



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring NACR CallNACK (an Avaya Agile Communication Environment™ Foundation Toolkit Client Application) with Avaya Aura® Session Manager and Avaya Aura® Communication Manager for Implicit Users - Issue 1.1

Abstract

These Application Notes describe the procedures for configuring NACR CallNACK (an Avaya Agile Communication Environment™ Foundation Toolkit client application) with Avaya Aura® Session Manager and Avaya Aura® Communication Manager for Implicit Users.

NACR CallNACK is configured as a Sequenced Application to be invoked during the originating sequence of a Implicit User. NACR CallNACK enables an administrator to set a policy for handling calls originated from various users. Based on the policy, which evaluates the called party address, outgoing calls may be allowed, blocked, or redirected to a predefined target. In the configuration tested, NACR CallNACK interoperates with Avaya Aura® Session Manager, Avaya Aura® Communication Manager via the Avaya Agile Communication Environment™ (ACE) Foundation Toolkit.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	3
1.1.	Foundation Toolkit.....	3
1.1.1.	Foundation Toolkit Runtime Services.....	4
1.1.2.	Foundation Toolkit SDK.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results.....	5
2.3.	Implicit User and Application Sequencing Considerations.....	5
2.4.	Support.....	5
3.	Reference Configuration.....	6
4.	Equipment and Software Validated.....	7
5.	Install and Configure Agile Communication Environment & Foundation Toolkit Runtime Services Server.....	8
5.1.	Linux Operating System Installation Notes.....	8
5.2.	Install Agile Communication Environment™.....	8
5.3.	Install Foundation Toolkit Runtime Services.....	8
5.4.	Configure ACE and Foundation Toolkit Runtime Services.....	10
6.	Configure Media Server.....	12
7.	WebSphere Configuration.....	19
8.	Configure Avaya Aura® Communication Manager Evolution Server.....	22
9.	Configure Avaya Aura® Session Manager.....	34
10.	Configure NACR CallNACK.....	53
11.	Verification Steps.....	55
12.	Conclusion.....	56
13.	Additional References.....	57

1. Introduction

These Application Notes describe the procedures for configuring NACR CallNACK (an Avaya Agile Communication Environment™ Foundation Toolkit client application) with Avaya Aura® Session Manager and Avaya Aura® Communication Manager for Implicit Users (i.e. users that do not register with Session Manager).

NACR CallNACK is configured as a Sequenced Application to be invoked during the originating sequence of an Implicit User. Sequenced Applications are invoked in a defined sequence by Session Manager during call setup (that is, during the processing of a SIP INVITE request).

NACR CallNACK enables an administrator to set a policy for handling calls originated from various users. Based on the policy, which evaluates the called party address, outgoing calls may be allowed, blocked, or redirected to a predefined target. In the configuration tested, NACR CallNACK interoperates with Avaya Aura® Session Manager, Avaya Aura® Communication Manager via the Avaya Agile Communication Environment™ (ACE) Foundation Toolkit.

Compliance testing focused on the ability of the NACR CallNACK application to properly block/allow calls from Implicit Users to the Public Switch Telephony Network (PSTN).

1.1. Foundation Toolkit

Foundation Toolkit has two components:

- Foundation Runtime Services (server)
- Foundation SDK (client)

The server and client-side library are connected by a persistent HTTP (Comet) connection. The server is deployed as part of the Avaya Agile Communication Environment™, and is linked into the Avaya Aura® network through Avaya Aura® Session Manager. The Avaya Aura® environment must include Avaya Aura® Session Manager and Avaya Aura® System Manager. The environment could also contain Avaya products such as Avaya Aura® Communication Manager and Avaya Media Server. Foundation Toolkit supports Communication Manager configured as a Feature Server and Communication Manager configured as an Evolution Server.

Session Manager is the core component within the Avaya Aura® Enterprise Edition solution, and is responsible for routing of all SIP traffic, including sequencing of applications. The applications sequenced by Session Manager are provided by other feature servers such as Foundation Toolkit or Communication Manager. For example, Session Manager may sequence a call barring application implemented as a Foundation Toolkit client application, such as NACR CallNACK.

1.1.1. Foundation Toolkit Runtime Services

The Foundation Runtime Services are the server-side part of the Foundation Toolkit.

The Foundation Runtime Services are installed by the Avaya Agile Communication Environment™ Installer and expose the functionality of Avaya Aura® as services to client applications, so client applications can make and receive calls, or manipulate call flows.

The Foundation Runtime Services, in combination with Avaya Aura® Session Manager, allow applications to:

- Initiate, reject and accept SIP call flows
- Inject media into a SIP call flow, for example:
 - Play messages, tones and music
 - Collect DTMF tones
 - Create two-party calls
 - Create multiparty conference calls
- Record parties in calls
- Route and proxy calls onward according to a user's configuration
- Apply call forwarding, call restrictions, call permissions and other enterprise rules and policies
- Route calls to personal assistant applications
- Route calls to voice mail

The Foundation Runtime Services are administered and monitored through the Agile Communication Environment™ Web-based graphical user interface.

1.1.2. Foundation Toolkit SDK

The Foundation SDK includes the Foundation Toolkit client-side libraries, which connect client applications to the server part of the Foundation Toolkit. The Foundation Toolkit client-side libraries expose the Foundation Toolkit API, which can be used to access the Foundation Toolkit services.

2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of NACR CallNACK with the Avaya SIP infrastructure (Avaya Agile Communication Environment™ Foundation Toolkit, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager). This section also covers the test results.

2.1. Interoperability Compliance Testing

The general test approach was to make calls from various Implicit Users to the PSTN and verify whether the calls were properly blocked or allowed. The following call flows were tested.

- Implicit User managed by the NACR CallNACK application dials a blocked PSTN number

- Implicit User managed by NACR CallNACK application dials an allowed PSTN number
- Implicit User not managed by NACR CallNACK application dials a blocked PSTN number
- Implicit User not managed by NACR CallNACK application dials allowed PSTN number

Only the first call flow of the four shown above should result in a blocked call. Blocked calls were redirected to an announcement on Communication Manager. Note, the configuration of announcements is outside the scope of these Application Notes and is therefore not described within this document.

2.2. Test Results

NACR CallNACK successfully passed compliance testing.

2.3. Implicit User and Application Sequencing Considerations

In a configuration where calls are routed from a SIP entity (e.g. Communication Manager) to Session Manager to invoke originating sequenced applications, and then the calls are then routed back to the same SIP entity, consider the following:

- Routing and call handling treatments must be in place to ensure a loop is not created between Session Manager and the SIP entity.
- The configuration should prevent users from bypassing the invocation of originating sequenced applications. For example, call restrictions should be provisioned to restrict users from placing calls that are not routed via Session Manager.
- The performance of systems within the configuration may be significantly impacted. For example, a call that would not normally involve Session Manager (e.g. a call from a non-SIP endpoint on a gateway to a local trunk on the gateway) will now require additional resources (trunks, call processing/memory, etc.) for the call to be routed to Session Manager to invoke sequenced applications.

Also note that originating sequenced applications are only applied only to the initial/first leg of a call from a user, and they are not applied after a call has been redirected.

2.4. Support

For technical support with the NACR CallNACK application, contact NACR at:

- Web: <http://www.nacr.com/>
- Phone: 888-321-NACR (6227)

3. Reference Configuration

Figure 1 illustrates the reference configuration used during compliance testing.

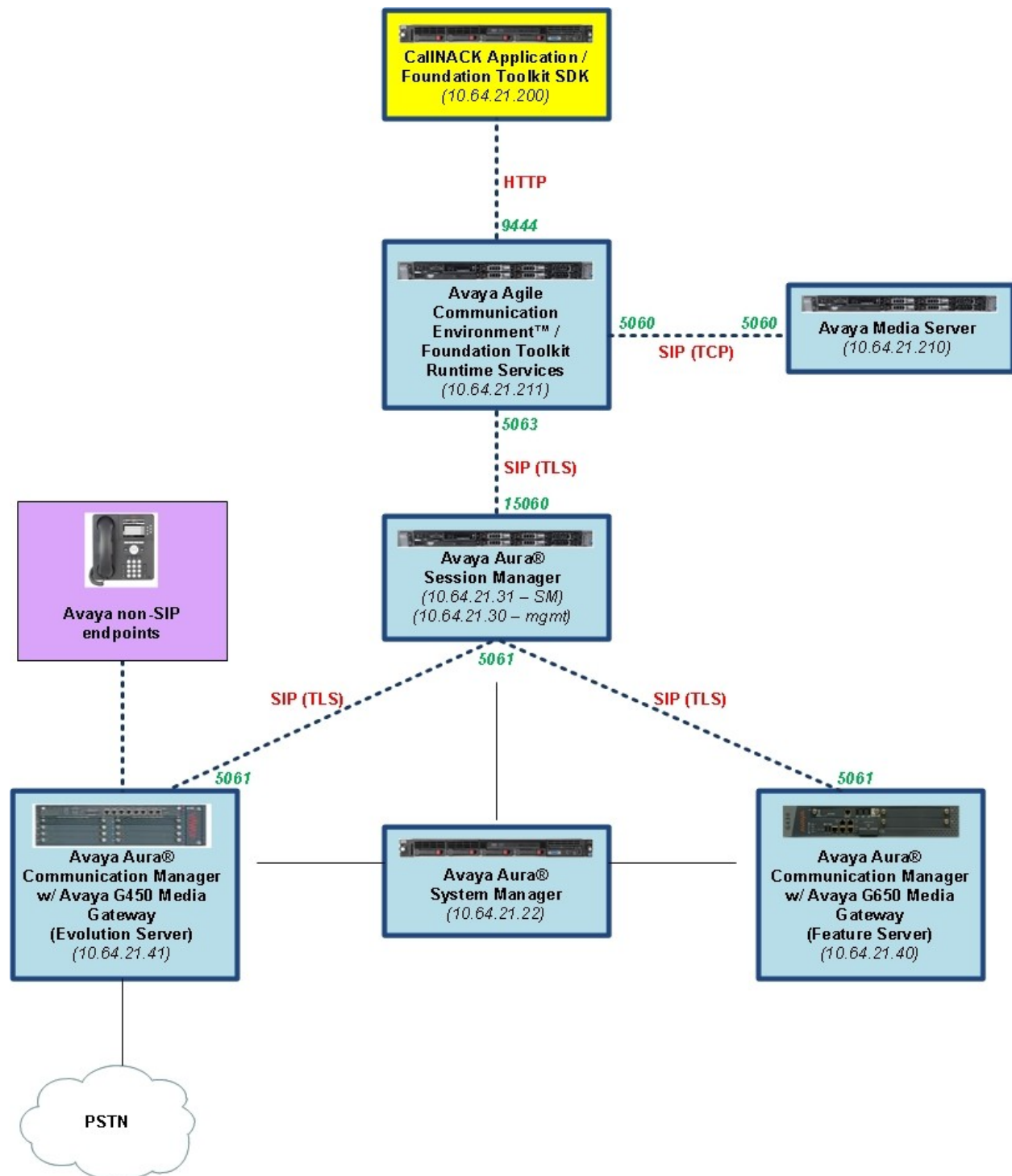


Figure 1: NACR CallNACK in an Avaya Environment

4. Equipment and Software Validated

The following equipment and software were used for the reference configuration:

Equipment	Software
HP ProLiant DL360 G7 Server	Avaya Agile Communication Environment 2.3.2 (w/ Foundation Toolkit Runtime Services)
HP ProLiant DL360 G7 Server	Avaya Media Server v.7.0.0.249
Avaya S8300D Server with a Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1, R016x.00.1.510.1, Patch 19009 (Avaya Aura® System Platform: 6.0.3.0.3)
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager: 6.1.0 (Build No. – 6.1.0.0.7345-6.1.5.106), Software Update Revision No : 6.1.6.1.1087 (Avaya Aura® System Platform: 6.0.3.0.3)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.1.2.0.612004
Application Server	NACR CallNACK version 1.1 Foundation Toolkit SDK (Sprint-5.3-Patch-1)
Avaya 9600 Series IP Deskphones (H.323	Release 3.1 Service Pack 2 (96x0) Release 6.0 Service Pack 4.1 (96x1G)

5. Install and Configure Agile Communication Environment & Foundation Toolkit Runtime Services Server

5.1. Linux Operating System Installation Notes

Avaya ACE and the Foundation Toolkit Runtime Services may be deployed on a server with either a Linux or Windows operating system. During compliance testing, a Linux based server was utilized. Refer to the *Avaya Agile Communication Environment™ Planning and Installation* documentation (**Section 13, Reference [1]**) for operating system installation details. The following Red Hat Enterprise Linux server OS release 5.4 for a 64-bit x86 architecture installation notes have been included here as an additional reference:

- During the Linux OS installation, when the “Package Group Selection” screen is displayed, check boxes for "Software Development" and "Web Server" and choose "Customize Now". Under "Development", select "Java Development".
- Security Enhanced Linux (SELinux) must be disabled.
- Disable the firewall. If a firewall is required, review the documentation (**Section 13, Reference [1]**) for additional instructions.

5.2. Install Agile Communication Environment™

Refer to the *Avaya Agile Communication Environment™ Planning and Installation* documentation (**Section 13, Reference [1]**) for ACE installation details. The following ACE installation notes have been included here as an additional reference:

- If the server used for the installation is not DNS resolvable, then it must be resolvable through the /etc/hosts file. Ensure that the host only resolves to one IP address and that the IP address is not 127.0.0.1. The hosts file must look similar to the following example.

```
Do not remove the following line, or various programs
that require network functionality will fail.
127.0.0.1 localhost.localdomain localhost
10.64.21.211 ace.avaya.com ace
```

During the ACE installation, the following parameters are required:

- **WebSphere primary administrative account password:** This is the password for the WebSphere admin user ID. This is the top level WebSphere user ID and has full privileges. Use this password to log in to the WebSphere administrative console.
Database password: The password for the database user ID root. This procedure sets the password.

5.3. Install Foundation Toolkit Runtime Services

The Foundation Toolkit installer installs the Foundation Toolkit Runtime Services on a platform hosting ACE. The Foundation Toolkit installer must be run after the ACE installer has successfully completed on a supported platform. Refer to the *Installing Avaya ACE Foundation Toolkit* documentation (**Section 13, Reference [2]**) for Foundation Toolkit Runtime Services

installation details. The following Foundation Toolkit Runtime Services installation notes have been included here as an additional reference:

During the Foundation Toolkit installation, the following parameters are required:

- **WebSphere primary administrative account password:** The administrative password for the WebSphere server hosting the Foundation Runtime Services.
- **Media Server SIP URI:** The SIP URI for the media server used by the Foundation Toolkit. For example:

<sip:msml@10.64.21.210:5060;transport=tcp>

If media services are not required by client applications, then **Media Server SIP URI** can be left blank. Note: The address part of the URI can use a host name or IP address.

- **Session Manager Address:** The address for the primary Session Manager for the ACE server. This is a fragment of a full SIP URI, excluding the part up to the @ delimiter. For example:

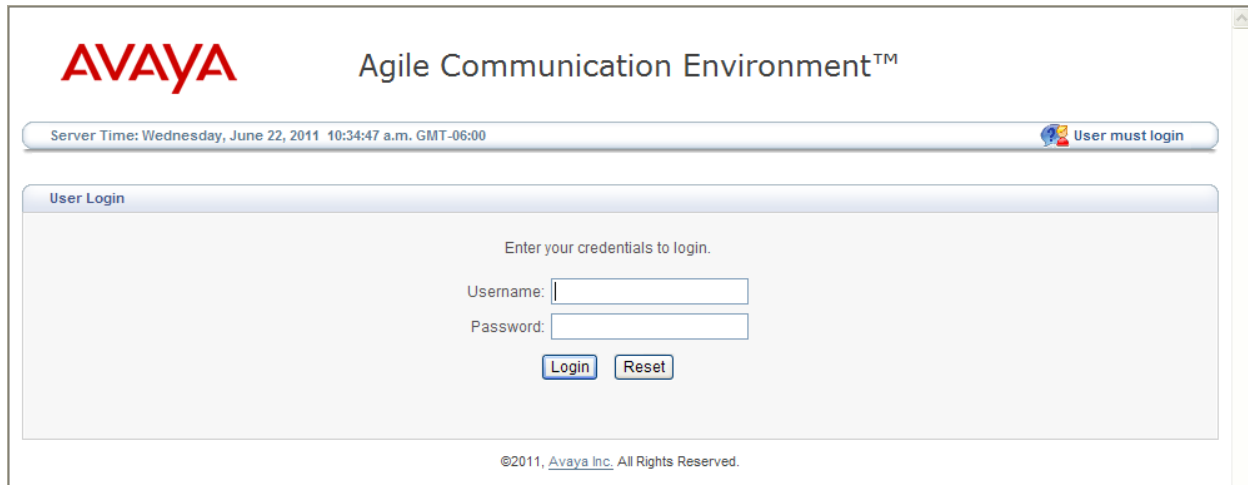
<sip:10.64.21.31:15060;transport=tls>

Note: The address string can use a host name or IP address. This should be the address of the Session Manager SIP Entity Interface.

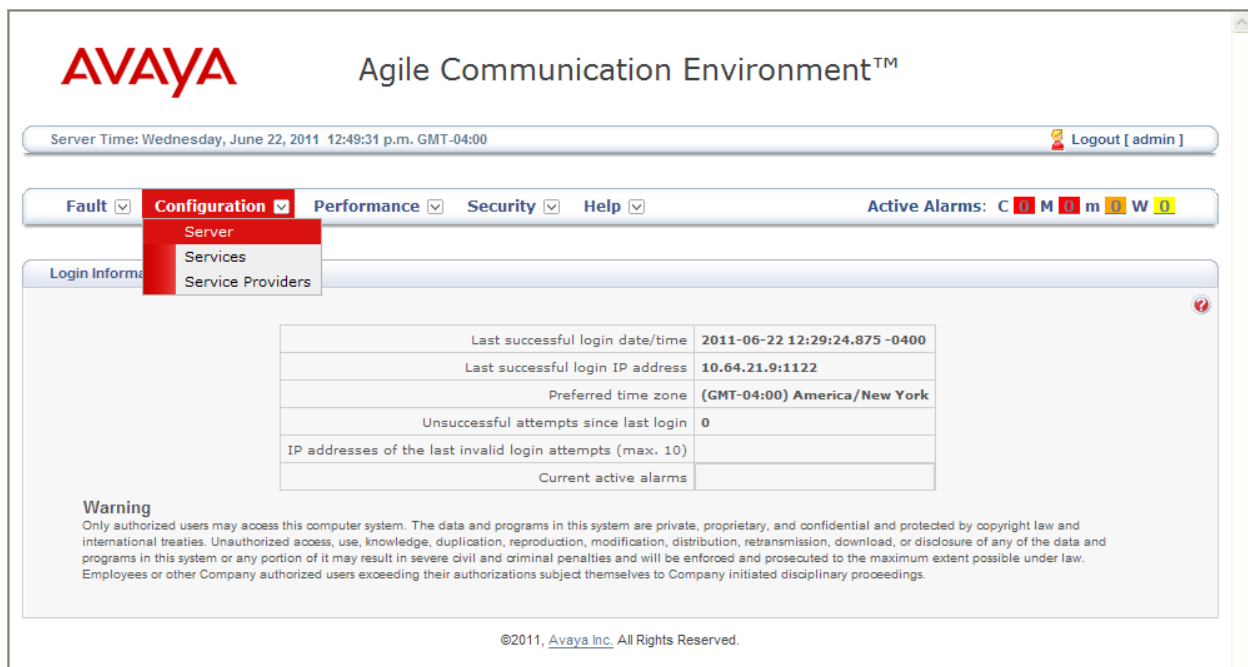
- **System Manager Hostname:** The host name or IP address of the server hosting System Manager.
- **System Manager Certificate Enrollment Password:** The trust management enrollment password set in System Manager.
- **Host name for SSL certificate:** The IP address or host name of the server hosting the ACE server. This host name is used by client applications to establish a secure connection.

5.4. Configure ACE and Foundation Toolkit Runtime Services

From a web browser, enter the following URL to access the ACE web interface: `https://<ip-address>/oamp/`, where `<ip-address>` is the IP address of the ACE server. The following User Login page is presented. Log in using the appropriate credentials.



The page following page is displayed. Navigate to **Configuration** → **Server**.



Last successful login date/time	2011-06-22 12:29:24.875 -0400
Last successful login IP address	10.64.21.9:1122
Preferred time zone	(GMT-04:00) America/New York
Unsuccessful attempts since last login	0
IP addresses of the last invalid login attempts (max. 10)	
Current active alarms	

Warning
Only authorized users may access this computer system. The data and programs in this system are private, proprietary, and confidential and protected by copyright law and international treaties. Unauthorized access, use, knowledge, duplication, reproduction, modification, distribution, retransmission, download, or disclosure of any of the data and programs in this system or any portion of it may result in severe civil and criminal penalties and will be enforced and prosecuted to the maximum extent possible under law. Employees or other Company authorized users exceeding their authorizations subject themselves to Company initiated disciplinary proceedings.

In the **ACE** navigation pane on the left, navigate to **ACE** → **<ip-address>** → **Services** → **Foundation Toolkit**. Verify the entries in the **Foundation Toolkit** pane on the right are correct. The **Media Server Address** and **Session Manager Address** fields are populated with value entered during installation of the Foundation Toolkit. The remaining fields are populated with default values.

The screenshot displays the Avaya Agile Communication Environment (ACE) web interface. At the top, the Avaya logo and "Agile Communication Environment™" are visible. Below this, a status bar shows the server time as "Wednesday, June 22, 2011 12:50:48 p.m. GMT-04:00" and a "Logout [admin]" link. A navigation bar contains tabs for "Fault", "Configuration", "Performance", "Security", and "Help", along with "Active Alarms: C 0 M 0 m 0 W 0".

The main content area is titled "Services" and features a left-hand navigation pane under the "ACE" section. The "Nodes" list includes "ACE", which is expanded to show "10.64.21.211". Under this node, the "Services" list includes "Audio Call (v3)", "Call Forwarding (v1)", "Call History (v1)", "Call Notification (v3.2)", "Call Notification (v3.8)", "Foundation Toolkit" (highlighted in red), "Location Supplier", "Presence (v3)", "Subscriber (v1.0)", "System Monitoring (v1)", "Terminal Location (v3)", "Third Party Call (v2)", "Third Party Call (v3)", "Turret (v1)", "User Profile (v1.5)", and "Providers".

The "Foundation Toolkit" configuration page is displayed on the right. It has two tabs: "Media Server" and "Performance Log". The "Media Server" tab is active, showing the following configuration fields:

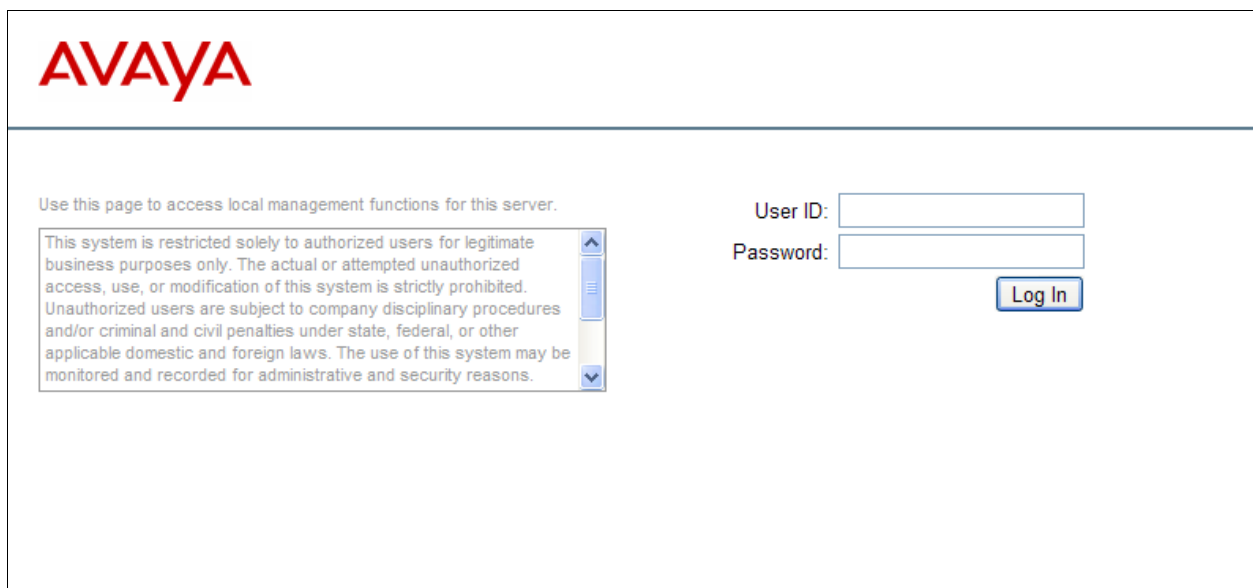
- Media Server Driver: JSR 309 driver for MAS
- Media Server Address: sip.msml@10.64.21.210:5060,lr
- Session Manager Address: sip:10.64.21.31:15060;transport=
- Proactive Monitoring Interval: 900
- Reactive Monitoring Interval: 10

At the bottom of the configuration fields are "Submit" and "Reset" buttons.

6. Configure Media Server

The Avaya Media Server must be installed when client applications make use of Foundation Toolkit media services (e.g. call recording, IVR, conferencing, etc.). During compliance testing, the CallNACK application redirected blocked calls to an announcement configured and stored on Communication Manager. However, even though the Media Server was not utilized by NACR CallNACK, configuration details are included here to demonstrate how the Media Server can be utilized play the announcement for blocked calls.

From a web browser, enter the following URL to access the Media Server web interface: `https:<ip-address>:8443/em/`, where `<ip-address>` is the IP address of the Media server. The following User Login page is presented. Log in using the appropriate credentials.



The image shows the Avaya Media Server User Login page. At the top left is the Avaya logo. Below it, a message states: "Use this page to access local management functions for this server." To the right of this message are two input fields: "User ID:" and "Password:". Below the "Password:" field is a "Log In" button. On the left side, there is a scrollable text box containing a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons."

The following page is displayed.

AVAYA

Avaya Media Server

[Help](#) | [Logout](#)

Managing: ams.avaya.com, 10.64.21.210
Home

System Status

Element Status

Cluster Status

Alarms

+ Logs

+ Monitoring

Applications

Operational State

Signaling Translations

Packaged Applications

Cluster Configuration

High Availability

Server Designation

Replication Settings

Load Balancing

Advanced Settings

System Configuration

Quick Setup

Server Profile

+ Network Settings

+ Signaling Protocols

+ Media Processing

+ Application Interpreters

+ Monitoring Settings

+ Session Detail Records

Logging Settings

+ Debug Tracing

Engineering Parameters

Field Promotion

Element Manager Settings

Licensing

General Settings

Monitoring

Server Status

Utilization Threshold

Advanced Settings

Tools

Software Inventory

+ Backup and Restore

Media Management

Session Detail Record Browser


Log Capture

Avaya Media Server

Welcome to the Element Manager for the following installed software packages:

Avaya Media Server - v.7.0.0.249

If you are a new user, or need assistance, please click [help](#)

 Please select a task from the left pane to get started.

Copyright 2010 Avaya Inc. All Rights Reserved

In the navigation pane on the left, navigate to **Licensing → General Settings**. Verify or apply your license. Note, the license key used during compliance testing has been grayed-out below.

AVAYA **Avaya Media Server** [Help](#) | [Logout](#)

Managing: ams.avaya.com, 10.64.21.210
[Home](#) » [Licensing](#) » General Settings

General Settings

Licensing: Nodal Licensing

Keys: [Grayed Out]

Changing this field will require the system to be restarted to take effect.

Save Cancel Restore Defaults

Copyright 2010 Avaya Inc. All Rights Reserved

In the navigation pane on the left, navigate to **System Configuration → Signaling Protocols → SIP → General Settings**.

- In the **Routing** area, clear **Enforce SIP Route Configuration**.
- In the **Access Control** area, clear **Trusted Node Access Only**.
- Click **Save**.

AVAYA Avaya Media Server Help | Logout

Managing: ams.avaya.com, 10.64.21.210
Home » System Configuration » Signaling Protocols » SIP » General Settings

General Settings

This task allows administrators to view and modify the SIP general settings.

[Transport Settings](#) | [Routing](#) | [Access Control](#) | [Session Audit](#) | [SIP Settings](#)

Transport Settings

- Enable SIP UDP Transport: ☒
- Enable SIP TCP Transport: ☒
- Enable SIP TLS Transport: ☒
- Enable SIP TLS Mutual Authentication: ☒
- Enforce SIP TLS in Secured Media Mode: ☒
- Always Approve SIP TLS Certificate: ☐

Routing

- Always use SIP default outbound proxy: ☒
- Enforce SIP Route Configuration: ☐**

Access Control

- Trusted Node Access Only: ☐**
- SIP Response Code When System/Application Locked: (400 - 699)

Save Cancel Restore Defaults

Copyright 2010 Avaya Inc. All Rights Reserved

In the navigation pane on the left, navigate to **System Configuration → Signaling Protocols → SIP → Domains and Accounts**. On the SIP Domains and Accounts page, add the domain names required for the network. During compliance testing, **avaya.com** was added.

The screenshot displays the Avaya Media Server web interface. The top header shows the Avaya logo, the title "Avaya Media Server", and links for "Help" and "Logout". Below the header, a management path is shown: "Managing: ams.avaya.com, 10.64.21.210" followed by a breadcrumb trail: "Home » System Configuration » Signaling Protocols » SIP » Domains and Accounts".

The left navigation pane is expanded to "System Configuration", which is further expanded to "Signaling Protocols", and finally to "SIP". Under the "SIP" section, "Domains and Accounts" is selected and highlighted.

The main content area is titled "SIP Domains and Accounts" and contains two sections: "Domains" and "Accounts".

Domains Section: This section has buttons for "Add...", "Edit...", and "Delete". Below these buttons is a table with a checkbox and a "Domain Name" column. The table contains three entries: "avaya.com", "eu.ubiquity.net", and "ubiquity.net".

Accounts Section: This section also has buttons for "Add...", "Edit...", and "Delete". Below these buttons is a table with checkboxes and columns for "Account Name", "Domain Name", and "Cluster Node". The table is currently empty.

At the bottom of the interface, a copyright notice reads: "Copyright 2010 Avaya Inc. All Rights Reserved".

To add a domain, click the **Add** button in the **Domains** section on the page above to get to the **Add SIP Domain** page shown below. Enter the domain in the **Name** field textbox and click **Save**.

AVAYA **Avaya Media Server** [Help](#) | [Logout](#)

Managing: ams.avaya.com, 10.64.21.210

[Home](#) » [System Configuration](#) » [Signaling Protocols](#) » [SIP](#) » [Domains and Accounts](#) » Add SIP Domain

Add SIP Domain

Name:

- System Status
 - Element Status
 - Cluster Status
 - Alarms
 - + Logs
 - + Monitoring
- Applications
 - Operational State
 - Signaling Translations
 - Packaged Applications
- Cluster Configuration
 - High Availability
 - Server Designation
 - Replication Settings
 - Load Balancing
 - Advanced Settings
- System Configuration
 - Quick Setup
 - Server Profile
 - + Network Settings
 - Signaling Protocols
 - SIP
 - General Settings
 - Domains and Accounts
 - Nodes and Routes
 - + MRCP
 - + Media Processing
 - + Application Interpreters
 - + Monitoring Settings
 - + Session Detail Records
 - Logging Settings
 - + Debug Tracing
 - Engineering Parameters
 - Field Promotion
 - Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Server Status
 - Utilization Threshold
 - Advanced Settings

Copyright 2010 Avaya Inc. All Rights Reserved

Copy media files to the Avaya Media Server:

- Connect to the Avaya Media Server host machine using SSH.
- Create a new directory named (for example) *Announcements/provisioned* at the location */opt/avaya/ma/MAS/platdata/filestorage/Announcements/provisioned*.

Copy the media files to the *provisioned* directory. For example, the media file *CallBlock.wav* to */opt/avaya/ma/MAS/platdata/filestorage/Announcements/provisioned*. The file can then be accessed client applications by using the path */Announcements/provisioned/CallBlock.wav*.

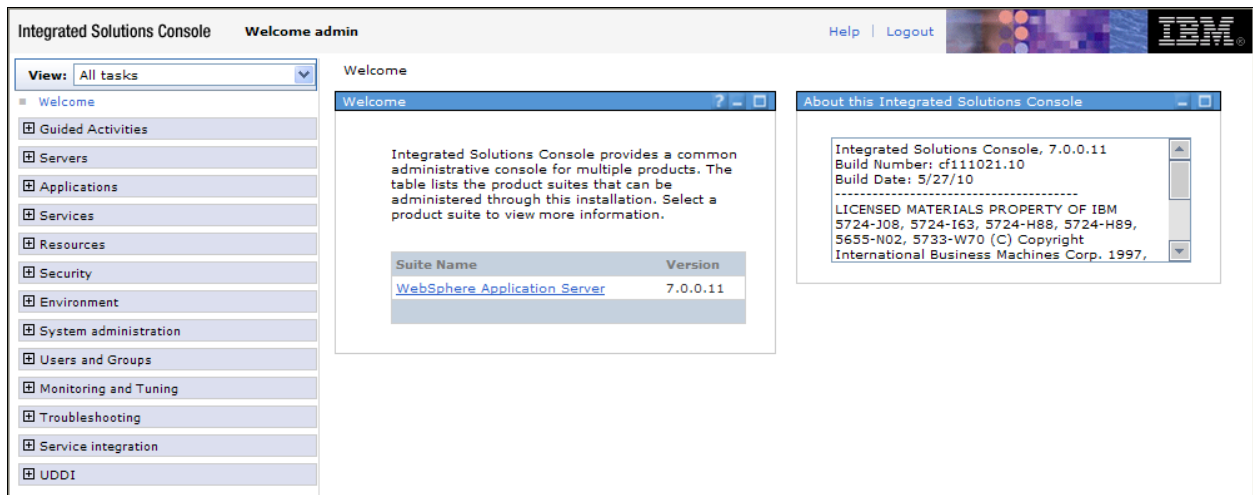
7. WebSphere Configuration

Log on to the WebSphere Integrated Solutions Console by navigating to the following URL in a web browser: <https://aceServer:9043/ibm/console/login.do?action=secure> where *aceServer* is the host name or IP address of the ACE server. The following User Login page is presented. Log in using the appropriate credentials.



The screenshot shows the 'Integrated Solutions Console' login page. It features a header with the IBM logo and a main area with the text 'Log in to the console.' Below this, there are input fields for 'User ID:' and 'Password:', followed by a 'Log in' button. The background of the page is a light gray with a faint globe graphic.

The following Welcome page is displayed.



The screenshot shows the 'Integrated Solutions Console' welcome page. The page has a header with 'Integrated Solutions Console' and 'Welcome admin', along with 'Help' and 'Logout' links. On the left, there is a navigation menu with a 'View: All tasks' dropdown and a list of categories: Welcome, Guided Activities, Servers, Applications, Services, Resources, Security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The main content area is titled 'Welcome' and contains a paragraph explaining the console's purpose. Below the paragraph is a table listing product suites. To the right of the main content, there is a box titled 'About this Integrated Solutions Console' containing version and build information.

Suite Name	Version
WebSphere Application Server	7.0.0.11

About this Integrated Solutions Console

Integrated Solutions Console, 7.0.0.11
Build Number: cf111021.10
Build Date: 5/27/10

LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88, 5724-H89,
5655-N02, 5733-W70 (C) Copyright
International Business Machines Corp. 1997,

In the navigation pane on the left, navigate to **Servers → Server Types → WebSphere application servers**. Verify that the **Status** of the Foundation Toolkit application server (**AAFT**) and the Avaya ACE application server (**server1**) has a solid green arrow (which indicates the application server is running).

Integrated Solutions Console Welcome admin Help | Logout IBM

Cell=Cell01, Profile=Dmgr01 Close page

Application servers

Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.

Preferences

New Delete Templates... Start Stop Restart ImmediateStop Terminate

Select	Name	Node	Host Name	Version	Cluster Name	Status
<input type="checkbox"/>	AAFT	Node01	ace.avaya.com	ND 7.0.0.11 CEA FEP 1.0.0.5		→
<input type="checkbox"/>	server1	Node01	ace.avaya.com	ND 7.0.0.11 CEA FEP 1.0.0.5		→

Total 2

HTTP access was enabled during compliance testing (which is the default setting). To disable HTTP access, follow the this procedure (not shown)

- Click the **AAFT** application server.
- On the next page, navigate to **Web Container Settings → Web container transport chains**.
- Click **HttpQueueInboundDefault**.
- Click to clear the **Enabled** check box. HTTP access by client applications to the Foundation Runtime Services will then be disabled. Client applications would only be able to connect using HTTPS.

In the navigation pane on the left, navigate to **Application → Application Types → WebSphere enterprise applications**. Verify a green arrow (which indicates “Started”) is shown as the **Application Status** for each enterprise application.

The screenshot displays the Integrated Solutions Console interface. The left navigation pane is expanded to show the path: **Applications** > **Application Types** > **WebSphere enterprise applications**. The main content area is titled **Enterprise Applications** and includes a toolbar with buttons for **Start**, **Stop**, **Install**, **Uninstall**, **Update**, **Rollout Update**, **Remove File**, **Export**, **Export DDL**, and **Export File**. Below the toolbar is a table with the following data:

Select	Name	Application Status
<input type="checkbox"/>	AppCore	➔
<input type="checkbox"/>	Omnius	➔
<input type="checkbox"/>	PersonalAssistant	➔

The status column shows a green arrow (➔) for each application, indicating they are started. The total count at the bottom is **Total 3**.

8. Configure Avaya Aura® Communication Manager Evolution Server

This section describes the Communication Manager Evolution Server configuration shown in **Figure 1**. Similar configuration steps are required (but are not shown) to set up a trunk from the Communication Manager Feature Server to Session Manager.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

Step	Description
1.	<p>License</p> <p>Use the display system-parameters customer-options command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to Page 2, and verify that there is sufficient remaining capacity for SIP trunks by comparing the Maximum Administered SIP Trunks field value with the corresponding value in the USED column.</p> <p>The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.</p> <pre> display system-parameters customer-options Page 2 of 11 OPTIONAL FEATURES IP PORT CAPACITIES USED Maximum Administered H.323 Trunks: 12000 32 Maximum Concurrently Registered IP Stations: 18000 15 Maximum Administered Remote Office Trunks: 12000 0 Maximum Concurrently Registered Remote Office Stations: 18000 0 Maximum Concurrently Registered IP eCons: 414 0 Max Concur Registered Unauthenticated H.323 Stations: 100 0 Maximum Video Capable Stations: 18000 0 Maximum Video Capable IP Softphones: 18000 1 Maximum Administered SIP Trunks: 24000 170 Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0 Maximum Number of DS1 Boards with Echo Cancellation: 522 0 Maximum TN2501 VAL Boards: 128 0 Maximum Media Gateway VAL Sources: 250 1 Maximum TN2602 Boards with 80 VoIP Channels: 128 0 Maximum TN2602 Boards with 320 VoIP Channels: 128 0 Maximum Number of Expanded Meet-me Conference Ports: 300 0 (NOTE: You must logoff & login to effect the permission changes.) </pre>

Step	Description
2.	<p>IP network region</p> <p>Use the display ip-network-region command to view the network region settings. The values shown below are the values used during compliance testing.</p> <ul style="list-style-type: none"> ▪ Authoritative Domain: <i>avaya.com</i> This field was configured to match the domain name configured on Session Manager (see Section 9, Step 2). The domain will appear in the “From” header of SIP messages originating from this IP region. ▪ Name: Any descriptive name may be used (if desired). ▪ Intra-region IP-IP Direct Audio: <i>no</i> Inter-region IP-IP Direct Audio: <i>no</i> By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Direct IP-IP Audio Connections must be disabled for signaling groups using Foundation Toolkit services. Shuffling can be further restricted at the trunk level on the Signaling Group form. ▪ Codec Set: <i>1</i> The codec set contains the list of codecs available for calls within this IP network region. <pre> Display ip-network-region 1 IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: MEDIA PARAMETERS Codec Set: 1 UDP Port Min: 2048 UDP Port Max: 3329 Intra-region IP-IP Direct Audio: no Inter-region IP-IP Direct Audio: no IP Audio Hairpinning? n DIFFSERV/TOS PARAMETERS Call Control PHB Value: 46 Audio PHB Value: 46 Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 RSVP Enabled? n </pre>

Step	Description
3.	<p>Codecs</p> <p>IP codec set 1 was used during compliance testing. Multiple codecs can be listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing.</p> <pre> display ip-codec-set 1 Page 1 of 2 IP Codec Set Codec Set: 1 Audio Silence Frames Packet Codec Suppression Per Pkt Size (ms) 1: G.711MU n 2 20 2: </pre>

Step	Description																										
4.	<p>Node Names</p> <p>Use the change node-names ip command to create a node name for the IP address of Session Manager. Enter a descriptive name in the Name column and the IP address assigned to Session Manager in the IP address column.</p>																										
	<div><div>change node-names ip</div><div><table><tr><th colspan="2">IP NODE NAMES</th></tr><tr><th>Name</th><th>IP Address</th></tr><tr><td>AES_21_46</td><td>10.64.21.46</td></tr><tr><td>CM_20_40</td><td>10.64.20.40</td></tr><tr><td>CM_22_12_CLAN1A</td><td>10.64.22.16</td></tr><tr><td>CM_22_12_CLAN2A</td><td>10.64.22.19</td></tr><tr><td>IPO_21_64</td><td>10.64.21.64</td></tr><tr><td>SM_20_31</td><td>10.64.20.31</td></tr><tr><td>SM_21_31</td><td>10.64.21.31</td></tr><tr><td>default</td><td>0.0.0.0</td></tr><tr><td>msgserver</td><td>10.64.21.41</td></tr><tr><td>procr</td><td>10.64.21.41</td></tr><tr><td>procr6</td><td>::</td></tr></table></div><div>Page 1 of 2</div></div>	IP NODE NAMES		Name	IP Address	AES_21_46	10.64.21.46	CM_20_40	10.64.20.40	CM_22_12_CLAN1A	10.64.22.16	CM_22_12_CLAN2A	10.64.22.19	IPO_21_64	10.64.21.64	SM_20_31	10.64.20.31	SM_21_31	10.64.21.31	default	0.0.0.0	msgserver	10.64.21.41	procr	10.64.21.41	procr6	::
IP NODE NAMES																											
Name	IP Address																										
AES_21_46	10.64.21.46																										
CM_20_40	10.64.20.40																										
CM_22_12_CLAN1A	10.64.22.16																										
CM_22_12_CLAN2A	10.64.22.19																										
IPO_21_64	10.64.21.64																										
SM_20_31	10.64.20.31																										
SM_21_31	10.64.21.31																										
default	0.0.0.0																										
msgserver	10.64.21.41																										
procr	10.64.21.41																										
procr6	::																										

Step	Description
5.	<p>Signaling Group Signaling group 1 was used for the signaling group associated with the SIP trunk group between Communication Manager and Session Manager. Signaling group 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Group Type: <i>sip</i> ▪ IMS Enabled?: <i>n</i> This field is set to <i>y</i> for a Communication Manager configured as a Feature Server. When configuring Communication Manager as an Evolution Server, set this field to <i>n</i>. ▪ Transport Method: <i>tls</i> ▪ Peer Detection Enabled?: <i>y</i> ▪ Peer Server: <i>SM</i> This field will automatically be populated when the Peer Detection Enabled? field is set to <i>y</i>. ▪ Near-end Node Name: <i>procr</i> This node name maps to the IP address of the Avaya S8300D Server. Node names are defined using the change node-names ip command. ▪ Near-end Listen Port: <i>5061</i> The listening port for Communication Manager. ▪ Far-end Node Name: <i>SM_21_31</i> This node name maps to the IP address of Session Manager. ▪ Far-end Listen Port: <i>5061</i> The listening port for Session Manager. ▪ Far-end Network Region: <i>1</i> This defines the IP network region which contains Session Manager. ▪ Far-end Domain: <i>avaya.com</i> This domain is sent in the “To” header of SIP messages of calls using this signaling group. ▪ Direct IP-IP Audio Connections: <i>n</i> Direct IP-IP Audio Connections must be disabled for signaling groups using Foundation Toolkit services. <pre> display signaling-group 1 SIGNALING GROUP Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tls Q-SIP? n SIP Enabled LSP? n IP Video? y Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM Near-end Node Name: procr Near-end Listen Port: 5061 Far-end Node Name: SM_21_31 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Domain: avaya.com Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload RFC 3389 Comfort Noise? n Session Establishment Timer(min): 3 Direct IP-IP Audio Connections? n IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6 </pre>

Step	Description
6.	<p>Trunk Group</p> <p>Trunk group 1 was used for the SIP trunk group between Communication Manager and Session Manager. Trunk group 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Group Type: <i>sip</i> This field sets the type of the trunk group. ▪ Group Name: Any descriptive name may be used (if desired). ▪ COR: <i>1</i> During compliance testing, trunk group 2 (not shown) was also assigned a COR value of 1, and it was used to access the PSTN. The stations used by Implicit Users were assigned a COR value of 2. COR 2 was configured with the Restricted Call List feature enabled, and the <i>change toll</i> command was used to restrict dialed strings that would be directly to trunk group 2 (and not pass through Session Manager). Thus, calls from the Implicit User stations directly to the PSTN via trunk group 2 were blocked by the station's COR and Restricted Call list. Calls to the PSTN via Session Manager were either blocked or allowed by the NACR CallNACK application. If the call was allowed, Session Manager routed the call back to Communication Manager over a trunk group with a COR value of <i>1</i> which did not have any call restrictions. ▪ TAC: <i>101</i> Enter an valid value consistent with the Communication Manager dial plan. ▪ Service Type: <i>tie</i> Set to tie. ▪ Member Assignment Method: <i>auto</i> Set to Auto. ▪ Signaling Group: <i>1</i> This field is set to the signaling group shown in the previous step. ▪ Number of Members: <i>50</i> This field represents the number of trunk group members in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk. <pre> display trunk-group 1 Page 1 of 21 TRUNK GROUP Group Number: 1 Group Type: sip CDR Reports: y Group Name: to SM_21_31 COR: 1 TN: 1 TAC: 101 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Member Assignment Method: auto Signaling Group: 1 Number of Members: 50 </pre>

Step	Description
	<p>Trunk Group – continued</p> <p>On Page 3:</p> <ul style="list-style-type: none"> The Numbering Format field was set to <i>unk-pvt</i>. This field specifies the format of the calling party number sent to the far-end. The default values may be retained for the other fields.
	<pre> display trunk-group 1 TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y Numbering Format: unk-pvt UUI Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Modify Tandem Calling Number: no Show ANSWERED BY on Display? y </pre> <p style="text-align: right;">Page 3 of 21</p>
7.	<p>Private Numbering</p> <p>Private Numbering defines the calling party number to be sent to the far-end. In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed across any trunk group will be sent as a 5 digit calling number. The calling party number is sent to the far-end in the SIP “From” header.</p>
	<pre> display private-numbering 0 NUMBERING - PRIVATE FORMAT Ext Len Ext Code Trk Private Total Grp(s) Prefix Len 5 5 Total Administered: 1 Maximum Entries: 540 </pre> <p style="text-align: right;">Page 1 of 2</p>

Step	Description																																																												
8.	<p>Automatic Route Selection</p> <p>Automatic Route Selection (ARS) was used to route PSTN calls to either the PSTN (i.e trunk group 2) or to Session Manager (i.e trunk group 1). Dialed strings beginning with 8130 were routed to the local PSTN trunk. Dialed strings beginning with 130 were routed to Session Manager. If a PSTN call routed to Session Manager was not blocked by the NACR CALLNACK application, Session Manager would then route the call back to the Communication Manager (where an “8” was added to the dialed string to route the call out the PSTN trunk).</p> <p>Use the change ars analysis command to create an entry in the ARS Digit Analysis Table. The example below shows dialed strings that begin with 8130 and are 12 digits long use route pattern 20 (which routes calls directly to the PSTN via trunk group 2).</p> <div><pre>change ars analysis 8130</pre><table><tr><th colspan="7">ARS DIGIT ANALYSIS TABLE</th><th>Page 1 of 2</th></tr><tr><th colspan="7">Location: all</th><th>Percent Full: 1</th></tr><tr><th>Dialed String</th><th>Total Min</th><th>Total Max</th><th>Route Pattern</th><th>Call Type</th><th>Node Num</th><th>ANI Req'd</th></tr><tr><td>8130</td><td>12</td><td>12</td><td>20</td><td>hnpa</td><td></td><td>n</td></tr></table></div> <p>The example below shows dialed strings that begin with 130 and are 11 digits long use route pattern 1 (which routes calls to Session Manager).</p> <div><pre>change ars analysis 130</pre><table><tr><th colspan="7">ARS DIGIT ANALYSIS TABLE</th><th>Page 1 of 2</th></tr><tr><th colspan="7">Location: all</th><th>Percent Full: 1</th></tr><tr><th>Dialed String</th><th>Total Min</th><th>Total Max</th><th>Route Pattern</th><th>Call Type</th><th>Node Num</th><th>ANI Req'd</th></tr><tr><td>130</td><td>11</td><td>11</td><td>1</td><td>hnpa</td><td></td><td>n</td></tr></table></div>	ARS DIGIT ANALYSIS TABLE							Page 1 of 2	Location: all							Percent Full: 1	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	8130	12	12	20	hnpa		n	ARS DIGIT ANALYSIS TABLE							Page 1 of 2	Location: all							Percent Full: 1	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	130	11	11	1	hnpa		n
ARS DIGIT ANALYSIS TABLE							Page 1 of 2																																																						
Location: all							Percent Full: 1																																																						
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd																																																							
8130	12	12	20	hnpa		n																																																							
ARS DIGIT ANALYSIS TABLE							Page 1 of 2																																																						
Location: all							Percent Full: 1																																																						
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd																																																							
130	11	11	1	hnpa		n																																																							

Step	Description
9.	<div><div>Route Pattern</div><div>Route pattern 20 was used to route calls to the PSTN via trunk group 2. Route pattern 20 was configured using the parameters highlighted below.</div><div><div><div>▪</div><div>Pattern Name:</div><div>Any descriptive name.</div></div><div><div>▪</div><div>Grp No: 2</div><div>This field is set to the PSTN trunk group number.</div></div><div><div>▪</div><div>FRL: 0</div><div>This field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive.</div></div><div><div>▪</div><div>No. Del Dgts: 1</div><div>This field was used to deleted the leading “8” prior to be routed out the PSTN trunk.</div></div></div></div>
<div><div>Change route-pattern 20</div><div>Page1 of 3</div><div><div><div><div>Pattern Number: 20</div><div>Pattern Name: PSTN</div></div><div><div>SCCAN? n</div><div>Secure SIP? n</div></div></div><div><div><div><div>Grp</div><div>FRL</div><div>NPA</div><div>Pfx</div><div>Hop</div><div>Toll</div><div>No.</div><div>Inserted</div></div><div><div>DCS/</div><div>IXC</div></div></div><div><div><div><div>No</div><div></div><div>Mrk</div><div>Lmt</div><div>List</div><div>Del</div><div>Digits</div><div>Dgts</div></div><div><div>QSIG</div><div>Intw</div></div></div><div><div><div>1: 20</div><div>19</div></div><div><div>n</div><div>user</div></div></div><div><div><div>2:</div><div></div></div><div><div>n</div><div>user</div></div></div><div><div><div>3:</div><div></div></div><div><div>n</div><div>user</div></div></div><div><div><div>4:</div><div></div></div><div><div>n</div><div>user</div></div></div><div><div><div>5:</div><div></div></div><div><div>n</div><div>user</div></div></div><div><div><div>6:</div><div></div></div><div><div>n</div><div>user</div></div></div></div></div><div><div><div><div>BCC</div><div>VALUE</div><div>TSC</div><div>CA-TSC</div><div>ITC</div><div>BCIE</div><div>Service/Feature</div><div>PARM</div><div>No.</div><div>Numbering</div><div>LAR</div></div><div><div>0</div><div>1</div><div>2</div><div>M</div><div>4</div><div>W</div><div>Request</div><div></div><div>Dgts</div><div>Format</div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div>Subaddress</div><div></div></div></div><div><div><div>1: yyyynnn</div><div>rest</div><div>none</div></div><div><div><div>2: yyyynnn</div><div>rest</div><div>none</div></div><div><div><div>3: yyyynnn</div><div>rest</div><div>none</div></div><div><div><div>4: yyyynnn</div><div>rest</div><div>none</div></div><div><div><div>5: yyyynnn</div><div>rest</div><div>none</div></div><div><div><div>6: yyyynnn</div><div>rest</div><div>none</div></div></div></div></div></div></div></div></div></div></div>	

Step	Description
	<p>Route Pattern (continued)</p> <p>Route pattern 1 was used to route calls to Session Manager. Route pattern 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Pattern Name: Any descriptive name. ▪ Grp No: 1 This field is set to the trunk group number defined in Step 6. ▪ FRL: 0 This field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive.
	<pre> change route-pattern 1 Page 1 of 3 Pattern Number: 1 Pattern Name: to SM_21_31 SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 1 0 2: 3: 4: 5: 6: n user n user n user n user n user n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress 1: y y y y y n n rest lev0-pvt none 2: y y y y y n n rest none 3: y y y y y n n rest none 4: y y y y y n n rest none 5: y y y y y n n rest none 6: y y y y y n n rest none </pre>
10.	<p>Incoming Call Handling Treatment</p> <p>For PSTN calls that were routed to Session Manager, allowed by the NACR CallNACK application, and then routed back to Communication Manager, a “steering digit” needed to be inserted to the number in order to route the call to the PSTN trunk. Without the steering digit, Communication Manager would simply route the call back to Session Manager and create a loop.</p> <p>The incoming call handling treatment for trunk group 1 was configured using the parameters highlighted below. Note 98 is inserted for PSTN numbers beginning with 1303. The 9 is the ARS feature access code (which will be stripped during normal call processing), and the 8 is the “steering digit” to route the calls to the PSTN trunk.</p> <pre> change inc-call-handling-trmt trunk-group 1 Page 1 of 30 INCOMING CALL HANDLING TREATMENT Service/ Number Number Del Insert Feature Len Digits tie 11 1303 </pre>

Step	Description
11.	<p>COR</p> <p>The ARS table is set up to route calls beginning with 8130 to the PSTN trunk. To prevent users from dialing that number directly, and bypassing the NACR CallNACK application, the Restricted Call List feature was enabled as shown below for COR 2. Next, the dialed string 81303 was added to the restricted call list as shown in the next step.</p>
	<div> <div>change cor 2</div> <div>Page 1 of 23</div> </div> <div> <div>CLASS OF RESTRICTION</div> <div> <div>COR Number: 2</div> <div>COR Description:</div> <div> <div>FRL: 0</div> <div>APLT? y</div> <div>Can Be Service Observed? n</div> <div>Calling Party Restriction: none</div> <div>Can Be A Service Observer? n</div> <div>Called Party Restriction: none</div> <div>Time of Day Chart: 1</div> <div>Forced Entry of Account Codes? n</div> <div>Priority Queuing? n</div> <div>Direct Agent Calling? n</div> <div>Restriction Override: none</div> <div>Facility Access Trunk Test? n</div> <div>Restricted Call List? y</div> <div>Can Change Coverage? n</div> <div>Access to MCT? y</div> <div>Fully Restricted Service? n</div> <div>Group II Category For MFC: 7</div> <div>Hear VDN of Origin Annc.? n</div> <div>Send ANI for MFE? n</div> <div>Add/Remove Agent Skills? n</div> <div>MF ANI Prefix:</div> <div>Automatic Charge Display? n</div> <div>Hear System Music on Hold? y</div> <div>PASTE (Display PBX Data on Phone)? n</div> <div>Can Be Picked Up By Directed Call Pickup? n</div> <div>Can Use Directed Call Pickup? n</div> <div>Group Controlled Restriction: inactive</div> </div> </div> </div>
12.	<p>Toll Analysis</p> <p>Use the <i>change toll</i> command to add the desired dialed strings to the Restricted Call List (RCL) as shown in the screen below.</p>
	<div> <div>change toll 8</div> <div>Page 1 of 1</div> </div> <div> <div>TOLL ANALYSIS</div> <div>Percent Full: 5</div> </div> <div> <div>Location: all</div> <div> <div>Total</div> <div>Toll</div> <div>CDR</div> <div><--Unrestricted Call List--></div> </div> <div> <div>Dialed String</div> <div>Min</div> <div>Max</div> <div>RCL</div> <div>List</div> <div>FEAC</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> <div>6</div> <div>7</div> <div>8</div> <div>9</div> <div>10</div> </div> <div> <div>81303</div> <div>12</div> <div>12</div> <div>x</div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div>

Step	Description
13.	Station Stations to be used by implicit users were assigned COR 2 to prevent direct access to the PSTN trunk.
<div><div>change station 53003</div><div>Page 1 of 5</div></div> <div><div>STATION</div><div><div>Extension: 53003</div><div>Type: 2420</div><div>Port: 001V201</div><div>Name: 53003</div></div><div><div>Lock Messages? n</div><div>Security Code: 123456</div><div>Coverage Path 1:</div><div>Coverage Path 2:</div><div>Hunt-to Station:</div></div><div><div>BCC: 0</div><div>TN: 1</div><div>COR: 2</div><div>COS: 1</div></div></div> <div><div>STATION OPTIONS</div><div><div>Loss Group: 2</div><div>Data Option: none</div><div>Speakerphone: 2-way</div><div>Display Language: english</div></div><div><div>Time of Day Lock Table:</div><div>Personalized Ringing Pattern: 1</div><div>Message Lamp Ext: 53003</div><div>Mute Button Enabled? y</div><div>Expansion Module? n</div></div><div><div>Survivable COR: internal</div><div>Survivable Trunk Dest? y</div></div><div><div>Media Complex Ext:</div><div>IP SoftPhone? n</div><div>Remote Office Phone? n</div><div>IP Video? n</div></div><div><div>Customizable Labels? y</div></div></div>	

9. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

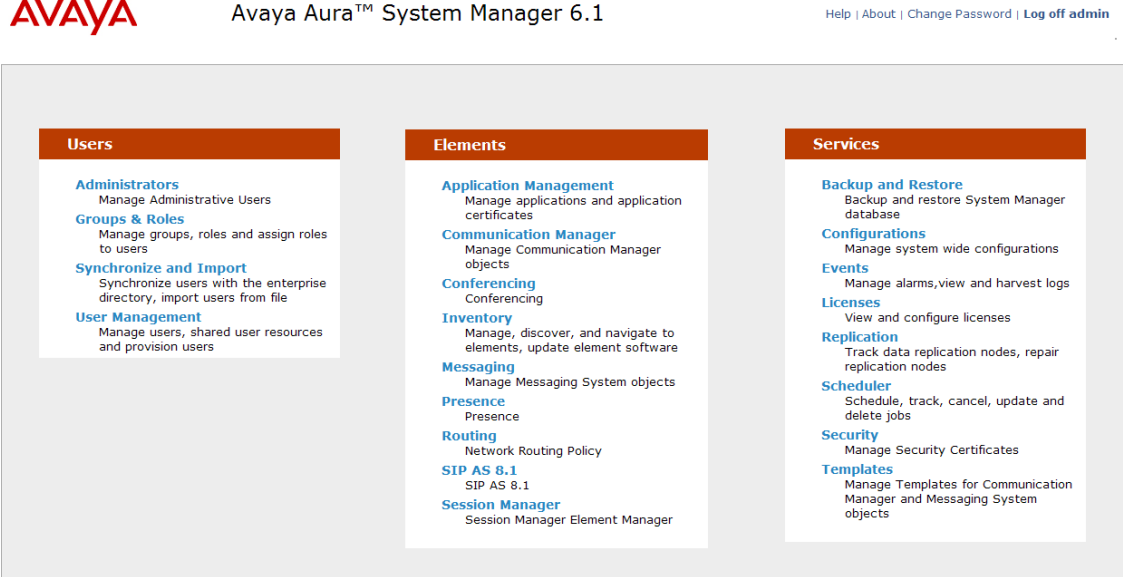
The Session Manager server provides the network interface for all inbound and outbound SIP signaling to all provisioned SIP entities. During compliance testing, the IP address assigned to the Security Module interface is 10.64.21.31 as specified in **Figure 1**. The Session Manager server also has a separate network interface used for connectivity to System Manager for provisioning. The IP address assigned to the Session Manager management interface is 10.64.21.30.

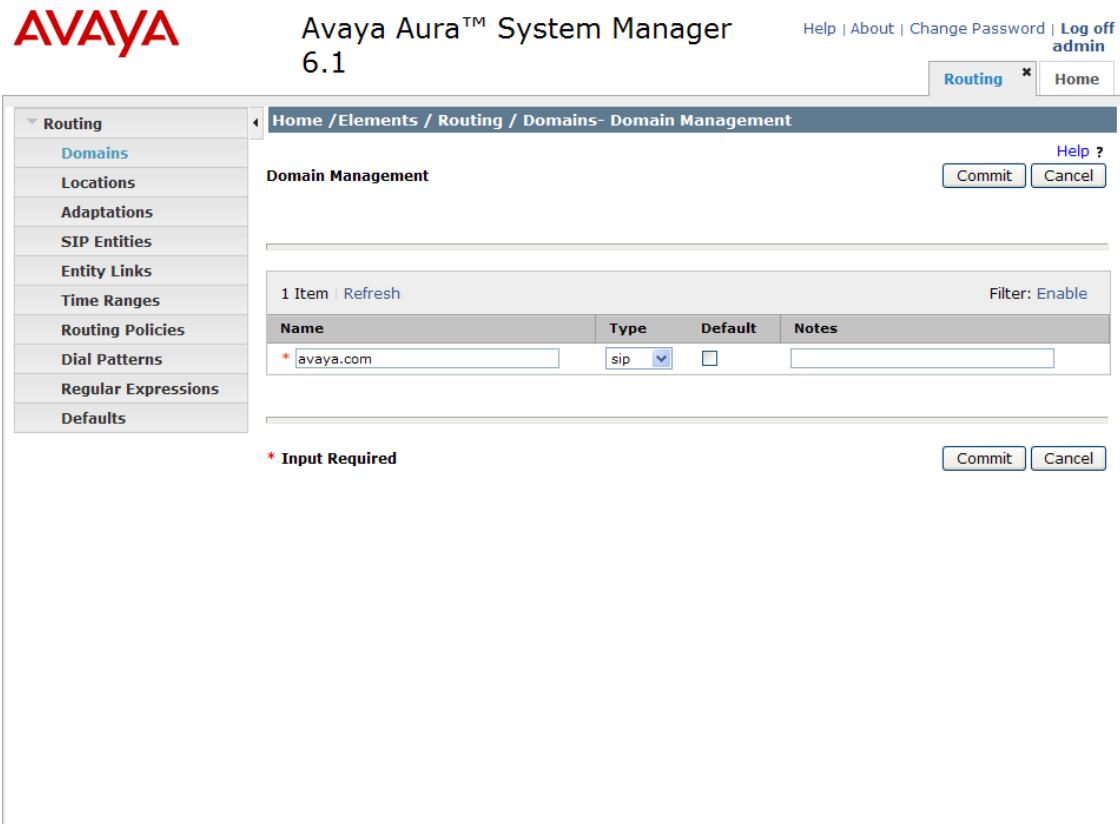
The procedures described in this section include configurations for the following:

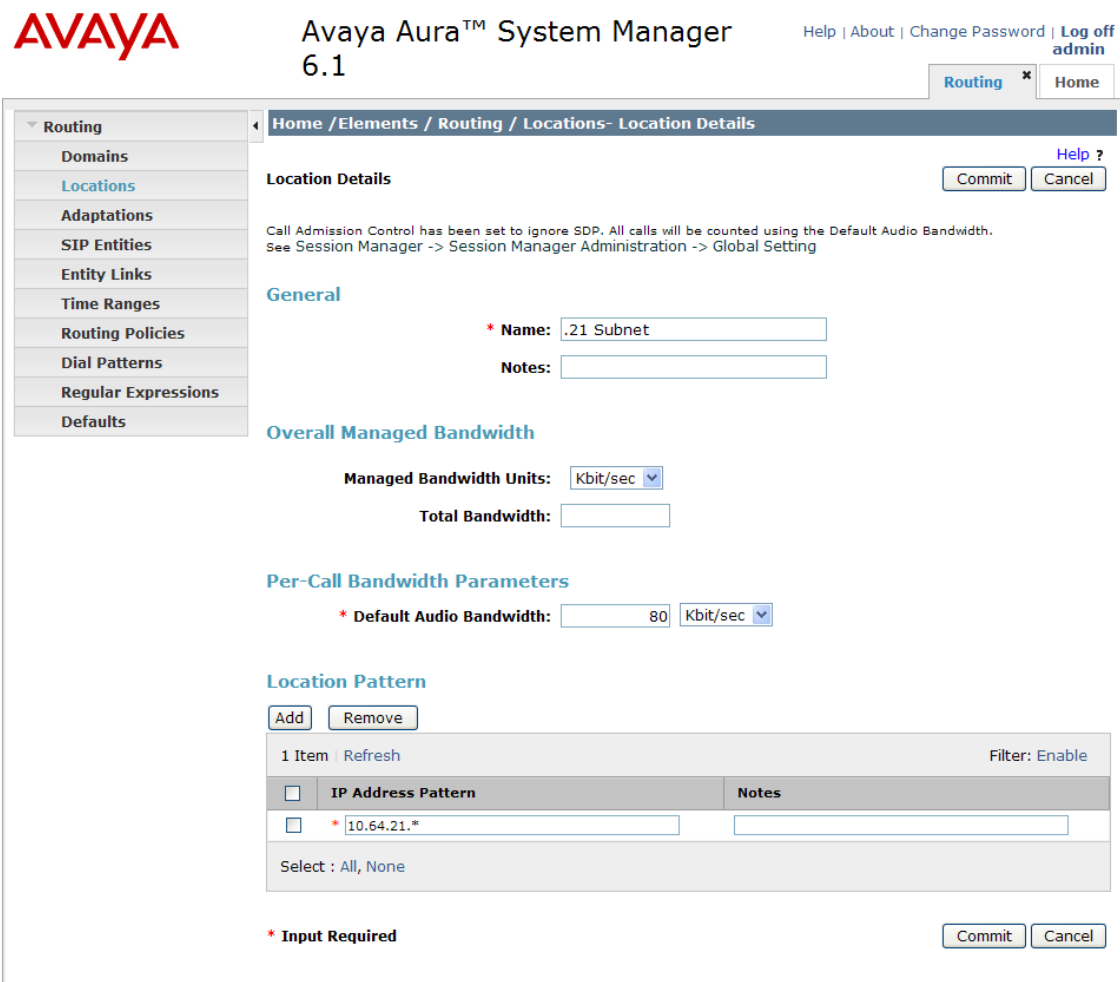
- **SIP Domains** – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- **Locations** – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.
- **SIP Entities** – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- **Entity Links** – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- **Time Ranges** – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Network Routing Policy may be associated with one or more Time Ranges during which the Network Routing Policy is in effect.
- **Routing Policies** – Routing Policies are used in conjunction with a Dial Patterns to specify a SIP Entity that a call should be routed to.
- **Dial Patterns** – A Dial Pattern specifies a set of criteria and a set of Network Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Network Routing Policies specified in the Dial Pattern. The

selected Network Routing Policy in turn specifies the SIP Entity to which the call is to be routed.

- **Applications** – Application entries are used to define and manage single applications with application attributes for inclusion into one or more application sequences.
- **Application Sequences** – An Application Sequence enables defining and managing an ordered set of applications using in call sequencing. These application sets can be associated as the origination and/or termination application sequence for a registered user's "Communication Profile" in the User Management module and enable routing every incoming, outgoing, or combined call for that user.
- **Implicit Users** – Implicit Users allow administering of certain dial patterns for users that do not register or connect with Session Manager. This functionality enables provisioning a set of originating and terminating sequenced application for such users.

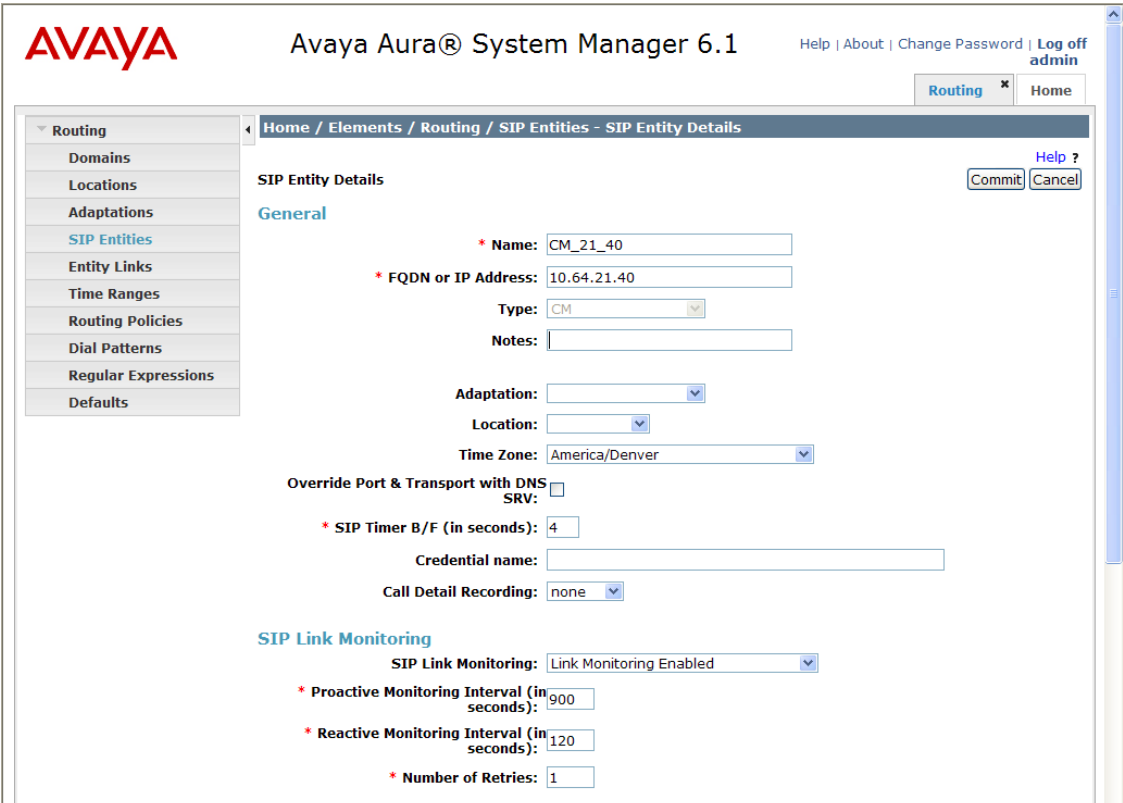
Step	Description
1.	<p>Login</p> <p>Access the Session Manager administration web interface by entering <code>https://<ip-addr>/network-login/</code> as the URL in an Internet browser, where <code><ip-addr></code> is the IP address of the System Manager server.</p> <p>Log in using appropriate credentials. The main page for the administrative interface is shown below.</p> 

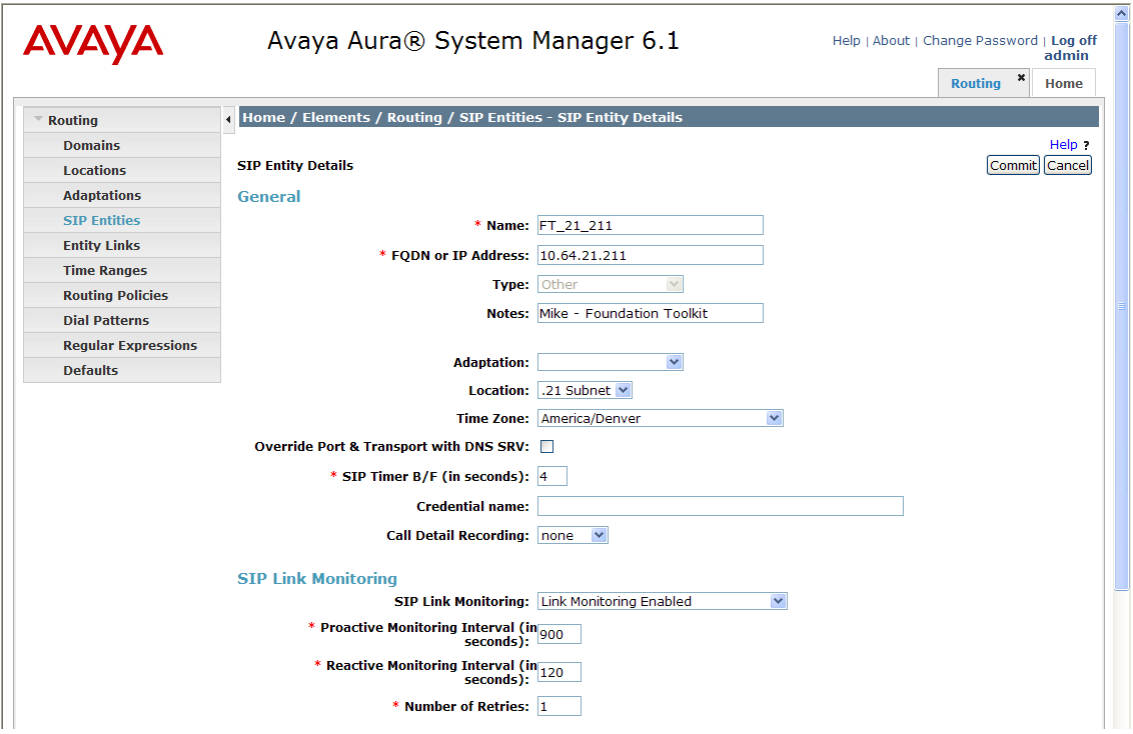
Step	Description
2.	<p>Add SIP Domain</p> <p>The Routing menu contains all the configuration tasks listed at the beginning of this section.</p> <p>During compliance testing, one SIP Domain was configured.</p> <p>Navigate to Routing→Domains, and click the New button (not shown) to add the SIP domain with</p> <ul style="list-style-type: none"> • Name: <i>avaya.com</i> (as set in Section 5, Step 2) • Notes: optional descriptive text <p>Click Commit to save the configuration.</p>  <p>The screenshot shows the Avaya Aura System Manager 6.1 interface. The top header includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the header, there are tabs for 'Routing' and 'Home'. The left sidebar shows a tree view under 'Routing' with 'Domains' selected. The main content area is titled 'Domain Management' and shows a table with one item: 'avaya.com' with type 'sip'. There are 'Commit' and 'Cancel' buttons at the bottom of the table.</p>

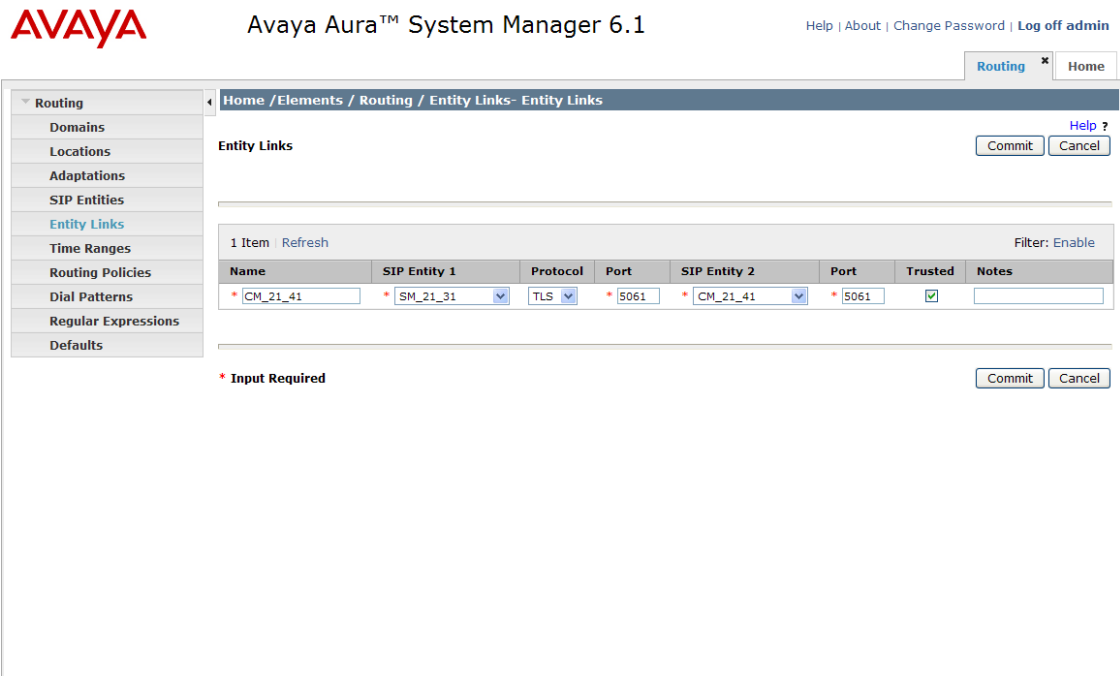
Step	Description
3.	<p>Add Location</p> <p>Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured at each site for compliance testing.</p> <p>Navigate to Routing→Locations and click the New button (not shown) to add the Location.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: a descriptive name • Notes: optional descriptive text <p>Under Location Pattern, click the Add button to add a new line:</p> <ul style="list-style-type: none"> • IP Address Pattern: 10.64.21.* • Notes: optional descriptive text <p>Click Commit to save the configuration.</p> 

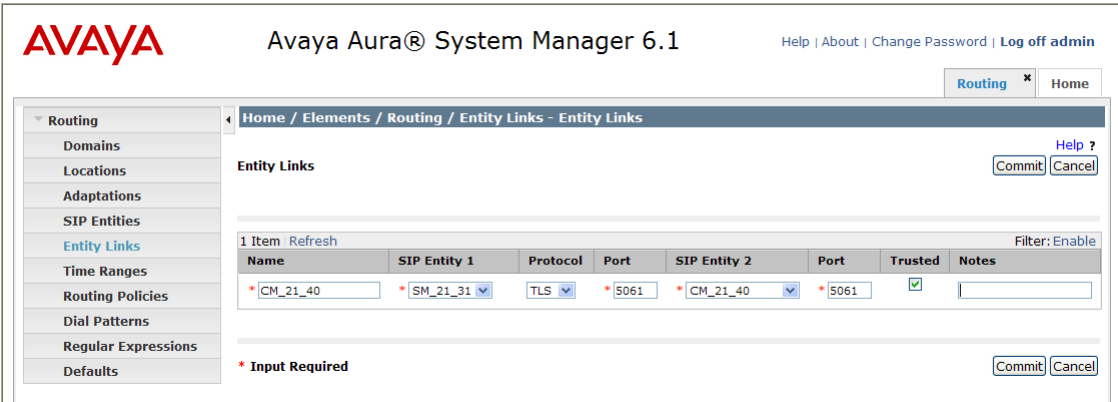
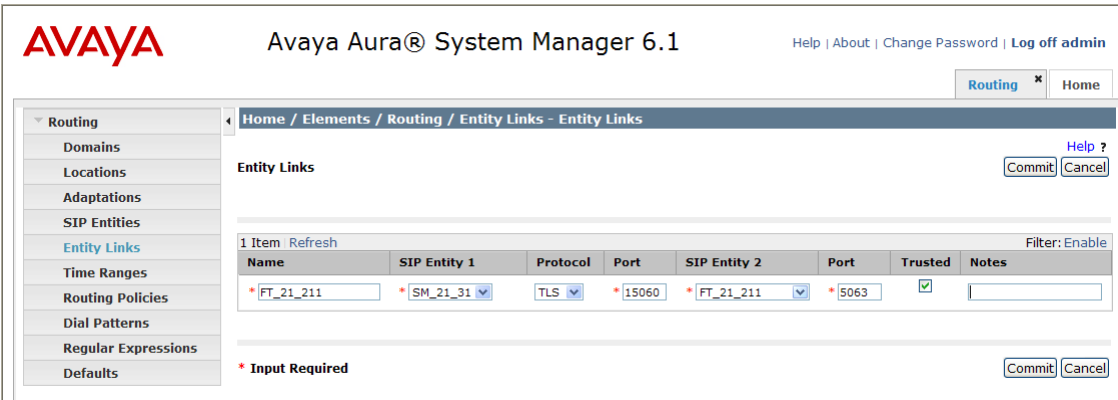
Step	Description
4.	<p>Add SIP Entities</p> <p>A SIP Entity must be added for Session Manager (not shown) and for each SIP-based telephony system supported by it using SIP trunks. During compliance testing, a SIP Entity was added for the Session Manager itself, two Communication Managers (one Evolution Server and one Feature Server), and the ACE/Foundation Toolkit server.</p> <p>Navigate to Routing→SIP Entities, and click the New button (not shown) to add a SIP Entity. The configuration details for the SIP Entity defined for the Communication Manager Evolution Server are as follows:</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: a descriptive name • FQDN or IP Address: <i>10.64.21.41</i> as specified in Figure 1. • Type: select <i>CM</i> <p>Default settings can be used for the remaining fields. Click Commit to save the SIP Entity definition.</p>

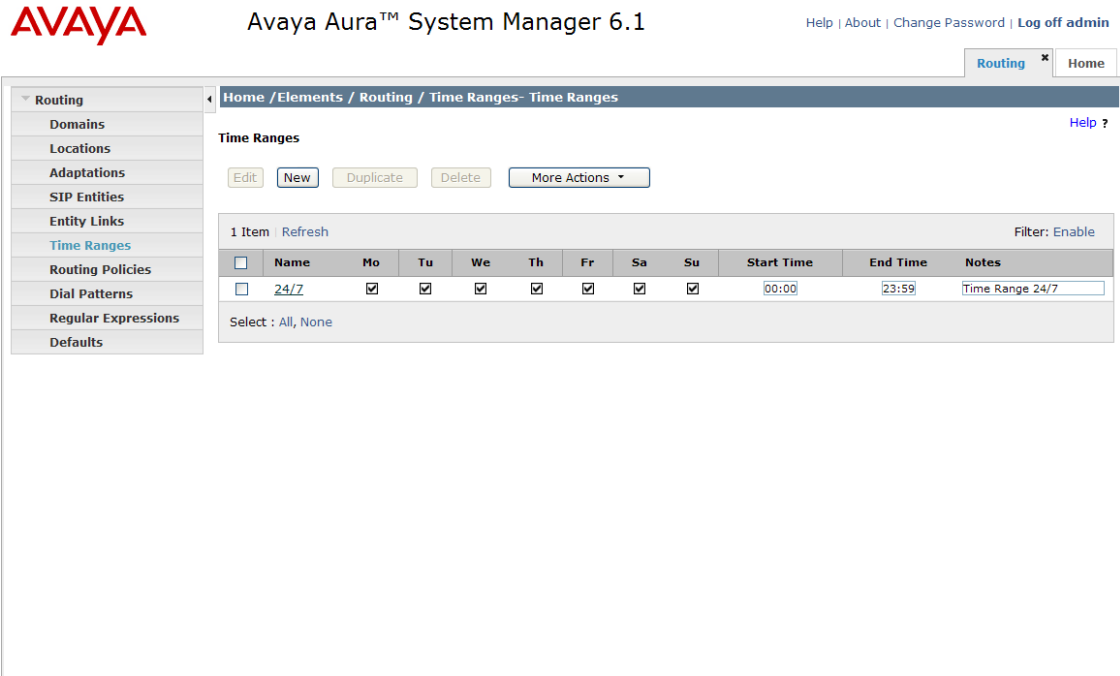
Step	Description														
	<div><div>Add SIP Entities (continued) – Communication Manager Evolution Server</div><div>The screen below shows the SIP Entity configuration details for the Communication Manager Evolution Server.</div><div><div><div><div>AVAYA</div><div>Avaya Aura™ System Manager</div><div>6.1</div></div><div><div>Help About Change Password Log off admin</div><div><div>Routing</div><div>Home</div></div></div></div><div><div><div>Routing</div><div>Domains</div><div>Locations</div><div>Adaptations</div><div>SIP Entities</div><div>Entity Links</div><div>Time Ranges</div><div>Routing Policies</div><div>Dial Patterns</div><div>Regular Expressions</div><div>Defaults</div></div><div><div>Home / Elements / Routing / SIP Entities- SIP Entity Details</div><div><div>SIP Entity Details</div><div><div>Commit</div><div>Cancel</div></div><div><div>General</div><div><div><div>* Name:</div><div>CM_21_41</div></div><div><div>* FQDN or IP Address:</div><div>10.64.21.41</div></div><div><div>Type:</div><div>CM</div></div><div><div>Notes:</div><div></div></div><div><div>Adaptation:</div><div></div></div><div><div>Location:</div><div></div></div><div><div>Time Zone:</div><div>America/Denver</div></div><div><div>Override Port & Transport with DNS SRV:</div><div><input type="checkbox"/></div></div><div><div>* SIP Timer B/F (in seconds):</div><div>4</div></div><div><div>Credential name:</div><div></div></div><div><div>Call Detail Recording:</div><div>none</div></div><div><div>SIP Link Monitoring</div><div><div>SIP Link Monitoring:</div><div>Use Session Manager Configuration</div></div><div><div>Entity Links</div><div><div>Add</div><div>Remove</div></div><div><div>1 Item</div><div>Refresh</div><div>Filter: Enable</div><table><tr><th></th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Trusted</th></tr><tr><td><input type="checkbox"/></td><td>SM_21_31</td><td>TLS</td><td>* 5061</td><td>CM_21_41</td><td>* 5061</td><td><input checked="" type="checkbox"/></td></tr></table></div></div></div></div></div></div></div></div></div></div>		SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_21_41	* 5061	<input checked="" type="checkbox"/>
	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted									
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_21_41	* 5061	<input checked="" type="checkbox"/>									

Step	Description
	<p>Add SIP Entities (continued) – Communication Manager Feature Server</p> <p>The screen below shows the SIP Entity configuration details for the Communication Manager Feature Server. Note the CM selection for Type.</p>  <p>The screenshot displays the 'SIP Entity Details' configuration page in Avaya Aura System Manager 6.1. The left sidebar shows a navigation menu with 'Routing' expanded, and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The configuration fields are as follows:</p> <ul style="list-style-type: none"> Name: CM_21_40 FQDN or IP Address: 10.64.21.40 Type: CM (selected from a dropdown) Notes: (empty text field) Adaptation: (empty dropdown) Location: (empty dropdown) Time Zone: America/Denver (selected from a dropdown) Override Port & Transport with DNS SRV: (unchecked checkbox) SIP Timer B/F (in seconds): 4 Credential name: (empty text field) Call Detail Recording: none (selected from a dropdown) SIP Link Monitoring: Link Monitoring Enabled (selected from a dropdown) Proactive Monitoring Interval (in seconds): 900 Reactive Monitoring Interval (in seconds): 120 Number of Retries: 1

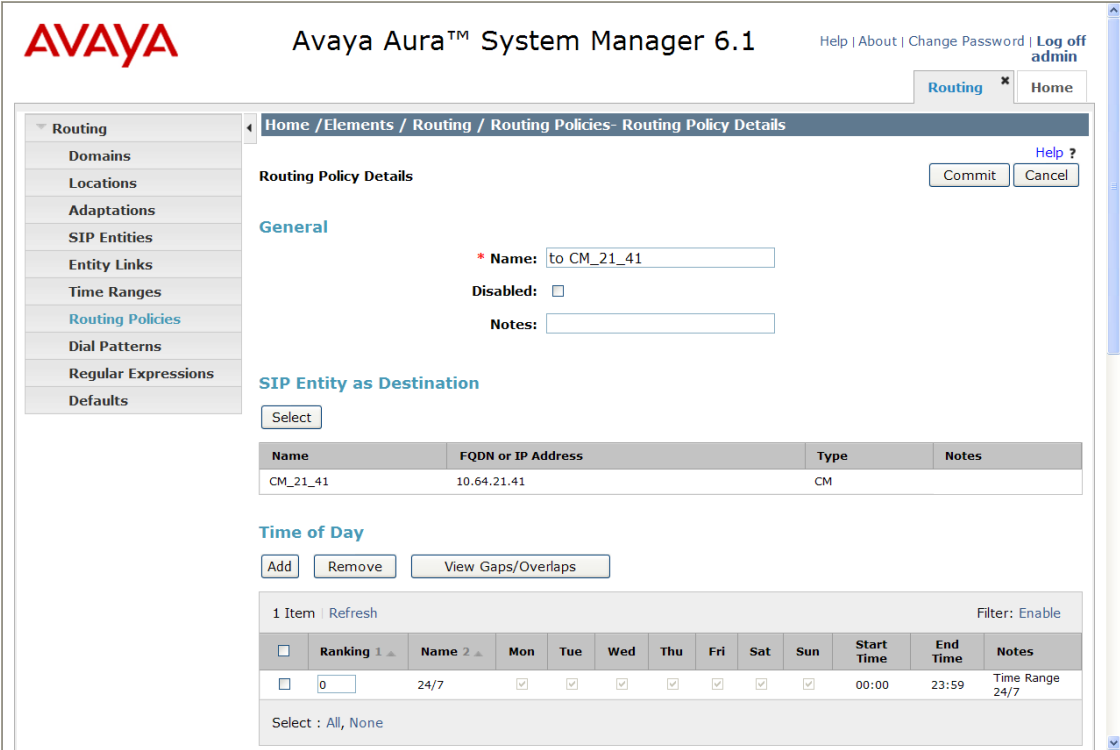
Step	Description
	<p>Add SIP Entities (continued) – ACE/Foundation Toolkit Server</p> <p>The screen below shows the SIP Entity configuration details for the ACE/Foundation Toolkit server. Note the <i>Other</i> selection for Type.</p> 

Step	Description
5.	<p>Add Entity Links</p> <p>A SIP trunk between Session Manager and a telephony system is described by an Entity link. Three Entity Links were created:</p> <ul style="list-style-type: none"> • Session Manager ↔ Communication Manger (Evolution Server) • Session Manager ↔ Communication Manger (Feature Server) • Session Manager ↔ Foundation Toolkit Server <p>Navigate to Routing→Entity Links, and click the New button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager to Communication Manager (Evolution Server).</p> <ul style="list-style-type: none"> • Name: a descriptive name • SIP Entity 1: select the Session Manager SIP Entity. • Port: 5061. This is the port number to which the other system sends SIP requests. • SIP Entity 2: select the Communication Manager SIP Entity. • Port: 5061. This is the port number on which the other system receives SIP requests. • Trusted: check this box • Protocol: select TLS as the transport protocol. • Notes: optional descriptive text <p>Click Commit to save the configuration.</p> 

Step	Description
	<p>Add Entity Links (continued) The Entity Link for connecting Session Manager to Communication Manager (Feature Server) was similarly defined as shown in the screen below.</p> 
	<p>Add Entity Links (continued) The Entity Link for connecting Session Manager to the Foundation Toolkit Server was similarly defined as shown in the screen below.</p> 

Step	Description
6.	<p>Add Time Ranges</p> <p>Before adding routing policies (configured in next step), time ranges must be defined during which the policies will be active. One Time Range was defined that would allow routing to occur at anytime.</p> <p>Navigate to Routing→Time Ranges, and click the New button to add a new Time Range:</p> <ul style="list-style-type: none"> • Name: a descriptive name • Mo through Su: check the box under each of these headings • Start Time: enter 00:00 • End Time: enter 23:59 <p>Click Commit to save this time range. The screen below shows the configured Time Range.</p>  <p>The screenshot shows the Avaya Aura™ System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. The breadcrumb trail is Home / Elements / Routing / Time Ranges- Time Ranges. The left sidebar lists various configuration options, with 'Time Ranges' highlighted. The main content area shows the 'Time Ranges' configuration page with buttons for Edit, New, Duplicate, Delete, and More Actions. Below these buttons is a table with one item, '24/7', which is active for all days of the week (Mo, Tu, We, Th, Fr, Sa, Su) from 00:00 to 23:59. The table also includes a 'Notes' column with the value 'Time Range 24/7'.</p>

Step	Description
7.	<p>Add Routing Policies Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. A Routing Policy was added for routing PSTN calls to the Communication Manager Evolution Server.</p> <p>Navigate to Routing→Routing Policies, and click the New button (not shown) to add a new Routing Policy.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: a descriptive name • Notes: optional descriptive text <p>Under SIP Entity as Destination Click Select to select the appropriate SIP Entity to which the routing policy applies (not shown).</p> <p>Under Time of Day Click Add to select the Time Range configured in the previous step (not shown).</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>

Step	Description
	<p>Add Routing Policies (continued)</p> <p>The screen below shows the configuration details for the Routing Policy to route calls to the Communication Manager (Evolution Server).</p>  <p>The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.1', and links for 'Help About Change Password Log off admin'. The left sidebar shows a tree view with 'Routing' expanded, containing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section has fields for 'Name' (to CM_21_41), 'Disabled' (checkbox), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one row: CM_21_41, 10.64.21.41, CM. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' and a 'Filter: Enable' option. Below is a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table contains one row: 0, 24/7, with checkboxes for all days of the week. At the bottom, it says 'Select : All, None'.</p>

Step	Description
8.	<p>Add Dial Patterns</p> <p>Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. 11-digit PSTN numbers beginning with “1303538” were routed to the Communication Manager Evolution Server for onward routing to the PSTN.</p> <p>Navigate to Routing→Dial Patterns, click the New button (not shown) to add a new Dial Pattern.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Pattern: dialed number or prefix • Min: minimum length of dialed number • Max: maximum length of dialed number • SIP Domain: select the SIP Domain created in Step 2 (or select –ALL– to be less restrictive) • Notes: optional descriptive text <p>Under Originating Locations and Routing Policies</p> <p>Click Add to select the appropriate originating Location and Routing Policy from the list (not shown).</p> <p>Under Time of Day</p> <p>Click Add to select the time range configured in Step 6.</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>

Add Dial Patterns (continued)

The screens below shows the configuration details for the Dialed Pattern defined for routing PSTN calls to Communication Manager Evolution Server.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details [Help ?](#) [Commit](#) [Cancel](#)

General

* **Pattern:** 1303538

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to CM_21_41	0	<input type="checkbox"/>	CM_21_41	

Select : All, None

Denied Originating Locations

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required [Commit](#) [Cancel](#)

9. Add Application

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

Navigate to **Session Manager → Application Configuration → Applications**, and click the **New** button to add an application for the NACR CallNACK application.

- **Name:** a descriptive name
- **SIP Entity:** Select the ACE/Foundation Toolkit Server SIP entity
- **Description:** optional descriptive text
- **Application Handle:** enter the application handle used by the NACR CallNACK application (i.e. *blockapp*)

Click **Commit** to save the Application. The screen below shows the configured application.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

Home / Elements / Session Manager / Application Configuration / Applications- Applications

Help ?

Application Editor

Commit Cancel

Application

*Name

*SIP Entity

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text" value="blockapp"/>
URI Parameters	<input type="text"/>

*Required

Commit Cancel

10. Add Application Sequences

An Application Sequence enables defining and managing an ordered set of applications using in call sequencing. These application sets can be associated as the origination and/or termination application sequence for a registered user's "Communication Profile" in the User Management module and enable routing every incoming, outgoing, or combined call for that user. It can all be used for Implicit Users by administering certain dial patterns for users that do not register or connect with Session Manager.

Navigate to **Session Manager → Application Configuration → Application Sequences**, and click the **New** button to add a new Application:

- **Name:** a descriptive name
- **Description:** optional descriptive text
- Under **Available Applications**, click the "+" symbol next to the application created in the previous step to move it up to **Applications in this Sequence**.

Click **Commit** to save the Application Sequence. The screen below shows the configured Application Sequence.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, Applications, Application Sequences, Implicit Users, NRS Proxy Users, System Status, and System Tools. The main content area is titled "Application Sequence Editor" and includes a "Commit" button and a "Cancel" button. Below the title, there are input fields for "Name" (Orig_CallBlocker_ImplicitUsers) and "Description" (Call Blocker for Implicit Users). The "Applications in this Sequence" section shows a table with one item: "Call Blocker" (FT_21_211, Mandatory, Foundation Toolkit - Call Blocker). The "Available Applications" section shows a list of 13 items, including "Call Blocker", "Call Director", and "Call Screening", each with a "+" icon to add it to the sequence.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager * Home

Home / Elements / Session Manager / Application Configuration / Application Sequences- Application Sequences

Help ?

Application Sequence Editor [Commit] [Cancel]

Application Sequence

*Name:

Description:

Applications in this Sequence

[Move First] [Move Last] [Remove]

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	1	Call Blocker	FT_21_211	<input checked="" type="checkbox"/>	Foundation Toolkit - Call Blocker

Select : All, None

Available Applications

13 Items | Refresh Filter: Enable

	Name	SIP Entity	Description
+	Call Blocker	FT_21_211	Foundation Toolkit - Call Blocker
+	Call Director	FT_21_211	Foundation Toolkit - Call Director
+	Call Screening	FT_21_211	Foundation Toolkit - Screen Incoming Calls

11. **Add Implicit Users (users that do not register with Session Manager)**
To add an Implicit User, navigate to **Session Manager → Application Configuration → Implicit Users**, and click the **New** button (not shown) to add a new Implicit User Rule:

- **Pattern:** Enter the dial pattern of the Implicit User station extensions to be managed by the NACR CallNACK application. The example below shows one specific station pattern; however, a less restrictive pattern may be defined to cover a range of station extensions.
- **Min:** Enter the minimum length of the pattern to be matched.
- **Max:** Enter the maximum length of the pattern to be matched.
- **Origination Application Sequence:** Select the Application Sequence from **Step 10**.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". A breadcrumb trail shows the path: "Home / Elements / Session Manager / Application Configuration / Implicit Users- Implicit Users". The left sidebar contains a tree view with categories like "Session Manager", "Network Configuration", "Device and Location Configuration", "Application Configuration", "Applications", "Application Sequences", "Implicit Users", "NRS Proxy Users", "System Status", and "System Tools". The "Implicit Users" category is selected. The main content area is titled "Implicit User Rule Editor" and contains a form for defining an "Implicit User Rule". The form includes fields for "Pattern" (with the value "53003"), "Min" (with the value "5"), and "Max" (with the value "5"). There is also a "Description" field. Below these are dropdown menus for "SIP Domain" (set to "-ALL-"), "Origination Application Sequence" (set to "Orig_CallBlocker_ImplicitUsers"), and "Termination Application Sequence" (set to "Select Termination Application Sequence..."). At the bottom of the form, there is a "*Required" label and two buttons: "Commit" and "Cancel".

10. Configure NACR CallNACK

This section describes the configuration of NACR CallNACK. It assumes that the application and all required software components have been installed and properly licensed.

During compliance testing, NACR delivered that application as a zip file. Expand the Zip file to C:/CallBlock

Within the *config* directory, open *callblock.properties* file and make the following edits:

- Set the **comet_url** parameter to specify the URL of the Foundation Toolkit Server's cometd servlet.
- Verify the value for the **applicationName** matches the **Application Handle** for the NARC CallNACK application configured in **Section 9, Step 9**. If they are different, then modify the **Application Handle** in **Section 9** to make them the same.
- Set the **sip.domain** parameter to the SIP Domain configured in **Section 9, Step 2**.
- For each Implicit User to be managed by the NACR CallNACK application, add/modify the user credentials as necessary and ensure the **user.#.sip_address** parameter for each user matches the **Pattern(s)** configured in **Section 9, Step 11**.
- Set the **blocked.number.proxy.touri** parameter to the extension of the announcement configured on Communication Manager (e.g. <extension>@domain).

The *callblock.properties* file used during compliance testing is shown below:

```
# Properties of the foundation server connection
#-----

# Mandatory: The URL to the foundation server's cometd servlet.
# This is typically 'http://<server>:<port>/<warname>/cometd'
comet_url = http://10.64.21.211:8080/foundation/cometd/

# Mandatory: Binding name of the application (here: the application)
# which connects to the foundation server
applicationName = blockapp

# ---- Keystore/Truststore setting used in case of HTTPS connection to the server
# (TLS will be enabled if the comet url starts with 'https...')
trustStorePassword=
keyStorePassword=
# Use a full path (file name included) to key-/truststore locations, e.g.
# 'c:/security/http/<filename>' (on Windows, do not use '\' delimiters) or
# '/opt/security/http/<filename>' (on Linux) or leave them empty (see below)
trustStoreLocation=
keyStoreLocation=
# If key-/truststore location path settings are empty:
# The application will take the filenames below and build pathes of the form
# '<Path to the web-app's WEB-INF folder>/<filename>' for usage as properties
# 'keyStoreLocation', 'trustStoreLocation'
trustStoreFile=
keyStoreFile=

##### Basic SIP settings

# SIP domain
```

```

sip.domain=avaya.com
# URI of the SIP location service
sip.location_service=sip:vsil.local

##### Web Application user definitions (user names have to be unique)

user.1.name=user1
user.1.password=avaya
user.1.sip_address=sip:53104@avaya.com
user.1.mail_address=xxx@xxx.com

user.2.name=user2
user.2.password=avaya
user.2.sip_address=sip:53105@avaya.com
user.2.mail_address=xxx@xxx.com

user.3.name=user3
user.3.password=avaya
user.3.sip_address=sip:53003@avaya.com
user.3.mail_address=xxx@xxx.com

#---- User Configuration Notes:
# Matching SessionManager user settings (administered via SystemManager):
# sip:32135@vsil.local: No sequenced application set
# sip:32136@vsil.local: No sequenced application set
# sip:32137@vsil.local: Application "Deflect to IVR" set (terminating sequence)

##### Properties of F-API sample applications

blocked.number.proxy.touri=sip:53999@avaya.com
## nonblocked.number.addto.uri=

```

Within the *config* directory, open *blockedNumbers.txt* file and edit the file to contain list of dialed numbers to be blocked (one entry per line).

During compliance testing, the NACR CallNACK application was started manually by executing a batch file. NACR was also developing a Windows Service for the application; however, the Windows Service was not available during testing. To execute the batch file, open a Command Prompt window and navigate to **C:\CallBlock** directory. Enter *run.bat* to start the application manually.

11. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager, navigate to **Session Manager→System Status→SIP Entity Monitoring**, and click on the appropriate SIP Entities to verify that the Entity Links each Communication Manager and the ACE/Foundation Toolkit server is up.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with categories like Session Manager, Dashboard, Session Manager, Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, Managed Bandwidth, and Usage. The main content area is titled 'SIP Entity, Entity Link Connection Status' and shows a summary view of entity links for SIP Entity FT_21_211. A table lists one item with details: Session Manager Name (SM_21_31), SIP Entity Resolved IP (10.64.21.211), Port (5063), Proto. (TLS), Conn. Status (Up), Reason Code (200 OK), and Link Status (Up).

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	SM_21_31	10.64.21.211	5063	TLS	Up	200 OK	Up

- From the Communication Manager SAT, use the **status signaling-group x** command to verify that the SIP signaling group is in-service (where **x** is the signaling group number associated with the trunk between Communication Manager and Session Manager).

```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

- From the Communication Manager SAT, use the **status trunk-group y** command to verify that the SIP trunk group is in-service (where **y** is the trunk group number for the trunk between Communication Manager and Session Manager).

```
status trunk 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	in-service/idle	no

- From an Implicit User managed by the NACR CallNACK application, dial a blocked PSTN number. Verify the call is blocked.
- From an Implicit User managed by NACR CallNACK application, dial an allowed PSTN number. Verify the call is allowed.
- From an Implicit User not managed by NACR CallNACK application, dial a blocked PSTN number. Verify the call is allowed.
- From an Implicit User not managed by NACR CallNACK application, dial an allowed PSTN number. Verify the call is allowed.

12. Conclusion

NACR CallNACK passed compliance testing. These Application Notes describe the procedures required for configuring NACR CallNACK (an Avaya Agile Communication Environment™ Foundation Toolkit client application) to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager for Implicit Users, to support the reference configuration shown in **Figure 1**.

13. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Avaya ACE Planning and Installation*, Doc ID: NN10850-004, March 2011
- [2] *Installing Avaya ACE Foundation Toolkit*, March 2011
- [3] *Avaya ACE Foundation Toolkit Developer's Guide*, March 2011
- [4] *Avaya AuraTM Communication Manager Feature Description and Implementation*, Doc ID: 555-245-205, August 2010.
- [5] *Administering Avaya AuraTM Communication Manager*, Doc ID: 03-300509, August 2010.
- [6] *Administering Avaya Aura® Session Manager*, Doc ID: 03-603324, May 2011.
- [7] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID: 03-6034723, April 2011.

Product documentation for NACR CallNACK may be may be obtained from NACR.

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.