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 SIP 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 SIP Users.

NACR CallNACK is configured as a Sequenced Application to be invoked during the originating sequence of a SIP 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 and 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

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 SIP Users.

NACR CallNACK is configured as a Sequenced Application to be invoked during the originating sequence of a SIP User call. 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 SIP 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 SIP Users to the PSTN and verify whether the calls were properly blocked or allowed. The following call flows were tested.

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

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

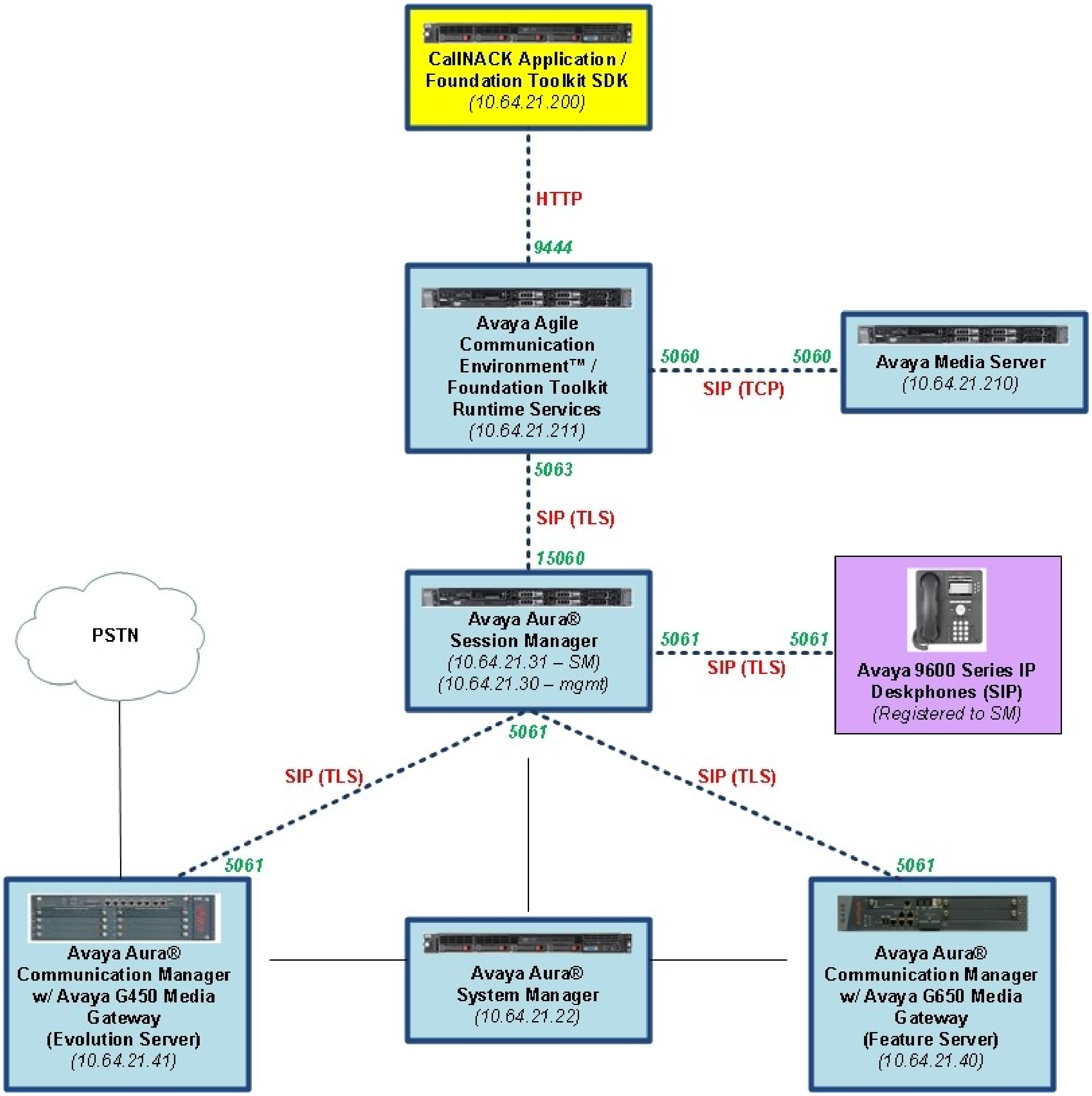


Figure 1: NACR CallNACK in an Avaya Environment

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
Windows Application Server	NACR CallNACK version 1.1 Foundation Toolkit SDK (Sprint-5.3-Patch-1)
Avaya 9600 Series IP Deskphones (SIP)	Release 2.6 Service Pack 4 (96x0) Release 6 Service Pack 2 (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

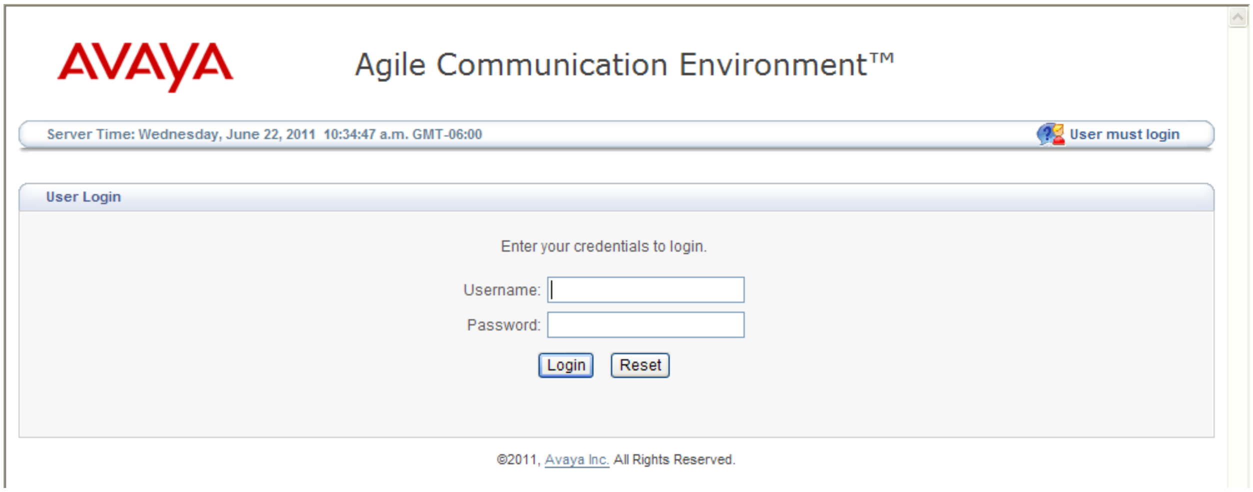
  If media services are not required by client applications, then **Media Server SIP URI** can be left blank. Note: The address part of the URI can use a host name or IP address.
- **Session Manager Address**: The address for the primary Session Manager for the ACE server. This is a fragment of a full 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 Inteface.
- **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.

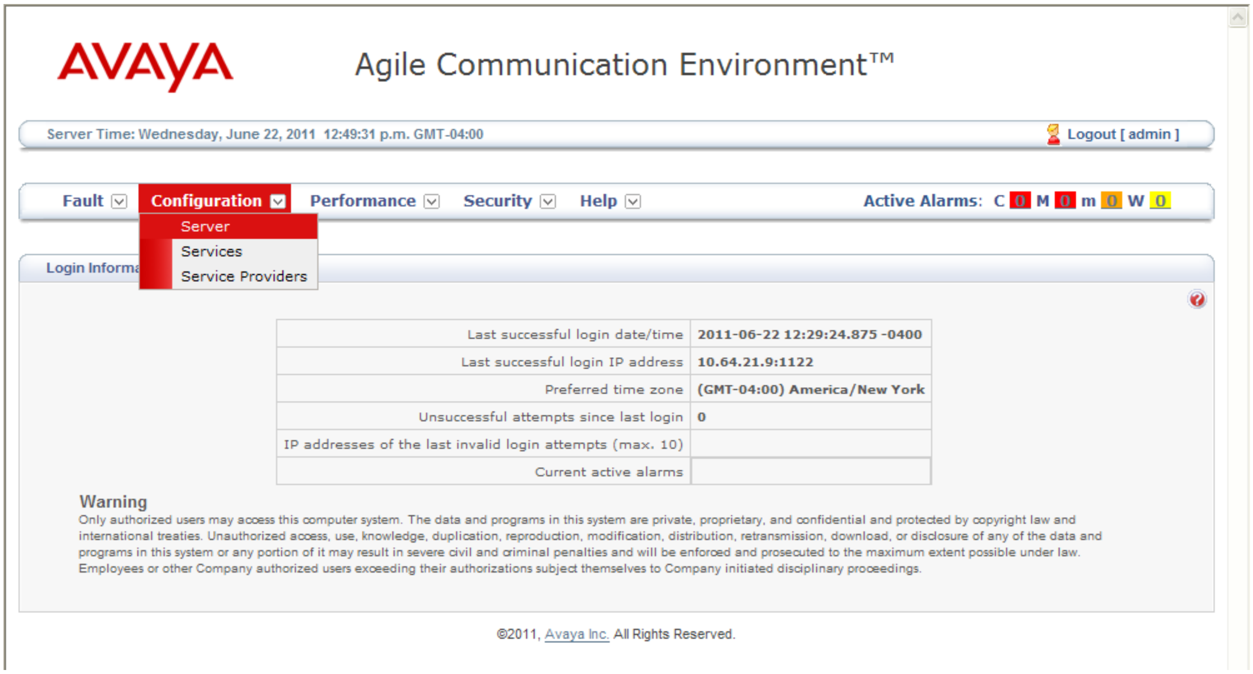


Server Time: Wednesday, June 22, 2011 10:34:47 a.m. GMT-06:00

Enter your credentials to login.

©2011, Avaya Inc. All Rights Reserved.

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



Server Time: Wednesday, June 22, 2011 12:49:31 p.m. GMT-04:00

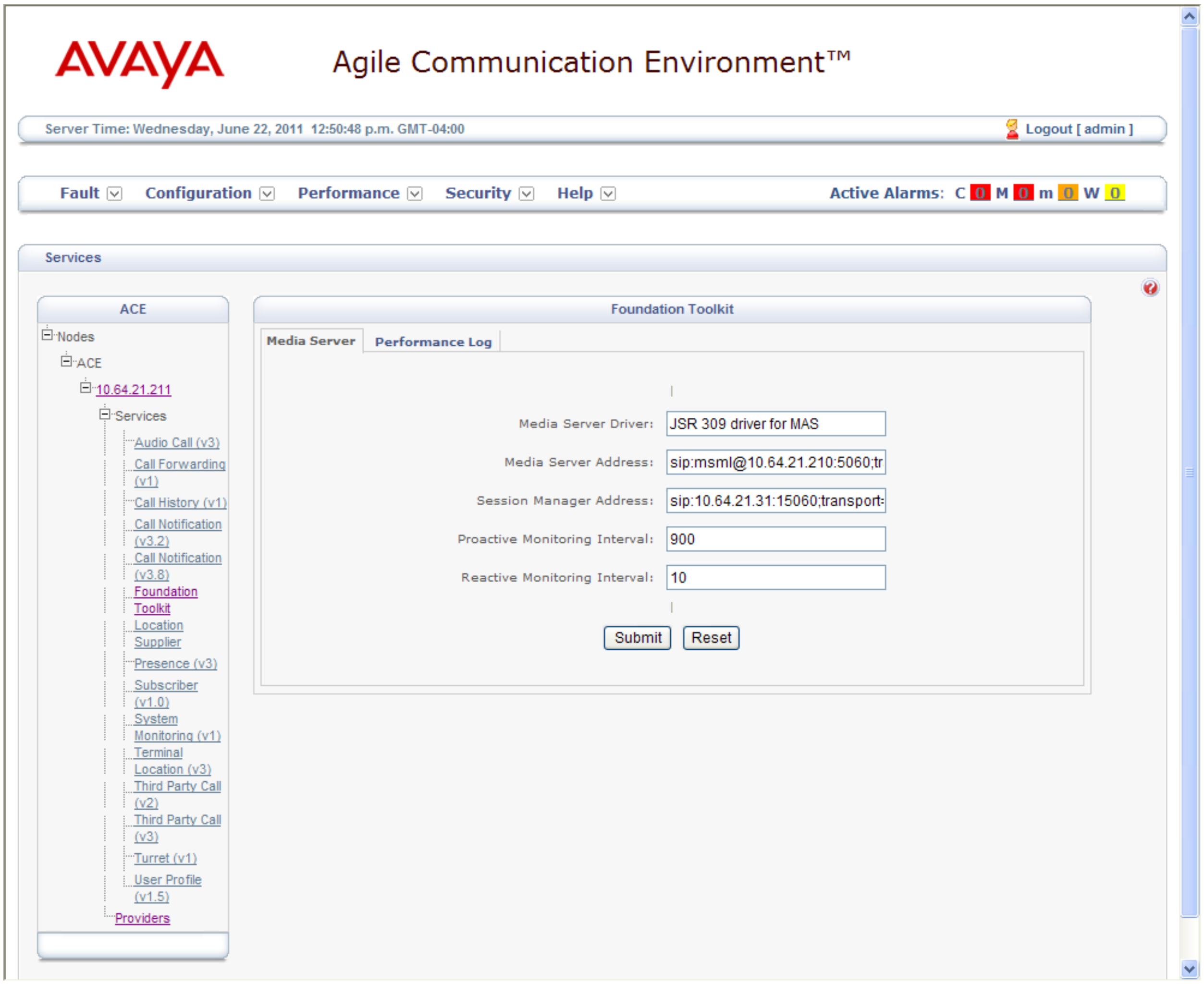
Last successful login date/time	2011-06-22 12:29:24.875 -0400
Last successful login IP address	10.64.21.9:1122
Preferred time zone	(GMT-04:00) America/New York
Unsuccessful attempts since last login	0
IP addresses of the last invalid login attempts (max. 10)	
Current active alarms	

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.

©2011, Avaya Inc. All Rights Reserved.

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.



Media Server Driver: JSR 309 driver for MAS

Media Server Address: sip:msml@10.64.21.210:5060;tr

Session Manager Address: sip:10.64.21.31:15060;transport=

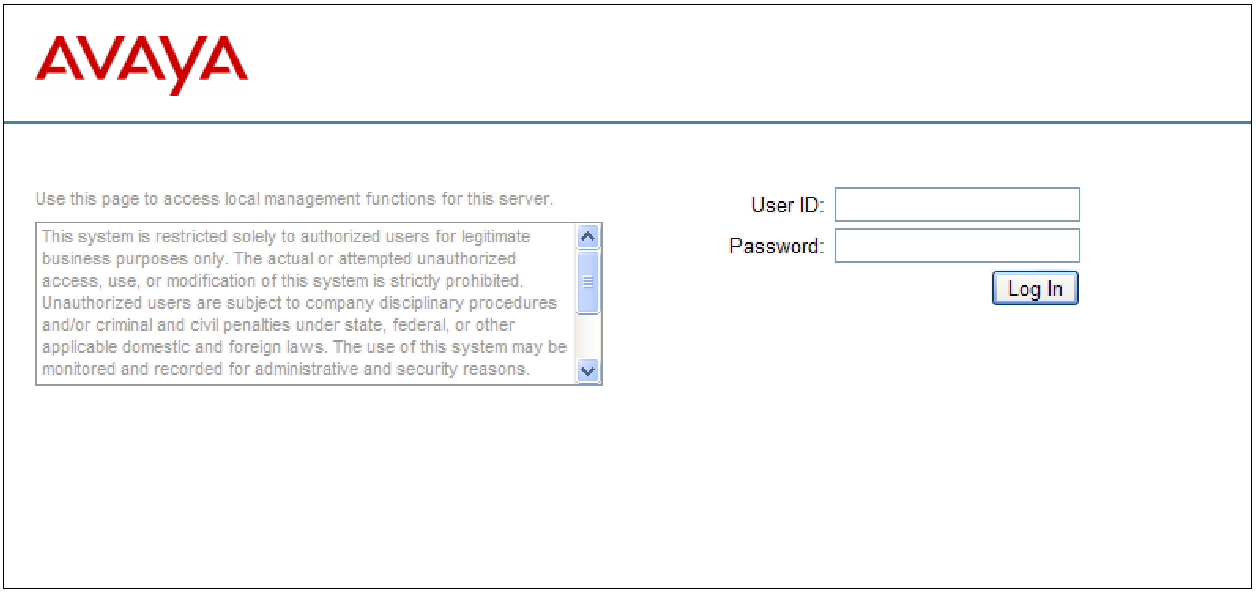
Proactive Monitoring Interval: 900

Reactive Monitoring Interval: 10

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.

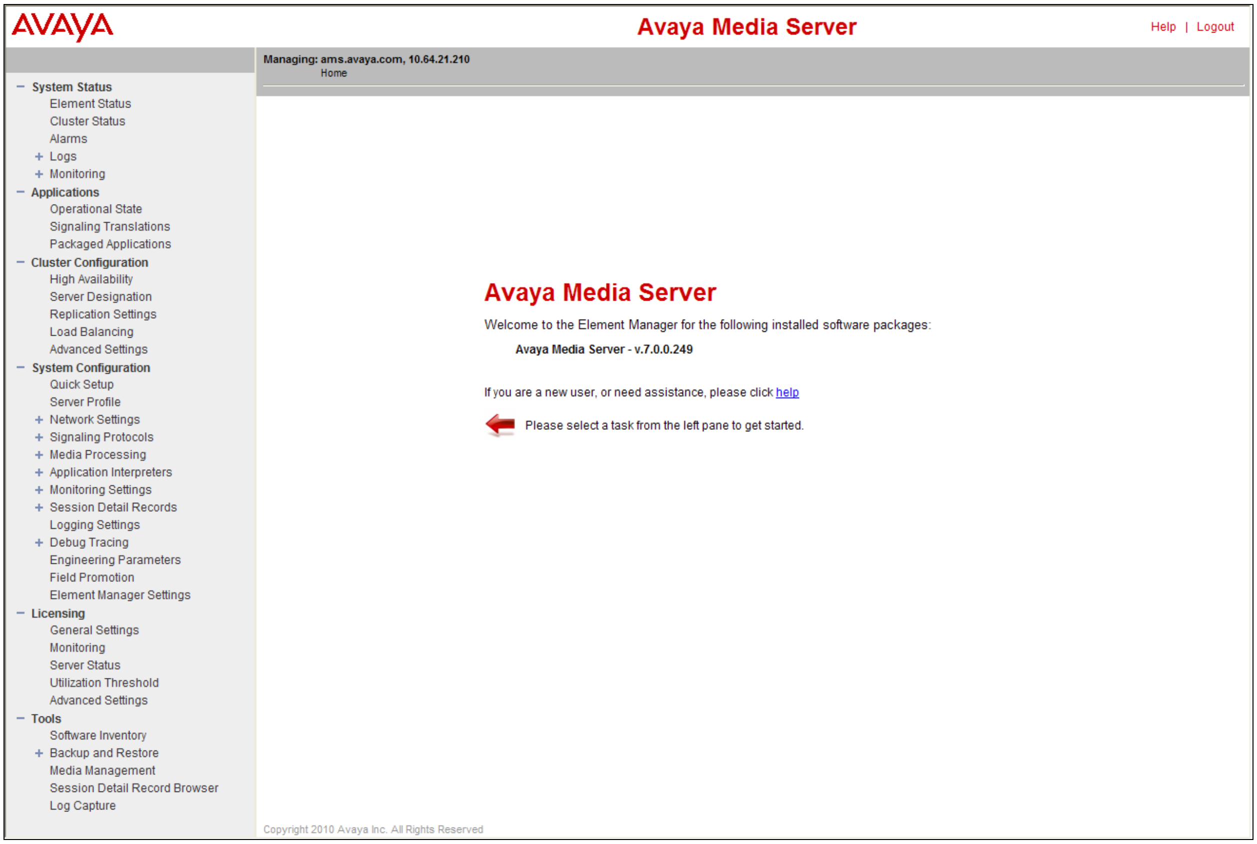
From a web browser, enter the following URL to access the Media Server web interface: https:<*ip-address*>:8443/em/, where <*ip-address*> is the IP address of the Media server. The following User Login page is presented. Log in using the appropriate credentials.



Use this page to access local management functions for this server.

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 Media Server

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

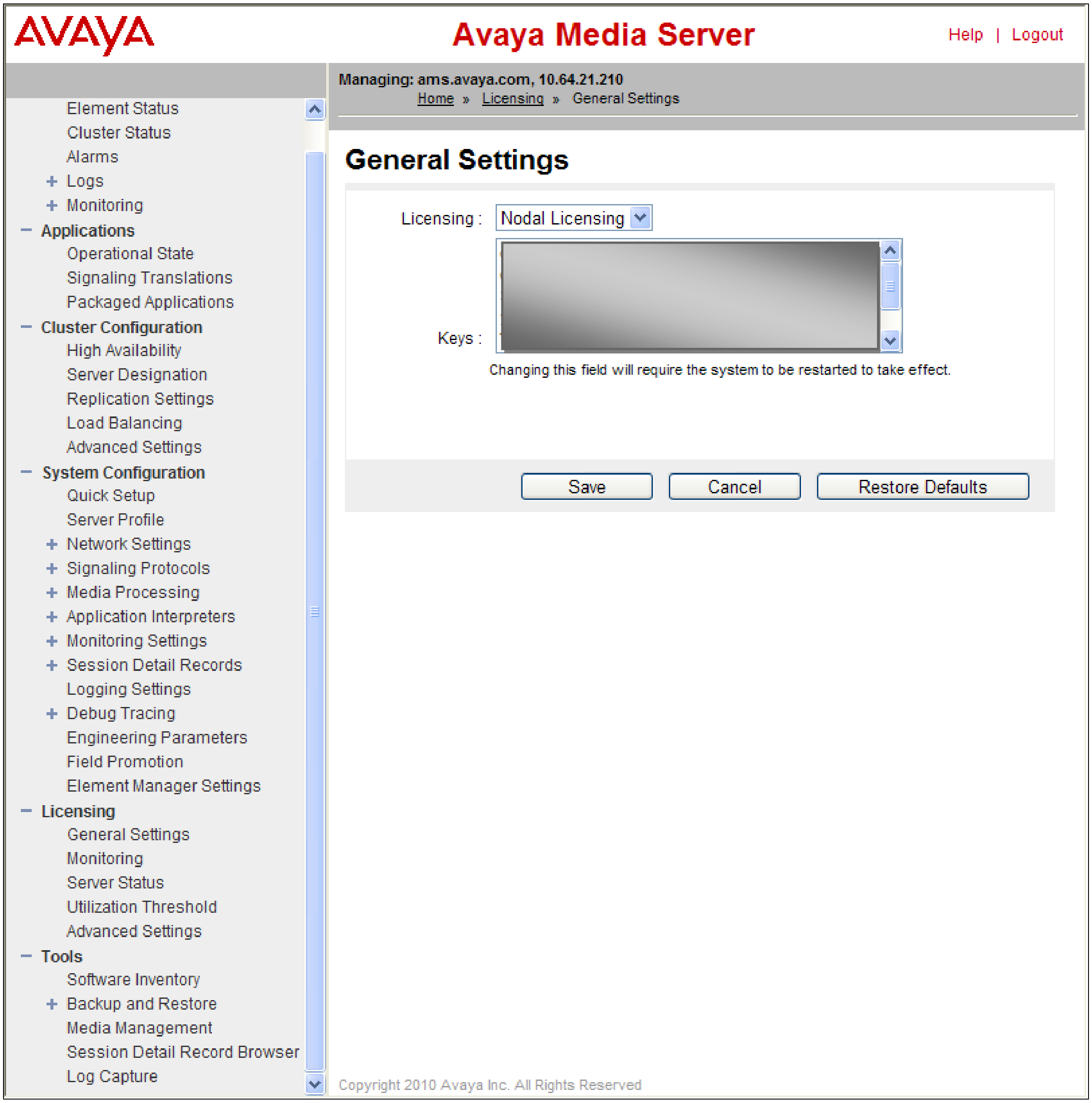
Avaya Media Server - v.7.0.0.249

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.



Managing: ams.avaya.com, 10.64.21.210

General Settings

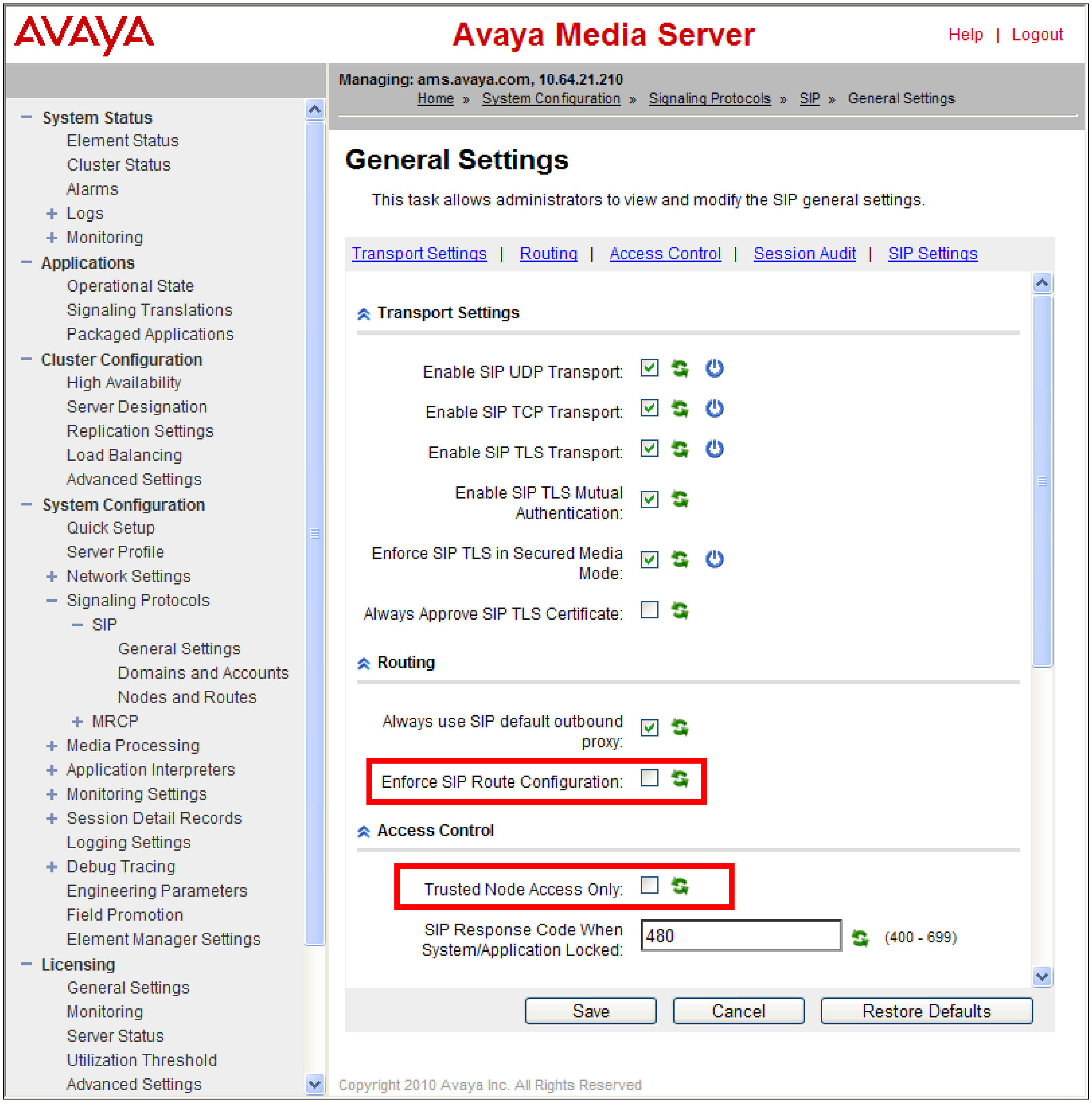
Licensing : Nodal Licensing

Keys : [redacted]

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

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**.



General Settings

This task allows administrators to view and modify the SIP general 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: ☐

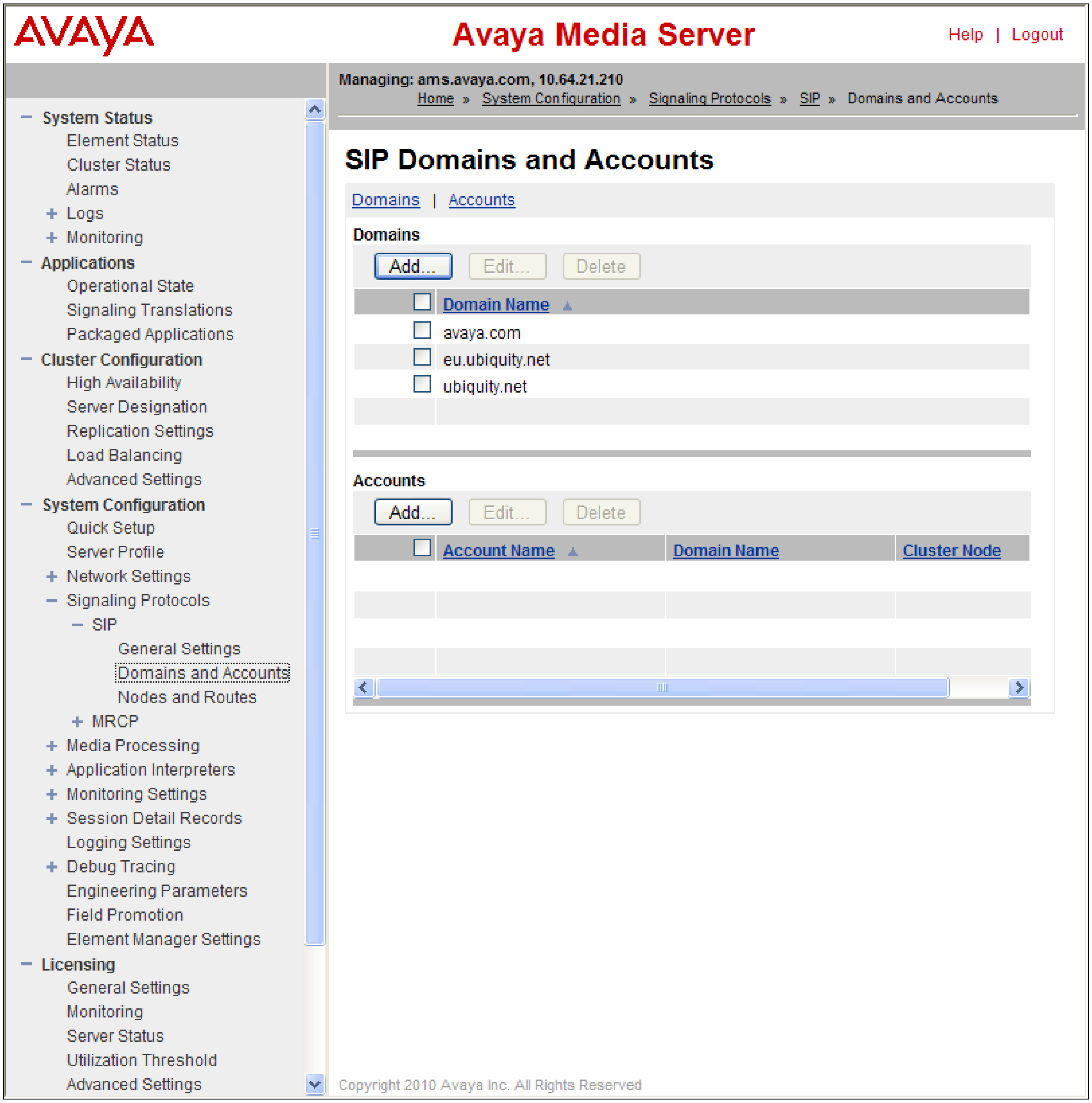
Routing

Always use SIP default outbound proxy: ☑
Enforce SIP Route Configuration: ☐

Access Control

Trusted Node Access Only: ☐
SIP Response Code When System/Application Locked: 480 (400 - 699)

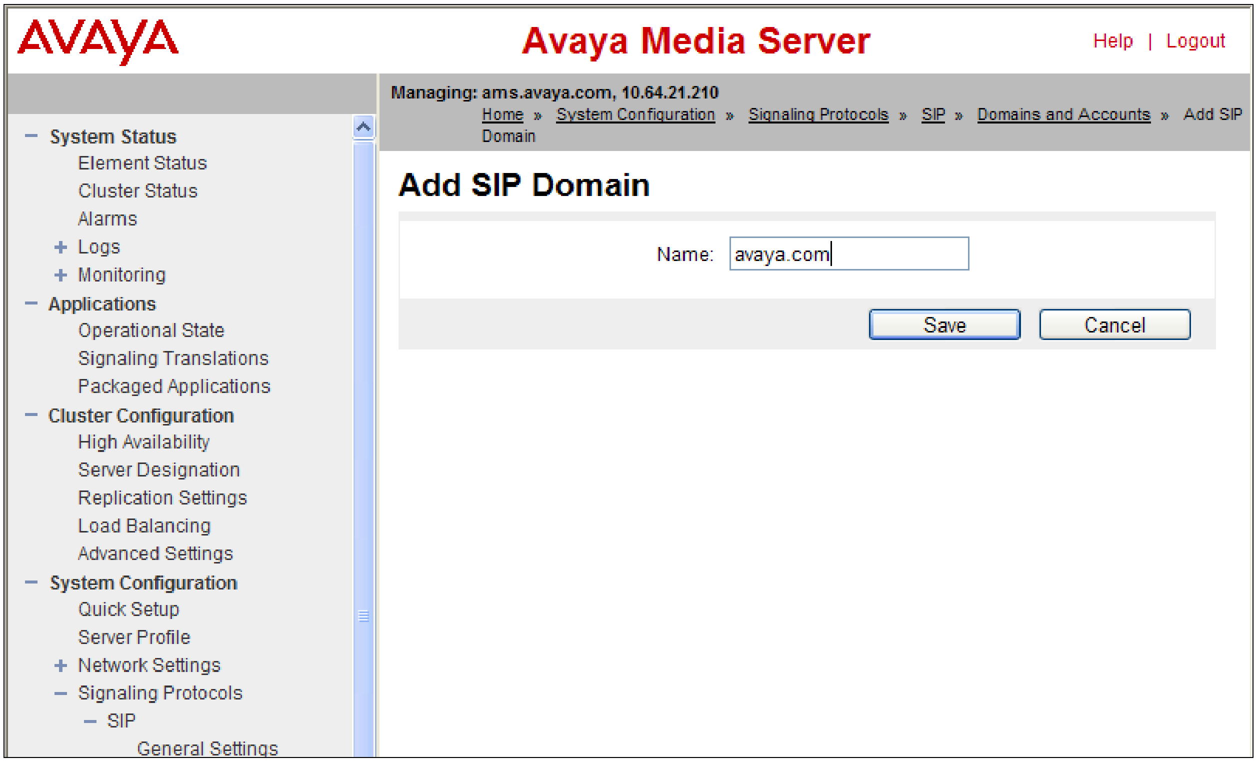
In the navigation pane on the left, navigate to **System Configuration → Signaling Protocols → SIP → Domains and Accounts**. On the SIP Domains and Accounts page, add the domain names required for the network. During compliance testing, avaya.com was added.



☐	Domain Name
☐	avaya.com
☐	eu.ubiquity.net
☐	ubiquity.net

☐	Account Name	Domain Name	Cluster Node

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**.



Name: avaya.com

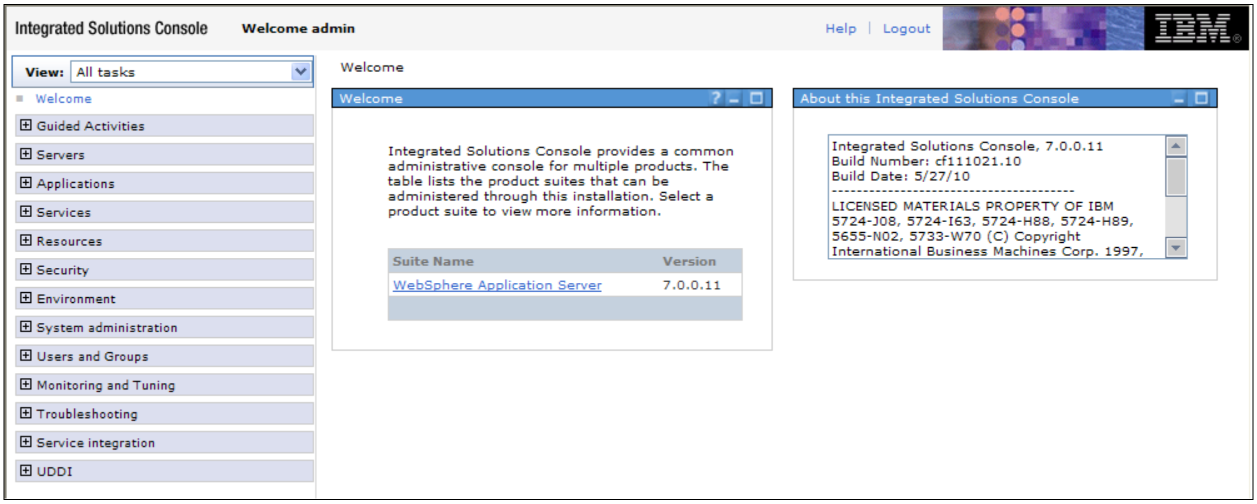
Copy media files to the Avaya Media Server:

- 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 following Welcome page is displayed.



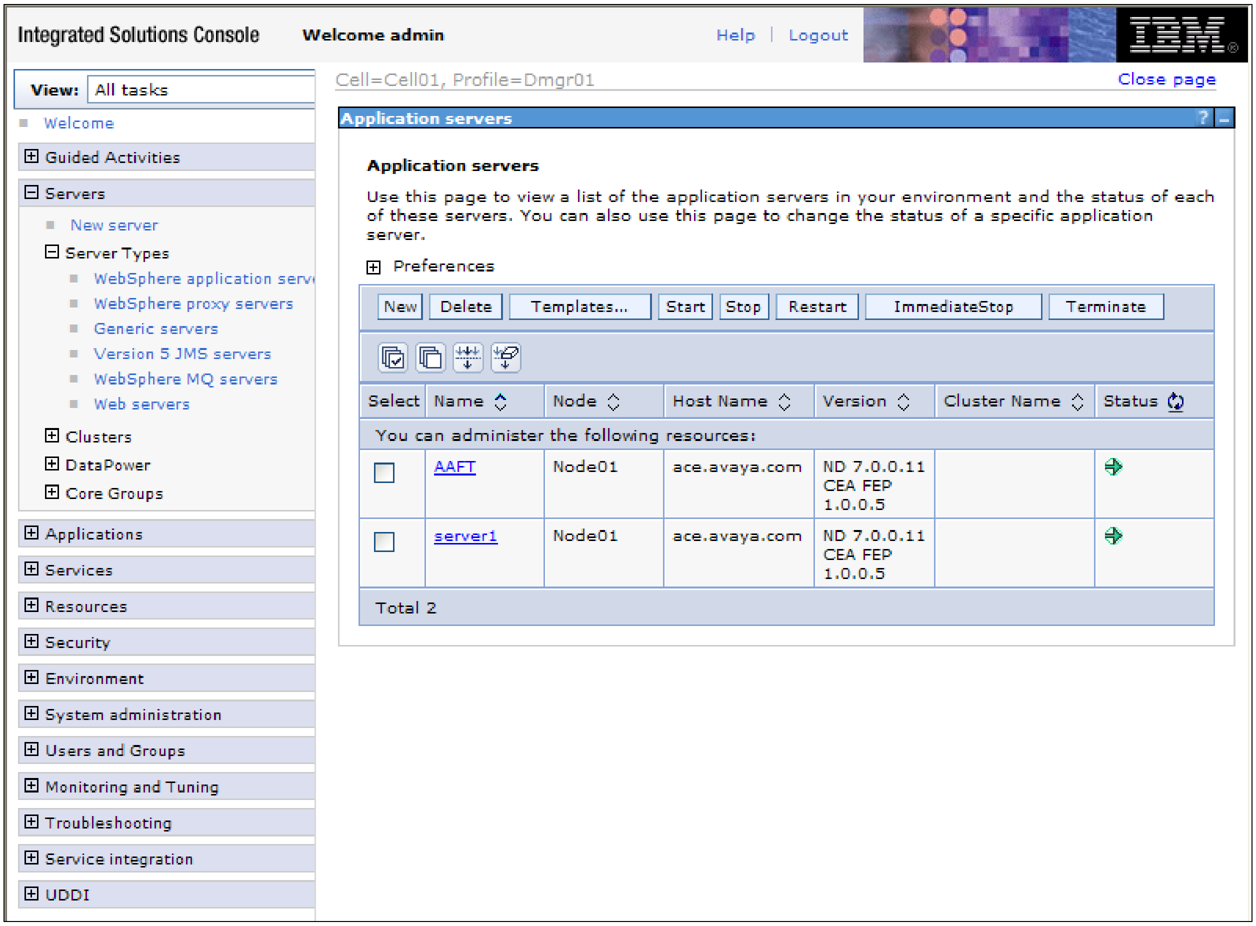
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	7.0.0.11

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).



Application servers

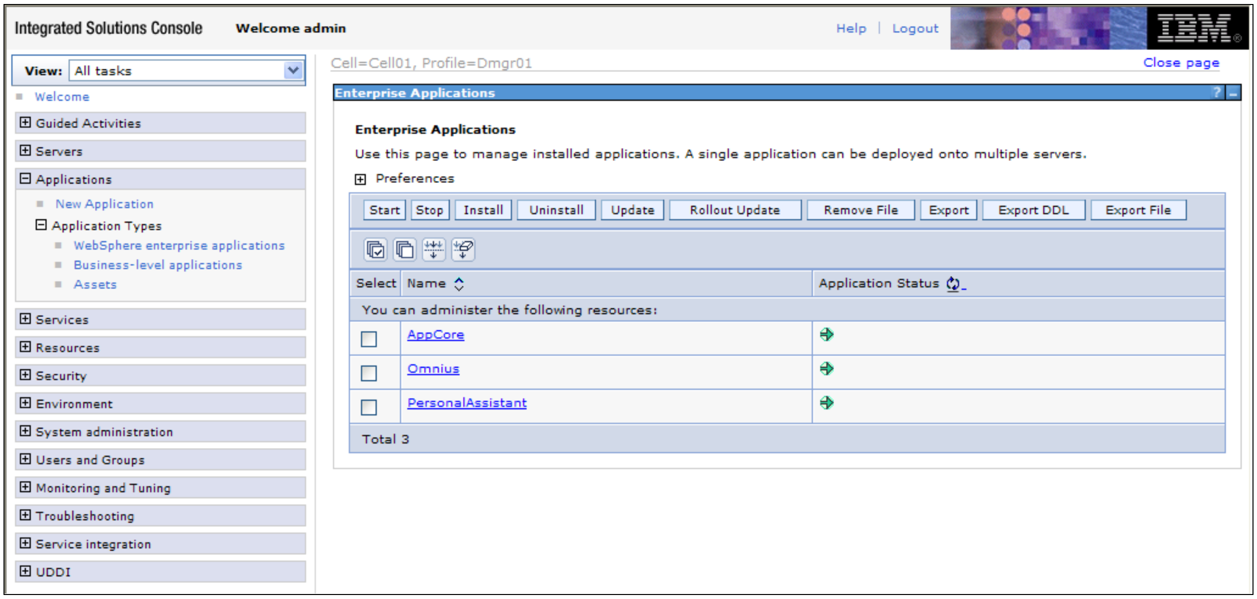
Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.

Select	Name	Node	Host Name	Version	Cluster Name	Status
You can administer the following resources:						
☐	AAFT	Node01	ace.avaya.com	ND 7.0.0.11 CEA FEP 1.0.0.5		➡
☐	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.



Cell=Cell01, Profile=Dmgr01

Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Select	Name	Application Status
You can administer the following resources:		
☐	AppCore	➔
☐	Omnius	➔
☐	PersonalAssistant	➔
Total 3		

8. Configure Avaya Aura® Communication Manager Feature Server

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

```
display system-parameters customer-options                      Page   2 of   11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 0
             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 0
                       Maximum Administered SIP Trunks: 24000 10
  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   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   1
          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.)
```

Step	Description
2.	**IP network region** Use the **display ip-network-region** command to view the network region settings. The values shown below are the values used during compliance testing. ▪ **Authoritative Domain**: ***avaya.com*** 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**: ***no*** **Inter-region IP-IP Direct Audio**: ***no*** 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**: ***1*** The codec set contains the list of codecs available for calls within this IP network region.

```
display ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
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                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Step	Description
3.	**Codecs** 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.

```
change 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: G.729             n         2        20
 3:
```

Step	Description
4.	**Node Names** 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.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
GATEWAY             10.64.21.1
SM_21_31            10.64.21.31
default             0.0.0.0
medpro1a03          10.64.21.84
procr               10.64.21.40
procr6              ::
```

Step	Description
5.	**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. ▪ **Group Type**: ***sip*** ▪ **IMS Enabled?**: ***y*** This field is set to ***y*** for a Communication Manager configured as an Feature server. When configuring Communication Manager as an Evolution Server, set this field to ***n***. ▪ **Transport Method: *tls*** ▪ **Peer Detection Enabled?**: ***y*** ▪ **Peer Server: *SM*** This field will automatically be populated when the **Peer Detection Enabled?** field is set to ***y***. ▪ **Near-end Node Name**: ***procr*** 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**: ***5061*** The listening port for Communication Manager. ▪ **Far-end Node Name**: ***SM_21_31*** This node name maps to the IP address of Session Manager. ▪ **Fear-end Listen Port**: ***5061*** The listening port for Session Manager. ▪ **Far-end Network Region**: ***1*** This defines the IP network region which contains Session Manager. ▪ **Far-end Domain**: ***avaya.com*** This domain is sent in the "To" header of SIP messages of calls using this signaling group. ▪ **Direct IP-IP Audio Connections**: ***n*** Direct IP-IP Audio Connections must be disabled for signaling groups using Foundation Toolkit services.

```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? y        Transport Method: tls
        Q-SIP? n                                             SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: SM_21_31
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: avaya.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

Step	Description
6.	**Trunk Group** 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. ▪ **Group Type:** ***sip*** This field sets the type of the trunk group. ▪ **Group Name:** Any descriptive name may be used (if desired). ▪ **TAC:** ***101*** Enter an valid value consistent with the Communication Manager dial plan. ▪ **Service Type:** ***tie*** Set to tie. ▪ **Member Assignment Method:** ***auto*** Set to Auto. ▪ **Signaling Group**: ***1*** This field is set to the signaling group shown in the previous step. ▪ **Number of Members:** ***10*** 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.

```
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: 10
```

Step	Description
	Trunk Group – continued On **Page 3**: ▪ The **Numbering Format** field was set to ***private***. 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.

```
display trunk-group 1                                         Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                   Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Step	Description
7.	**Private Numbering** 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.

```
display private-numbering 0                                   Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 5  5                                          5     Total Administered: 1
                                                        Maximum Entries: 540
```

Step	Description
8.	**Automatic Alternate Routing** Automatic Alternate Routing (AAR) was used to route local calls to Session Manager. Use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table. The example below shows dialed strings that begin with ***5*** and are ***5*** digits long use route pattern ***1*** (to Session Manager).

```
display aar analysis 0                                            Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    5                    5    5     1        aar          n
```

Step	Description
9.	**Automatic Route Selection** Automatic Route Selection (ARS) was used to route PSTN calls to Session Manager. Session Manager then routed the calls to the Communication Manager Evolution Server which was configured with a trunk to the PSTN (not shown). 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 ***130*** and are ***11*** digits long use route pattern ***1*** (to Session Manager).

```
change ars analysis 130                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    130                  11   11    1        hnpa         n
```

Step	Description
10.	**Route Pattern** Route pattern 1 was used to route calls to Session Manager. Route pattern 1 was configured using the parameters highlighted below. ▪ **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.

```
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                    0                                         n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     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
```

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.

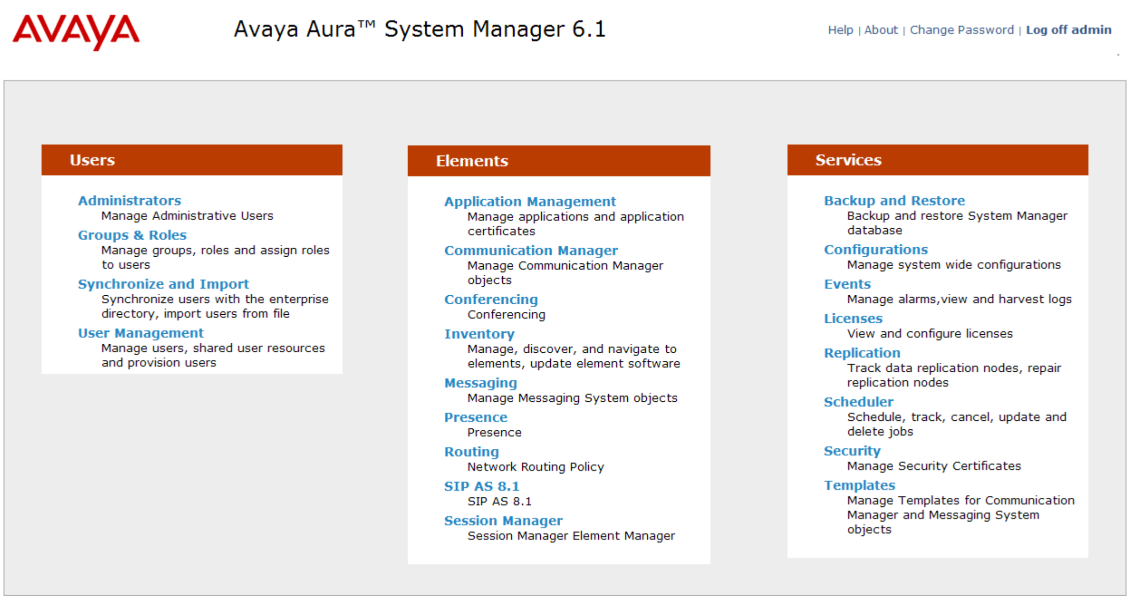
The Session Manager server provides the network interface for all inbound and outbound SIP signaling to all provisioned SIP entities. During compliance testing, the IP address assigned to the Security Module interface is 10.64.21.31 as specified in **Figure 1**. The Session Manager server also has a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

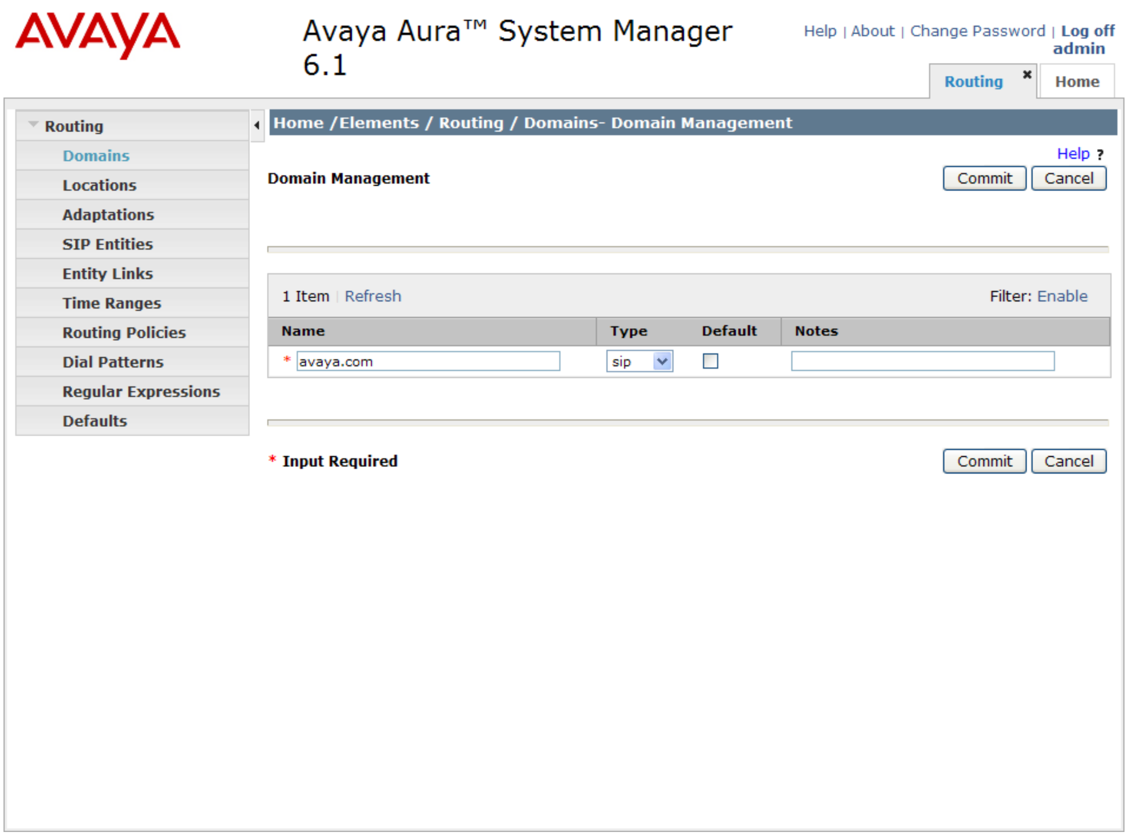
The procedures described in this section include configurations for the following:

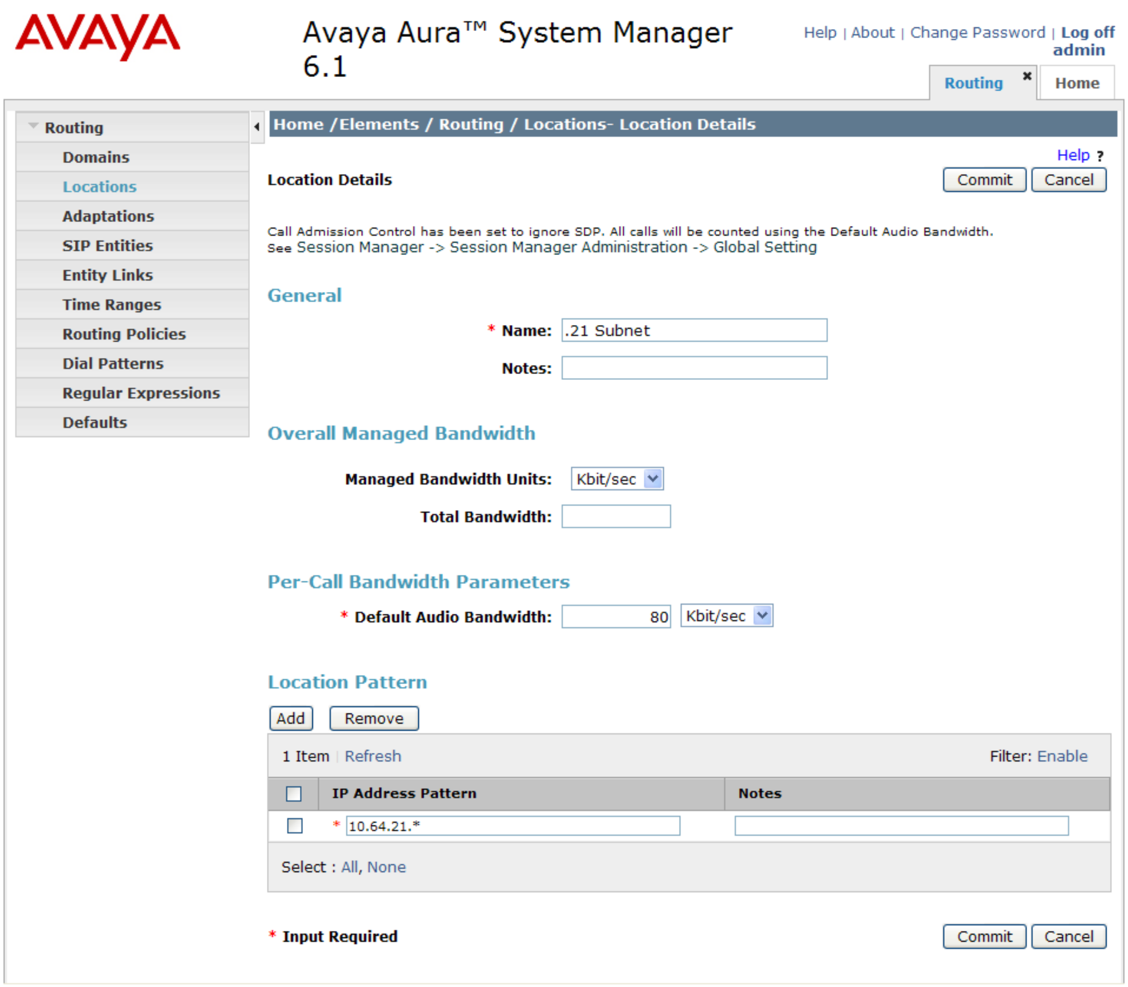
- **SIP Domains** – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls 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.
- **Users** – Users that register with Session Manager.

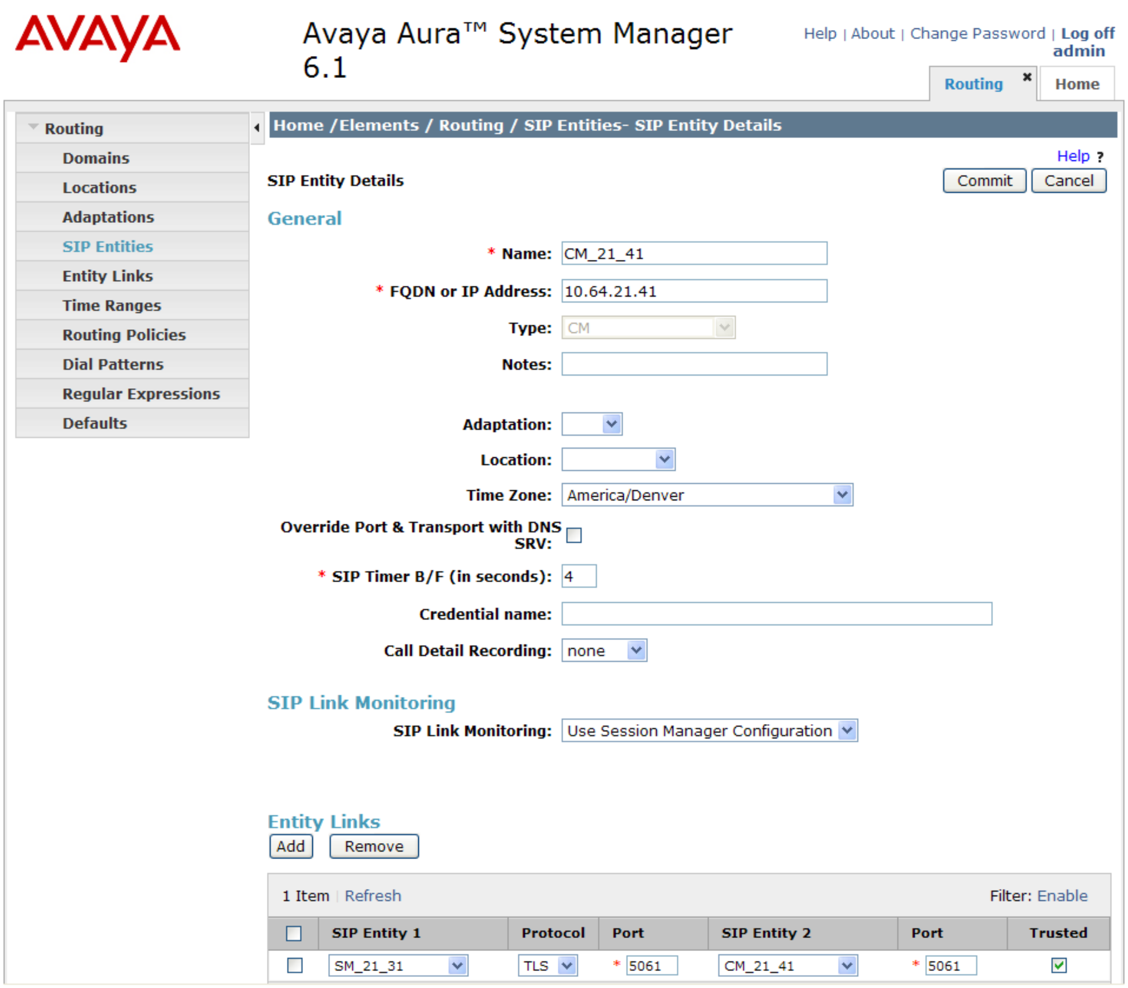
Step	Description
1.	**Login** Access the Session Manager administration web interface by entering https://<*ip-addr*>/network-login/ as the URL in an Internet browser, where <*ip-addr*> is the IP address of the System Manager server. Log in using appropriate credentials. The main page for the administrative interface is shown below.  Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin **Users** Administrators – Manage Administrative Users Groups & Roles – Manage groups, roles and assign roles to users Synchronize and Import – Synchronize users with the enterprise directory, import users from file User Management – Manage users, shared user resources and provision users **Elements** Application Management – Manage applications and application certificates Communication Manager – Manage Communication Manager objects Conferencing – Conferencing Inventory – Manage, discover, and navigate to elements, update element software Messaging – Manage Messaging System objects Presence – Presence Routing – Network Routing Policy SIP AS 8.1 – SIP AS 8.1 Session Manager – Session Manager Element Manager **Services** Backup and Restore – Backup and restore System Manager database Configurations – Manage system wide configurations Events – Manage alarms,view and harvest logs Licenses – View and configure licenses Replication – Track data replication nodes, repair replication nodes Scheduler – Schedule, track, cancel, update and delete jobs Security – Manage Security Certificates Templates – Manage Templates for Communication Manager and Messaging System objects

Step	Description
2.	**Add SIP Domain** The **Routing** menu contains all the configuration tasks listed at the beginning of this section. During compliance testing, one SIP Domain was configured. Navigate to **Routing→Domains**, and click the **New** button (not shown) to add the SIP domain with • **Name**: ***avaya.com*** (as set in **Section 8, Step 2**) • **Notes**: optional descriptive text Click **Commit** to save the configuration.  Avaya Aura™ System Manager 6.1 Home /Elements / Routing / Domains- Domain Management Domain Management 1 Item Refresh Filter: Enable Name: * avaya.com Type: sip Default: ☐ Notes: * Input Required

Step	Description
3.	**Add Location** Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured at each site for compliance testing. Navigate to **Routing→Locations** and click the **New** button (not shown) to add the Location. Under **General**: - **Name**: a descriptive name - **Notes**: optional descriptive text Under **Location Pattern**, click the **Add** button to add a new line: - **IP Address Pattern**: ***10.64.21.**** - **Notes**: optional descriptive text Click **Commit** to save the configuration.  Home /Elements / Routing / Locations- Location Details Location Details Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting General * Name: .21 Subnet Notes: Overall Managed Bandwidth Managed Bandwidth Units: Kbit/sec Total Bandwidth: Per-Call Bandwidth Parameters * Default Audio Bandwidth: 80 Kbit/sec Location Pattern ☐ IP Address Pattern | Notes ☐ * 10.64.21.* | * Input Required

Step	Description
4.	**Add SIP Entities** 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. 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 Feature Server are as follows: Under **General**: • **Name**: a descriptive name • **FQDN or IP Address**: ***10.64.21.40*** as specified in **Figure 1**. • **Type**: select ***CM*** Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

Step	Description
	Add SIP Entities (continued) – Communication Manager Evolution Server The screen below shows the SIP Entity configuration details for the Communication Manager Evolution Server.



SIP Entity Details

General

* Name: CM_21_41

* FQDN or IP Address: 10.64.21.41

Type: CM

Notes:

Adaptation:

Location:

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

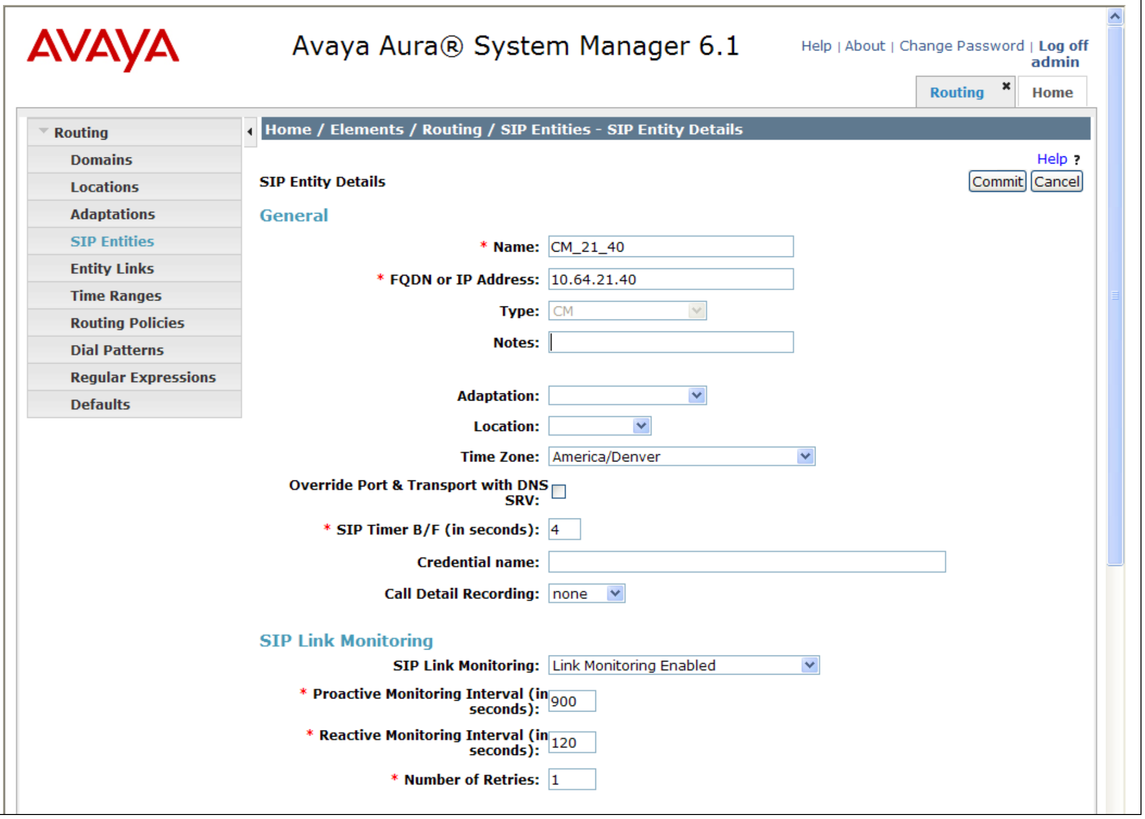
SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item | Refresh Filter: Enable

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM_21_31	TLS	* 5061	CM_21_41	* 5061	☑

Step	Description
	Add SIP Entities (continued) – Communication Manager Feature Server The screen below shows the SIP Entity configuration details for the Communication Manager Feature Server. Note the ***CM*** selection for **Type**. 

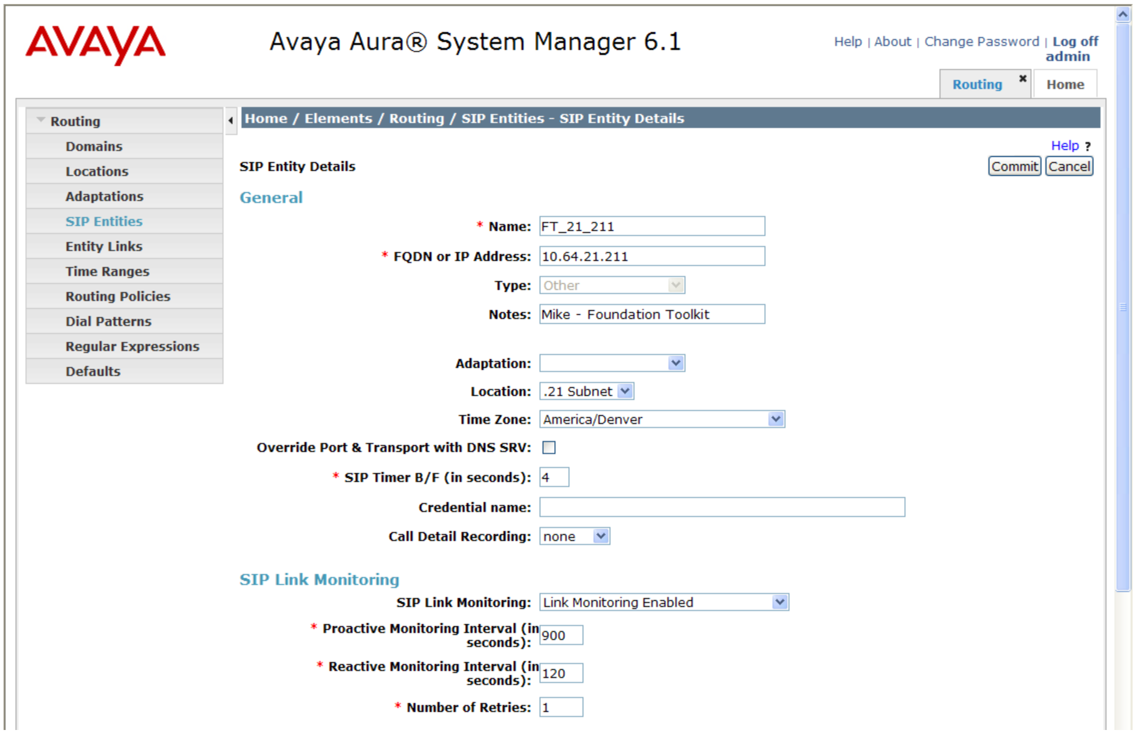
SIP Entity Details

General

* Name: CM_21_40
* FQDN or IP Address: 10.64.21.40
Type: CM
Notes:
Adaptation:
Location:
Time Zone: America/Denver
Override Port & Transport with DNS SRV: ☐
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled
* Proactive Monitoring Interval (in seconds): 900
* Reactive Monitoring Interval (in seconds): 120
* Number of Retries: 1

Step	Description
	Add SIP Entities (continued) – ACE/Foundation Toolkit Server The screen below shows the SIP Entity configuration details for the ACE/Foundation Toolkit server. Note the ***Other*** selection for **Type**.  SIP Entity Details General * Name: FT_21_211 * FQDN or IP Address: 10.64.21.211 Type: Other Notes: Mike - Foundation Toolkit Adaptation: Location: .21 Subnet Time Zone: America/Denver Override Port & Transport with DNS SRV: ☐ * SIP Timer B/F (in seconds): 4 Credential name: Call Detail Recording: none SIP Link Monitoring SIP Link Monitoring: Link Monitoring Enabled * Proactive Monitoring Interval (in seconds): 900 * Reactive Monitoring Interval (in seconds): 120 * Number of Retries: 1

Step	Description
5.	**Add Entity Links**

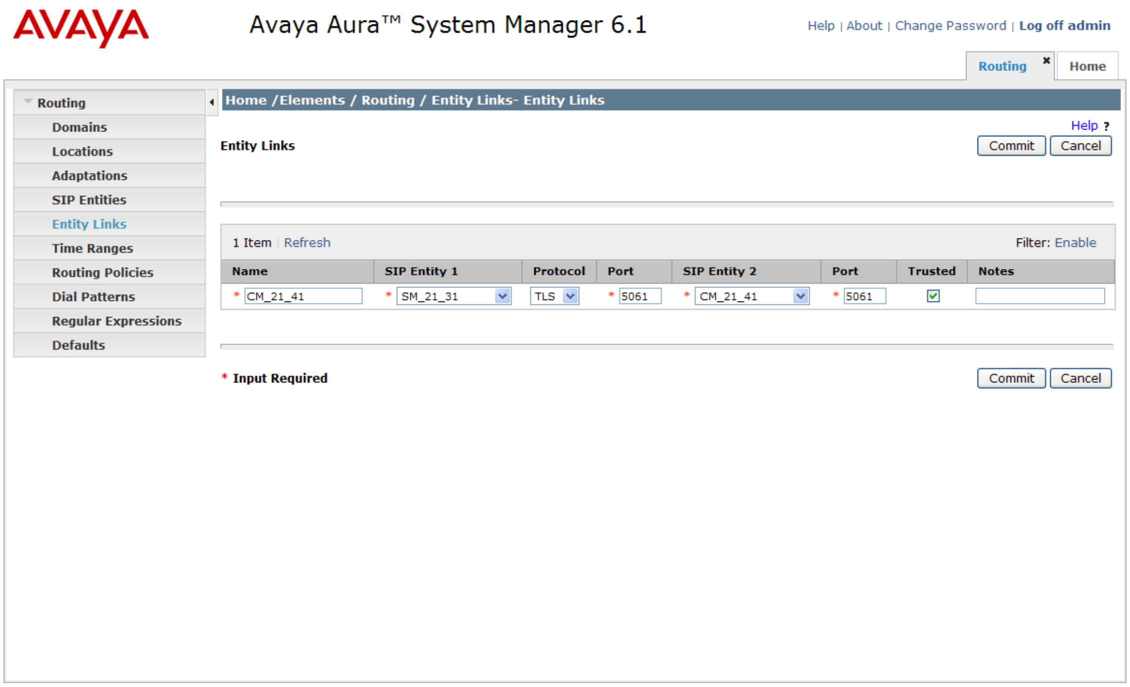
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Three Entity Links were created:

- Session Manager ←→ Communication Manger (Evolution Server)
- Session Manager ←→ Communication Manger (Feature Server)
- Session Manager ←→ Foundation Toolkit Server

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.

- **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

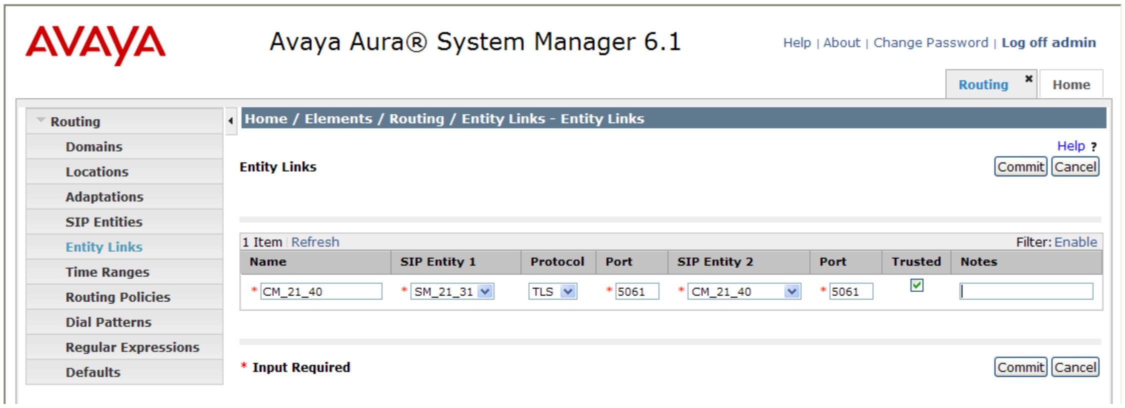
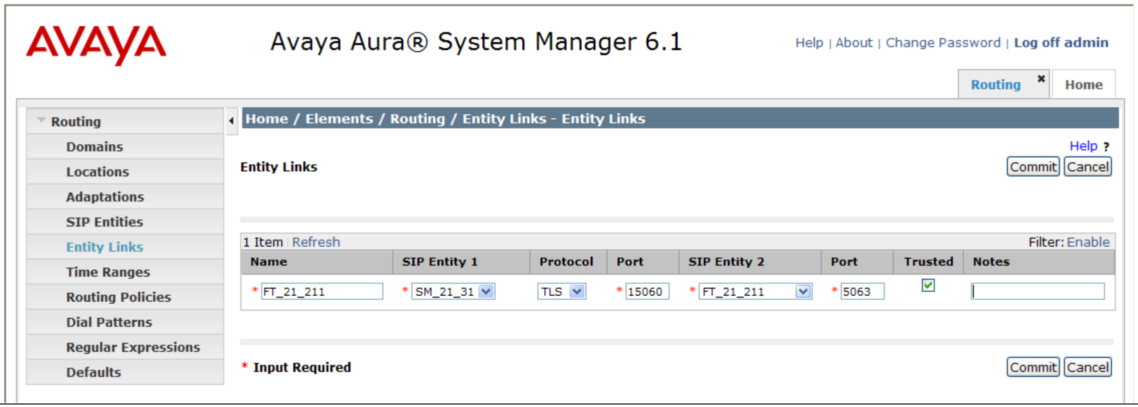
Click **Commit** to save the configuration.



Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CM_21_41	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	☑	

* Input Required

Step	Description
	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.  Home / Elements / Routing / Entity Links - Entity Links Entity Links 1 Item Name: CM_21_40 SIP Entity 1: SM_21_31 Protocol: TLS Port: 5061 SIP Entity 2: CM_21_40 Port: 5061 Trusted: ☑ Notes: * Input Required
	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.  Home / Elements / Routing / Entity Links - Entity Links Entity Links 1 Item Name: FT_21_211 SIP Entity 1: SM_21_31 Protocol: TLS Port: 15060 SIP Entity 2: FT_21_211 Port: 5063 Trusted: ☑ Notes: * Input Required

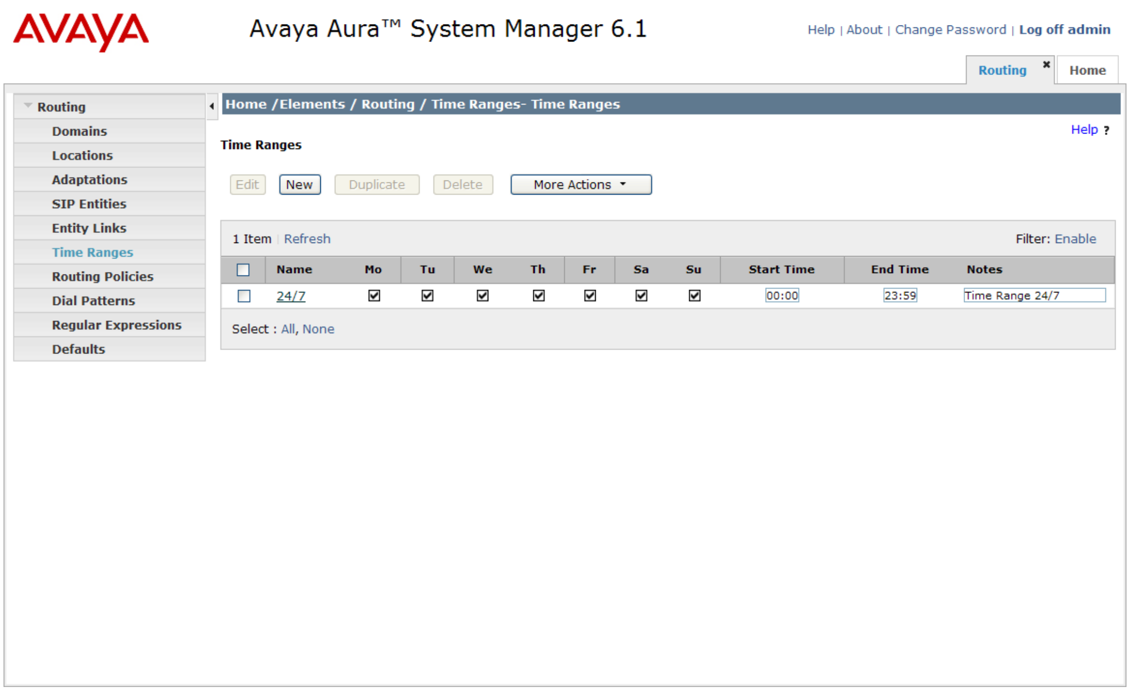
Step	Description
6.	**Add Time Ranges**

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.

Navigate to **Routing→Time Ranges**, and click the **New** button to add a new Time Range:

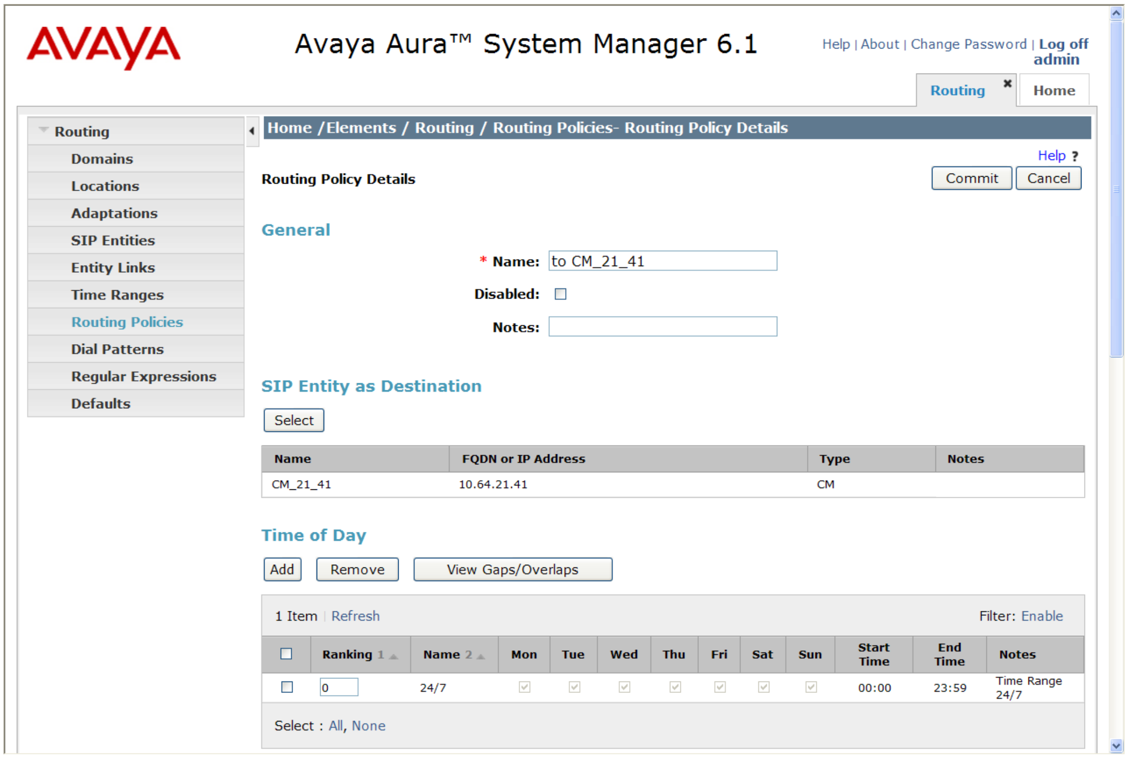
- **Name**: a descriptive name
- **Mo** through **Su**: check the box under each of these headings
- **Start Time**: enter ***00:00***
- **End Time**: enter ***23:59***

Click **Commit** to save this time range. The screen below shows the configured Time Range.



☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Step	Description
7.	**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. Navigate to **Routing→Routing Policies**, and click the **New** button (not shown) to add a new Routing Policy. Under **General**: • **Name**: a descriptive name • **Notes**: optional descriptive text Under **SIP Entity as Destination** Click **Select** to select the appropriate SIP Entity to which the routing policy applies (not shown). Under **Time of Day** Click **Add** to select the Time Range configured in the previous step (not shown). Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

Step	Description
	Add Routing Policies (continued) The screen below shows the configuration details for the Routing Policy to route calls to the Communication Manager (Evolution Server). 

Routing Policy Details

General

* Name: to CM_21_41

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM_21_41	10.64.21.41	CM	

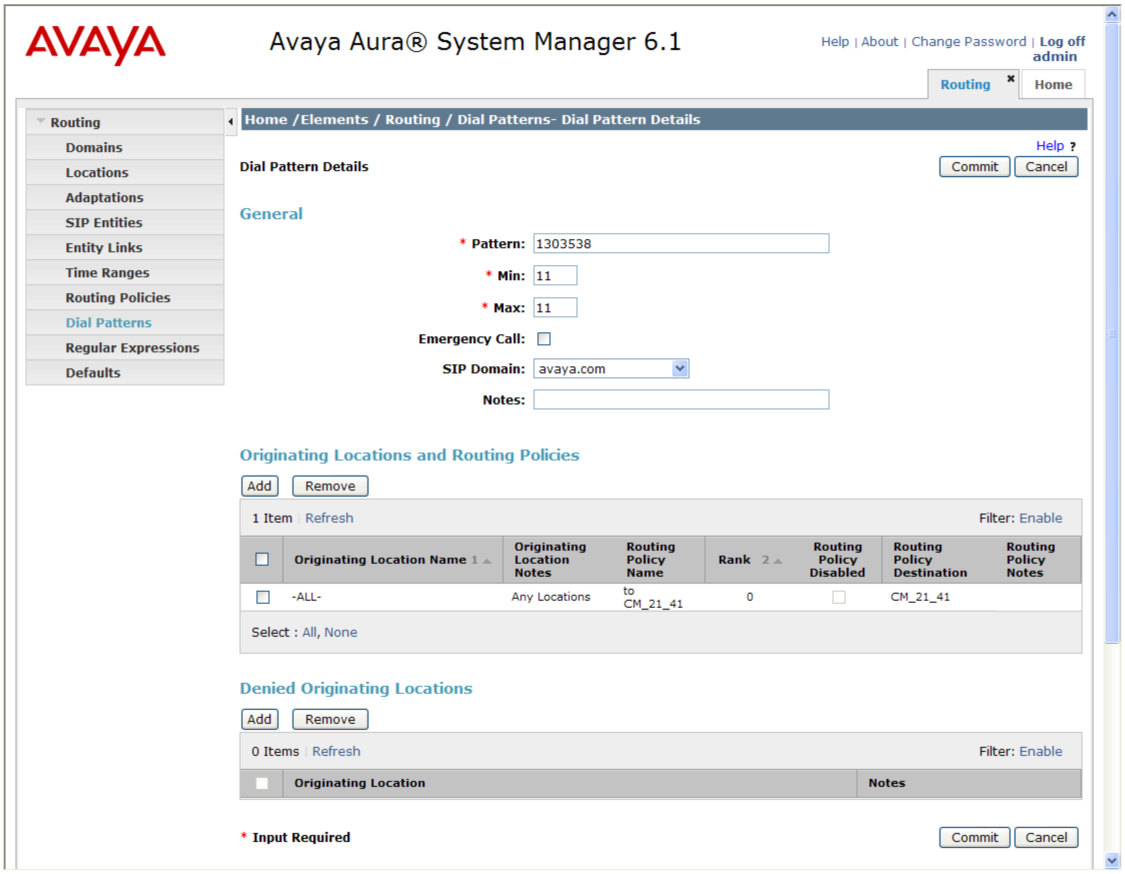
Time of Day

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Step	Description
8.	**Add Dial Patterns** 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. Navigate to **Routing→Dial Patterns**, click the **New** button (not shown) to add a new Dial Pattern. Under **General**: • **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 Under **Originating Locations and Routing Policies** Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown). Under **Time of Day** Click **Add** to select the time range configured in **Step 6**. Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

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.



Dial Pattern Details

General

* Pattern: 1303538

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

1 Item | Refresh   Filter: Enable

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	to CM_21_41	0	☐	CM_21_41	

Select : All, None

Denied Originating Locations

0 Items | Refresh   Filter: Enable

☐	Originating Location	Notes

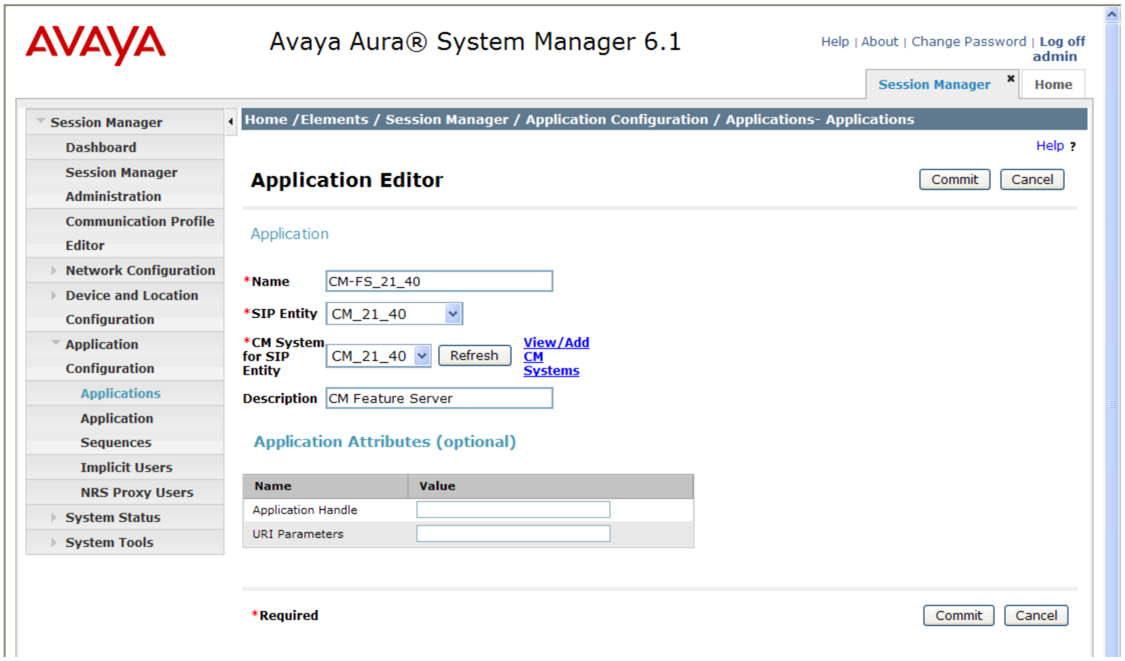
* Input Required

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 a new Application for the Communication Manager Feature Server:

- **Name**: a descriptive name
- **SIP Entity**: Select the Communication Manager Feature Server SIP entity
- **Description**: optional descriptive text



Application Editor

Application

*Name CM-FS_21_40
*SIP Entity CM_21_40
*CM System for SIP Entity CM_21_40
Description CM Feature Server

Application Attributes (optional)

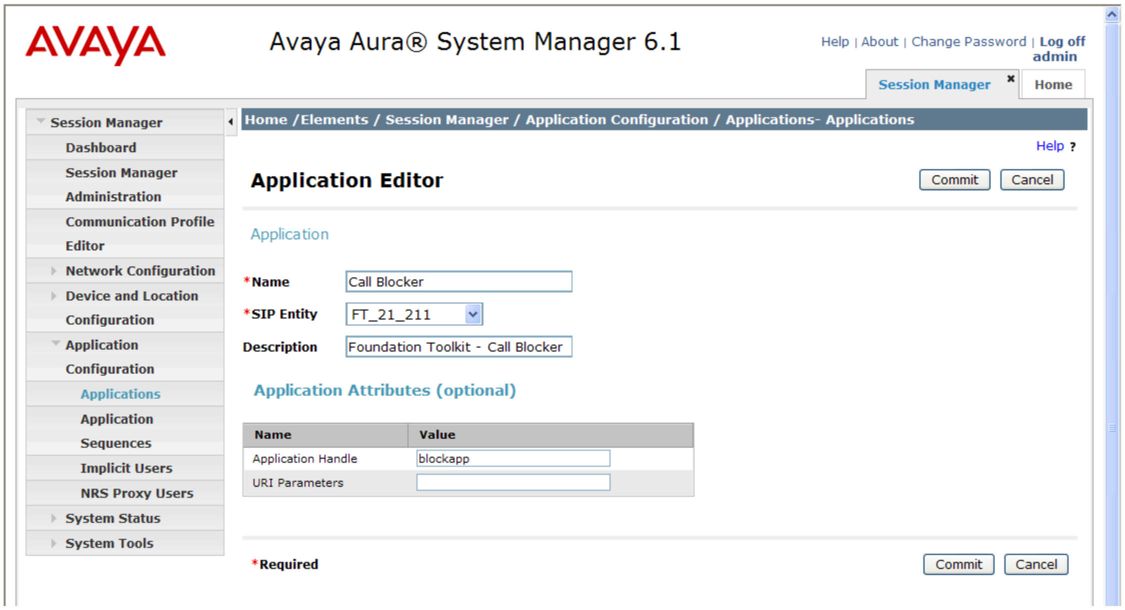
Name	Value
Application Handle	
URI Parameters	

*Required

Add Application (continued)
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.



*Name: Call Blocker
*SIP Entity: FT_21_211
Description: Foundation Toolkit - Call Blocker

Name	Value
Application Handle	blockapp
URI Parameters	

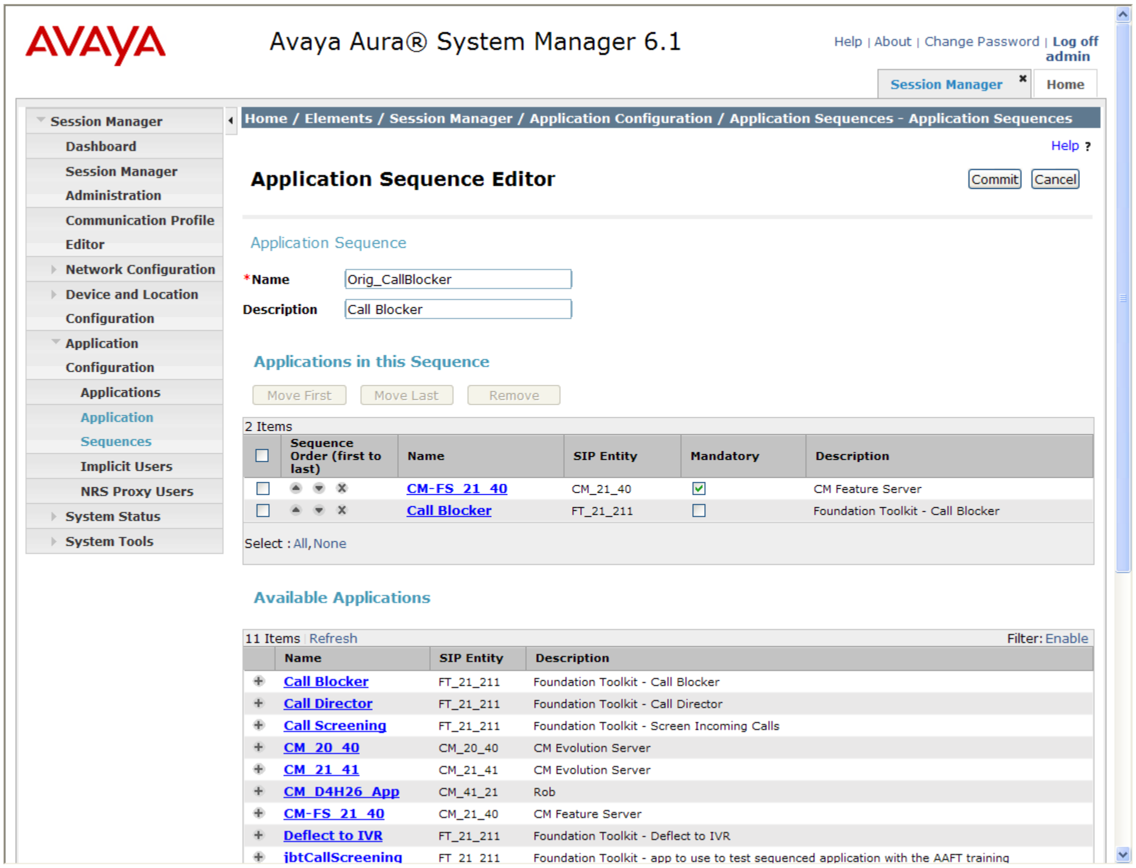
10. **Add Application Sequences**

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.

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 two Applications created in the previous step to move them up to **Applications in this Sequence**. The Communication Manager Feature Server application should be mandatory and first in the sequence order.

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



Application Sequence Editor

Application Sequence

*Name: Orig_CallBlocker

Description: Call Blocker

Applications in this Sequence

2 Items

☐	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
☐	▲ ▼ ✕	CM-FS_21_40	CM_21_40	☑	CM Feature Server
☐	▲ ▼ ✕	Call Blocker	FT_21_211	☐	Foundation Toolkit - Call Blocker

Available Applications

11 Items

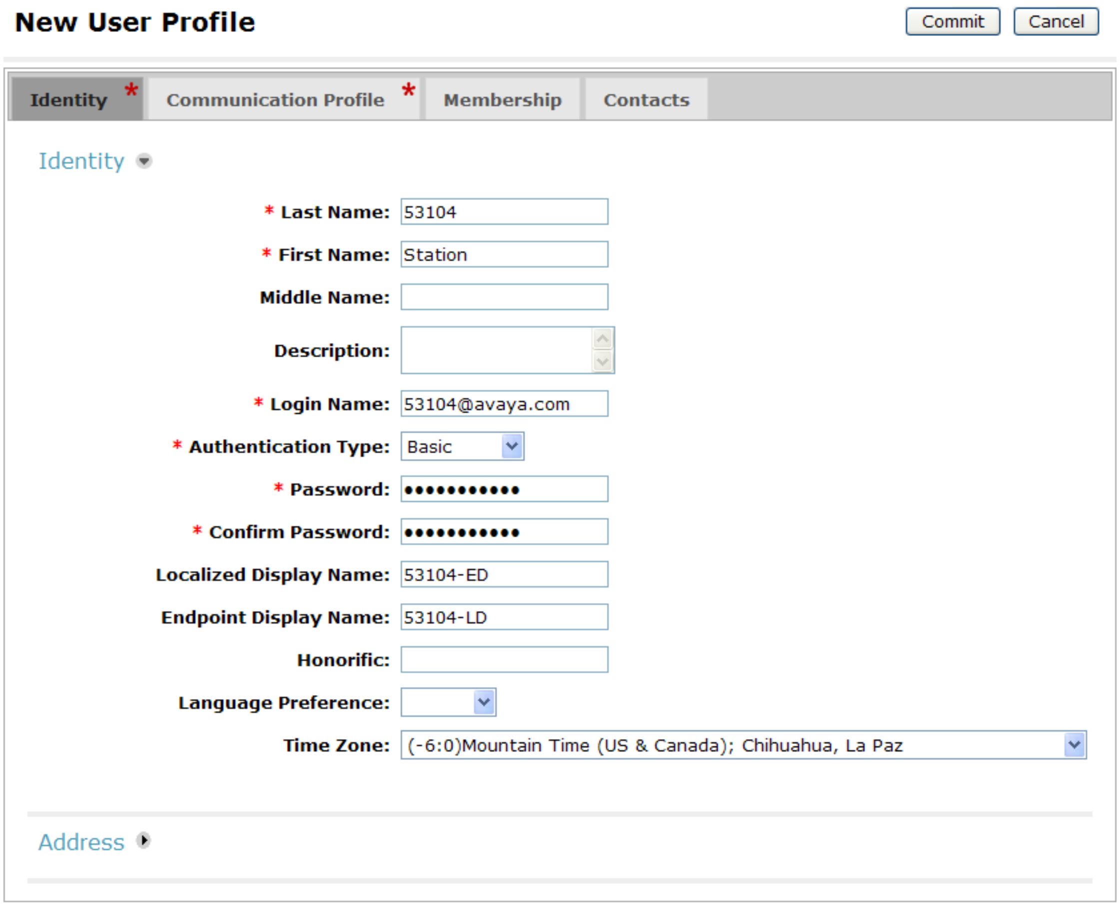
	Name	SIP Entity	Description
+	Call Blocker	FT_21_211	Foundation Toolkit - Call Blocker
+	Call Director	FT_21_211	Foundation Toolkit - Call Director
+	Call Screening	FT_21_211	Foundation Toolkit - Screen Incoming Calls
+	CM_20_40	CM_20_40	CM Evolution Server
+	CM_21_41	CM_21_41	CM Evolution Server
+	CM_D4H26_App	CM_41_21	Rob
+	CM-FS_21_40	CM_21_40	CM Feature Server
+	Deflect to IVR	FT_21_211	Foundation Toolkit - Deflect to IVR
+	jbtCallScreening	FT 21 211	Foundation Toolkit - app to use to test sequenced application with the AAFT training

11. **Add Users (users that register with Session Manager)**

To add a SIP user, navigate to **User Management → Manage Users →**, and click the **New** button to add a new User:

Under *Identity*:

- **Last**: Enter the last name of the user.
- **First**: Enter the first name of the user.
- **Login Name**: Enter a unique system login given to the user. It takes the form of username@domain (e.g. "53104@avaya.com") and it is used to create the user's primary handle.
- **Authentication Type**: Select "Basic" to have the user's login authenticated by an Avaya Authentication Server.
- **Password** and **Confirm Password**: Enter the password used to log into System Manger.
- **Localized Display Name**: Enter the localized display name of the user.
- **Endpoint Display Name**: Enter the full text name of the user represented in ASCII to support displays that cannot handle localized text.
- **Time Zone**: Select the preferred time zone of the user.



* Last Name: 53104

* First Name: Station

Middle Name:

Description:

* Login Name: 53104@avaya.com

* Authentication Type: Basic

* Password: ●●●●●●●●●●●

* Confirm Password: ●●●●●●●●●●●

Localized Display Name: 53104-ED

Endpoint Display Name: 53104-LD

Honorific:

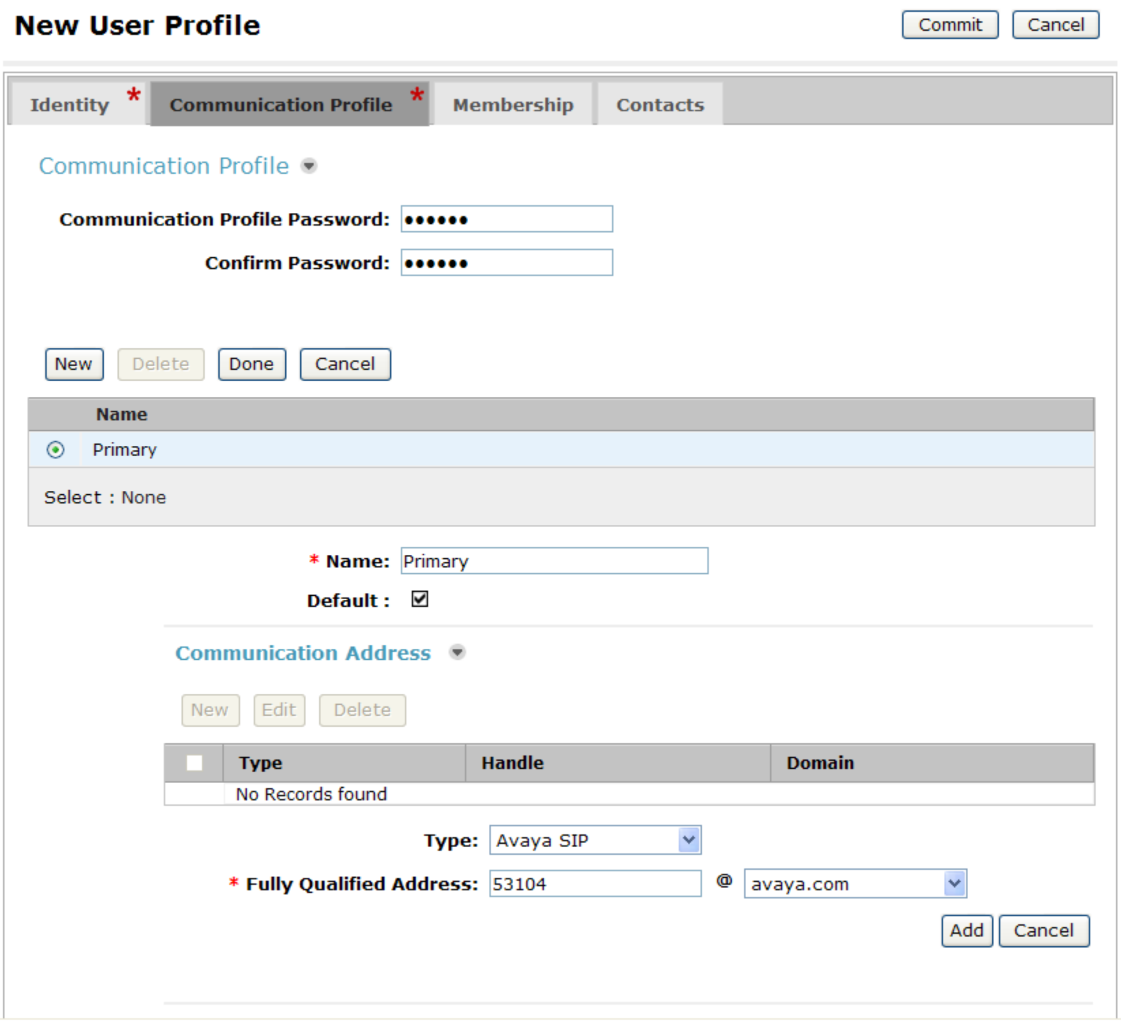
Language Preference:

Time Zone: (-6:0)Mountain Time (US & Canada); Chihuahua, La Paz

Add Users (continued – Communication Profile tab)

Under *Communication Profile*:

- **Communication Profile Password** and **Confirm Password**: Enter the user's station password/security code.
- **Type**: Select ***Avaya SIP***
- **Fully Qualified Address**: Enter the station's extension and select the appropriate domain for the user.
- Click the **Add** button.



Communication Profile Password: ••••••

Confirm Password: ••••••

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

☐	Type	Handle	Domain
	No Records found		

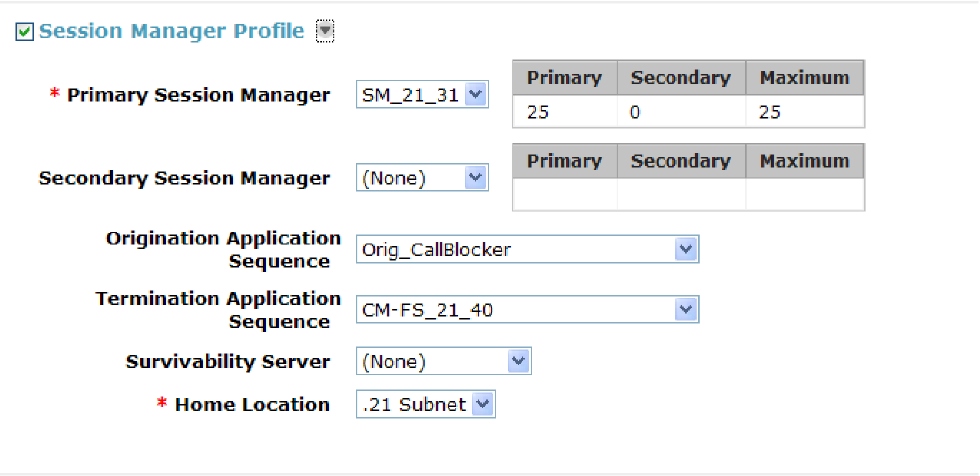
Type: Avaya SIP

* Fully Qualified Address: 53104 @ avaya.com

Add Users (continued – Communication Profile tab)

Under *Session Manager Profile*:

- **Primary Session Manager**: Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile.
- **Origination Application Sequence**: Select the Application Sequence from **Step 10** that will be invoked when calls are routed from this user.
- **Termination Application Sequence**: Select an Application Sequence that will be invoked when calls are routed to this user.
- **Home Location**: Select the Home Location of this user.



☑ Session Manager Profile

* Primary Session Manager: SM_21_31

Primary	Secondary	Maximum
25	0	25

Secondary Session Manager: (None)

Primary	Secondary	Maximum

Origination Application Sequence: Orig_CallBlocker

Termination Application Sequence: CM-FS_21_40

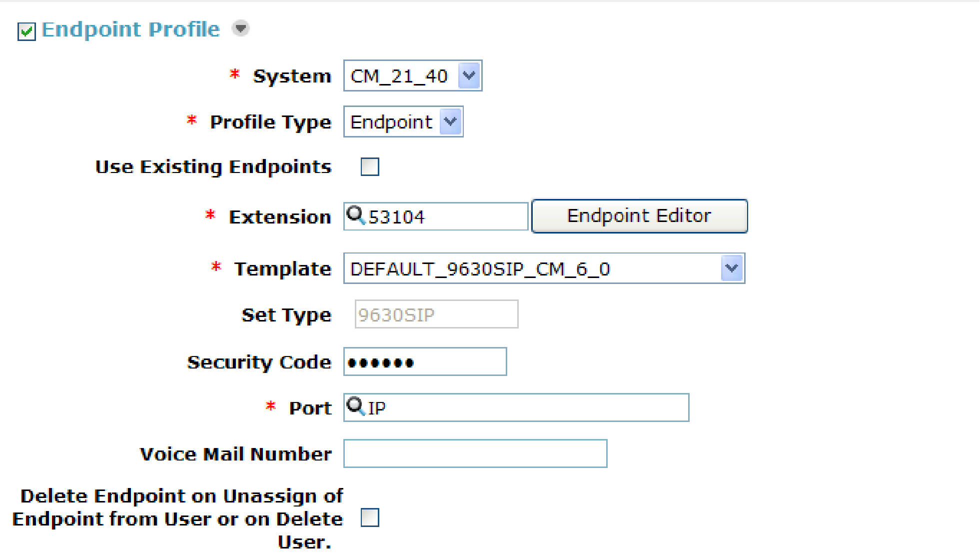
Survivability Server: (None)

* Home Location: .21 Subnet

Add Users (continued – Communication Profile tab)

Under *Endpoint Profile*:

- **System**: Select the Communication Manager system where the endpoint exists.
- **Profile Type**: Select ***Endpoint***.
- **Use Existing Endpoints:** Check this box to use an endpoint already administered in Communication Manager. Otherwise, leave the box unchecked.
- **Extension**: Enter the extension of the endpoint that you want to associate with this user.
- **Template**: Select an appropriate template for the endpoint.
- **Security Code**: Enter the security code to be used by the endpoint when registering to the Session Manager.
- **Port**: Select ***IP***.



☑ Endpoint Profile

* System: CM_21_40

* Profile Type: Endpoint

Use Existing Endpoints: ☐

* Extension: 53104

* Template: DEFAULT_9630SIP_CM_6_0

Set Type: 9630SIP

Security Code: ••••••

* Port: IP

Voice Mail Number:

Delete Endpoint on Unassign of Endpoint from User or on Delete User.: ☐

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 the 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 NACR 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 SIP 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 **Login name** of the corresponding user 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 appplication 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=
```

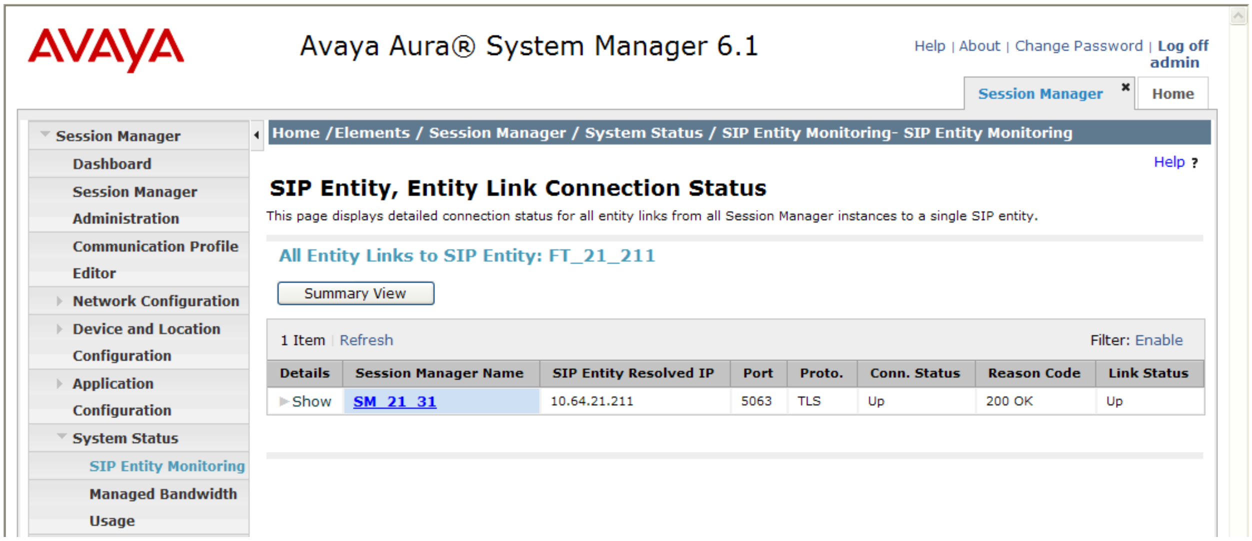
Within the ***config*** directory, open ***blockedNumbers.txt*** file and edit the file to contain list of dialed numbers to be blocked (one entry per line).

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.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: FT_21_211

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 a SIP User managed by the NACR CallNACK application, dial a blocked PSTN number. Verify the call is blocked.
- From a SIP User managed by NACR CallNACK application, dial an allowed PSTN number. Verify the call is allowed.
- From a SIP User not managed by NACR CallNACK application, dial a blocked PSTN number. Verify the call is allowed.
- From a SIP 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 SIP 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 Aura™ Communication Manager Feature Description and Implementation*, Doc ID: 555-245-205, August 2010.
[5] *Administering Avaya Aura™ 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.

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.