What's New in Avaya Aura™ Communication Manager, Avaya Servers and Media Gateways for Release 6.0

Release 6.0
03-601818
Issue 5.0
June 2010

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

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.

Preventing Toll Fraud

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

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya 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.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Downloading Documentation

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

Contents

Chapter 1: What's new in Communication Manager

This chapter presents an overview of the new features and enhancements for Avaya Aura® Communication Manager 6.0 running on Avaya S8xxx servers with associated Avaya media gateways.

Communication Manager templates overview

Communication Manager as a template is a virtualized version that runs on System Platform. The Communication Manager template image has all the features that Communication Manager supports whether the image is on a duplicated server or a branch server. The templates support Communication Manager duplication on S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. The templates support Communication Manager which configures as Main, Survivable Core Server, or Survivable Remote Server. In addition, with the templates you can use their network infrastructure without dedicated control networks.

Note:

The Communication Manager installation and administration Web pages refer to Survivable Core as Enterprise Survivable Server (ESS) and Survivable Remote as Local Survivable Processor (LSP), respectively.

The advantages of using a solution as a template on System Platform are as follows:

- Simplified and faster installation of the solution
- Efficient licensing of applications and solutions
- Avaya common look-and-feel Web Console (Web Graphical User Interface) for server, virtual machine, application, and overall solution management.
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel
- Coordinated backup and restore
- Coordinated software upgrades

The Communication Manager templates come in two categories: Avaya Aura® for Communication Manager Main/Survivable Core and Avaya Aura® for Communication Manager Survivable Remote. The templates in each category are as follows:

- Avaya Aura® for Communication Manager Main/Survivable Core template category contains the following templates:
  - Simplex CM Main/Survivable Core
  - Duplex CM Main/Survivable Core
  - Embedded CM Main
- Avaya Aura® for Communication Manager Survivable Remote template category contains the following templates:
  - Simplex Survivable Remote
  - Embedded Survivable Remote

Avaya Aura® for Communication Manager Main/Survivable Core

The Communication Manager Main/Survivable Core templates include the following applications:

- Communication Manager
- Communication Manager Messaging

  Note:

  You can gain access to Communication Manager Messaging only if you configure Communication Manager as the main server. You cannot gain access to Communication Manager Messaging and Utility Services on Duplex Main/Survivable Core.
- Utility Services

You can install Simplex Main/Survivable Core and Duplex Main/Survivable Core templates on an S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server.

Note:

The S8800 Server is no longer sold. You can only install the S8800 Server as an upgrade.

You can install the Simplex Main/Survivable Core template on an S8510 Server with a total 8-Gb memory as an upgrade only. You can install the Embedded Main template on an S8300D Server in a G250, G350, G430, G450, or G700 Branch Gateway.

Avaya Aura® for Communication Manager Survivable Remote

The Communication Manager Survivable Remote templates include the following applications:

- Communication Manager
- Branch Session Manager
- Utility Services

You can install the Simplex Survivable Remote on an S8800, HP ProLiant DL360 G7, or Dell™ PowerEdge™ R610 Server. You can install Simplex Survivable Remote on an S8510 Server with 8-Gb memory as an upgrade only. You can install Embedded Survivable Remote on S8300D Server in a G250, G350, G430, G450, or G700 Branch Gateway. You can use both templates in the following two scenarios:

- Communication Manager Evolution Server
- Communication Manager Feature Server

Note:

For information on template capacities, see the *Avaya Aura® Communication Manager System Capacities Table*.

Server roles

Feature server

Communication Manager configured as a feature server provides features to SIP endpoints. It only supports SIP endpoints that are registered to an Avaya Aura® Session Manager. Communication Manager configured as a feature server uses the IP Multimedia Subsystem (IMS) half-call model that allows full application sequencing. It is connected to Session Manager via an IMS-enabled SIP signaling group and an associated SIP trunk group.

The Communication Manager feature server has the following constraints:

- The dial plan for IMS users must route all PSTN calls back to Session Manager over the IMS trunk group. The dial plan does not support routing of such calls directly to ISDN trunks.
- Traditional phones, such as DCP, H.323, ISDN, and analog are not supported.
- G650 port networks are not supported.

G430 and G450 gateways provide connection preserving failover and failback to Survivable Core and Survivable Remote processors.

Half-call model

The half-call model separates the processing of a call request into two phases:

- Origination, where services are applied to the originator of the call.
- Termination, where services are applied to the call recipient.

The origination and termination phases of the call are separate operations and may be performed by different feature servers.

Application sequencing works only when all the servers in a sequence support the half-call model. The number of originating sequenced applications may be different from the number of terminating sequenced applications.

Evolution server

Communication Manager configured as an evolution server is equivalent to the traditional Communication Manager. Evolution server provides Communication Manager features to both SIP and non-SIP endpoints. Communication Manager uses the full-call model.

The connection from the evolution server to the Session Manager server is a non-IMS signaling group. Communication Manager is administered as an evolution server by disabling IMS on the signaling group to Session Manager. Session Manager handles call routing for SIP endpoints and allows the SIP endpoints to communicate with all other endpoints that are connected to the evolution server.

With Communication Manager configured as an evolution server:

- H.323, digital, and analog endpoints register with Communication Manager
- SIP endpoints register with Session Manager
- All endpoints receive service from Communication Manager

Branch gateways provide connection preserving failover and failback to Survivable Core and Survivable Remote processors. Communication Manager as an evolution server can support IP-connected port networks, but they are not connection preserving.

Full-call model

In the full call model, the processing of a call request is done in one step. The origination and termination parts of the call are processed without a break. Classic Communication Manager adheres to the full-call model.

Because application sequencing expects the applications to follow the half-call model and because Communication Manager administered as an evolution server supports full-call model, no other sequenced application should be provisioned along with evolution server.

For the full-call model, the **IMS-enabled?** field on the SIP Signaling Group screen must be set to **n** (disabled).

Survivable remote server

In a survivable remote environment, each IP endpoint and each H.248 Media Gateway is manually configured with a list of call controllers during initialization. If for any reason, the communication between an H.248 Media Gateway and its primary controller stops, the H.248 Media Gateways and the IP endpoints register with a call controller on its list. If the survivable remote server is in the list of call controllers, the H.248 Media Gateway and the IP endpoint registers with the survivable remote server. The H.248 Media Gateway registers with the survivable remote server, then the IP telephone registers with the survivable remote server.

The Processor Ethernet (PE) interface on a survivable remote server is used for:

- Connectivity to three adjuncts: Call Detail Recording (CDR), Application Enablement Services (AE Services), and Call Management System (CMS).
- H.323 and H.248 registration.

You can have both survivable core servers and survivable remote servers in a survivable core server configuration.

Survivable core server

In a survivable core server environment, the IPSI contains a priority list of survivable core servers. If for any reason, the communication between the IPSI and the main server is lost, the IPSI requests service from the highest ranking survivable core server on its list. The survivable core server accepts the request and assumes control of the port networks.

The survivable core server provides the same functionality and the same capacity as the main server. Through the IPSI circuit pack in the port network, the survivable core server can provide service to a H.248 Media Gateway. The survivable core server can also provide service to each media gateway through C-LAN connections in the port networks.

A single survivable core server can use the Processor Ethernet interface to connect to CDR, AESVCS, and CMS. Duplex servers can use the Processor Ethernet interface to connect to CDR and Avaya Aura® Messaging.

Communication Manager 6.0 has the following capabilities:

- Processor Ethernet is supported on simplex and duplex servers for the connection of H.323 devices, H.248 Media Gateways, SIP trunks, and most adjuncts.
- The capabilities of survivable core servers are enhanced to support connection of IP devices to the Processor Ethernet interface as well as to C-LAN interfaces located in the port networks.
- When Processor Ethernet is used on duplex servers, it must be assigned to an IP address and an active server IP address that is shared between the servers. This address is known as an IP-alias. The active server is the only server that responds on the IP-alias.

Table 1 provides information on template types that can be used as a Survivable remote or core server for Communication Manager.

Template type	S8300D	S8510	S8800
Duplex Survivable Core			Y

Template type	S8300D	S8510	S8800
Simplex Survivable Core		Y	Y
Simplex Survivable Remote		Y	Y
Embedded Survivable Remote	Y		
Embedded Main	Y		

Communication Manager license

Obtaining and installing the license file

Use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files for Communication Manager 6.0 and later Collaboration ServerSolution for Midsize Enterprise licensing. PLDS is an online, Web-based tool for managing license entitlements and electronic delivery of software and related license files.

Earlier versions of Communication Manager, except Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template, continue to use the Remote Feature Activation (RFA) online tool for license files. Communication Manager 5.2.1 that is part of Avaya Aura® Midsize Business Template uses PLDS to manage licenses. After you obtain the license file, use WebLM to install the license file. WebLM is a Web-based application for managing licenses and is installed as part of System Platform in the Console Domain.

The license file is an Extensible Markup Language (XML) file. The license file has the information regarding the product, major release, and license features and capacities.

For Communication Manager 6.0 and later, you must install license files on the Communication Manager main server and not on survivable servers. Survivable servers receive licensing information from the main server.

If you license a duplicated pair configuration, you must install the license file on both servers. The system does not synchronize the license file from active server to standby server.

A 30-day grace period applies to new installations or upgrades to Communication Manager 6.0Collaboration ServerSolution for Midsize Enterprise. You have 30 days from the day of installation to install a license file.

Customer Option features and the license file

Communication Manager has two categories of Customer Option features:

- Unlicensed Customer Option features that are available to all customers with the purchase of Communication Manager 6.0.
- Licensed Customer Option features that customers purchase and are controlled by the license file.

A specific feature in the Communication Manager license file may enable or map to multiple features on the Customer Options form. For example, ASAI Features (FEAT_CM_ASAI_PCKG) in the license file enables multiple ASAI-related features on the Customer Options form, including ASAI Link Core Capabilities and ASAI Link Plus Capabilities. Unlicensed features are available to all customers and are not included in the license file.

The Communication Manager System Management Interface (SMI) provides the ability to enable or disable individual Customer Option features that have an on or off (yes or no) setting. This capability is available only for the Customer Option features to which you are entitled. Features to which you are entitled include unlicensed features plus any licensed features that are entitled based on the license file. This capability does not apply to capacity features and other types of features that do not have an on or off setting.

How Communication Manager acquires licenses from WebLM

At startup, Communication Manager contacts WebLM and requests license release, features, and capacities. WebLM responds to Communication Manager, which then uses the acquired features and capacities to set license permissions in the Communication Manager software.

Communication Manager acquires all of the feature capacity from WebLM, regardless of actual usage. For example, if the Maximum Stations (VALUE_CM_STA) feature is set to 36,000 in the license file, Communication Manager acquires capacity for all 36,000 stations regardless of the number of stations currently configured. Actual license usage can be viewed on the Customer Options form in the System Administration Terminal (SAT) interface.

Every 9 minutes, Communication Manager sends a request to WebLM to renew its license information. Because of this time interval, you may have to wait up to 9 minutes for a newly installed license file to take effect on Communication Manager.

Communication Manager license features

A specific feature in the Communication Manager license file may enable or map to multiple features on the Customer Options form. For example, ASAI Features (FEAT_CM_ASAI_PCKG) in the license file enables multiple ASAI-related features on the Customer Options form, including ASAI Link Core Capabilities and ASAI Link Plus Capabilities. Unlicensed features are available to all customers and are not included in the license file.

The following table summarizes the mapping of features in the Communication Manager license file to Customer Option features.

License feature	Communication Manager Customer Option features
Edition (VALUE_CM_EDITION)	`Standard` enables all unlicensed Customer Option features. `Enterprise` maps to the Multinational Locations Customer Option feature. Also enables all unlicensed Customer Option features.
Maximum Stations (VALUE_CM_STA)	Maps to multiple Customer Option features, notably Maximum Stations.

License feature	Communication Manager Customer Option features
Maximum Analog Stations (VALUE_CM_ANALOG)	Specifies the number of analog stations to which the customer is entitled.
Maximum Survivable Processors (VALUE_CM_SP)	Maps directly to the Maximum Survivable Processors Customer Option feature.
Maximum ESS Stations (VALUE_CM_ESS_STA)	Specifies the number of Survivable Core station licenses to which the customer is entitled.
Maximum LSP Stations (VALUE_CM_LSP_STA)	Specifies the number of Survivable Remote station licenses to which the customer is entitled.
Maximum Mobility Enabled Stations (VALUE_CM_MOBILITY)	Maps to multiple Off-PBX Telephones Customer Option features.
Maximum Video Capable IP Softphones (VALUE_CM_VC_IPSP)	Maps to the Maximum Video Capable IP Softphones Customer Option feature.
ASAI Features (FEAT_CM_ASAI_PCKG)	Maps to ASAI-related Customer Option features including ASAI Link Core Capabilities and ASAI Link Plus Capabilities.
Maximum Expanded Meet-Me Conference Ports (VALUE_CM_EMMC_PORTS)	Maps to the Maximum Number of Expanded Meet-Me Conference Ports Customer Option feature.
Access Security Gateway (FEAT_CM_ASG)	Maps to the Access Security Gateway Customer Option feature.
IP Endpoint Registration Features (for example, IP_Soft)	Map directly to Customer Option features of the same name, for example, IP_Soft.
Support End Date (VALUE_CM_SED)	Specifies the Support End Date (SED) used for Avaya Service Pack and Dot Release Guardian. If the Support End Date feature is available in the Communication Manager license file, the value is in DD-Month-YYYY format (for example, 01 June 2012). If the Support End Date feature is not available in the license file, Communication Manager does not perform the Support End Date validations.

Secure Access Link

Avaya uses an architecture which significantly changes and improves the local and remote access methods used to support Communication Manager. Secure Access Link (SAL) uses IP connectivity for access and modems are no longer supported with Communication Manager 6.0. Customers have complete control of when and how Avaya, or any other service provider, can access customer equipment.

SAL is the exclusive remote support tool for Avaya Global Support Services. SAL must be registered, configured and made operational during installation in order to receive support from Avaya.

System Platform comes preinstalled with key SAL components necessary for remote customer support.

For more information, see https://support.avaya.com.

Access and administer Communication Manager

You can access and administer Communication Manager in the following ways:

- Starting a SAT session
- Accessing the System Management Interface
- Accessing the System Platform Web Console
- Logging on to the System Manager web interface

Starting a SAT session

Before you begin

- To use Telnet, enable the Telnet service for Communication Manager.
- To connect the portable computer directly to the services port, enable IP forwarding.

Procedure

1. Enter the IP address for Communication Manager, for example:
    - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in **Port** field.

- To use Telnet, enter `telnet 192.152.254.201 5023`.

2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.

Accessing the System Management Interface

About this task

You can gain access to System Management Interface (SMI) remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.
3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.

6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager System Management Interface.

Accessing the System Platform Web Console

Before you begin

If you want to gain access to the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access System Platform through the services port on page 20.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7, and Firefox 3.6 and later.

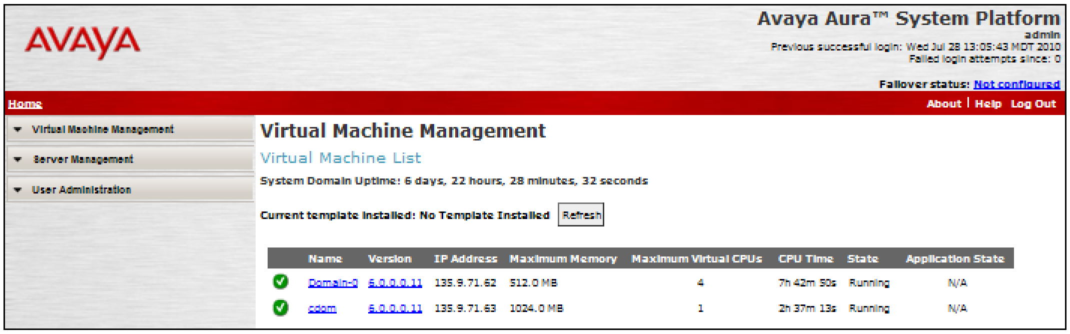
2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

> **Note:**
> This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.
7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.



admin
Previous successful login: Wed Jul 28 13:05:43 MDT 2010
Failed login attempts since: 0
Failover status: Not configured

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 6 days, 22 hours, 28 minutes, 32 seconds

Current template installed: No Template Installed

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	135.9.71.62	512.0 MB	4	7h 42m 50s	Running	N/A
✓	cdom	6.0.0.0.11	135.9.71.63	1024.0 MB	1	2h 37m 13s	Running	N/A

Related topics:

Enabling IP forwarding to access System Platform through the services port on page 20

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console. You can set the IP forwarding status as enabled or disabled during installation of System Platform. The system enables IP forwarding by default. If you disabled IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.

   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`service_port_access enable`** and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as admin.
   c. In the command line, type **`ip_forwarding disable`** and press **Enter**.

      An alternative to the above command is **`service_port_access disable`**.

Logging on to System Manager Web interface

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

Before you begin

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

Procedure

1. On the browser, open the System Manager URL (`https://<Fully Qualified Domain Name>/SMGR`).
2. In the **User ID** field, enter the user name.
3. In the **Password** field, enter the password.
4. Click **Log On**.

   If your user name and password:

   - Match an authorized System Manager user account, the System Manager home page appears with the System Manager *version_number*. The System Manager home page displays a navigation menu. This menu provides access to shared services with which you can perform various operations supported by System Manager. The tasks you can perform depends on your user role.
   - If you enter incorrect login credentials on the System Manager login page, System Manager displays an error message and prompts you to re-enter the user name and password so that you can log in again.

New features

This release of Communication Manager includes several new features, which are described in the following topics:

Administer location per station

Use the Administer location per station feature to:

- Allow IP telephones and softphones connected through a VPN to be associated with the branch that an employee is assigned to.
- Allow a VPN connected employee to have the same dialing experience as others in the office who are connected through a gateway.

The Administer location per station feature adds a **Location** field on the Station screen that overrides most of the location administration associated with the station. The **Location** field is added only for H.323 and SIP station types.

Note:

To use the Administer location per station feature with an H.323 softphone, administer the extension as an IP telephone type.

Alerting Tone for Outgoing Trunk Calls

Use the Alerting Tone for Outgoing Trunk Calls feature to apply an alerting tone to an outgoing trunk call after an administrable amount of time. The outgoing trunk alerting timer starts after the called party connects to the trunk. The outgoing trunk call is considered answered if:

- The network provides an answer supervision line signal.
- An ISDN CONNect message is received.
- The Answer Supervision Timeout timer expires.
- The call classifier classifies the call as answered.
- The Outgoing End of Dial Timer expires.

However, the timer does not apply to incoming trunk calls that connect to outgoing public network trunks, with the exception of remote access. The outgoing trunk alerting timer is cancelled if the outgoing trunk drops or is dropped before the timer expires.

The outgoing trunk alerting timer only affects outgoing public network trunks (CO, DIOD, FX, WATS, and ISDN public-network).

Delayed Caller ID Alerting for Name Display Update

Use this feature to administer the delayed caller ID information sent to the analog telephone.

For analog telephones, the caller ID information (caller's number and name) is sent to the telephone as a burst between the first and second rings. When a call is received over an ISDN trunk in North America, the caller information can be delivered either in the SETUP message or in a subsequent FACILITY message.

The display for IP and digital telephones can be updated with the caller information, based on the **US NI Delayed Calling Name Update** field on ISDN Trunk Group screen.

For analog caller ID telephones, the Delayed Caller ID Alerting for Name Display Update feature enables the following:

- Communication Manager waits for the FACILITY message before delivering an incoming call to the called user.
- Administer the time to wait for the FACILITY message which includes the caller information.

If no FACILITY message is received before the timer expires, the called analog telephone rings without displaying the caller ID information.

G.711 Music on hold

Communication Manager enables to use the clarity and sharpness of the G.711 codec while playing music on hold to internal or external callers. You can administer to use G.729 or other lower quality codecs for bandwidth resource conservation. When music is played for hold treatment, Communication Manager automatically redirects the media to use the clearer G.711 codec. When hold is released, Communication Manager automatically returns to the previously used lower quality codec.

IP DECT

Use the Digital Enhanced Cordless Telecommunications (IP DECT) feature to support an IP DECT system, an IP-based cordless telephony and messaging system for connection to private telephone exchanges.

The IP DECT system provides a complete integration of voice functions. Communication is done through IP trunks using the H.323/X-mobile interface. The IP DECT stations on Communication Manager side use the XMOBILE station type.

New licensing tool

Avaya has replaced its proprietary licensing system, (RFA), with a third-party solution called PLDS. Customers who do not want to perform their own license management operations in PLDS can opt for Avaya or the Partner perform those operations for them.

Note:

RFA must be used for generating license files for earlier releases of Communication Manager.

For more information, see *Getting Started with Avaya PLDS* and http://plds.avaya.com/.

PLDS

The Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

When you place an order for a PLDS-licensed software product such as Communication ManagerCollaboration ServerSolution for Midsize Enterprise, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. The WebLM host ID is the MAC address of the server and is obtained from the WebLM Web interface.

QSIG over SIP

Use the QSIG over SIP (Q-SIP) feature to enable calls between two Communication Manager systems interconnected by an IP network that uses SIP signaling with the full range of QSIG functionality.

The Q-SIP feature enables you to:

- Use SIP trunking as transport for private networking while maintaining all QSIG features.
- Migrate from QSIG transported over an ISDN private network to QSIG transported over a SIP network, one-communication system at a time.

SIP Direct Media

SIP Direct Media is supported by Communication Manager for Session Initiation Protocol (SIP) calls. SIP Direct Media signals the direct talk path between SIP endpoints before a call connects.

SIP Direct Media provides the following enhancements to SIP calls:

- Eliminates shuffling of SIP calls after call connects.
- Eliminates clipping on the talk path.
- Reduces the number of signaling messages for each SIP call.
- Reduces Communication Manager processing for each SIP call and increases the capacities of Communication Manager, Session Manager (SM), and SIP Busy Hour Call Completions (BHCC).
- Determines the media path early in the call flow and uses fewer media processor resources to configure the system.

Note:

When you originate a SIP call through Avaya Integral Enterprise Edition (formerly called Tenovis I55) and route the SIP call through Session Manager to Communication Manager, the system disables the SIP Direct Media feature. This results in a successful call.

Support for IPv6

Communication Manager supports IPv6, the new standard for specifying an IP address. By default, IPv6 is disabled.

The following components support IPv6 and IPv4 in a dual stack implementation:

- Communication Manager call server and Processor Ethernet

  including Avaya Site Administration
- System Platform
- 96xx series IP telephones

Enhanced features

This release of Communication Manager includes several enhanced features, which are described in the following topics.

Allow IGAR to use H.323 and SIP trunks

In general, IGAR is intended for configurations where the IP network is not reliable enough to carry bearer traffic. If you have more than one IP network available, use H.323 or SIP trunks for IGAR. To carry the bearer traffic through H.323 or SIP trunks, administer the following fields:

- Set the **IGAR Over IP Trunks** field on the Feature-Related System Parameters screen.
- If appropriate for your network, set the **Incoming Dialog Loopbacks** field on the SIP Signaling Group screen.

Communication Manager security, privacy and safety

Communication Manager provides security features for detecting probable breaches, taking measures to protect the system, notification and tracking activities. It also provides real-time media encryption for environments where enhanced voice privacy over a LAN/WAN is required.

Communication Manager supports:

- Industry Standard STRP (Secure Real Time Protocol) for authentication and media encryption,
- Real Time Media and Signaling Encryption
- Access Security Gateway
- Malicious Call Tracking
- Toll Fraud protection
- Emergency Calling Services (E911)

You can isolate Communication Manager telephony servers from the rest of the enterprise network to safeguard them from viruses, worms, Denial of Service (DoS), and other attacks. It uses the minimum number of services and access ports to reduce susceptibility to malicious attacks, and employs encryption between servers, gateways and endpoints to secure the voice stream and signaling channels.

See *Avaya Aura® Communication Manager Security Design* for further information.

Communication Manager SIP video infrastructure enhancements

SIP is a text-based protocol that is designed to set up, modify, and tear down communication sessions between users. Once sessions are established, the content of these sessions can be voice, video, instant messaging, or any other communications method.

SIP, an Internet-centric protocol that provides basic functionality beyond that of H.323, was originally designed to place the intelligence in the endpoints rather than within the network. It is practical to have some intelligence to be in the network. SIP architecture promises increased resiliency, scalability, and rapid application development.

Presently, Avaya Aura® Session Manager offers these advantages:

- Make and receive SIP telephone calls
- Many advanced features and services
- Secure Instant Messaging (IM)
- The ability to subscribe to and receive presence notifications

Enhanced coverage and ringback for logged off IP/PSA/TTI stations

In Communication Manager 6.0, the **Don’t Answer Criteria For Logged Off IP/PSA/TTI Stations** field is removed from the System Parameters Customer Options screen. If the **Don't Answer Criteria For Logged Off IP/PSA/TTI Stations** field is administered in Communication Manager 5.2.1 or earlier, after a Communication Manager upgrade the **Criteria for Logged Off/PSA/TTI stations** field will contain the same value.

To enable call coverage for logged off IP/PSA/TTI stations you must administer the **Criteria for Logged Off/PSA/TTI Stations** field on the System Parameters Call Coverage/Call Forwarding screen. The call then redirects to coverage after the number of rings exceed the number specified in the **Number of Rings** field for logged off IP/PSA/TTI coverage criteria.

For more information about the **Criteria For Logged Off IP/PSA/TTI Stations**, **Logged off/ PSA/TTI**, and **Number of Rings** fields, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

For information on call coverage, see *Avaya Aura® Feature Description and Implementation*, 555-245-205.

Multinational E.164 extension prefixes

Dial Plan is enhanced in Communication Manager 6.0 and later to introduce dial prefixes to be dialed before an extension. These dial prefixes are not part of the extension. This enhancement provides a way to avoid dial plan conflicts between long, unique extensions and short numbers used for dialing within a branch or a location. Using dial prefix, you can consolidate E.164 extensions in one digit block, which frees up other leading digits for short intra-branch dialing.

A sample scenario where the dial prefix enhancement is helpful:

- Single Communication Manager server with gateways in two or more countries.
- Extensions that match E.164 public numbers.

- Short dialing within locations and branches.
- Countries involved have long E.164 numbers.

Avaya recommends that you put extensions into a block of numbers with a single leading digit or group of digits. This keeps other leading digits available for short intra-branch dialing. In some branches, public E.164 numbers can be 13 digits long, which means there is no room for an extra leading digit. A dial prefix gives you a way to work around this limitation.

Native Support of Avaya 1408 and 1416 digital telephones

Native support of Avaya 1408 (1400 Mid) and 1416 (1400 High) digital telephones is available from Communication Manager 6.0 and later. Communication Manager supports call processing features for the Avaya 14xx digital telephones just like Avaya 24xx digital telephones, along with support for the following:

- Fixed feature buttons (Hold, Conference, Transfer, Message waiting lamp, Drop and Redial)
- Message button
- 40 Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality (including Group Listen)
- Eight call appearances or feature buttons

Note:

To allow firmware upgrades and to utilize the new capabilities of the sets, the phone type must be administered as either 1408 or 1416.

Native Support of Avaya 1408 digital telephone

Communication Manager provides native administration for the Avaya 1408 digital telephone. The Avaya 1408 digital telephone administration is similar to the Avaya 2410 digital telephone with the same fields and default values except for the following:

- Support for eight call appearances or feature buttons
- No **Customizable Labels** field
- No **Media Complex Ext** field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4

Native Support of Avaya 1416 digital telephone

Communication Manager provides native administration for the Avaya 1416 digital telephone. The Avaya 1416 digital telephone administration is similar to the Avaya 2420 digital telephone with the same fields and default values except for the following:

- Support for 16 call appearances or feature buttons
- No **Customizable Labels** field

- No **Data Option** field
- No **Media Complex Ext** field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4
- Support for **Button Modules** field rather than **Expansion Module** field

BM32 Button Support

The Avaya 1416 digital telephone uses the BM32 button expansion module. Communication Manager supports two BM32 buttons for the Avaya 1416 digital telephone.

PKI enhancement

Communication Manager allows replacing the default Communication Manager certificate with the customer's PKI certificates in addition to the use of existing certificates. Customers can now comply to their corporate security standards and separate their Web server from the call server.

Scalability

System capacities have been expanded for many products and features.

For the entire list of updated capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.

SIP feature expansion

Communication Manager adds the following new capabilities to SIP 96XX and one-X Communicator endpoints:

- Call Pickup Alerting: Adds visual alerting on the call pickup buttons for any incoming calls. This feature enables you to identify when to pick up a call.
- One-X Portal SIP Integration: You can use one-X Portal user interface with SIP Deskphones to allow thin client capabilities.
- One-X Mobile SIP Integration: You can use one-X Mobile client with SIP Deskphones with simultaneous ringing, seamless call transfer between devices, and robust mobility features.
- Internal Calling Party Number Block: Brings the name and number privacy features used for outside calls to internal calls for SIP stations.
- Call Park/Un-park Button: Simplifies the process of parking and un-parking calls to SIP stations.

- SIP stations in Hunt Groups: You can insert SIP stations in Hunt Groups that can either be a homogenous set of SIP stations, or a mixture of SIP and non-SIP stations.
- Third-party Message Waiting Indication (MWI): MWI provides a visual indication when a monitored third-party has pending voice mail. For example, to allow one or more people to monitor a shared voice mailbox.
- Transfer to Voicemail: SIP stations have soft key to transfer calls directly to the voicemail box of the owner of the line or to the bridged appearance where the call is received.

SIP SRTP enhancements

Use the Session Description Protocol (SDP) capability negotiation to support the Direct Media functionality and enhance the SIP Secure Real-Time Transport Protocol (SRTP) capability in Communication Manager .

Note:

SIP SRTP enhancements in Communication Manager supporting SDP capability negotiation cause some memory overhead on the system. However, the memory overhead is insignificant and does not involve any bandwidth overhead.

The SIP SRTP enhancements in Communication Manager do the following:

- Allow the SIP User Agent (UA) to provide both SRTP and non-SRTP capabilities in a single SDP.
- Support Direct Media functionality in Communication Manager by eliminating the requirement of NULL INVITE at the callee leg during the initial call setup.
- Simplify the SIP SRTP call flow.
- Enable SIP endpoints and Communication Manager to provide complete encryption capabilities to each other, increase the call shuffling capability of Communication Manager.

Hardware

Supported servers

Communication Manager 6.0, runs on only three servers: Avaya S8300D Server, Avaya S8510 Server, and the Avaya S8800 Server. These servers are the only ones that have the required memory and hard drives to run Communication Manager on System Platform. Only the Avaya

S8300D Server and Avaya S8800 Server are currently being sold. However, if you have an S8510, you may add the necessary memory and hardware to upgrade to Release 6.0.

New telephones and firmwares

This release of Communication Manager includes the following new telephones and firmwares:

- SIP firmware version 1.0 for the 1603SW-I IP Deskphone
- SIP firmware version 2.6 for the 9600 Series IP Deskphones
- 9600 Series IP Deskphones

  9608, 9611G, 9621G, and 9641G IP Deskphones
- 3720 and 3725 DECT Handsets
- 1408 and 1416 Digital Deskphones
- IP DECT Radio Base Station for 3720 and 3725 DECT Handsets
- Avaya one-X Attendant Console

For more information on the list of telephones, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Upgrades

This release of Communication Manager includes several upgrade procedures, which are described in the following topics:

Upgrade paths

The following table provides the supported upgrade paths from various releases of Communication Manager to Release 6.2. Notice that you cannot upgrade some servers to Release 4.0.5 or Release 5.2.1 directly. You must upgrade to Release 4.0.5 or Release 5.2.1 on a supported server, respectively, before you complete the upgrade to Release 6.2.

Release	Requirement
Release 1.x.x (DEFINITY R)	Restore translations to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 2.x (DEFINITY SI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.

Release	Requirement
Release 3.x.x (DEFINITY CSI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.
Release 1.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.
Release 1.x.x (S8700)	Upgrade to Release 4.0.5 before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610.
Release 2.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.
Release 2.x.x (S8500A, S8700, S8710 wDAL1)	Upgrade to Release 4.0.5 with memory upgrade before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610. For S8710, upgrade to Release 5.2.1 before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610, You do not require to upgrade the memory.
Release 2.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 3.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 3.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 4.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 4.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.0.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.1.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.2.1	Install a preupgrade service pack before you upgrade to Release 6.2.
Release 6.0.1	Upgrade software-only to Release 6.2.

Special circumstances

Consider the following special situations when upgrading Communication Manager to Release 6.x.

- If you have Communication Manager Messaging or Intuity Audix 770 enabled on the existing system, backup and restore that dataset separately on the upgraded system.
- If you have Communication Manager and SIP Enablement Services (SES) coresident on the S8300 Server, you cannot restore SES on the new server because Communication Manager Release 6.x does not support SES.
- If you have SES on the existing system and want to use the same SIP signaling group for Session Manager:
    - To edit the **Peer Server** field, set the **Peer Detection Enabled** field to `n`. By default, the system sets the **Peer Detection Enabled** field to `y` .
    - In the **Peer Server** field, enter `SM` or `Others`.
- If the existing system has SIP integrated Modular Messaging, the upgrade process automatically prefixes a + character to the phone number.

Important:

You must remove the + character manually from the phone number. For instructions, see *Messaging Application Server (MAS) Administration Guide*.

- If you use Unicode phone messages on the existing system, reinstall the Unicode phone messages file after the upgrade.

Preupgrade requirements

Make sure that you:

- Order all the hardware. The hardware must be available onsite.
- Download all the software and service packs
- Have the applications you need on the computer you will use to perform the upgrade.
- Identify a server with adequate disk space to store the datasets.
- Obtain the updated translations from the STS team. You require the updated translations for DEFINITY Server upgrades only.

Hardware requirements

- HP DL360 G7 or Dell R610 Server to replace an existing standalone server that you cannot upgrade to Release 6.x
- S8300D Server to replace an existing embedded server that you cannot upgrade to Release 6.x
- Release 6.0 Migration Kit for S8510 Server or S8800 Server to reuse the existing servers
- Required Ethernet CAT5 cables
- Five blank DVDs to burn the iso images on.

Software requirements

Download the following software from the appropriate Web site:

- System Platform from PLDS
- The Communication Manager templates from PLDS
- The license file from PLDS. You must have the MAC address from the System Platform Web Console Domain, as displayed on the Server Properties page of the WebLM server.
- The authentication or password file from the Authentication File System (AFS)
- Preupgrade and postupgrade service packs from the Avaya Support Web site at http://support.avaya.com.

Application requirements

Install the following applications on your computer:

- Internet Explorer 7.x or 8.x browser
- Firefox 2.x or 3.x browser. Only System Platform supports this browser.

  Release 6.2 supports Firefox 3.6 version and later.
- A Secure Shell application such as PuTTY.

Upgrade process

The following list provides the high-level upgrade sequence for upgrade paths that start with a server running Communication Manager Release 4.0.5 and Release 5.2.1.

1. Communication Manager on any survivable remote server (formerly local survivable processors)
2. Latest firmware on all Avaya H.248 Branch Gateway
3. Latest firmware on the media modules within the H.248 Branch Gateway
4. Communication Manager on any survivable core server (formerly enterprise survivable servers)
5. Latest firmware on all TN circuit packs (if using port networks)
6. Communication Manager on the main server
7. Latest firmware on all telephones

When you replace the server, verify the general tasks you complete on a simplex server from the following checklist:

Task	Notes	√
Make sure that the site has the server and other hardware.		

Task	Notes	√
Obtain the required software and pre- and post-upgrade service packs.		
Make sure you have the server and disk space available to back up the upgrade data set. You cannot use a flashcard to restore files to System Platform.		
Make sure you have the required documentation and release notes on hand.		
For DEFINITY Servers: • Save and freeze translations. • Send the translations to the STS team a few weeks before the upgrade and obtain the updated translations from STS.		
Record the IP addresses and other data on the existing server that you need to install System Platform and Communication Manager.	Use the worksheets provided in the appendices to make sure that you capture all the needed information.	
Convert private control networks to the corporate LAN.	Release 6.x does not support private networks (CNA and CNB). For instructions, see Converting private control networks to corporate LAN.	
Complete the routine preupgrade tasks on the existing server.		
Back up all the files on the existing server in case you need to roll back to the original release.		
Install the preupgrade service pack on the existing server.	**Important:** If for some reason you want to rollback the upgrade, you must deactivate the preupgrade patch.	
Back up the Communication Manager data set to be restored on the new server.		
Back up the Communication Manager Messaging data set that you will restore on the new server if messaging is enabled.		
For a standalone server, shut down the existing server and remove all power cords and cables. For an embedded server, remove all cables from the faceplate, shut down the existing		

Task	Notes	√
server, and remove it from the H.248 Branch Gateway.		
Install one of the following servers in the rack and connect the power cord and cables: • HP DL360 G7 Server • Dell R610 Server • S8300D Server. Install this embedded server in a branch gateway.	You can install the new server before completing the tasks on the existing server. From Release 6.0.1 onwards, Communication Manager supports upgrading to HP DL360 G7 Servers or Dell R610 Servers.	
Install System Platform on the server.	On the new server, you can do this before completing the tasks on the existing server.	
Get the license file from PLDS and install it on the WebLM server you access through the System Platform Web Console.	On the new server, you can do this before completing the tasks on the existing server.	
Get the authentication file from AFS and install the file through the System Platform Web Console.	On the new server, you can do this before completing the tasks on the existing server.	
Install the appropriate Communication Manager template through the System Platform Web Console.	On the new server, you can do this before completing the tasks on the existing server.	
Install postupgrade service pack, if required, through the System Platform Web Console.		
Restore the Communication Manager dataset through the System Platform Web Console.		
Configure Communication Manager through System Management Interface.	System Management Interface (SMI) was formerly known as Maintenance Web interface.	
Reboot the server through System Platform Web Console or System Management Interface. **Important:** Check the status of other devices and applications that depend on Communication Manager, such as Call Management System (CMS) and Call Center. After you complete the Communication Manager upgrade, reboot the applications if required.		

Task	Notes	√
Restore the Communication Manager Messaging data set through the System Management Interface.		
Configure Communication Manager Messaging.		
Complete the postupgrade administration.		
Back up all the files.		
Register the upgraded system.		

Special application activation process

Special applications, also known as green features, meet special requirements requested by one or more customer. Until now, Avaya has charged a fee to the customer to activate the special application. Communication Manager now offers many of these special applications to all customers at no additional cost and no change to the license. Customers may activate the special applications by themselves using their own super-user login. Although these special features are available to customers, they may have not gone through extensive testing. So customers must use at their own risk.

Some of the special features should not be set without the right configurations, and some features should not be set together at the same time. Otherwise, the feature may not operate as expected, the system performance could be affected or both. To avoid users from setting those features accidentally, Communication Manager has identified those features and marked them as restricted. For those restricted features, customers must contact Avaya's Custom Development team to activate.

For a list of these unrestricted special features and information about them, see *Avaya Aura® Communication Manager Special Application Features*, which is available on http://support.avaya.com.

Other changes

This release of Communication Manager includes several other changes, which are described in the following topics:

No support for CNA and CNB

Communication Manager no longer supports private control networks (Control Network A and Control Network B).

No support for fiber connectivity, CSS, and ATM

Communication Manager no longer supports any form of fiber connectivity, including direct, Center Stage Switch (CSS), and Asynchronous Transfer Mode (ATM). Communication Manager supports IP port connectivity (IP-PNC) only.

No support for SIP Enablement Services

Communication Manager no longer supports SIP Enablement Services (SES). SIP support is available through Avaya Aura® Session Manager.

Chapter 2: What's new in Communication Manager Messaging

This chapter presents an overview of the new features and enhancements for Avaya Aura® Communication Manager Messaging 6.0 running on Avaya S8xxx servers.

Communication Manager Messaging Embedded supports S8300D, S8510, and S8800 Servers. Communication Manager Messaging Federal supports only S8800 Server.

All the features listed in this section are applicable to Communication Manager Messaging and Communication Manager Messaging Federal.

Communication Manager Messaging templates overview

Communication Manager Messaging Embedded uses the Simplex Main/Survivable Core and Embedded Main templates and Federal uses the CMM Federal (stand-alone) template.

For more information on templates that run on System Platform, see Communication Manager templates overview.

For information on template capacities, see *Avaya Aura® Communication Manager System Capacities Table*, 03-300511.

Related topics:

Communication Manager templates overview on page 9

Communication Manager Messaging license features

The following table shows the mapping of features in the Communication Manager Messaging license file to features.

License feature	Communication Manager Messaging features
CM Messaging Offer (VALUE_CMM_OFFER)	EMBEDDED allows up to 6000 mailboxes. FEDERAL_MARKET allows up to 15,000 mailboxes.

License feature	Communication Manager Messaging features
Maximum CM Messaging Mailboxes (VALUE_CMM_MAILBOX)	Maps directly to the CM Messaging Mailboxes feature.

Access and administer Communication Manager Messaging

You can access and administer Communication Manager Messaging and Communication Manager Messaging Federal from the Web interface in the following ways:

- Accessing the System Management Interface
- Accessing the System Platform Web Console
- Logging on to the System Manager Web interface

For information on accessing and administering procedures, see Access and administer Communication Manager.

You can access and administer Communication Manager Messaging and Communication Manager Messaging Federal from the command line in the following ways:

- Using the SSH connection type
- Using DOM0 shell prompt

For information on accessing and administering command line procedures, see *Implementing Communication Manager Messaging Federal*, 18-603643.

Related topics:

Access and administer Communication Manager on page 17

SIP integration for Communication Manager Messaging

SIP integration support allows customers to standardize on SIP for their communications solution. SIP integration is through Session Manager to Communication Manager. H.323 integration with Communication Manager continues to be supported.

Note:

Communication Manager Messaging Federal does not support SIP integration.

Secure Access Link support for alarming and remote access

The SAL Gateway supports alarming for products that do not generate SNMP traps but can send log entries through syslog. SAL also provides remote support capabilities.

New and enhanced features

This release of Communication Manager Messaging includes several new and enhanced features, which are described in the following topics:

Login profiles for messaging

You can create a user-based profile and associate it to an existing Communication Manager profile or to a custom-created Communication Manager profile.

The Communication Manager Messaging application uses the user-based profiles created in Communication Manager. User-based profiles enable you to allow a user to access only a specific set of administration Web pages.

For example, you can create a login account and assign it the privileged administrator profile (sa). By default, it is associated to Communication Manager profile 18. This profile provides access equivalent to the customer super user login. The unprivileged administrator profile (vm) is associated to Communication Manager profile 19. This profile provides access equivalent to the customer non-super user login.

System Manager support for subscriber management

Communication Manager Messaging subscriber management can be done using Avaya Aura® System Manager.

SRTP encoding

Secure Real-Time Transport Protocol (SRTP) protocol seamlessly encrypts audio streams for calls over Communication Manager Messaging. It allows AES-128-CM encryption with 32 and 80-byte authentication.

Note:
TN2302 media processors do not support SRTP.

Support for IPv6

Communication Manager Messaging Federal supports IPv6, the new standard for specifying an IP address.

Hardware

Supported servers

Communication Manager Messaging Embedded 6.0, runs on three servers: Avaya S8300D Server, Avaya S8510 Server, and the Avaya S8800 Server. Communication Manager Messaging Federal 6.0, runs on only Avaya S8800 Server. Only the Avaya S8300D Server and Avaya S8800 Server are currently being sold. However, if you have an S8510, you must add the necessary memory and hardware to upgrade to Release 6.0.

Upgrades

Migration paths

The migration paths to Communication Manager Messaging Release 6.0 are:

- Intuity Audix 5.1 to CMM Federal 6.0
- Intuity Audix LX 1.1 to CMM Federal 6.0
- Intuity Audix LX 2..0 to CMM Federal 6.0
- Intuity Audix 4.4 to CMM Federal 6.0
- Intuity Audix 5.1 to CMM 6.0
- Intuity Audix LX 1.1 to CMM 6.0
- Intuity Audix LX 2..0 to CMM 6.0

- Intuity Audix 4.4 to CMM 6.0
- CMM 5.2.1 to CMM 6.0. For more information, see *Upgrading to Avaya Aura® Communication Manager Release 6.0*.

Chapter 3: What's new in System Platform

Release 6.2

Avaya Aura® System Platform 6.2 builds upon the previous release (6.0.*x*) and offers the following features:

- Customer provided hardware
- Enhanced High Availability
- SAL deployment on Services Virtual Machine
- SNMPv2 MIB support
- Kernel and RPM patching and rollback
- System Manager extension packs as plug-ins
- Patch and Dot licensing
- Automatic remote upgrades and updates (Remote API)

Release 6.0

Avaya Aura® System Platform 6.0 supports the following existing features:

- CentOS and Xen
- Template upgrade without touching unchanged virtual machines
- Multiple virtual disks per virtual machine
- IPv6
- Federal market-compliance and enhanced security
- S8300D server support
- Controlling front panel LEDs
- Bonded NIC support
- Performance monitoring tool

Index