed dial button on the telephone can be programmed to an FNE. For Avaya telephones that support AST, the following advanced features are supported (* indicates Avaya 9600 Series IP Telephones only):

•Features noted as SB in **Table 2** can be configured in Communication Manager using station buttons, which are automatically downloaded to the telephone at login time

•Contacts centrally stored and administered on SES

•Dial plan information is automatically downloaded and used to detect end of dialing*

•Full bridged appearance functionality *

•On-hook/Off-hook status monitoring for use with presence and busy indicators*

Table 2 indicates for the Avaya telephone models which method is used to support each feature. Communication Manager automatically handles many other standard features such as call coverage, trunk selection using Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS), Class Of Service/Class Of Restriction (COS/COR), and voice messaging.

Operational Notes (See Table 2)

Call Forward

It is recommended that this feature be administered as an Communication Manager FNE or station button rather than using local call forward features of the telephone (LB), such as are available on the Avaya 4600 Series IP Telephones (see [8]). Local call forward does not benefit from the call coverage features available in Communication Manager (e.g., voice mail).

Bridged Appearances

Full bridged appearance capabilities, including, alerting, call answer, busy indication, line selection, and call origination are supported only on Avaya 9600 Series IP Telephones. For Avaya 4600 Series IP Telephones and one-X Desktop Edition, only bridged alerting (ringing the bridging station) and call answer (answering the call on behalf of the bridged station) are supported, and no station "button" is displayed for that appearance.

FEATURE	**Avaya 4600** Series	**Avaya 9600** Series & one-X Desktop	COMMENTS
Basic Calling features			
Extension to extension call	YES	YES	
Intercept tones/displays	YES	YES	Reorder (for announcements, see Section 5.2)
Call Waiting	YES	YES	
Do Not Disturb	FNE	SB	Via send-all-calls
Speed Dial buttons	YES	YES	Except 4602SW
Message Waiting Support	YES	YES	
SIPPING Features			
Call Hold	LB	LB	
Consultation Hold	LB	LB	
Music on Hold	YES	YES	
Unattended Transfer	LB	LB	
Attended Transfer	LB	LB	
Call Forward Unconditional	LB/	SB	See Section 3.2.1
Call Forward Busy	LB/	SB	See Section 3.2.1
Call Forward No Answer	LB/	SB	See Section 3.2.1
Conference - 3rd party added	LB	LB	
Conference - 3rd party joins	LB	LB	
Find-Me	YES	YES	Via coverage paths (Section 5.8)

Incoming Call Screening	YES	YES	Via Class Of Restriction (Section 5.7)
Outgoing Call Screening	YES	YES	Via Class Of Restriction (Section 5.7)
Call Park/Unpark	FNE	SB	
Call Pickup	FNE	SB	
Automatic Redial	FNE	SB	Via Automatic Callback
OPS - Additional Station-Side Features			
Bridged Appearance	SB	SB	9600 Series; alerting only for others (Section
Calling Number Block	FNE	SB	
Calling Number Unblock	FNE	SB	
Conference on Answer	FNE	FNE	
EC500 Activate/Deactivate	FNE	SB	
EC500 Extend Call	NO	SB	9600 Series only
Extended Group Call Pickup	FNE	FNE	
Directed Call Pick-Up	FNE	SB	
Drop Last Added Party	LB	LB	
Last Number Dialed	LB	LB	Local menu or FNE
Malicious Call Trace	FNE	SB	
Malicious Call Trace Cancel	FNE	SB	
One Touch Recording	NO	SB	
Priority Call	FNE	SB	See Section 5.6
Send All Calls	FNE	SB	
Send All Calls Cancel	FNE	SB	
Transfer to Voice Mail	FNE	SB	
Whisper Page	FNE	SB	

Table 2: SIP Telephony Feature Support

(FNE = Feature Name Extension, LB = Local Button, SB = Station Button)

Administer SIP Enablement Services

The following steps describe configuration of SES for use with Avaya 4600 and 9600

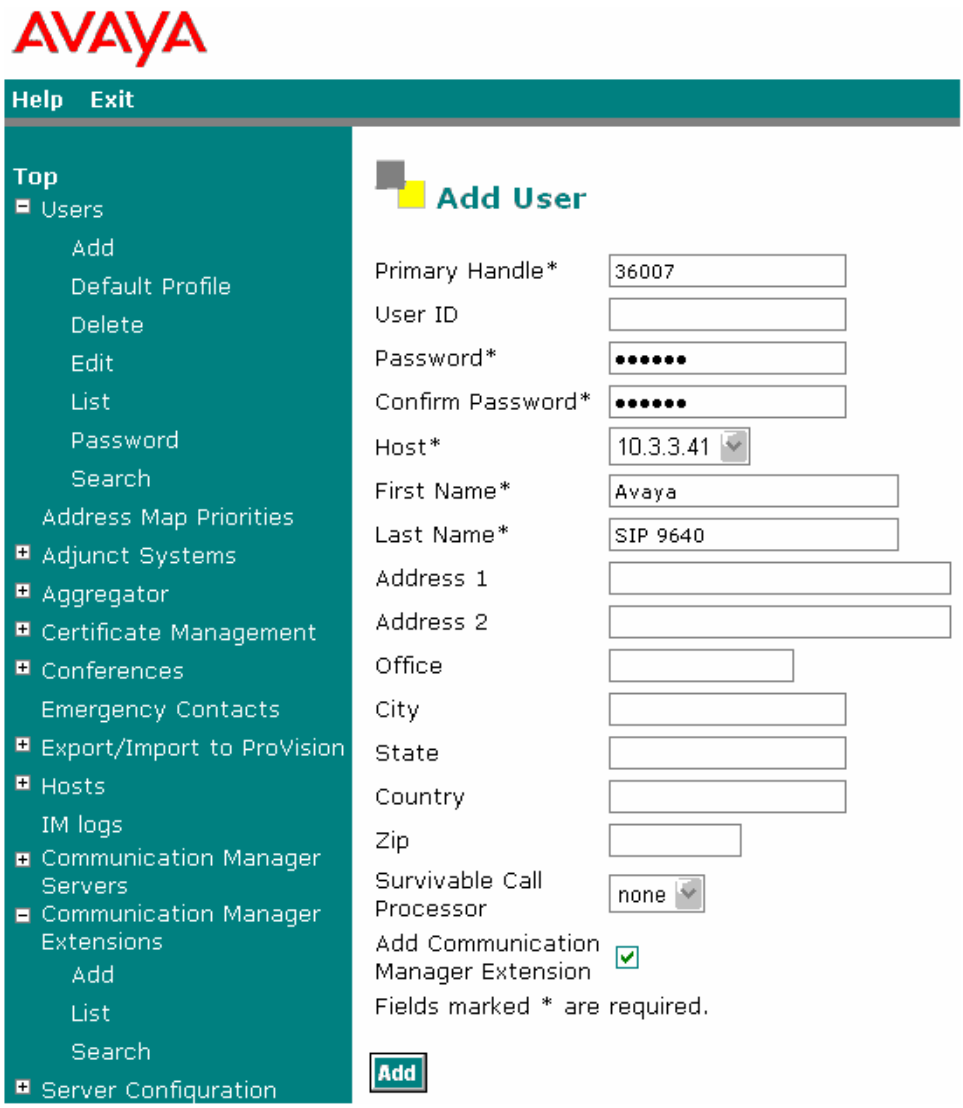
Series IP Telephones and Avaya one-X Desktop Edition. Other standard administration functions are covered in [4, 5].

Steps	Description

1.	Log into the SIP Enablement Services administration web interface using the appropriate credentials. Expand the **Users** heading on the left side of the page and click on **Add**.

Steps	Description

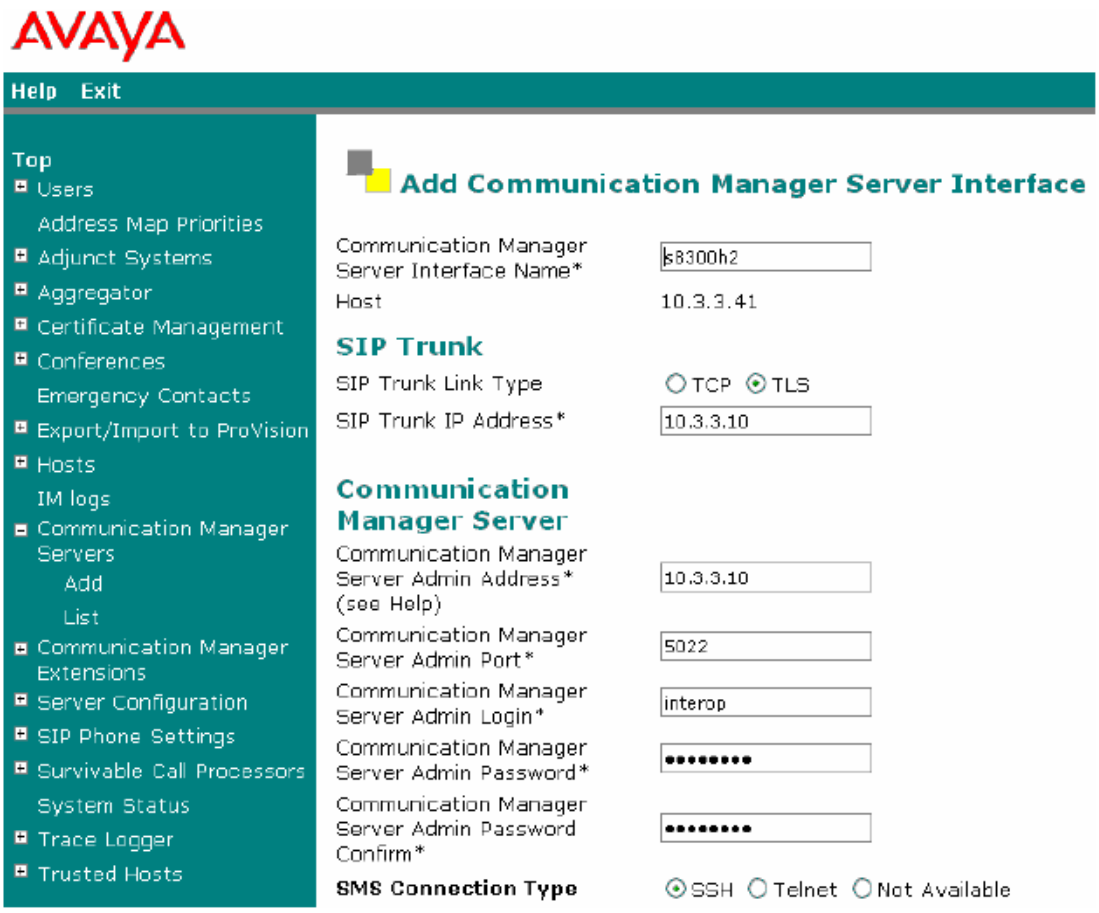
2. The *Add User* page will be displayed. Fill in the required fields (indicated by *). Enter the extension number or the user's handle in the **Primary Handle** field. The extension number is used for Avaya 4600 and 9600 Series IP Telephones, as shown below. The user's handle can be used when configuring Avaya one-X Desktop Edition, where the handle can be used for applications such as Presence and Instant Messaging. For the one-X Desktop Edition user in the sample configuration (see Section 6.2), the handle would be "joesip". The **Password** and **Confirm Password** fields should match those entered at the corresponding telephone at login time. The **Host** field should be set to the SES Home or Home/Edge server to which the telephone will register. In this configuration, the Avaya 9640 IP Telephone registers to Home 2. **First Name** and **Last Name** are for reference purposes only. Check the **Add Communication Manager Extension** checkbox. Click on **Add**, and then **Continue** on the confirmation page.



Steps	Description
3.	The *Add Communication Manager Extension* page will be displayed. Enter the user's telephone extension in the **Extension** field. Since the user is being added to Home 2, the **Communication Manager Server** corresponding to the SIP trunk between the Avaya S8300 Server and Home 2 is selected automatically. Click on **Add**, and then **Continue** on the subsequent confirmation page. 
4.	Repeat **Steps 1-3** for each user to be added to the system.

Steps	Description

5.	If AST telephones are to be supported, the following fields under *Communication Manager Server* must be correctly populated in the *Communication Manager Server Interface* page for each server defined. Set **Communication Manager Server Admin Address** to the Avaya Server IP address, **Communication Manager Server Admin Port** to "5022", **Communication Manager Server Admin Login** to the desired login name, and **Communication Manager Server Admin Password** to the desired password. The login and password must agree with those configured in Communication Manager (see Section 5.9.3). Check "SSH" for **SMS Connection Type**. Click on **Add** (not shown).



Configure Communication Manager

This section highlights the important System Access Terminal (SAT) commands for defining the telephone as a SIP station in Communication Manager, and administering support for the features indicated in **Table 2**. As mentioned in Section 3.1, many other standard Communication Manager features are available to these stations. For additional documentation on SIP administration, see References [2-3]. Log in to the SAT with the appropriate permissions.

Verify SIP Telephone Capacity

Use the **display system-parameters customer-options** command to verify that **Maximum Off- PBX Telephones – OPS** has been set to the value that has been licensed, and that this value will accommodate addition of the SIP telephones.

```
display system-parameters customer-options                    Page   1 of  10
                            OPTIONAL FEATURES

    G3 Version: V15                            Software Package: Standard
      Location: 1                           RFA System ID (SID): 1
      Platform: 7                           RFA Module ID (MID): 1

                                                          USED
                            Platform Maximum Ports: 900   372
                                  Maximum Stations: 450   72
                             Maximum XMOBILE Stations: 0    0
                  Maximum Off-PBX Telephones - EC500: 0     0
                  Maximum Off-PBX Telephones -   OPS: 200   55
                  Maximum Off-PBX Telephones - PBFMC: 10    3
                  Maximum Off-PBX Telephones - PVFMC: 0     0
                  Maximum Off-PBX Telephones - SCCAN: 0     0
```

Define System Features

Use the **change system-parameters features** command to administer system wide features for the SIP telephones. Those related to features listed in **Table 2** are shown in bold. These are all standard Communication Manager features.

```
change system-parameters features                              Page   4 of  17
                     FEATURE-RELATED SYSTEM PARAMETERS
         Reserved Slots for Attendant Priority Queue: 5
                          Time before Off-hook Alert: 10
              Emergency Access Redirection Extension:
 Number of Emergency Calls Allowed in Attendant Queue: 5
 Maximum Number of Digits for Directed Group Call Pickup:4
             Call Pickup on Intercom Calls? y         Call Pickup Alerting? n
 Temporary Bridged Appearance on Call Pickup? y       Directed Call Pickup? y
                  Extended Group Call Pickup: simple

  Deluxe Paging and Call Park Timeout to Originator? n
 Controlled Outward Restriction Intercept Treatment: tone
Controlled Termination Restriction (Do Not Disturb): tone
         Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS        Authorization Codes Enabled? n
              Controlled Toll Restriction Replaces: none
```

```
change system-parameters features                              Page  17 of  17
                     FEATURE-RELATED SYSTEM PARAMETERS

INTERCEPT TREATMENT PARAMETERS
       Invalid Number Dialed Intercept Treatment: announcement  35010
                   Invalid Number Dialed Display:
    Restricted Number Dialed Intercept Treatment: announcement  35011
                 Restricted Number Dialed Display:
   Intercept Treatment On Failed Trunk Transfers? n

WHISPER PAGE
   Whisper Page Tone Given To: paged

6400/8400/2420J LINE APPEARANCE LED SETTINGS
                  Station Putting Call On Hold: green  wink
                   Station When Call is Active: steady
        Other Stations When Call Is Put On Hold: green  wink
             Other Stations When Call Is Active: green
                                      Ringing: green  flash
                                         Idle: steady
          Display Information With Bridged Call? n
                           Pickup On Transfer? Y

DIGITAL STATION LINE APPEARANCE LED SETTINGS
                  Station Putting Call On Hold: green  wink
                   Station When Call is Active: steady
        Other Stations When Call Is Put On Hold: green  wink
             Other Stations When Call Is Active: green
                                      Ringing: green  flash
                                         Idle: steady
          Display Information With Bridged Call? n
                           Pickup On Transfer? y
```

Define the Dial Plan

Please note that the dial plan information shown is for the example configuration only, and should be tailored to meet customer requirements. Use the **change dialplan analysis**

command to define the dial plan formats used in the system. This includes all telephone extensions, Feature Name Extensions (FNEs), and Feature Access Codes (FACs). To define the FNEs for the features listed in **Table 2**, a Feature Access Code (FAC) must also be specified for the corresponding feature[4]. In the sample configuration, telephone extensions are five digits long and begin with 3, FNEs are five digits beginning with 7, and the FACs have formats as indicated with **Call Type** “fac”.

```
change dialplan analysis                                    Page   1 of  12
                         DIAL PLAN ANALYSIS TABLE
                                                          Percent Full:    0

      Dialed  Total  Call      Dialed  Total  Call      Dialed  Total  Call
      String  Length Type      String  Length Type      String  Length Type
        0       3    fac
        1       3    dac
        3       5    ext
        6       3    fac
        7       5    ext
        8       1    fac
        9       1    fac
        *       2    fac
        #       2    fac
```

Feature Access Codes (FACs)

Use change feature-access-codes to define the access codes for the FNEs, shown in bold.

```
change feature-access-codes                                 Page   1 of   8
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: 601
         Abbreviated Dialing List2 Access Code: 602
         Abbreviated Dialing List3 Access Code: 603
Abbreviated Dial - Prgm Group List Access Code:
                     Announcement Access Code: 606
                      Answer Back Access Code: 605
                        Attendant Access Code:
     Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *5     Deactivation: #5
Call Forwarding Activation Busy/DA: *2     All: 612    Deactivation: #2
   Call Forwarding Enhanced Status:         Act:       Deactivation:
                       Call Park Access Code: 604
                     Call Pickup Access Code: *6
CAS Remote Hold/Answer Hold-Unhold Access Code: #6
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
                   Contact Closure   Open Code:          Close Code:
```

```
change feature-access-codes                                    Page   2 of   8
                          FEATURE ACCESS CODE (FAC)
                  Contact Closure  Pulse Code:
                 Data Origination Access Code:
                     Data Privacy Access Code:
              Directed Call Pickup Access Code: 654
       Directed Group Call Pickup  Access Code:
     Emergency Access to Attendant Access Code:
        EC500 Self-Administration Access Codes:
                   Enhanced EC500 Activation: 660    Deactivation: 661
          Enterprise Mobility User Activation:       Deactivation:
  Extended Call Fwd Activate Busy D/A      All:     Deactivation:
       Extended Group Call Pickup Access Code: 621
              Facility Test Calls Access Code:
                         Flash Access Code: 678
            Group Control Restrict Activation:       Deactivation:
                  Hunt Group Busy Activation: *8     Deactivation: #8
                         ISDN Access Code:
                Last Number Dialed Access Code: *9
    Leave Word Calling Message Retrieval Lock: *1
  Leave Word Calling Message Retrieval Unlock: #1
```

```
change feature-access-codes                                    Page   3 of   8
                          FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message:
           Leave Word Calling Cancel A Message:
   Limit Number of Concurrent Calls Activation:       Deactivation:
              Malicious Call Trace Activation: 613    Deactivation: 614
         Meet-me Conference Access Code Change:

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:       Dissociate Code:
        Per Call CPN Blocking Code Access Code: 615
      Per Call CPN Unblocking Code Access Code: 616

                  Priority Calling Access Code: *7
                          Program Access Code: *0

       Refresh Terminal Parameters Access Code: 694
             Remote Send All Calls Activation:       Deactivation:
              Self Station Display Activation:
                    Send All Calls Activation: *3     Deactivation: #3
         Station Firmware Download Access Code:
```

```
change feature-access-codes                                    Page   4 of   8
                            FEATURE ACCESS CODE (FAC)
                        Station Lock Activation:        Deactivation:
     Station Security Code Change Access Code: 699
               Station User Admin of FBI Assign:                  Remove:
  Station User Button Ring Control Access Code:
             Terminal Dial-Up Test Access Code: 695
Terminal Translation Initialization Merge Code:          Separation Code:
            Transfer to Voice Mail Access Code: #9
          Trunk Answer Any Station Access Code:
              User Control Restrict Activation: 691    Deactivation: 692
  Voice Coverage Message Retrieval Access Code:
 Voice Principal Message Retrieval Access Code:
           Whisper Page Activation Access Code: 620
```

Define Feature Name Extensions (FNEs)

The FNEs can be defined using the **change off-pbx-telephone feature-name-extensions** command. This command is used to support both SIP telephones and Extension to Cellular. The fields that have been left blank correspond to those used exclusively for Extension to Cellular.

```
change off-pbx-telephone feature-name-extensions set 1          Page   1 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
                    Set Name:

     Active Appearance Select: 70024
          Automatic Call Back: 70003
   Automatic Call-Back Cancel: 70004
             Call Forward All: 70005
  Call Forward Busy/No Answer: 70006
          Call Forward Cancel: 70007
                    Call Park: 70008
        Call Park Answer Back: 70009
                Call Pick-Up: 70010
         Calling Number Block: 70012
       Calling Number Unblock: 70013
         Conference on Answer: 70011
        Directed Call Pick-Up: 70014
        Drop Last Added Party: 70015
    Exclusion (Toggle On/Off): 70016
   Extended Group Call Pickup: 70025
       Held Appearance Select:
```

```
change off-pbx-telephone feature-name-extensions set 1          Page   2 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

      Idle Appearance Select:
          Last Number Dialed: 70019
       Malicious Call Trace: 70029
  Malicious Call Trace Cancel: 70021
        Off-Pbx Call Enable: 70027
       Off-Pbx Call Disable: 70028
             Priority Call: 70000
           Send All Calls: 70001
      Send All Calls Cancel: 70002
        Transfer On Hang-Up:
     Transfer to Voice Mail: 70023
    Whisper Page Activation: 70026
```

Specify Class of Service (COS)

Use the **change cos** command to set the appropriate service permissions to support the corresponding features (shown in bold). For the example, COS 1 was used. On Page 2, set the value of **VIP Caller** to "y" only if all calls made by telephones with this COS should be priority calls. Note that calls made by such VIP telephones will not follow the normal coverage path defined for the called telephone.

```
change cos                                                      Page   1 of   2
CLASS OF SERVICE

                            0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 Auto Callback              n  y  y  n  y  n  y  n  y  n  y  n  y  n  y  n
 Call Fwd-All Calls         n  y  n  y  y  n  n  y  y  n  n  y  y  n  n  n
 Data Privacy               n  n  n  y  n  y  y  y  y  n  n  n  n  y  y  y
 Priority Calling           n  y  n  n  n  n  n  n  n  y  y  y  y  y  y  n
 Console Permissions        y  n  y  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert             n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net  n  n  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Call Forwarding Busy/DA    n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Personal Station Access (PSA) n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding All    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding B/DA   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Trk-to-Trk Transfer Override  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 QSIG Call Offer Originations  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Contact Closure Activation  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

```
change cos                                                  Page   2 of   2
                              CLASS OF SERVICE

                              0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 VIP Caller                   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n

 Masking CPN/Name Override    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Call Forwarding Enhanced     y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Priority Ip Video            n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Ad-hoc Video Conferencing    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

Specify Class of Restriction (COR)

Use the **change cor** command to enable applicable calling features. To use the Directed Call Pickup feature, the **Can Use Directed Call Pickup** and **Can Be Picked Up By Directed Call Pickup** fields must be set to “y” for the affected stations. Set **Access to MCT?** To “y” if Malicious Call Trace can be activated. In the sample configuration, the telephones were assigned to COR 2. Note that CALLING PERMISSION on pages (4-23) can be used to implement a form of centralized call screening for groups of stations and trunks.

```
change cor 2                                                Page   1 of  23
                            CLASS OF RESTRICTION

               COR Number: 2
          COR Description: Stations

                      FRL: 0                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
 Partitioned Group Number: 1        Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

           Access to MCT? y              Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n
            MF ANI Prefix:               Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                      Can Be Picked Up By Directed Call Pickup? y
                                 Can Use Directed Call Pickup? y
                                 Group Controlled Restriction: inactive
```

```
change cor 2                                                    Page   4 of  23
                                CLASS OF RESTRICTION

CALLING PERMISSION (Enter "y" to grant permission to call specified COR)

  0? y      15? y      30? y      44? y      58? y      72? y      86? y
  1? y      16? y      31? y      45? y      59? y      73? y      87? y
  2? y      17? y      32? y      46? y      60? y      74? y      88? y
  3? n      18? y      33? y      47? y      61? y      75? y      89? y
  4? y      19? y      34? y      48? y      62? y      76? y      90? y
  5? y      20? y      35? y      49? y      63? y      77? y      91? y
  6? y      21? y      36? y      50? y      64? y      78? y      92? y
  7? y      22? y      37? y      51? y      65? y      79? y      93? y
  8? y      23? y      38? y      52? y      66? y      80? y      94? y
  9? y      24? y      39? y      53? y      67? y      81? y      95? y
 10? y      25? y      40? y      54? y      68? y      82? y      96? y
 11? y      26? y      41? y      55? y      69? y      83? y      97? y
 12? y      27? y      42? y      56? y      70? y      84? y      98? y
 13? y      28? y      43? y      57? y      71? y      85? y      99? y
 14? y      29? y
```

Add Coverage Path

Configure the coverage path to be used for the voice messaging hunt group, which is group “h1” in the sample configuration. The default values shown for **Busy?**, **Don’t Answer?**, and **DND/ SAC/Goto Cover?** can be used for the *Coverage Criteria*. Here, the **Number of Rings** before the call goes to voice messaging has been extended from the default of 2 to 4 rings.

```
add coverage path 1                                             Page   1 of   1
                              COVERAGE PATH

                 Coverage Path Number: 1
                                                 Hunt after Coverage? n
                     Next Path Number: 1         Linkage   1    1

COVERAGE CRITERIA

    Station/Group Status    Inside Call     Outside Call
             Active?            n               n
               Busy?            y               y
      Don't Answer?             y               y          Number of Rings: 4
                All?            n               n
 DND/SAC/Goto Cover?            y               y
   Holiday Coverage?            n               n

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1             Rng: 3  Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

Add Stations

This section is divided into three subsections. Section 5.9.1 covers station administration for basic (non-AST) stations, which includes Avaya 4600 Series IP Telephones.[5] Section 5.9.2 covers administration for additional features available via AST on Avaya 9600 Series IP telephones and Avaya one-X Desktop Edition. Section 5.9.3 covers configuration of the login access to the Communication Manager server that is required by SES to retrieve station button information that is relayed to AST telephones.

Add Basic (non-AST) Stations

Use the **add station** command to add a station for each telephone to be supported. Assign the same extension as the Communication Manager extension administered in SES. Use "4620SIP" for the **Station Type** and be sure to include the **Coverage Path** for voice messaging or other hunt group if applicable. Use the **COS** and **COR** values administered in the previous sections. The **Name** field is optional and is shown on the display of telephones receiving calls from this station. Use defaults for the other fields on Page 1. Note that on Page 1, the **Security Code** is *not* required. The **Userid** and **Password** configured in SES for this telephone is used for authentication when the user log into the telephone.

```
add station 34001                                          Page   1 of   5
                                   STATION

Extension: 34001                      Lock Messages? n                BCC: 0
     Type: 4620SIP                    Security Code: 123456            TN: 1
     Port: S00081                   Coverage Path 1: 1                COR: 2
     Name: Avaya 4621               Coverage Path 2:                  COS: 1
                                    Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19        Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 34001
           Speakerphone: 2-way             Mute Button Enabled? y
       Display Language: english              Expansion Module? n
 Survivable GK Node Name:
         Survivable COR: internal            Media Complex Ext:
   Survivable Trunk Dest? y                       IP SoftPhone? n




                                          Customizable Labels? y
```

On Page 2, note the following:

•If this telephone will have a bridged appearance for another telephone (see Page 3 for this station), then **Bridged Call Alerting** should be set to "y", so that this phone will ring when the other telephone is called. Note that no other operational behaviors of the bridged appearance feature apply to basic (non-AST) SIP telephones (e.g., off-hook indication, bridge-on, busy indication, etc.).

•By default, the last call appearance is reserved for outgoing calls from the telephone. If it is desirable to allow an incoming call to use the last available call appearance when all others are occupied, set the **Restrict Last Appearance** field to “n”. In this mode, all call appearances are available for making or receiving calls. But note that if all appearances are in use, transferring a call will not be possible, since there is no longer an appearance

reserved for the outgoing call to the transfer-to party.[6]

•Set **MWI Served User Type** to the appropriate value for the voice messaging system. In the sample configuration, Communication Manager Messaging uses QSIG signaling, and so the value is set to “qsig-mwi”.

```
add station 34001                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                     Coverage Msg Retrieval? y
  LWC Log External Calls? n                               Auto Answer: none
            CDR Privacy? n                          Data Restriction? n
   Redirect Notification? y                 Idle Appearance Preference? n
 Per Button Ring Control? n                Bridged Idle Line Preference? n
   Bridged Call Alerting? y                    Restrict Last Appearance? n
  Active Station Ringing: single
                                                        EMU Login Allowed? n
       H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed
        Multimedia Mode: enhanced
    MWI Served User Type: qsig-mwi             Display Client Redirection? n
                                              Select Last Used Appearance? n
                                               Coverage After Forwarding? s
```

On Page 3 under the heading **BUTTON ASSIGNMENTS**, fill in the number of call appearances (“call-appr” buttons) that are to be supported for the telephone. Use the following guidelines for determining the correct number:

•To support certain transfer and conference scenarios, the minimum number of “call-appr” buttons should be 3.

•The number of call appearances should agree with the number specified in the

PHNNUMOFSA parameter in the `46xxsettings.txt` file (See Section 6.1, Step 2).

```
add station 34001                                          Page   4 of   5
                                    STATION
 SITE DATA
      Room:                                          Headset? n
      Jack:                                          Speaker? n
     Cable:                                         Mounting: d
     Floor:                                      Cord Length: 0
   Building:                                       Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5: no-hld-cnf
 2: call-appr                            6:
 3: call-appr                            7:
 4: brdg-appr  Btn:1  Ext:34176          8:
```

Under the same heading, enter the function button names, if required, for FNEs that will be used at the phone. Only the FNEs shown in **Table 3** require the station to have a corresponding function button. For bridged alerting, the bridged appearance “brdg-appr” button is required, as shown above. Although entering other buttons is allowed on the form, these are the only function buttons that are supported on basic (non-AST) SIP stations.

FNE Name	Function Button Name
Automatic Callback,	auto-cback
Conference on Answer	no-hld-cnf

Table 3: Feature Name Extensions Requiring Station Buttons

In the sample configuration, three line appearances were administered at the telephone for extension 34001. Bridged alerting was defined on station 34176 and the Conference On Answer FNE was included in the speed dial button programming. Note that only the bridged *alerting* function is supported on basic SIP stations.

Use the **change off-pbx-telephone station-mapping** command to map the Communication Manager extension (34001) to the same SIP Enablement Services Communication Manager extension. Enter the field values shown. **Trunk Selection** indicates the SIP trunk group corresponding to the SES to which this telephone will register. **Configuration Set** can be a set that has default values in Communication Manager.

```
change off-pbx-telephone station-mapping 34001                Page   1 of   2
                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station        Application Dial   CC  Phone Number      Trunk       Config
 Extension                  Prefix                      Selection   Set
 34001            OPS           -     34001              10         1
```

On Page 2, change the **Call Limit** to match the number of "call-appr" entries in the **add station** form. Also make sure that **Mapping Mode** is set to "both" (the default value for a newly added station). **Bridged Calls** should be set to "none"

```
change off-pbx-telephone station-mapping 34001                Page   2 of   2
                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Call       Mapping      Calls       Bridged        Location
 Extension     Limit      Mode         Allowed     Calls
 34001          3        both          all         none
```

Add AST Stations

The following configuration should be performed on the **add station** form to enable additional features supported on Avaya 9600 Series IP Telephones and Avaya one-X Desktop Edition. On Page 1, specify "9600SIP" for the **Station Type** for Avaya 9600 Series IP Telephones. Specify "4620" for Avaya one-X Desktop Edition. Fill in the other fields in the same way as for basic stations. Note that on Page 1, the **Security Code** is *not* required. The **Userid** and **Password** configured in SES for this telephone is used for authentication at login time.

```
add station 36007                                             Page   1 of   6
                                   STATION

Extension: 36007                      Lock Messages? n              BCC: 0
     Type: 9600SIP                    Security Code:                 TN: 1
     Port: S00023                   Coverage Path 1: 1              COR: 2
     Name: Avaya SIP 9640           Coverage Path 2:                COS: 1
                                    Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19        Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 36007
           Speakerphone: 2-way             Mute Button Enabled? y
       Display Language: english                Button Modules: 0
 Survivable GK Node Name:
         Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? n




                                                Customizable Labels? y
```

•On Page 3 under the heading **BUTTON ASSIGNMENTS**, specify any additional AST-supported function buttons desired. The list of supported buttons is shown in **Table 4**.

```
add station 36007                                          Page   4 of   6
                                    STATION
 SITE DATA
      Room:                                          Headset? n
      Jack:                                          Speaker? n
     Cable:                                         Mounting: d
     Floor:                                      Cord Length: 0
   Building:                                       Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                           5: call-park
 2: call-appr                           6: call-pkup
 3: call-appr                           7: ec500      Timer? n
 4: brdg-appr  B:1  E:34001             8: extnd-call

    voice-mail Number:
```

In the example for the Avaya 9640 IP Telephone, the following buttons were configured:

Buttons 1-3: Call appearances

Button 4: Bridged appearance on station 34001

Button 5: Call Park

Button 6: Call Pickup

Button 7: EC 500 activation

Button 8: EC 500 Extend Call

Note that many function buttons correspond to FNE codes. Unlike the basic Avaya 4600 Series SIP telephones, the AST-capable telephones do not require FAC/FNE codes for those features to be dialed or defined locally on the telephone as speed dial buttons. Buttons that are configured on the station form are automatically displayed the next time the telephone registers with SES. Also, features such as send-all-calls and send-all-calls-cancel are supported with the single “sac” button, whereas two separate FNE codes are required on the basic telephones. By default, the following function buttons are made available on both Avaya 9600 Series IP telephones and Avaya one-X Desktop Edition:

- Transfer to Voicemail
- Extended Group Call Pickup
- Call Park Answer Back

The following screens show the station administration for Avaya one-X Desktop Edition, which is identical to that for the Avaya 9600 Series IP Telephones, except that the **Station Type** field should be specified as “4620”. Different function buttons have been configured on Page 4 for illustrative purposes. Note that on Page 1, the **Security Code** is *not* required. The **Userid** and

Password configured in SES for this telephone is used for authentication at login time.

```
add station 34004                                          Page   1 of   5
                                  STATION

Extension: 34004                      Lock Messages? n              BCC: 0
     Type: 4620                       Security Code:                 TN: 1
     Port: S00005                   Coverage Path 1: 1              COR: 2
     Name: Joe SIP                  Coverage Path 2:                COS: 1
                                    Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 34004
           Speakerphone: 2-way              Mute Button Enabled? y
       Display Language: english               Expansion Module? n
 Survivable GK Node Name:
         Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? n




                                           Customizable Labels? y
```

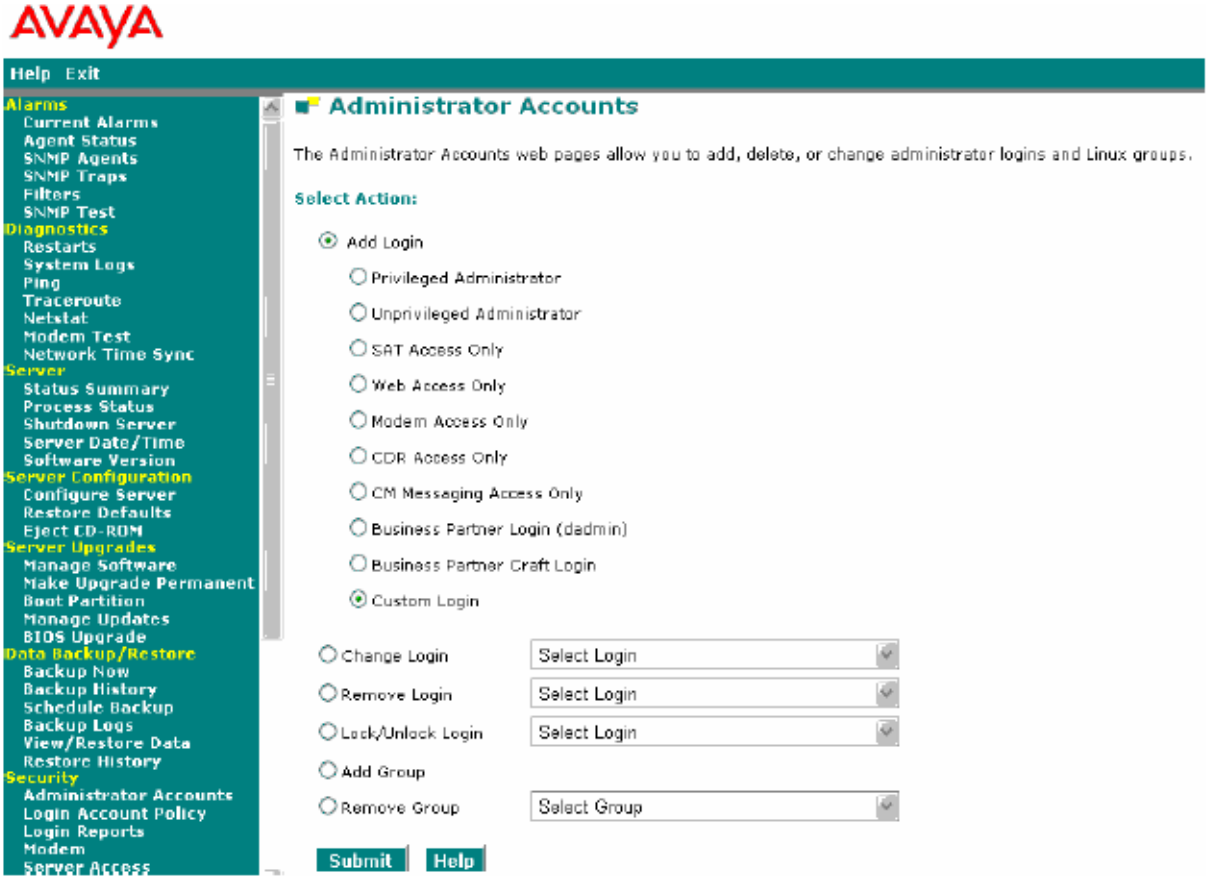
```
add station 34004                                          Page   4 of   5
                                  STATION
 SITE DATA
      Room:                                            Headset? n
      Jack:                                            Speaker? n
     Cable:                                           Mounting: d
     Floor:                                         Cord Length: 0
  Building:                                           Set Color:

ABBREVIATED DIALING
     List1:                   List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                          5: call-pkup
 2: call-appr                          6: priority
 3: call-appr                          7: auto-cback
 4: call-park                          8: whisp-act
```

Function	Function Button Name	Supported on…	
		Avaya 9600 Series IP Telephones	Avaya One-X Desktop Edition
One-touch recording	audix-rec	√	√
Automatic call back	auto-cback	√	√
Bridged appearance	brdg-appr	√	
Call forward all	call-fwd	√	√
Call park	call-park	√	√
Call pickup	call-pkup	√	√
Call forward busy/don't-answer	cfwd-bsyda	√	√
Calling party name block	cpn-blk	√	√
Calling party name unblock	cpn-unblk	√	√
Directed call pickup	dir-pkup	√	√
EC500 mode on/off	ec500	√	√
EC500 extend call	extnd-call	√	
Priority call	priority	√	√
Send all calls/cancel	send-calls	√	√
Whisper page	whisp-act	√	√

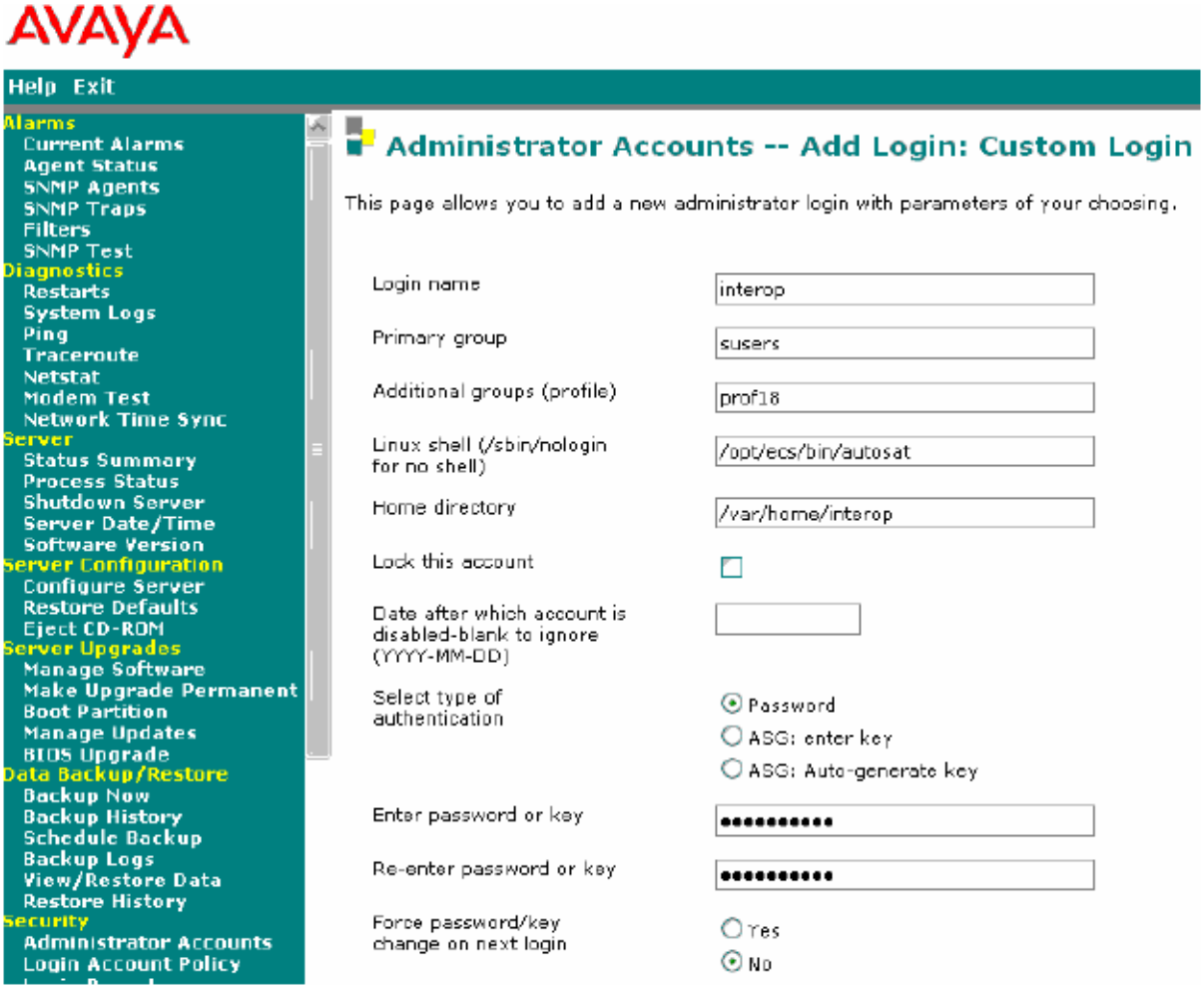
Table 4: AST-Supported Station Buttons

Configure Login Access by SES

The login/password credentials defined in Step 5 of Section 4 are used by SES to retrieve from Communication Manager the function buttons that have been defined for AST telephones. Use the System Management Interface of Communication Manager to configure these credentials. Select **Administrator Accounts** under the *Security* section on the left side. As shown below, under *Select Action*, select **Add Login** and **Custom Login**. Click on **Submit**.



The screen shown below will be displayed. Enter the desired **Login name**. Fill in the **Primary group**, **Additional groups (profile)**, and **Linux shell (/sbin/nologin for no shell)** fields exactly as shown. Enter the desired password in **Enter password or key** and **Re-enter password or key**. The login and password must match those used when configuring the corresponding *Add Communication Server Interface* screen in SES (see Step 5 in Section 4). The remaining settings can be left at their default values. Click on **Submit** (not shown).



Configure Avaya SIP Telephones

The following sections describe the initial configuration steps for Avaya 4600 and 9600 Series IP telephones and Avaya one-X Desktop Edition.

Configure Avaya 4600 and 9600 Series IP Telephones

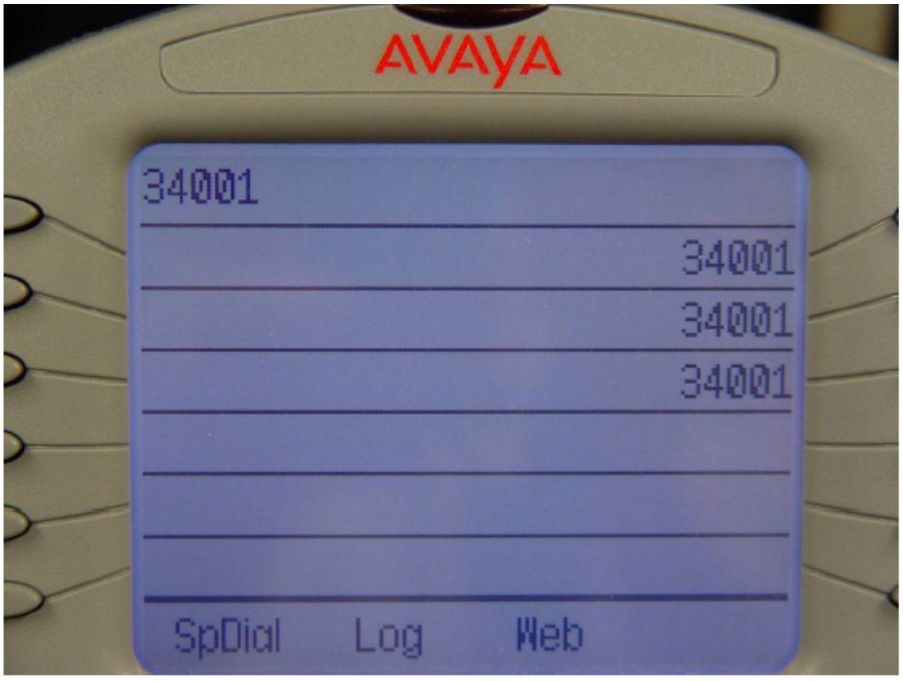
Avaya 4600 and 9600 Series IP Telephones can support either the H.323 or SIP protocols, and they require different application firmware for each. This section describes the steps required to

convert a telephone from H.323 to SIP, or to upgrade the SIP firmware to a specific release. It is assumed that a PC running an HTTP server is available on the network.

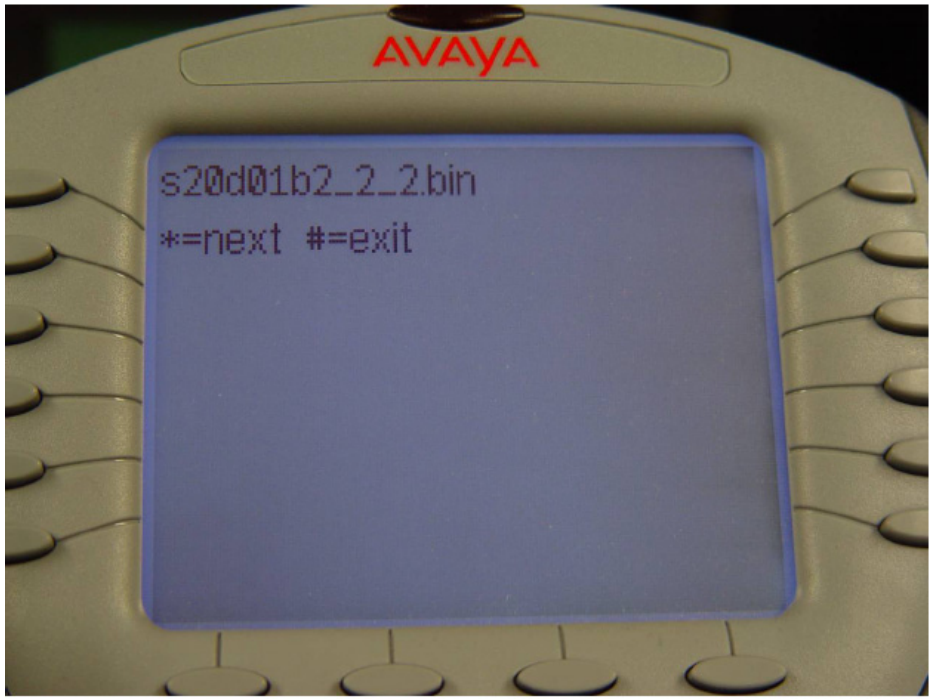
Steps	Description
1.	Obtain the zip files for the SIP firmware release of the Avaya 4600 and 9600 Series IP telephones. For the sample configuration, the files are: *96xx_SIPR2_0_4_053008.zip* *46xxH323_071008.zip* *46xxSIP_upgrade_071008.zip* Extract the files in the order shown above into the HTTP directory on the PC that will be accessed by the telephones during the boot process. Among the extracted files is a file named *96xxupgrade.txt* (46xxupgrade.scr for the 4600 Series), which when accessed by the telephone will cause the SIP firmware to be loaded. The last file listed above contains a SIP- centric upgrade file, which must be extracted last to overwrite the upgrade file contained in 46xxH323_071008.zip.

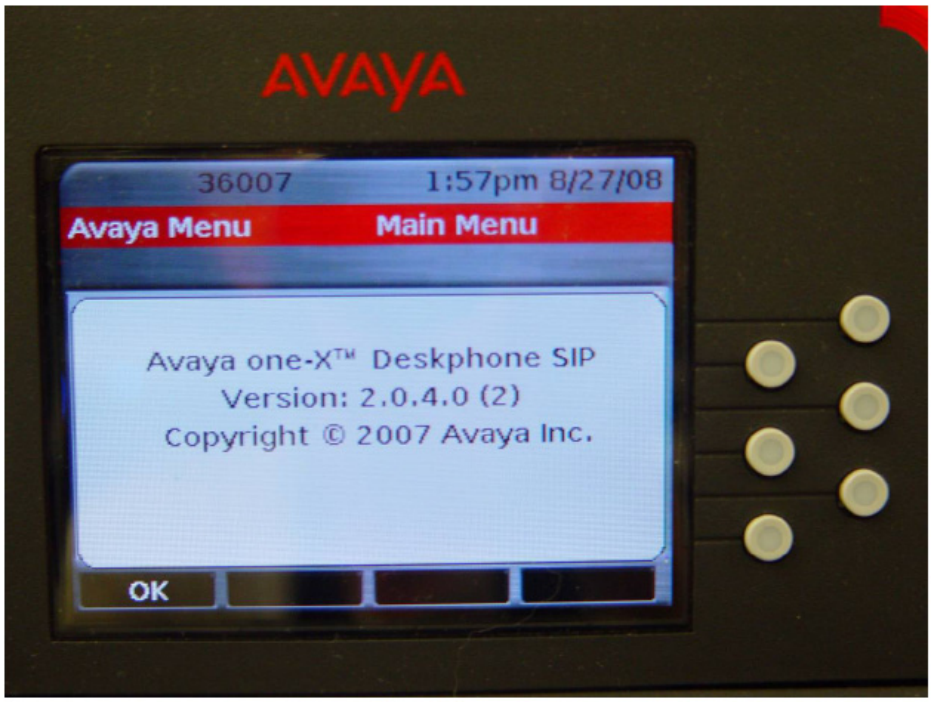
2. Obtain a copy of the 46xxsettings.txt file from the Avaya support site. Edit the file, specifying the following parameters. Note that many other telephone parameters can be set as desired to configure time displays, audio parameters, etc., but are not required for basic operation of the telephone with SES and Communication Manager. See [8, 9] for more details. The settings shown below can be used for both Avaya 4600 and 9600 Series IP Telephones, and corresponds to the sample configuration of Figure 1. Although not covered here, information on Secure RTP (SRTP) support in the Avaya 9600 Series can be found in a separate Application Note [10].

```
## Avaya Environment Enabled (9600 Series only)
##   If set to 1, SIP/AST features and use of PPM are
##   available.
##     0 for 3rd party proxy
##     1 for Avaya SES (default)
SET ENABLE AVAYA ENVIRONMENT 1
##
## SIPDOMAIN sets the domain name to be used during
##  registration.
SET SIPDOMAIN companyx.com
##
##  SIPPROXYSRVR (9600 series) and SIPREGISTRAR (4600 series)
##  sets the IP address or Fully-Qualified
##  Domain Name (FQDN) of the SIP Proxy server(s).
SET SIPPROXYSRVR 10.3.3.41
SET SIPREGISTRAR 10.3.3.41
##
##  PHNNUMOFSA sets the number of Session Appearances the
##  telephone should support.  The default is 3 and valid
##  values are 1-5.  Applicable to 4600 Series only, and should
##  agree with the Avaya Communication Manager station and
##  off-pbx station-mapping forms.  9600 series appearances
##  are controlled by the station form, which also should match
##  the off-pbx form (P.2).
SET PHNNUMOFSA 3
##
##  DIALPLAN accelerates dialing by defining the dial plan
##  used in the phone.  Applicable to 4600 Series only.
##  The default is null ("").
##  The sample value below supports 5 digit extensions beginning
##  with 3, 10-digit ARS dialing with and without "1", and
##  the feature access codes defined in Section 5.4.
##  See Reference [8] for more details.
SET DIALPLAN     "3xxxx|91xxxxxxxxxx|9[2-9]xxxxxxxxx|#[1-9]|*[1-9]|6xx"
##
## Voice Mail Telephone Number (4600 Series only)
##   Specifies the telephone number to be dialed
##   automatically when the telephone user presses the Messaging button.
SET MSGNUM 35000
##
##  MWISRVR sets the IP address or Fully-Qualified Domain
##  Name (FQDN) of the Message Waiting server.
SET MWISRVR 10.3.3.41
```

3.	Connect the telephone to power and the network. Verify that the SIG parameter is set to "SIP"7: **4600 Series:** Press "*" when the phone displays "Press * to program." If DHCP is not used, set the IP address, network mask, gateway, and file server parameters. Press # to cycle through all of the parameter settings until "Enter command:" is displayed. Press Mute S I G on the keypad to view the current value, and change it if necessary. If necessary, press Mute R E S E T. **9600 Series:** Press the Program soft key, followed by the craft access code sequence. If DHCP is not used, use the arrow buttons to set the IP address, network mask, gateway, and file server parameters. Scroll to the SIG parameter. Select it to view the current value, and change it if necessary. Save and/or exit from the configuration menus and the telephone will reset.
4.	The telephone will download the upgrade file and begin the upgrade process. When this process has completed, it will download the 46xxsettings.txt file and prompt for the Extension and Password. The extension and password entered should match the UserID and Password fields administered in SES for this user. The telephone will then register to SES. The 4621 IP Telephone in the sample configuration should look as follows: 

5.	The 9640 IP Telephone in the sample configuration should look as shown below. The available function buttons should match those administered on the station form in Communication Manager (see Section 5.9.2). With the exception of bridged appearances, these buttons are normally displayed by pressing the **`left`** or **`right`** arrow key. Some buttons can be shown on the main phone display by pressing the **Menu** key and navigating to **Options & Settings…->Assign Favorites Entries**, as was done for the EC500 and Extend Call buttons shown below 

6.	Verify the firmware version on 4600 Series IP Telephones by pressing Mute V-I-E-W on the keypad, followed by * until the firmware load file name is displayed. This name should match the file name in the 46xxupgrades.scr file. 

7.	On the 9600 Series IP Telephone, press Menu followed by the arrow keys to select About one-X Deskphone. The firmware version displayed should match the file name in the `96xxupgrades.txt file`. 

Configure Avaya one-X Desktop Edition

Avaya one-X Desktop Edition is a SIP soft phone that runs on several standard PC and Microsoft Windows operating system platforms. Like the 9600 Series IP Telephones8, one-X Desktop Edition supports AST. This section summarizes the configuration steps required to support SIP AST using Avaya one-X Desktop Edition with SES and Communication Manager. It assumes that the program has already been installed on the appropriate platform, and focuses on the configuration screens necessary to successfully register Avaya one-X Desktop Edition with SES and enable the AST feature set. See [11] for more details on operation and features.

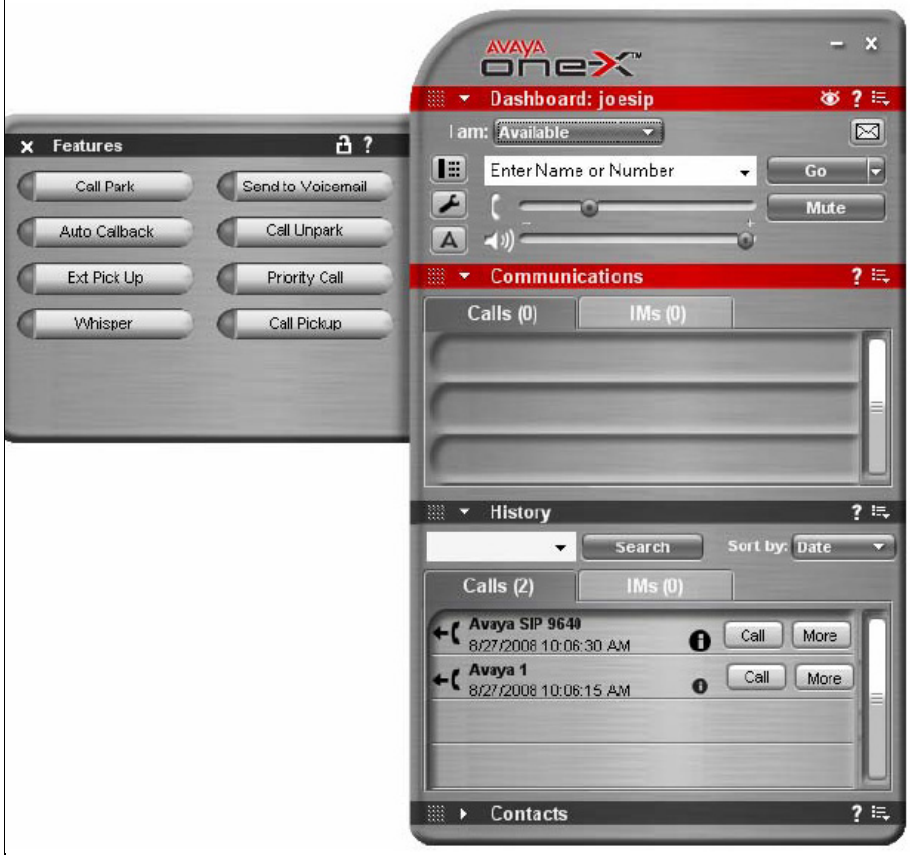
Steps	Description
1.	On the PC, run the one-X Desktop Edition program. When the program is run for the first time, a setup wizard will present several screens used to specify server and user parameters. The following steps show how the parameters should specified based on the sample configuration, as well as how to verify that registration with AST capabilities has been successfully completed
2.	In the Account: User Name and Password screen, enter the display name in **My Name**, user handle ("joesip") and company domain name ("@companyx.com") in **Username**, and **Password**. The handle and password should match the **UserID** and **Password** fields administered in SES for this user. Click on Next. 

3.	In the Profile screen, enter a network Profile Name, and select "Local Area Network" for the **Connection Type.** Click on **Next.** 
4.	In the SIP Server/Licensing Server screen, enter the IP address of the SES server to which one-X Desktop Edition will register in **SIP Server Address**, in this case Home 1. Enter the IP address of the SES server on which the **Licensing server** resides in Licensing Server. The License Server runs on the Home/Edge server or on the Edge server in multiple home configurations. It runs on Server 1 of the duplex pair for HA Edge configurations. In the sample configuration, it is running on Server 1 of the Edge server. Click on **Next**. 

5.	In the Dialing Rules screen, fill in the appropriate fields based on the desired dial plan. Note that the values entered should be compatible with the dial plan administration in Communication Manager. For example, **What number do you dial for an outside line** should match the ARS feature access code configured in Section 5.4. Click on **Next.** 
6.	In the Voicemail Integration (Optional) screen, check **Enable voicemail integration** if desired. To have the voice mail hunt group extension automatically dialed when the voicemail icon is pressed (See Step 9), enter this extension in **Dial the voicemail extension:**. Click on **Next**. 

7.	Initial setup is now complete, as indicated by the following screen. Click on **Finish**. 
8.	When Avaya one-X Desktop Edition is started, the following dashboard display appears. Click on **Login** to log in and begin making calls. 

9.	The following display shows the result of successful login, registration with SES, and completion of two calls. The configuration parameter values assigned in the previous steps can be changed at any time by clicking on the Settings icon. Pressing the voice mail icon will place a call into the voice mail system. The presence of the "A" icon indicates that AST support is available. 

10.	Clicking on the AST icon will display the function buttons configured for this station. These buttons can be selected to invoke the corresponding function. The buttons that were configured for the sample configuration are shown below (See Section 5.9.2). 

Verification Steps

The following steps can be used to verify and/or troubleshoot installations in the field.

Registration and Button Display

12. Verify registration with SES as described in Section 6. If errors occur during the registration process:

    a.Verify that the **Userid** and **Password** administered for this user in SES match those entered at registration time.

    b. Verify that the **SIPDOMAIN** parameter in the `46xxsettings.txt` file contains the same **SIP Domain** that was defined in the *System Properties* page of the SES host to which this phone is registering.

13. For AST telephones such as Avaya 9600 Series IP Telephones and Avaya one-X Desktop Edition, if the function buttons configured in Communication Manager are not displayed, verify that the login and password configured in SES (Step 5, Section 4) and Communication Manager (Section 5.9.3) are the same. This is required so that SES can access Communication Manager to obtain station button and contacts information. To verify that the login has been correctly configured:

    a. Log in to the SES Command Line Interface (CLI) via PuTTY or other CLI

    client.

    b. Use Secure Shell (`ssh`) to log into the Communication Manager server address using port 5022 and the login credentials administered on SES. For the sample configuration, the command would be

    ssh interop@10.3.3.10 -p 5022

    c. Verify that the login is successful and the SAT interface is displayed.

14. If the AST icon is not displayed on Avaya one-X Desktop Edition, select the **settings** icon and select **Advanced**. Verify that the **Communication Protocol** is “TLS”. AST is not supported for “TCP”.

Basic Calls

15. Verify basic calls among the configured telephones. If basic calls cannot be completed successfully (for example, if Communication Manager responds to an incoming INVITE with “403 Screening Failure – 399 restricted access”), verify that the **Authoritative Domain** in the ip-network-region form associated with the telephones matches that configured in SES and the telephones (see 1(b), Section 7.1). The network region for the called telephone is the network region of the SIP signaling group specified in the **Trunk Selection** Field on Page 2 of the off-pbx station-mapping form. The network region for the calling station is that

of the SIP trunk on which the call is serviced, unless the IP address of the telephone is covered by an ip-network-map entry.

16. For calls coming in on a SIP trunk from a foreign SIP domain (as indicated by the domain portion of the From header in the INVITE message), verify that a SIP trunk has been configured whose signaling-group contains a **Far-end Domain Name** value that matches this foreign domain, or a blank value. A blank value will ensure that this SIP trunk will be used for any unknown domains.

Calling Features

1. Test supported features according to **Table 2** and feature deployment plans at the site. Verify Communication Manager features by pressing the appropriate soft key (Avaya 9600 Series IP Telephones and Avaya one-X Desktop Edition), or (speed) dialing the FNE (Avaya 4600 Series IP Telephones). If busy or intercept tone is heard, check Communication Manager for the correct FNE, proper permissions under COS/COR, and the proper station button assignment to support the feature.
2. Call a telephone that currently has no voice messages, and leave a message. Verify that the message-waiting indicator (MWI) illuminates on the called telephone. Call the voice mail system from that telephone. Use the voice messaging menus to retrieve and delete the voice message, verifying that DTMF is interpreted correctly by the system, and that the message waiting indicator extinguishes. If no MWI changes occur, ensure that the SIP trunk signaling group in Communication Manager on which the NOTIFY message to SES is sent contains the SIP domain of SES in the **Far-end Domain Name**. The signaling group is selected based on the off-pbx station-mapping form for the telephone. But note that if two SIP trunks have been configured with identical near- and far-end node names, the trunks are treated as one large trunk, with the lower numbered signaling group being used for MWI. If that trunk is defined with a foreign domain name, then NOTIFY messages sent for MWI state changes will be ignored by SES.

Conclusion

This appendix have described the administration steps required to support Avaya 4600

Series, 9600 Series, and one-X Desktop Edition users with SIP Enablement Services and Communication Manager. Basic telephony service has been addressed. Details on additional telephone and system features can be found in the respective administrative manuals in the following section.

Additional References

[1]*Session Initiation Protocol Service Examples - draft-ietf-sipping-service-examples-15*, SIPPING Working Group, Internet-Draft, 7/16/2007, available at http://tools.ietf.org/wg/sipping/draft-ietf-sipping-service-examples/draft-ietf-sipping- service-examples-15.txt.

[2]*Avaya Extension to Cellular and OPS Installation and Administration Guide*, Doc ID 210-100-500, available at http://support.avaya.com.

[3]*SIP Support in Avaya Aura® Communication Manager Running on Avaya S83xx Servers*, Doc ID 555-245-206, available at http://support.avaya.com.

[4]*Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, available at http://support.avaya.com.

[5]*Installing, Administering, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services*, Doc ID 03-600768, available at http://support.avaya.com.

[6]*4600 Series IP Telephone LAN Administrator Guide*, Doc ID 555-233-508, available at http://support.avaya.com.

[7]*Avaya Aura® SIP Enablement Services (SES) Implementation Guide*, Doc ID 16-300140, available at http://support.avaya.com.

[8]*4600 Series IP Telephone LAN Administrator Guide*, Doc ID 555-233-507, available at http://support.avaya.com.

[9]*Avaya one-X Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide,* Doc ID 16-601944, available at http://support.avaya.com.

[10]*Configuring Secure Real-Time Transport Protocol (SRTP) and G.722 Audio using Avaya*

9600-Series IP Telephones running SIP and H.323 Firmware, available at http://support.avaya.com.

[11]*one-X Desktop Edition Getting Started*, Doc ID 16-600973, available at http://support.avaya.com.

Glossary

A

Access code — A dial code of 1 to 3 digits that activates a feature, cancels a feature, or accesses an outgoing <SIP Enablement>.

Access Security Gateway — See <SIP Enablement>.

Adjunct server — See <SIP Enablement>.

Adjunct system — See <SIP Enablement>.

Alias — An alternative name for an object, such as a variable, file, or device.

ART — Automatic Registration Tool. ART allows customers and technicians to register newly installed products for warranty and service support.

ASG — Access Security Gateway. A software module that secures Avaya Global Services login accounts on SES servers. Each login attempt on these accounts is met with a one-time challenge string that must be answered with the correct one-time response.

Avaya Communication Manager — An open, scalable, highly reliable, and secure telephony application. Communication Manager provides user functionality and system management functionality, intelligent call routing, application integration and extensibility, and Enterprise Communications networking.

Baseboard Management Controller (BMC) — A specialized microcontroller embedded on the motherboard of the server which allows to perform hardware related operations regardless of the main CPU status. SES uses the BMC in cable duplex setups of S8800 or HP DL360 G7 servers in order to allow a server to reset its peer.

B-channel — Bearer channel. A 64-kbps channel or a 56-kbps channel that carries a variety of <SIP Enablement> information streams. A B-channel carries voice at 64 kbps, data at up to 64 kbps, <SIP Enablement> voice encoded at 64 kbps, and voice at less than 64 kbps, alone or combined. See also <SIP Enablement>.

Bearer channel (B-channel) — A 64-kbps channel or a 56-kbps channel that carries a variety of <SIP Enablement> information streams. A B-channel carries voice at 64 kbps, data at up to 64 kbps, WebLM voice encoded at 64 kbps, and voice at less than 64 kbps, alone or combined. See also <SIP Enablement>.

Baseboard Management Controller (BMC) — A specialized microcontroller used in S8800 and HP DL360 G7 servers to allow a server to reset its peer. It is embedded on the motherboard of the server and allows to perform hardware related operations regardless of the main CPU status.

Backup In a duplicated configuration supporting local failover, this is the server that is synchronized and ready to interchange with the <SIP Enablement> server. Sometimes referred to as the <SIP Enablement>.

Bus A multiconductor electrical path that transfers information over a common connection from any of several sources to any of several destinations. *See also* <SIP Enablement>; <SIP Enablement>.

C

CA Certificate Authority.

Cable duplicated An alternate term for Cable duplex

Call Detail Recording (CDR) A file that uses software and hardware to record call data. CDR was formerly called Station Message Detail Recording (SMDR). *See also* <SIP Enablement>.

Call Detail Recording utility (CDRU) Software that collects, stores, filters, and provides output of call detail records. *See also* <SIP Enablement>.

Carrier An enclosed shelf that contains vertical slots that hold <SIP Enablement>s.

CCRON Coverage of calls redirected off-network.

Central office (CO) Telephone switching equipment that provides local telephone service and access to toll facilities for long distance calling.

CDR Call detail record. A file that uses software and hardware to record call data. CDR was formerly called Station Message Detail Recording (SMDR). *See also* <SIP Enablement>.

CDRU Call detail recording utility. Software that collects, stores, filters, and provides output of call detail records. *See also* <SIP Enablement>.

Channel 1. A <SIP Enablement>-switched call.

2. A communications path that transmits voice and data.
3. In <SIP Enablement> transmission, all the contiguous time slots or non-contiguous time slots that are necessary to support a call. For example, an H0-channel uses six 64-kbps time slots. (4) A digital signal-0 (DS0) on a T1 facility or an E1 facility that is not specifically associated with a logical circuit-switched call. *See also* <SIP Enablement>.

Circuit 1. An arrangement of electrical elements through which electric current flows.

2. A <SIP Enablement> or a transmission path between two or more points.

Circuit pack A circuit card on which electrical <SIP Enablement>s are printed, and integrated circuit (IC) chips and electrical components are installed. A circuit pack is installed in a <SIP Enablement> <SIP Enablement>. One example is the TN2302.

CCITT Comitte Consultatif International Telephonique et Telegraphique. *See* <SIP Enablement>.

CCS See <SIP Enablement>.

Class of Restriction (COR) A feature that allows up to 96 classes of call-origination restrictions and call-termination restrictions for telephones, telephone groups, <SIP Enablement>s, and <SIP Enablement>s. *See also* <SIP Enablement>.

Class of Service (COS) A feature that uses a number to specify whether telephone users can activate the Automatic Callback (ACB), Call Forwarding All Calls, Data Privacy, or Priority Calling features. *See also* <SIP Enablement>.

C-LAN circuit pack Controlled local area network. A <SIP Enablement> (TN799B) in an Avaya DEFINITY port network (PN) that provides <SIP Enablement> connectivity to adjuncts over Ethernet or <SIP Enablement>. The C-LAN circuit pack serves as the network interface for a DEFINITY server. The C-LAN terminates IP (<SIP Enablement> and <SIP Enablement>), and relays those sockets and connections up to the Avaya DEFINITY server.

CLI Command line interface.

CO Central office. Telephone switching equipment that provides local telephone service and access to toll facilities for long distance calling.

Co-resident A SES solution in which SES and Communication Manager reside on the same server. See <SIP Enablement>.

Combined server An SES server that performs functions of both a home server and an edge server. See <SIP Enablement>.

Communication Manager (CM) Avaya Communication Manager, an open, scalable, highly reliable, and secure telephony application. Communication Manager provides user functionality and system management functionality, intelligent call routing, application integration and extensibility, and Enterprise Communications networking.

Communications system A software-controlled processor complex that interprets dial pulses, tones, and keyboard characters, and makes the proper connections within the system and externally. The communications system consists of a <SIP Enablement> computer, software, storage devices, and <SIP Enablement>s, with special hardware to perform the connections. A communications system provides communications services for the telephones on customer premises and the <SIP Enablement>s on customer premises, including access to <SIP Enablement>s and <SIP Enablement>s. *See also* <SIP Enablement>.

Controlled Local Area Network (C-LAN) circuit pack A <SIP Enablement> (TN799B) in an Avaya DEFINITY port network (PN) that provides <SIP Enablement> connectivity to adjuncts over Ethernet or <SIP Enablement>. The C-LAN circuit pack serves as the network interface for a DEFINITY server. The C-LAN terminates IP (<SIP Enablement> and UDP), and relays those sockets and connections up to the Avaya DEFINITY server.

COR Class of Restriction. A Communication Manager feature that allows up to 96 classes of call-origination restrictions and call-termination restrictions for telephones, telephone groups, <SIP Enablement>s, and <SIP Enablement>s. *See also* <SIP Enablement>.

COS Class of Service. A feature that uses a number to specify whether telephone users can activate the Automatic Callback (ACB), Call Forwarding All Calls,

	Data Privacy, or Priority Calling features of Communication Manager. *See also* <SIP Enablement>.
CPN	Called-party number.
CPN/BN	Calling-party number/billing number.
CPE	Customer premises equipment. Equipment that is connected to the telephone <SIP Enablement>, and that resides on a customer site. CPE can include telephones, modems, fax machines, video conferencing devices, switches, and so on.

D

D-channel	Data channel. A 16-kbps channel or a 64-kbps channel that carries signaling information or data on an <SIP Enablement> or <SIP Enablement>. *See also* <SIP Enablement>.
Data module	An interconnection device between a Basic Rate Interface (BRI) or a digital communications protocol (<SIP Enablement>) interface of the <SIP Enablement>, and the <SIP Enablement> or <SIP Enablement>.
Data terminal	An input/output (I/O) device that has either switched access or direct access to a <SIP Enablement> or to a processor interface.
DCE	Data communications equipment. Equipment on the <SIP Enablement> side of a communications link that makes the binary serial data from the source or the transmitter compatible with the communications <SIP Enablement>. DCE is usually a modem, a <SIP Enablement>, or a <SIP Enablement>.
DCHP	Dynamic host configuration protocol. An IETF <SIP Enablement> (RFCs 951, 1534, 1542, 2131, and 2132) that assigns IP addresses dynamically from a pool of addresses instead of statically. DHCP provides the IP address to the SIP device.
DCP	Digital communications protocol. A proprietary <SIP Enablement> that transmits both digitized voice and digitized data over the same communications link. A DCP link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels, and thus two telephones or data modules. The I1 channel is the DCP channel that is assigned on the first page of the 8411 Station screen. The I2 channel is the DCP channel that is assigned on the analog adjunct page of the 8411 Station screen, or on the data module page.
DECM	Distributed Enterprise Central Management. Integrated Management for Communication Manager Branch Edition is the true term for this concept, ant that includes DOLM and DOCM. It is the Central Management interface for Avaya Communication Manager Branch Edition.
Dynamic Host Configuration Protocol (DHCP)	An IETF <SIP Enablement> (RFCs 951, 1534, 1542, 2131, and 2132) that assigns IP addresses dynamically from a pool of addresses instead of statically.
DID	Direct Inward Dialing.

Digital The representation of information by discrete steps. Compare with *analog*.

Digital Communications Protocol (DCP) A proprietary <SIP Enablement> that transmits both digitized voice and digitized data over the same communications link. A DCP link consists of two 64-kbps information (I) <SIP Enablement>s, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels, and thus two telephones or <SIP Enablement>s. The I1 channel is the DCP channel that is assigned on the first page of the 8411 Station screen. The I2 channel is the DCP channel that is assigned on the analog adjunct page of the 8411 Station screen, or on the data module page.

DIMM Dual Inline Memory Module.

Distributed server An SES configuration in which the edge server and the home server reside on physically different machines. See <SIP Enablement>.

DNS Domain Name Service, a system that stores information about host names and domain names in a kind of distributed database on networks, such as the Internet. DNS provides an IP address for each host name, and lists the mail exchange servers accepting e-mail for each domain.

DOCM Distributed Office central manager, the managing server that manages branch servers.

DOLM Distributed Office local manager, the managing server at a branch.

DRBD Distributed redundant block device.

DTE Data terminal equipment. Equipment that comprises the endpoints in a connection over a data <SIP Enablement>. In a connection between a <SIP Enablement> and a host, the terminal, the host, and the associated modems or <SIP Enablement>s comprise the DTE.

DTMF Dual-tone multifrequency. The touchtone signals that are used for in-band telephone signaling.

Duplicated The host configuration supporting local failover by using the interchange of the <SIP Enablement> and <SIP Enablement> servers. Any host node may comprise two interconnected servers. Compare with <SIP Enablement>.

E

Edge server In Avaya's SIP architecture, this is the <SIP Enablement> that forwards requests to and from the customer's network. It sends inbound SIP requests or messages to the home proxy servicing the specified user.

Extension A number from 1 digit to 5 digits that routes calls through a <SIP Enablement>. With a Uniform Dial Plan (<SIP Enablement>) or a main-satellite dialing plan, extensions also route calls through a <SIP Enablement>.

F

feature A specifically defined function or service that the system provides.

FNE Feature Name Extension

FNU Feature Name URI

FTP	File Transfer Protocol.
FQD or FQDN	Fully qualified domain name. A fully qualified domain name consists of a host and domain name, including the top-level domain, for example, `Bill.Gates.MSN.com`.

G

GB	Gigabyte(s).

H

H.323	An <SIP Enablement> standard for switched multimedia communication between a LAN-based multimedia endpoint and a gatekeeper. *See also* <SIP Enablement>.
HA or HAP	High Availability or High Availability Platform.
handle	A handle is the way SES and Communication manager recognize an end user, or perhaps a group. A handle could be an end user's telephone extension, real name, a nickname, or a designation. Handles may have two URIs available for contacting the end user, perhaps a DID extension, or an e-mail address.
Home server	This is the domain providing service to a SIP user, used in registering that user with a home proxy. A home server is designated generally as a <SIP Enablement>, and the series of Host screens administer it.
Host name	See <SIP Enablement>.
Host computer	A computer that is connected to a <SIP Enablement>, and that processes data from data entry devices. In SES, a host is an S8300C, S8500B, or S8500C. In addition, a host holds either the <SIP Enablement> server, the <SIP Enablement> server, or acts as a combined home/edge. Contrast this with <SIP Enablement>.

I

ICMP	Short for Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The **`ping`** command, for example, uses ICMP to test an Internet connection.
IE	*See* <SIP Enablement>.
IEEE	*See* Institute of Electrical and Electronics Engineers (IEEE).
IETF	Internet Engineering Task Force. One of two technical working bodies of the Internet Activities Board. The IETF develops new <SIP Enablement>/<SIP Enablement> standards for the Internet.
Integrated Lights Out (ILO3)	Used as the BMC module in the HP DL360 G7 server.
Integrated Management Module (IMM)	Used as the BMC module in the S8800 server.

IM Instant Messaging. The instant-messaging client software required for release R3.x of Avaya SES is a version of the Avaya IP Softphone R5 or later, or SIP Softphone R2 or later.

Initialization and Administration System (INADS) A software tool that is used by Avaya Services personnel for communication, remote management and troubleshooting of customers' alarms and traps.

information element (IE) The name for the data fields within an <SIP Enablement> Layer 3 message.

Interchange Term used for when the <SIP Enablement> server in a <SIP Enablement> configuration relinquishes control and its <SIP Enablement> server takes over that control, running the SIP software applications and services for this SES node. This is the <SIP Enablement> feature.

IP Internet protocol. A connectionless <SIP Enablement> that operates at layer 3 of the <SIP Enablement> model. IP protocol is used for Internet addressing and routing packets over multiple <SIP Enablement>s to a final destination. IP protocol works in conjunction with <SIP Enablement>.

IP interface A C-LAN, ethernet processor interface, or procr that lets the server connect using internet protocol.

ISDN Integrated Services Digital Network. A <SIP Enablement> or a <SIP Enablement> that provides end-to-end <SIP Enablement> communications for all services to which users have access. An ISDN uses a limited set of standard, multipurpose, user-network interfaces that are defined by the <SIP Enablement>. Through internationally accepted standard interfaces, an ISDN provides digital <SIP Enablement> switching communications or packet switching communications within the network. An ISDN provides links to other ISDNs to provide national digital communications and international digital communications. *See also* <SIP Enablement>, <SIP Enablement>.

ISDN-BRI Integrated Services Digital Network Basic Rate Interface. The interface between a communications system and terminal that includes two 64-kbps <SIP Enablement>s for transmitting voice or data, and one 16-kbps <SIP Enablement> for transmitting associated B-channel call control and out-of-band signaling information. ISDN-BRI also includes 48 kbps for transmitting framing and D-channel contention information, for a total interface speed of 192 kbps. ISDN-BRI serves ISDN terminals and <SIP Enablement> terminals that are fitted with ISDN terminal adapters. *See also* <SIP Enablement>.

ISDN-PRI Integrated Services Digital Network Primary Rate Interface. The interface between multiple communications systems that in North America includes 24 64-kbps channels that correspond to the North American digital signal-level 1 (DS1) standard rate of 1.544 Mbps. The most common arrangement of channels in ISDN-PRI is 23 64-kbps <SIP Enablement>s for transmitting voice and data, and one 64-kbps <SIP Enablement> for transmitting associated B-channel call control and out-of-band signaling information. With nonfacility-associated signaling (NFAS), ISDN-PRI can include 24 B-channels and no D-channel. *See also* <SIP Enablement>, <SIP Enablement>.

ITU	International Telecommunications Union. An international organization that sets universal standards for data communication, including <SIP Enablement>. ITU was formerly known as International Telegraph and Telephone Consultative Committee (<SIP Enablement>).

K

KVM	Keyboard, Video display monitor, and (optional) Mouse switch. Allows one set of these devices to control more than one computer, but one at a time.

L

LAN	Local area network. A networking arrangement that is designed for a limited geographical area. Generally, a LAN is limited in range to a maximum of 6.2 miles, and provides high-speed carrier service with low error rates. Common configurations are daisy chain, star (including <SIP Enablement>-switched), ring, and bus.
Local failover	The feature supports database replication and interchange, as needed, between two servers (one <SIP Enablement>, one <SIP Enablement>), which are connected in a <SIP Enablement> configuration.

M

MAC	MAC address or MAC name. Media Access Control address, a 48-bit hardware address that uniquely identifies each node, interface card, or device of a network.
Communication Manager Server	1. In SES specifically, a communication manager server refers to the Linux-based hardware on which Avaya Communication Manager has been installed. 2. Avaya Communication Manager Server. A family of application-enabling processing platforms based on open CPUs and industry-standard operating systems. Communication Manager servers provide multiprotocol networking that includes, but is not limited to, Internet Protocol (IP). In addition to supporting a highly diversified network architecture, communication manager servers provide user functionality, system management functionality, intelligent call routing, application integration, mobility, and conferencing.
MIB	Management information base (or block). A directory listing logical names of resources on a network, pertinent to the network's system management.
MM	**Modular Messaging.** An Avaya messaging system configurable as a SIP adjunct and comprised of one or more telephony servers and one message store.
MAS	Modular Messaging Telephony Server. There may be 1-15 of these servers in an MM Adjunct System.

N

NAME1	Legacy name, Latin characters, usually displayable, for example Eurofont and Kanafont encoding.

NAME2 UTF-8 encoding. Used for multibyte character sets such as Chinese ideograms Hiragana, Katakana, and Hangul

Narrowband A <SIP Enablement>-switched call at a data rate of 64 kbps or less. All switch calls that are not <SIP Enablement> are considered to be narrowband. *Compare with* <SIP Enablement>.

Network A series of points, <SIP Enablement>s, or stations that are connected by communications <SIP Enablement>s.

Network duplicated An alternate term for network duplex.

Network region Network Region is a flexible administrative concept. A network region is an attribute associated with Communication Manager resources. It is used in the administration of, among other things, resource allocation and security.

For example, when an H.323, or SIP, IP endpoint requires a Gateway Resource to set up a talk path with a non-IP endpoint, like a DCP telephone, for example, Communication Manager checks the network region parameter to attempt to get that gateway resource from the same Network Region, that is, as near to the endpoint as possible, to minimize trunk usage and delay.

NIC Network Interface Card.

Node A switching point or a control point for a <SIP Enablement>. Nodes are either tandem or terminal. Tandem nodes receive signals and pass the signals on. Terminal nodes originate a transmission path or terminate a transmission path.

Nonce Random value sent in a communications protocol exchange, often used to detect replay attacks.

O

OATS Origination and Termination Signaling. Formerly known as an origination-based call flow or 'W' call flow. In a call-flow diagram, this describes the direction, initiation, and termination of signaling.

OSI Open Systems Interconnect. A system of seven independent communication <SIP Enablement>s defined by the International Standardization Organization (ISO). Each of the seven protocols enhances the communications services of the layer below, and shields the layer above from the implementation details of the lower layer. In theory, this structure can be used to build <SIP Enablement>s from independently developed layers.

off-PBX station (OPS) A telephone that <SIP Enablement> does not control, such as a cellular telephone or the home telephone of a user. The features of Communication Manager can be extended to an OPS through switch administration by associating the extension of the office telephone with the off-site telephone.

OPS Outboard Proxy SIP.

Open Systems Interconnect (OSI) A system of seven independent communication <SIP Enablement>s defined by the International Organization for Standards or ISO. Each of the seven layers enhances the communications services of the layer below, and shields the layer above from the implementation details of the lower layer. In theory, this

	structure can be used to build <SIP Enablement>s from independently developed layers.
origination-based call flow	See <SIP Enablement>.
O/S	Operating System.
P	
Packet	A group of bits that is used in <SIP Enablement> and that is transmitted as a discrete unit. A packet includes a message element and a control <SIP Enablement>. The message element is the data. The control IE is the header. In each packet, the message element and the control IE are arranged in a specified format.
Packet Assembly/ Disassembly (PAD)	The process of packetizing control data and user data from a transmitting device before the data is forwarded through the packet network.The receiving device disassembles the <SIP Enablement>s, removes the control data, and then reassembles the packets, thus reconstituting the user data in its original form.
Packet bus	A <SIP Enablement> with a wide bandwidth that transmits <SIP Enablement>s.
Packet switching	A data-transmission technique that segments and routes user information in discrete data envelopes that are called *<SIP Enablement>s*. Control information for routing, sequencing, and error checking is appended to each packet. With packet switching, a <SIP Enablement> is occupied only during the transmission of a packet. On completion of the transmission, the channel is made available for the transfer of other packets.
PAD	Packet assembly/disassembly. The process of packetizing control data and user data from a transmitting device before the data are forwarded through the packet network.The receiving device disassembles the packets, removes the control data, and then reassembles the packets, reconstituting the user data in original form.
PBX	Private Branch Exchange. *See* <SIP Enablement>.
PCI	PC interface (card).
PDU	In telecommunications, the term protocol data unit (PDU) has the following meanings: 1. Information that is delivered as a unit among peer entities of a network and that may contain control information, address information, or data. 2. In layered systems, a unit of data that is specified in a protocol of a given layer and that consists of protocol-control information of the given layer and possibly user data of that layer. Source: from Federal Standard 1037C
POTS	Plain Old Telephone Service. Basic voice communications with standard, single-line phones accessing the <SIP Enablement>.

PPM	Personal Profile Manager. This is the server software that supports the SIP PIM interface that lets the end user manage their demographic data. Personal Profile Manager (PPM) is a centralized repository of personalized data, such as contact lists or access control lists. PPM provides a Web Services interface that allows a client, such as a SIP telephone or SIP Softphone, to download a particular user's profile, thus allowing the user the mobility to move around to different devices but maintain access to the user's unique information. As an example, a user might log in one day at a telephone at a service desk, and then the next from a Softphone while working from home. In each case, the user's personal profile would appear at each of those devices.
PPP	Point-to-Point Protocol. A standard that largely replaces SLIP, allowing a computer to use <SIP Enablement> with a regular telephone line.
port	A data-transmission access point or voice-transmission access point on a device that is used for communicating with other devices.
PPM	Personal Profile Manager. The interface that TSP users have that allows them to personalize their telephone usage.
Processor ethernet	A logical connection between the server itself and a network interface card. The way this connection is administered in Communication Manager determines what type of traffic the NIC allows.
Primary	In a duplicated configuration supporting local failover, this is the server that is running the SIP applications and services. Sometimes referred to as the active server, server A, or others. Compare with <SIP Enablement>.
Private network	A <SIP Enablement> that is used exclusively for the telecommunications needs of a particular customer.
Procr	See <SIP Enablement>.
Protocol	A set of conventions or rules that governs the format and the timing of message exchanges. A protocol controls error correction and the movement of data.
Proxy server	An intermediary server for making requests on behalf of other client entities. The job of an Avaya SIP proxy is to ensure that a request is sent to the entity closest to the specified user. For example, an edge proxy server interprets and forwards requests intended for specific users to their particular home proxy servers.
Proxy trust domain	Includes those SIP servers and gateways, but not endpoints with identities administered on the server running SES.
Public network	A <SIP Enablement> to which all customers have open access for local calling and long distance calling.
Public switched telephone network (PSTN)	The public worldwide voice telephone <SIP Enablement>.
PSTN	Public Switched Telephone Network.

Public network A <SIP Enablement> to which all customers have open access for local calling and long distance calling.

R

RAS Remote Access Server or, in Microsoft Windows operating systems, Remote Access Service.

RFA Remote Feature Activation is a web-based application that obtains Avaya authentication and licensing files. RFA is a tool and its output is a license file. RFA produces license files for 14 different products, one of which is Communication Manager. The home page for this application is at http://rfa.avaya.com.

RMB Remote Maintenance Board (RMB) is a remote servicing module for servers.

RFC Request for Comments designates Internet Engineering Task Force (IETF) standards that are drafts.

RNIS Remote Network Implementation Services is a contract installation services group within Avaya Inc.

RPM Red Hat Package Manager.

RSA Remote Supervisor Adapter. This module is in the S8500A server and acts as a remote maintenance board or remote servicing module. S8500A is no longer supported. Contrast with <SIP Enablement>.

RTC Real Time Communication.

RTCP Real Time Control Protocol.

RTP Real time transfer protocol. An <SIP Enablement> <SIP Enablement> (RFC 1889 and 3550) that addresses problems occurring when video and other exchanges with real-time properties are delivered over a <SIP Enablement> designed for data. RTP gives higher priority to video and other real-time interactive exchanges than to connectionless data.

S

S8800 A hardware platform from IBM x3550 series. The S8800 Server supports SIP Enablement services as a simplex or duplex standalone.

S8400 A hardware platform for use as an Avaya server that is a single module. The S8400 uses a flash drive, and the SAMP functionality is on the board. No separate chassis is required.

S8500 A hardware platform from the IBM x305 series. This machine uses an RSA for a remote maintenance board.

S8500B A hardware platform from the IBM x306 series. This machine uses a SAMP for a remote maintenance board.

SAMP Server Availability Management Processor. This module is in the S8500B, S8500C and S8510 server, and acts as a remote servicing module or <SIP Enablement>. See <SIP Enablement>.

SCCAN The Seamless Converged Communications Across Networks (SCCAN) solution offers voice and data access from a single SCCAN handset integrated with a desk phone across the corporate Wireless Local Area Network (WLAN) and public Global System for Mobile communication (GSM) and cellular networks.

SAT System Access Terminal. Application providing Communication Manager a command-line interface.

SCP Secure Copy Protocol.

Survivable call processor. The server provides limited call processing between the phones on a home if the SES network should fail.

Secondary Another name for the <SIP Enablement> server, or server B, in a <SIP Enablement> configuration. Compare with <SIP Enablement>.

SES **SIP Enablement Services**, formerly the Converged Communications Server (CCS). SES hosts are Avaya proxy and registrar servers for <SIP Enablement>, supporting instant messaging.

SFTP Secure File Transfer Protocol, or <SIP Enablement>.

\single An SES host configuration with one server per node. Compare with <SIP Enablement>.

SIP Session initiation protocol. An IETF standard (RFC 3261) signaling <SIP Enablement> for Internet conferencing, telephony, presence, events notification, and instant messaging. SIP initiates call setup, routing, authentication, and other feature messages to endpoints within an IP domain. *See also* <SIP Enablement>, <SIP Enablement>.

SIP adjunct server A server integrated with SES via SIP and an element of a SIP adjunct system.

SIP adjunct system A system integrated with SES via SIP. It may consist of one or more servers.

SMS System Management Services.

Short Message Service which is similar to paging. SMS is a service for sending short text messages to mobile phones and devices.

SNMP Simple Network Management Protocol.The industry-standard protocol that governs network management and the monitoring of network devices and the functions of those devices. The user of SNMP is not necessarily limited to TCP/IP networks, but can be implemented on Ethernet and Open Systems Interconnect (<SIP Enablement>) transports.

SOAP **S**imple **O**bject **A**ccess **P**rotocol is a light-weight protocol for exchanging messages between computer software, typically in the form of software componentry. The word object implies that the use should adhere to the object-oriented programming paradigm.

SOAP is an extensible and decentralized framework that can work over multiple computer network protocol stacks. Remote procedure calls can be modeled as an interaction of several SOAP messages. SOAP is one of the enabling protocols for Web services.

	SOAP can be run on top of all the Internet Protocols, but HTTP is the most common and the only one standardized by the W3C. SOAP is based on XML, and its design follows the Head-Body software markup pattern, like HTML. The optional **Header** contains meta-information such as information for routing, security, and transactions. The **Body** transports the main information, sometimes known as the "payload." The payload is compliant with an XML Schema.
SSH	Secure SHell is a protocol for secure remote login and other secure network services over an unsecure network. It provides for server authentication and data integrity with perfect port-forwarding secrecy.
SSG	Secure Services Gateway. The SSG is an Avaya server installed within a DMZ on the customer's network. It terminates the customer end of a secure link, such as VPN or frame relay, to Avaya remote servicing tools. In the inbound direction, the SSG provides secure remote access to multiple Avaya products on the customer's network, making detailed audit logs and full administrative control available to the customer. In the outbound direction, the SSG collect INADS SNMP alarms from multiple Avaya products and forwards them to alarm receivers on the Avaya network.
SSP	SIP Service Provider. A third-party provider of SIP-based VoIP services.
Standalone	A SIP solution that is not sharing a server with Communication Manager. See <SIP Enablement>.
Subscriber	A <SIP Enablement> subscriber (end user) is one of the following: an <SIP Enablement> R3.x host or other SIP <SIP Enablement>, a SIP user, or a communication manager server running <SIP Enablement>.
Switch	Any kind of telephone switching system. *See also* <SIP Enablement>.
SSH	Secure SHell is a protocol for secure remote login and other secure network services over an insecure network. It provides for server authentication, and data integrity with perfect port-forwarding secrecy.
SSL	Secure Socket Layer.
Subscriber	A subscriber is one of the following: a SIP Enablement Services host or other SIP <SIP Enablement>, a SIP user (per Contact), or a server (running <SIP Enablement> 2.0 or later).
Switch	Any kind of telephone switching system. *See also* <SIP Enablement>.

T

TAC	Trunk access code. A dial access code used to access a specific trunk.
TCP	Transmission Control Protocol. A connection-oriented transport-layer <SIP Enablement>, IETF STD 7. RFC 793, that governs the exchange of sequential data. Whereas the <SIP Enablement> deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data, and also guarantees that packets are delivered in the same order in which the packets are sent.

TCP/IP — *See* <SIP Enablement>. *See also* <SIP Enablement>.

Tme-Division Multiplex (TDM) bus — A <SIP Enablement> that is time-shared regularly by pre allocating short <SIP Enablement>s to each transmitter. In a <SIP Enablement>, all <SIP Enablement> <SIP Enablement>s are connected to the <SIP Enablement>, and any port can send a signal to any other port. *See also* <SIP Enablement>.

Time-division multiplexing (TDM) — A form of multiplexing that divides a transmission <SIP Enablement> into successive <SIP Enablement>s. *See also* <SIP Enablement>.

Time slot — In the <SIP Enablement>, a time slot refers to either a digital signal level-0 (DS0) on a T1 facility or an E1 facility, or a 64-kbps unit on the <SIP Enablement> or fiber connection between <SIP Enablement> networks (PNs) that is structured as 8 bits every 125 microseconds.

tie trunk — A telecommunications <SIP Enablement> that directly connects two private switching systems.

TLS — Transport Layer Security which is an IETF standard (RFC 2246) that supersedes Netscapes' Secure Socket Layer (SSL) and provides host-to-host data connections with encryption and certification at the transport layer.

TSP — Toshiba Business Phone 1020A.

trunk — A dedicated communications <SIP Enablement> between two <SIP Enablement>s or <SIP Enablement>s.

trunk group — Telecommunications <SIP Enablement>s that are assigned as a group for certain functions, and that can be used interchangeably between two <SIP Enablement>s or <SIP Enablement>s.

U

UDP — 1. User datagram protocol. A packet format that is included in the <SIP Enablement> suite of <SIP Enablement>s. UDP is used for the unacknowledged transmission of short user messages and control messages.

2. Uniform Dial Plan.

Unicode — UTF-8, shift JIS, or Asian character encoding for multibyte languages.

URI — Uniform resource identifiers. URIs (also called URLs) are short strings of characters that identify resources on the world-wide web. They make resources available under a variety of naming schemes and access methods such as HTTP, FTP, SIP, and Internet mail in the same way.

URL — Uniform Resource Location

USB — Universal serial bus. A high-speed serial interface used to add a printer, a modem, a keyboard, a mouse, or another peripheral device to a personal computer.

V

VDN — Vector directory numbers

VMM	VoIP Monitoring Manager. This application checks with the endpoint device, perhaps every 5 seconds or so, to check the quality of service on the device. VMM is administered on the <SIP Enablement> and other Host screens in SES.
VMON	VoIP Monitoring. See <SIP Enablement>.
VoIP	Voice over IP. A set of facilities that use the <SIP Enablement> to manage the delivery of voice information. In general, VoIP means to send voice information in digital form in discrete packets instead of in the traditional <SIP Enablement>-committed <SIP Enablement>s of the <SIP Enablement>. Users of VoIP and Internet telephony avoid the tolls that are charged for ordinary telephone service.

W

WebLM	Web-based License Management, a server application that manages various software licenses.
wideband	A <SIP Enablement>-switched call at a data rate that is greater than 64 kilobits per second. A circuit-switched call on a single T1 facility or a single E1 facility with a bandwidth that is between 128 kilobits per second and 1536 kilobits per second (T1) or 1984 kilobits per second (E1) in multiples of 64 kilobits per second. H0, H11, H12, and N x digital signal-level 0 (DS0) calls are wideband. Compare with <SIP Enablement>.
W call flow	See <SIP Enablement>.

Index of SNMP traps

F

H

I

L

M

N

P

R

S

V

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W