Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Vision 2020 3.1HA from Enghouse Interactive AB with Avaya Communication Server 1000 and Avaya Aura® Session Manager using a SIP Trunk connection – Issue 1.0

Abstract

These Application Notes describe how to configure an Avaya Communication Server 1000 and an Avaya Aura® Session Manager to interface with Vision 2020 3.1HA, which is operating as an attendant answering position. Vision 2020 3.1HA is a software application from Enghouse Interactive AB installed on a Windows server that interfaces with Avaya Communication Server 1000 using a SIP connection via Avaya Aura® Session Manager and provides users with the call functions of an attendant console without having to install a hardware attendant position.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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.

1. Introduction

These Application Notes describe the compliance tested configuration for Avaya Communication Server 1000E R7.6 and Avaya Aura® Session Manager R7.0 with Vision 2020 HA (hereafter referred as Vision) release 3.1 from Enghouse Interactive AB. Vision is a client/server based application running on Microsoft Windows 2012 Server operating systems. Vision provides users with an attendant answering position for Avaya Communication Server 1000E that does not require attendant telephony hardware e.g., Avaya 2250 attendant console. Vision connects to the Avaya Communication Server 1000 using a SIP connection via Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using an Avaya Communication Server 1000E (Communication Server 1000). The Vision server uses a SIP connection to the Communication Server 1000 call server via Session Manager. See **Figure 1** for a network diagram. A basic Distance Steering Code configuration (DSC) was configured on the Communication Server 1000 to route all calls to the Vision attendant position. If a call is made from the Vision attendant console to the PSTN the call will route from the Vision console via a SIP trunk to Session Manager then to the PSTN. During compliance testing simulated PSTN PRI/T1 trunks were used. Vision can perform the usual range of attendant call functions, i.e., centralized answering position; extend PSTN calls to users, place PSTN calls on behalf of internal users, perform internal telephone directory lookups.

During tests, calls are placed to a number associated with the Vision attendant position. Session Manager routes all calls destined for the Vision server over the SIP connection. The Vision server then automatically places a call to the telephone the attendant is using for answering purposes. When the attendant answers the call, the Vision server bridges the two calls. When the attendant extends the call to another phone, Vision server performs a SIP Re-Invite to connect caller and called user directly. It is possible to have multiple Vision attendant positions on a Communication Server 1000 system.

A variety of Avaya telephones were installed and configured on the Communication Server 1000. The Vision attendant client provides a view of contacts, schedules, and communication tasks and was installed on the same server as the Vision Server, but can be installed on a separate platform if required.

Note: The Vision server places a call to the attendant's deskphone, for compliance testing an Avaya IP phone was used as the attendant's deskphone. When the attendant is called the Vision server calls the Avaya IP phone and bridges the call.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by

DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Vision 2020 did not include use of any specific encryption features as requested by Enghouse Interactive AB.

2.1. Interoperability Compliance Testing

The compatibility tests included the following.

- Incoming internal and external calls
- Outgoing internal and external calls
- Blind and announced transfer with answer
- Directing calls to busy extensions
- Call queuing and retrieval

2.2. Test Results

Tests were performed to insure full interoperability between the Vision and the Communication Server 1000. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

For technical support for Enghouse Interactive AB products, please use the following web link.
http://www.enghouseinteractive.com/solutions/

Enghouse Interactive AB can also be contacted as follows.
Phone: +46 (0)8 457 30 00
Fax: +46 (0)8 31 87 00
E-mail: Visionsupport@enghouse.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Server 1000, System Manager and Session Manager. The Vision 8020HA server connects the Communication Server 1000 using a SIP Trunk via Session Manager. An Avaya 1140 IP deskphone was used as the Vision 8030HA Attendant telephone during compliance testing. A PRI/T1 trunk on Media Gateway Controller (MGC) was configured to connect to the simulated PSTN.

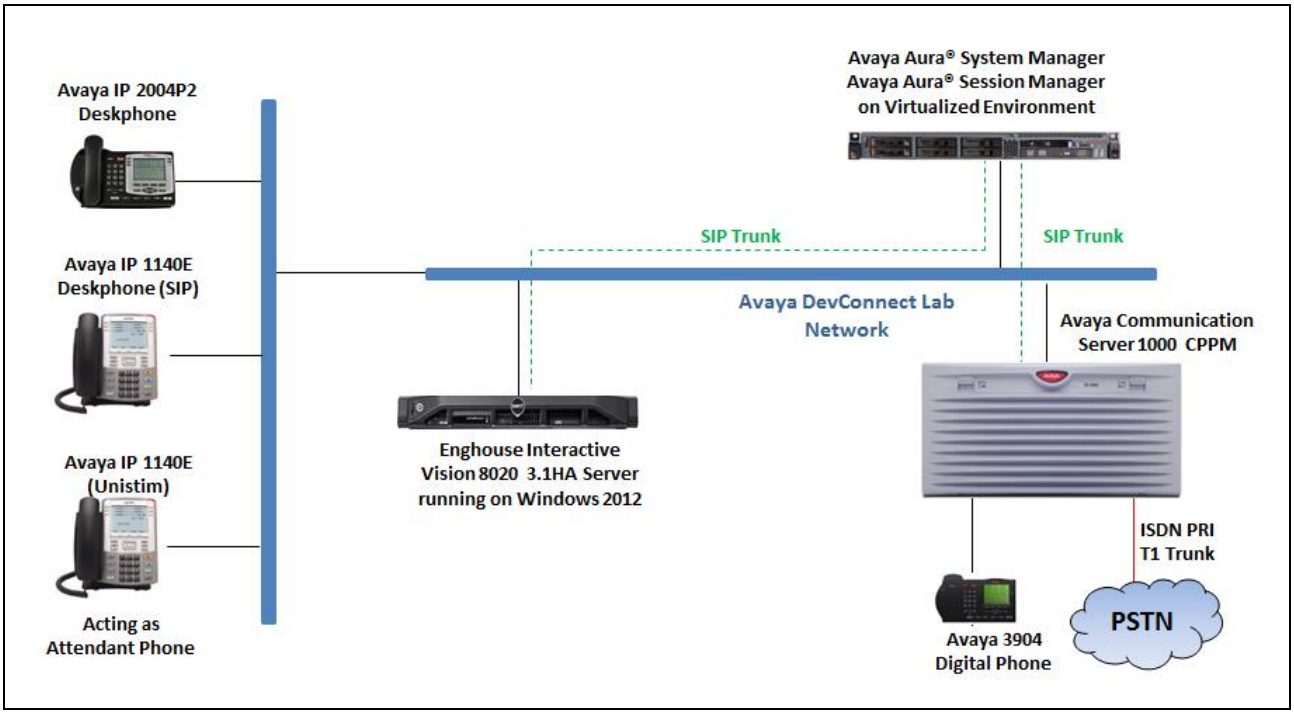


Figure 1: Configuration for Avaya Communication Server 1000, Avaya Aura® Session Manager and Enghouse Vision 2020 3.1HA

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Communication Server 1000	7.65 SP8
Avaya Aura® Session Manager running on virtualized environment	7.0.1.2.701114
Avaya Aura® System Manager running on virtualized environment	7.0.1.2 SP2
Avaya 11xx Series IP Telephone • 1140 (UNIStim) • 1140 (SIP)	 C95 4.03.09
Avaya 2004P2 IP Telephone	DCQ
Avaya 3904 Digital Telephone	-
Vision 2020 HA Server and Client running on Microsoft Windows 2012 R2 Server	3.1

5. Configure Avaya Communication Server 1000

The document assumes that route, trunk and dialing plan of the Avaya CS 1000 have been configured. This section only describes the details on how to configure the Avaya CS 1000 Signaling gateway to connect to the Session Manager via SIP trunk using the Element Manager.

Prerequisites: An Avaya CS1000 server which has been:

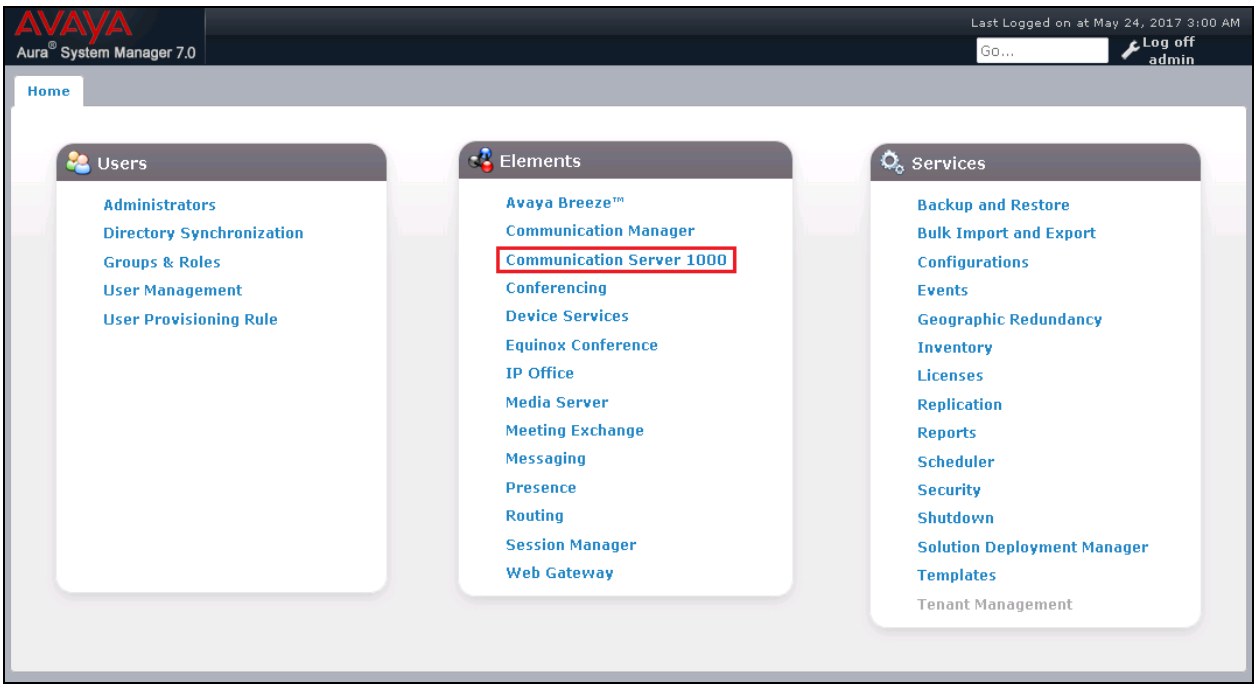
- Installed with CS 1000 Release 7.6 Linux Base.
- Joined CS 1000 Release 7.6 Security Domain.
- Deployed with SIP Trunk Application.

For more information on CS 1000 installation, maintenance, and upgrades, see **Section 10**. The following software packages are enabled in the key code. If any of these features have not been enabled, please contact your Avaya account team or Avaya technical support at http://www.avaya.com.

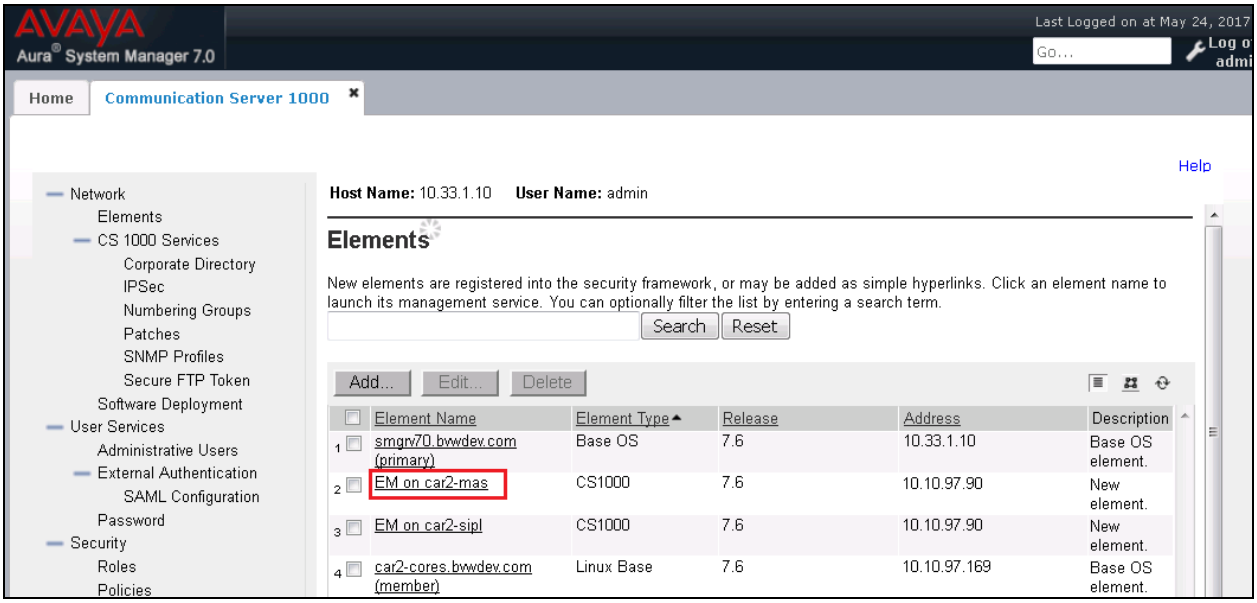
Package Mnemonic	**Package Number**	**Package Description**	**Package Type (New or Existing or Dependency)**	**Applicable Market**
SIP	406	SIP Service package	New package	Global
FFC	139	Flexible Feature Codes	Existing package	Global
SIPL_ Nortel	415	Avaya SIP Line	Existing package	-
SIPL_3ThirdParty	416	Third Party SIP Line	Existing package	-

5.1. Log in to Avaya Communication Server 1000 System

Since release 7.6 Avaya CS 1000 Elements is integrated to System Manager, to access the Element Manager of CS 1000 first log in the System Manager. The screen below shows the System Manager home page with **Communication Server 1000** entry in the Elements table. Click on the **Communication Server 1000** to access to CS 1000 Elements, the Elements webpage will be opened in the new window.

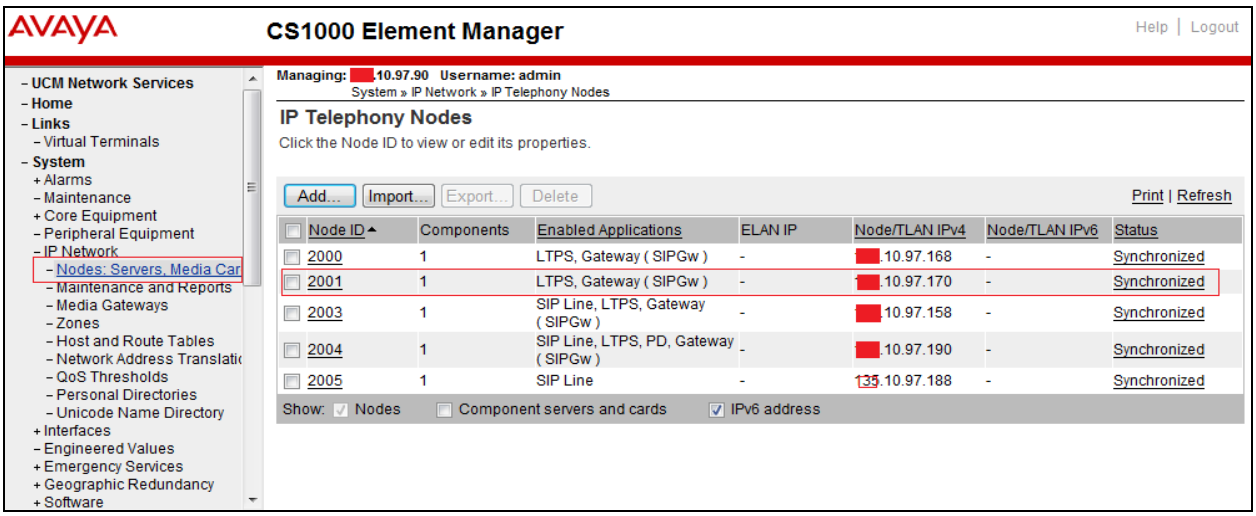


The **Elements** page is shown in the following screenshot. Click Element Name of the CS 1000 that needs to be accessed as highlighted in the red box.

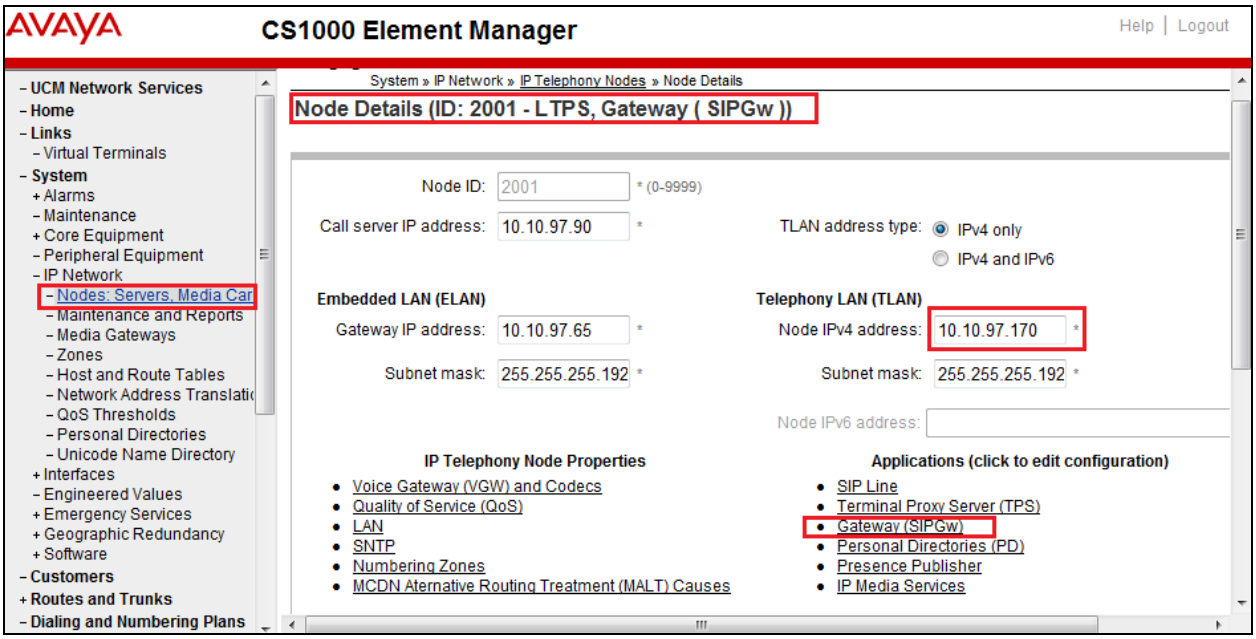


5.2. Administer an IP Telephony Node

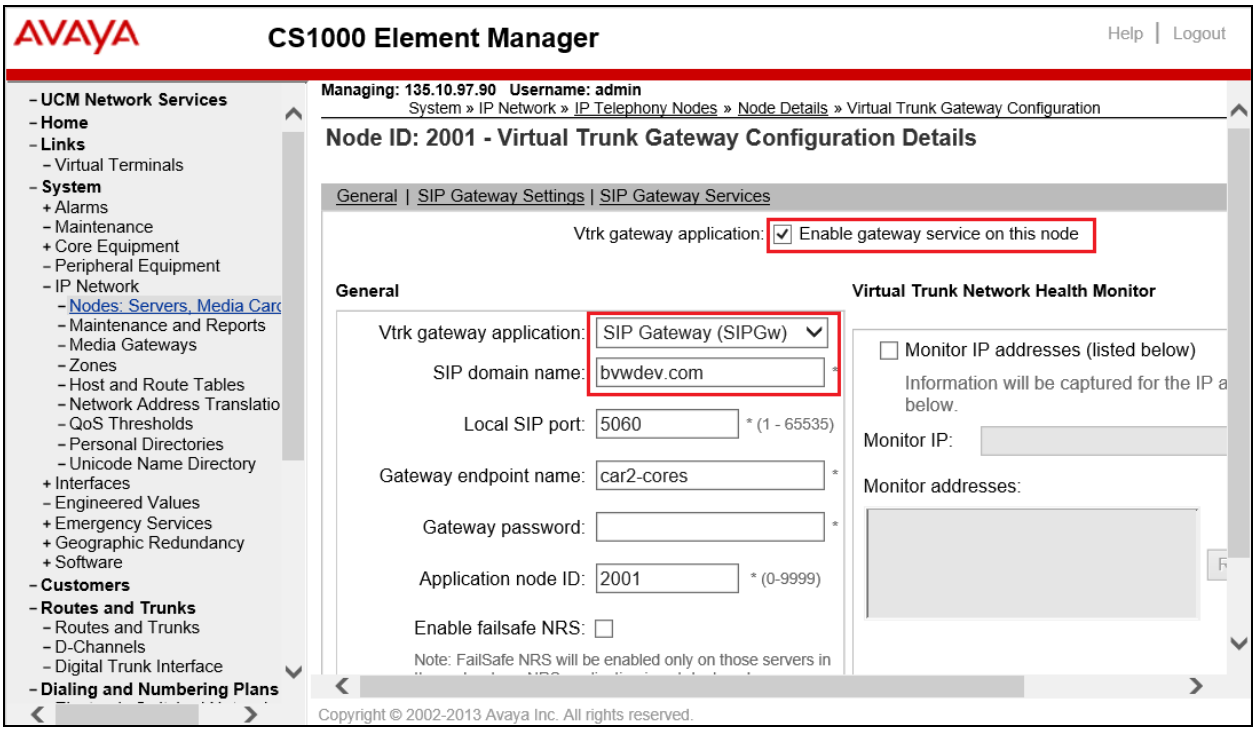
These application notes assume that the basic CS 1000 configuration has already been administered and that IP Telephony Node has already been created. This section describes the steps for configuring a Node (Node ID 2001) in CS 1000 IP network to work with Voice4net. Select **System → IP Network → Nodes: Servers, Media Cards** and then click on the **Node ID 2001** as shown below.



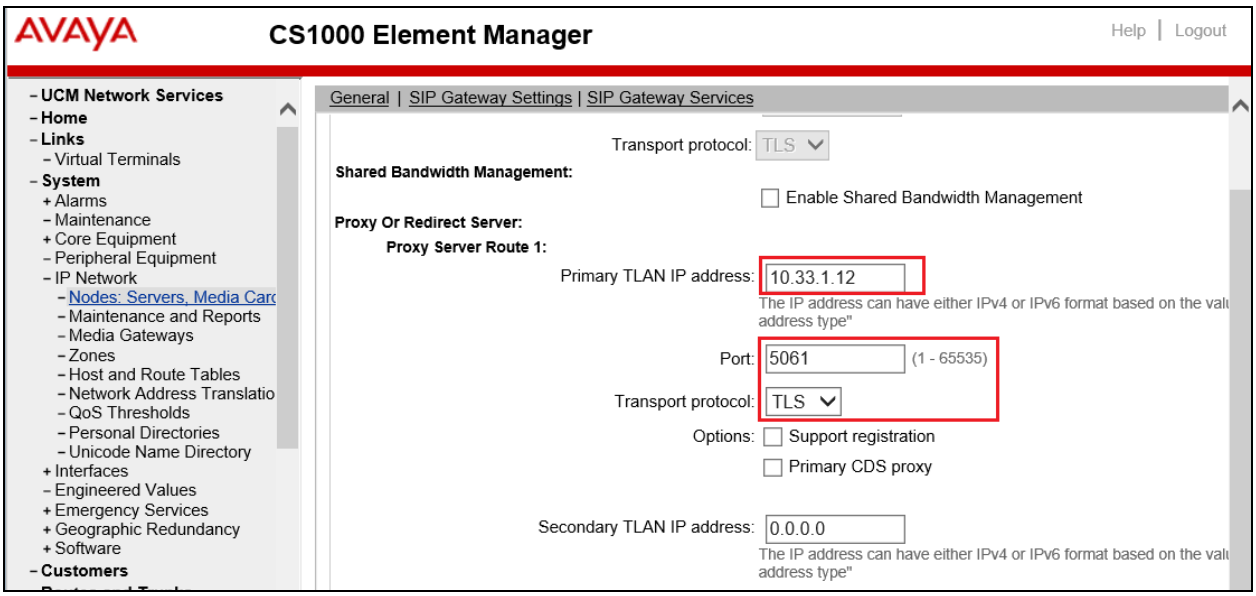
The **Node Details** page will appear. Scroll down under the **Applications**, click on the **Gateway (SIPGw)** link, the **Virtual Trunk Gateway Configuration Details** page will appear in the next two screenshots. The node IP address 10.10.97.170 is used to establish SIP trunk with Session Manager.



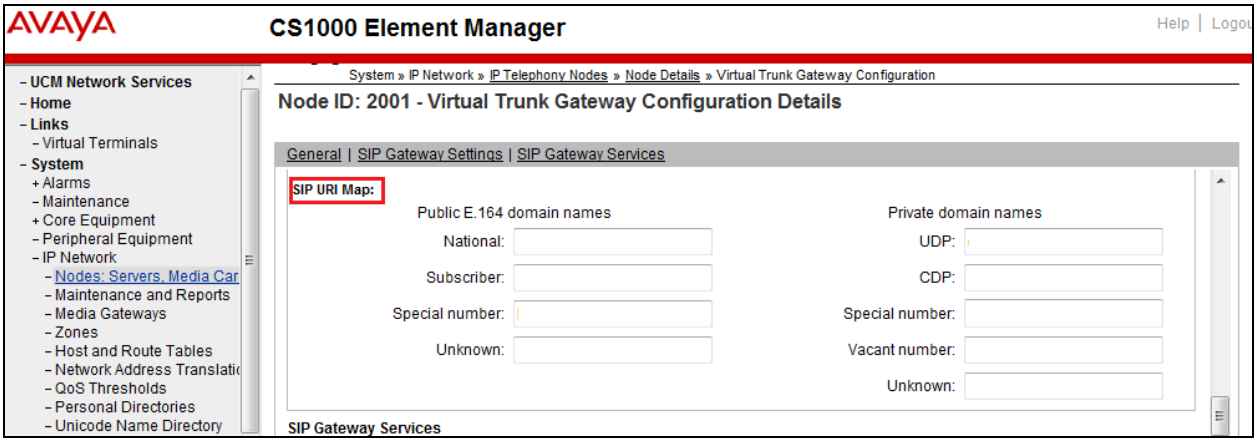
In the **Node ID: 2001- Virtual Trunk Gateway Configuration Details**, enter the information highlighted in the red-box for the **General** and **SIP Gateway Settings**. All other fields are kept at default. Click **Save**. Note: SIP domain name **bvwdev.com** should be matched with SIP domain created in **Section 6.2**.



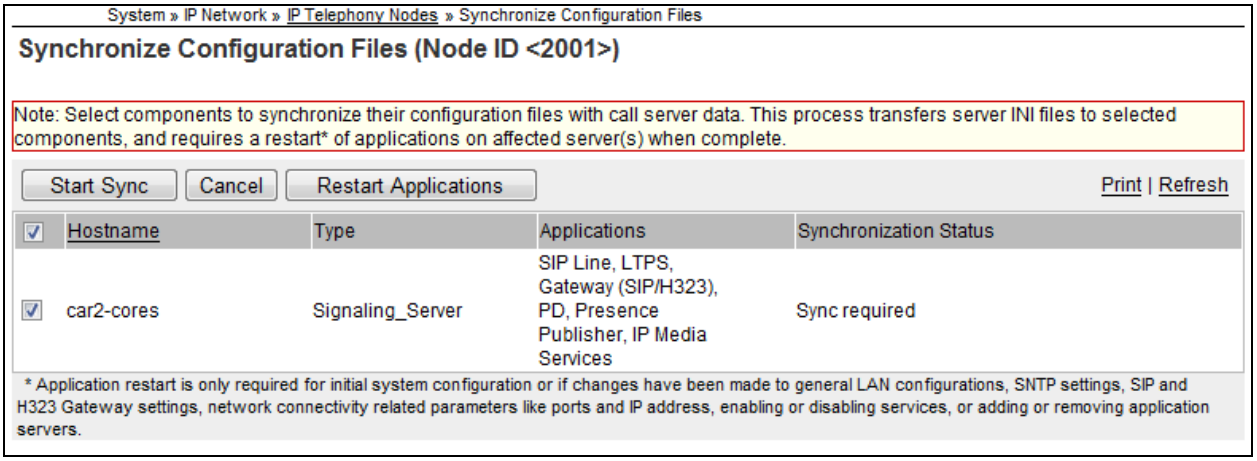
Enter the IP address **10.33.1.12** of signaling Session Manager in the **Primary TLAN IP address** field, port **5061** in the Port field and select **TLS** in the Transport protocol dropdown menu.



On the same page, scroll-down the parameters box to the **SIP URI Map** section. Under the **Public E.164 domain names** and **Private domain names** subsections, leave all fields as blank, which remove the phone context in Invite message sent from CS 1000.

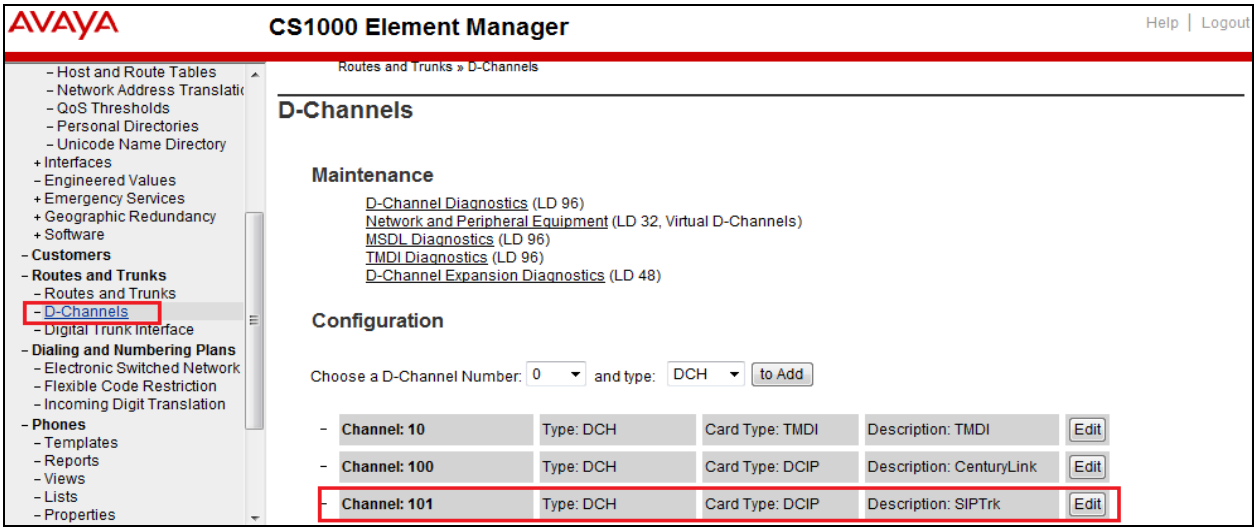


Afterwards, click **Save**, the system will bring back the **Node ID** page (not shown). Then click **Save** button on the **Node ID** page and that will take the user to the **Node Saved** page (not shown). Click on the **Transfer Now** button, when finished it will bring the user to the **Synchronize Configuration Files** page. Then click **Start Sync** button (not shown) to complete the configuration saved process.

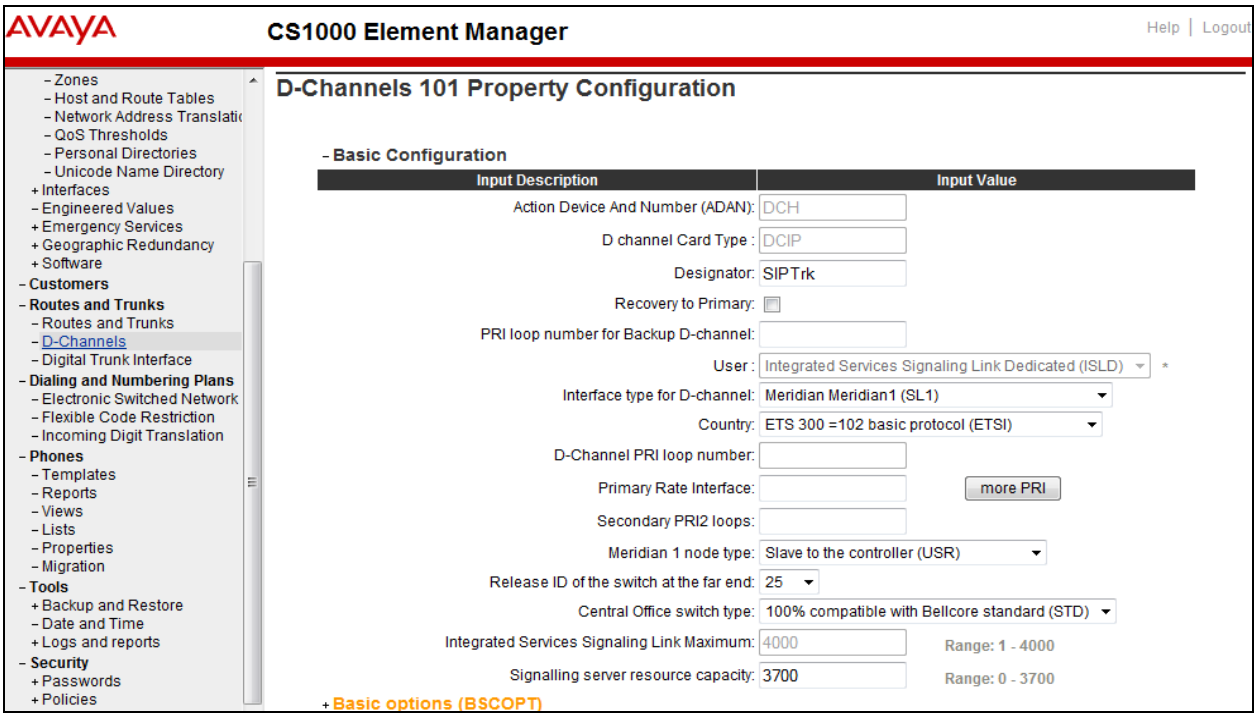


5.3. Administer D-Channel for SIP Trunk

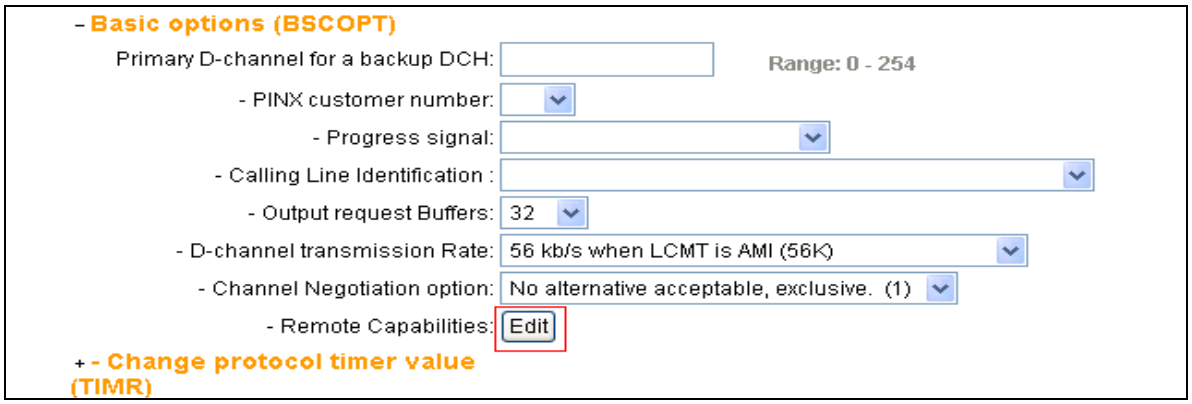
From the homepage of Element Manager, expand the menu **Routes and Trunks → D-Channels** and select the **D-Channels** tab. The **D-Channel 101** as shown below was used for the compliance test.



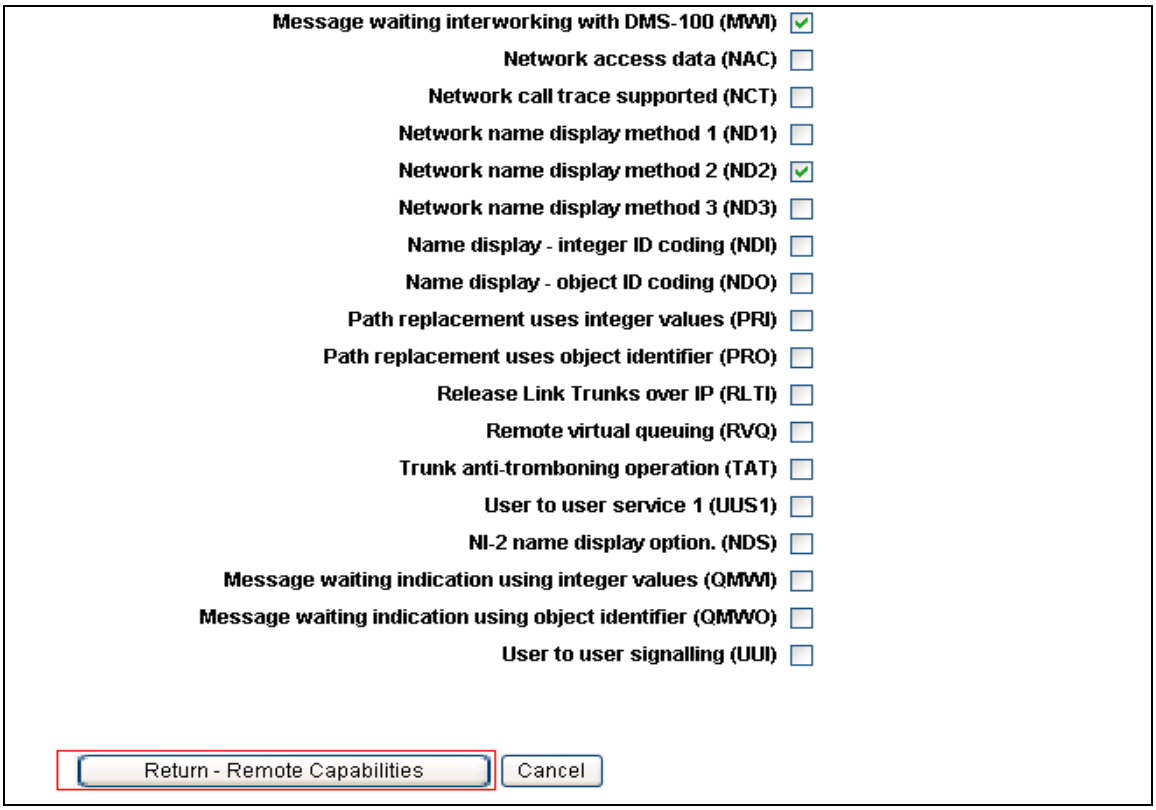
Click **Edit** button on the **D-channel 101**. The screen below shows the **Basic Configuration** section of this D-channel. Select **D-Channel is over IP (DCIP)** in the **D-Channel Card Type**, enter a description in the **Designator** box and keep all other values at their defaults.



Continue to expand the **Basic options (BSCOPT)** section. Keep all fields at default and click on **Edit** button in the **Remote Capabilities** field.



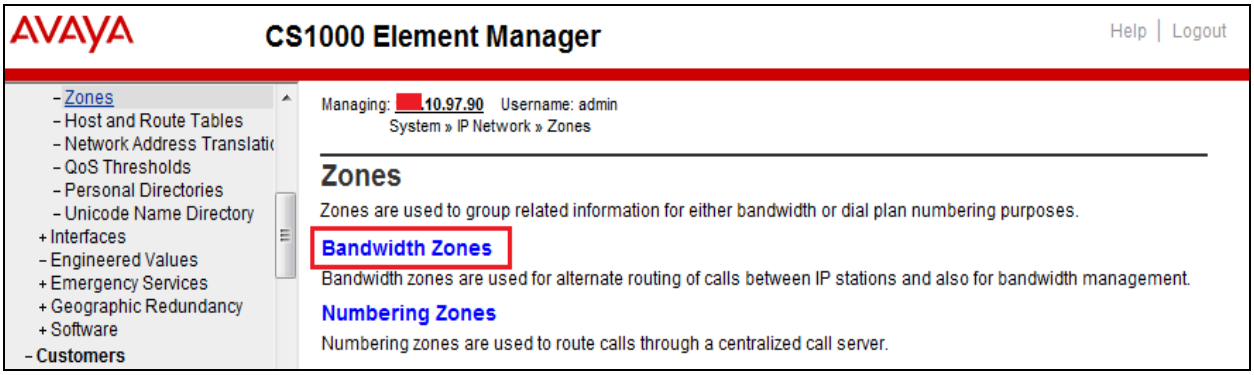
The **Remote Capabilities Configuration** page is displayed. Make sure that **Message waiting interworking with DMS-100 (MWI)** and **Network name display method 2 (ND2)** check boxes checked**.** Click on **Return – Remote Capabilities** button to return to the D-Channel page.



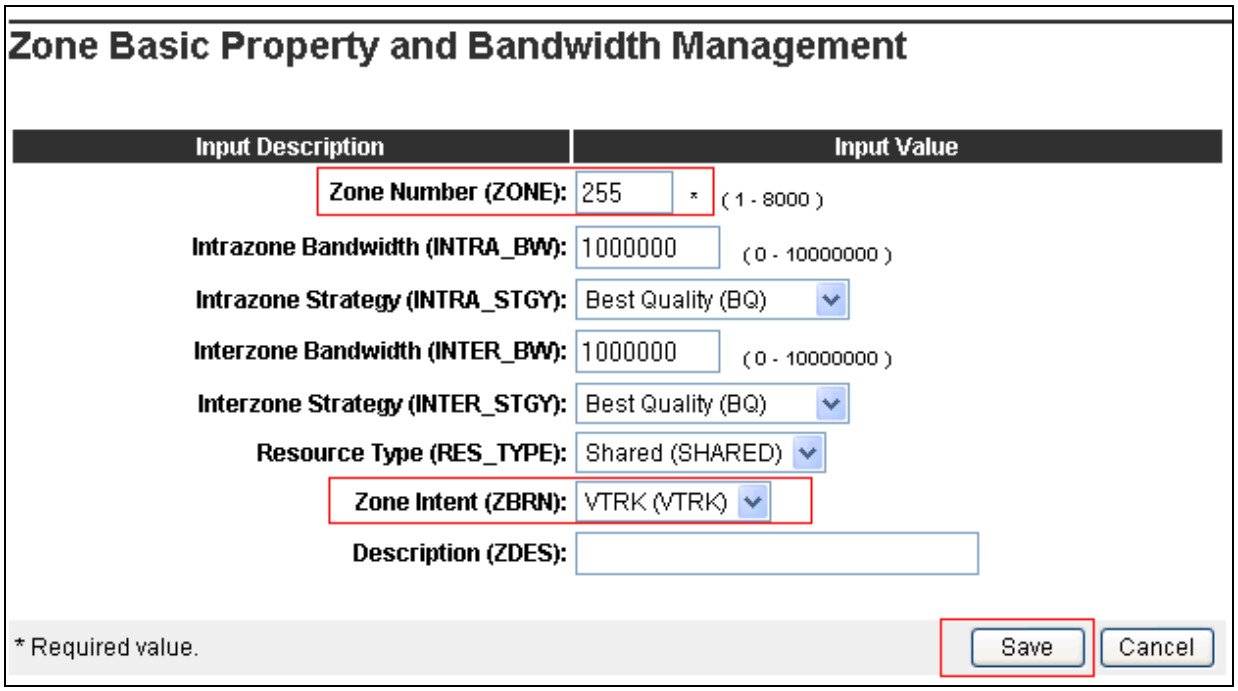
Keep all values at default for the **Change protocol time value (time)** and **Advanced options (ADVOPT)** sections. Click on the **Submit** button in the bottom of the D-channel configuration page to save and complete.

5.4. Administer Zone Bandwidth

To configure a Zone, from the homepage of Element Manager expand the menu **System → IP Network → Zones** and select the **Zones** tab. The **Zones** page is displayed in the right-hand side as shown below.

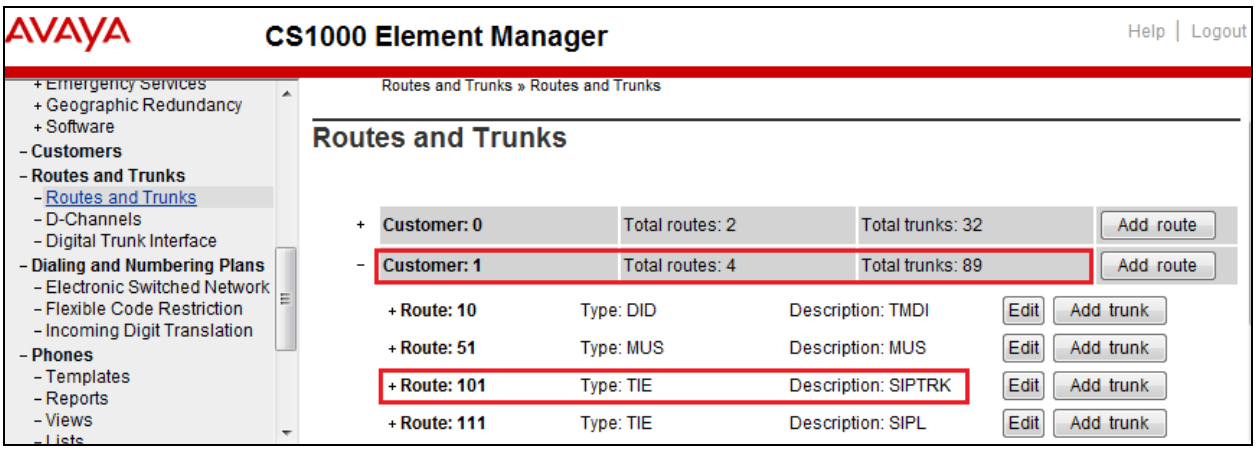


Click on the **Bandwidth Zones** link. The **Bandwidth Zones** page is displayed (screen not shown) and clicks on the **Add** button to add a new zone. The **Zone Basic Property and Bandwidth Management** page is displayed. Enter number **255** in the **Zone Number**, select **Zone Intent (ZBRN)** as **VTRK** (this zone is intended to use for virtual trunks) and keep other fields at their defaults. Click on **Save** button to save changes and complete to add the new zone.

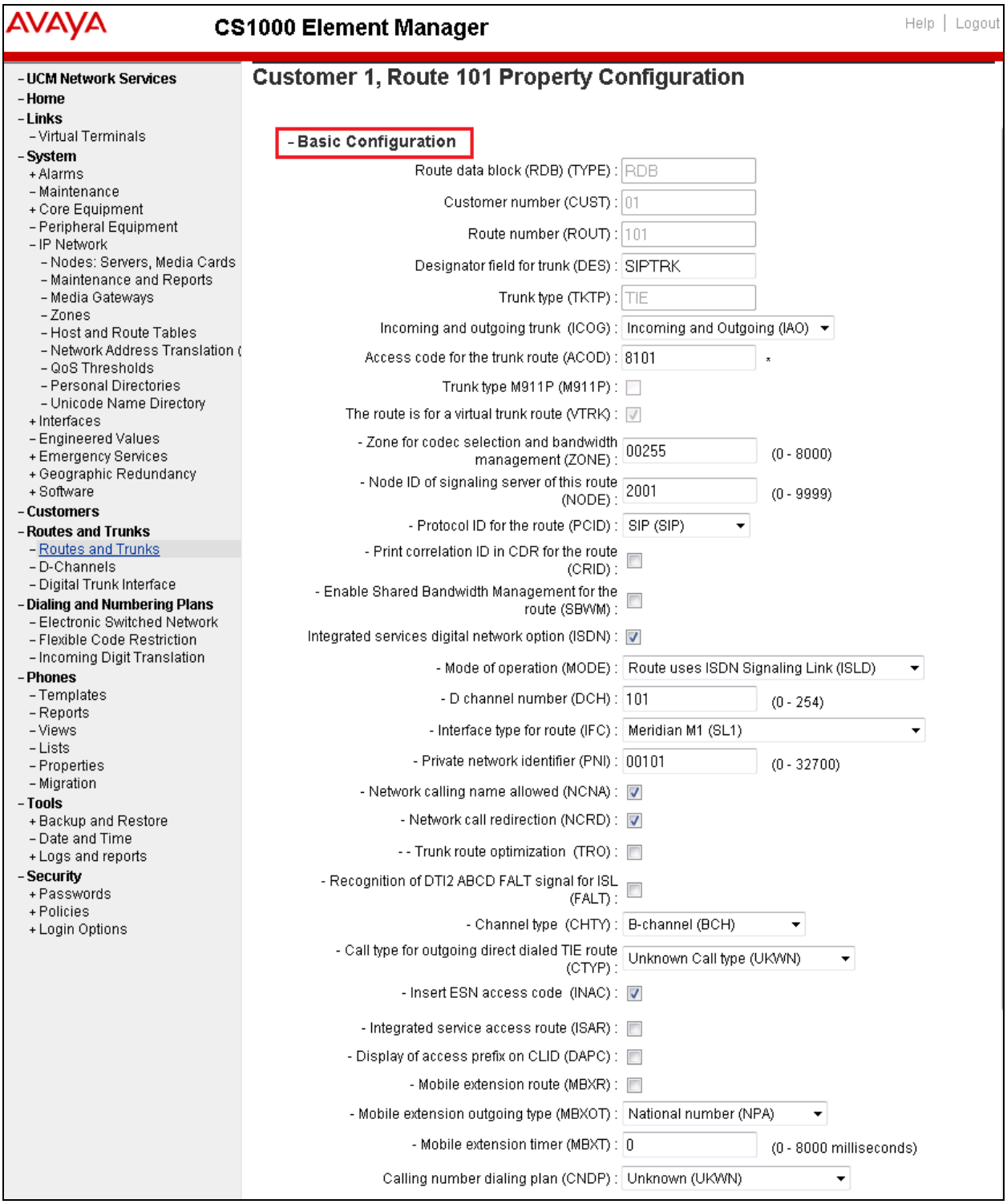


5.5. Administer SIP Route

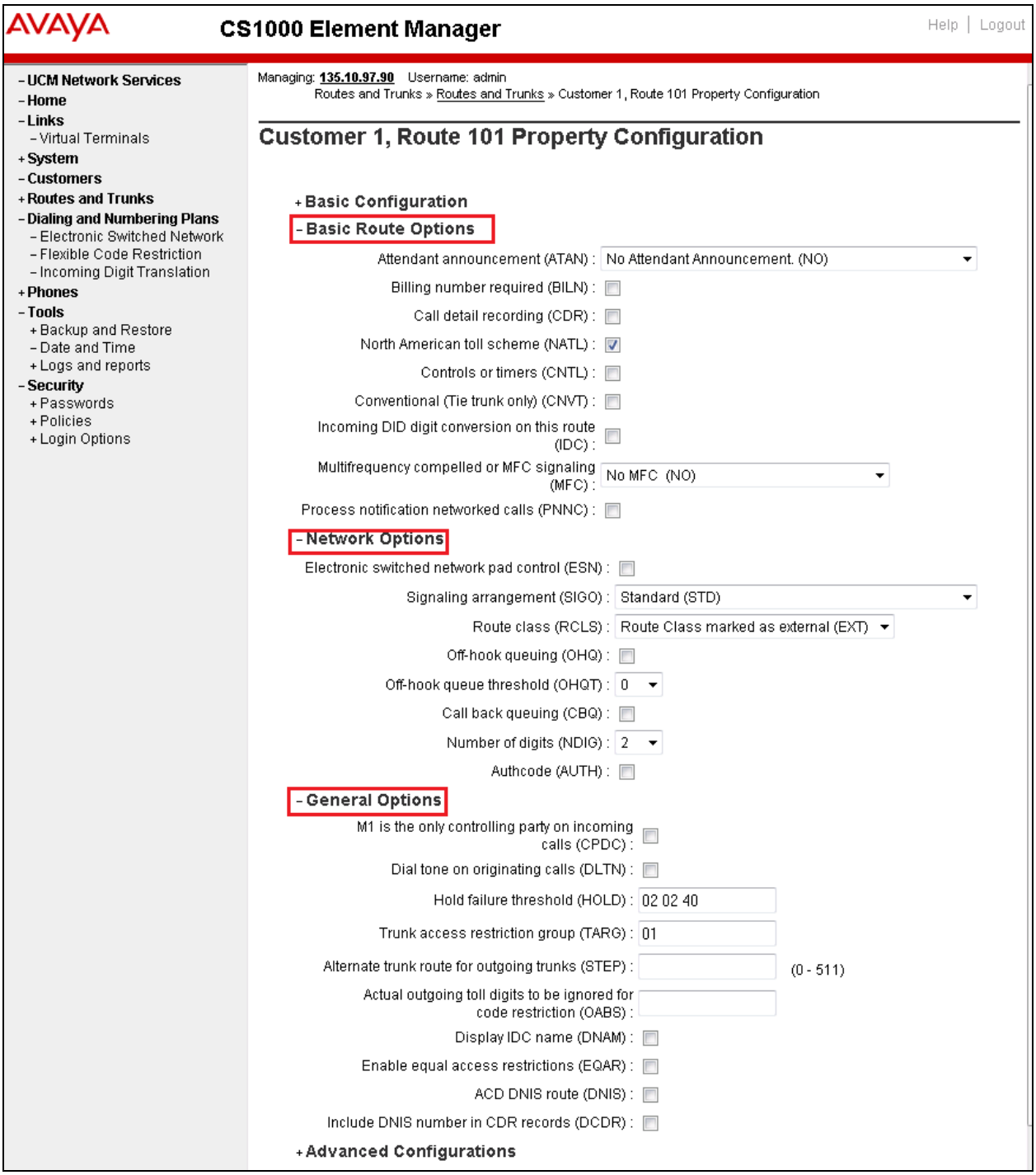
To configure a SIP Route, from the homepage of Element Manager, navigate to **Routes and Trunks → Routes and Trunks**. The **Routes and Trunks** page is displayed in the right-hand side. In the compliance test, the route and trunks were created in the **Customer 1**. Expand the **Customer: 1** there is SIP route **101** already created and used for the compliance test as shown in the screen below.



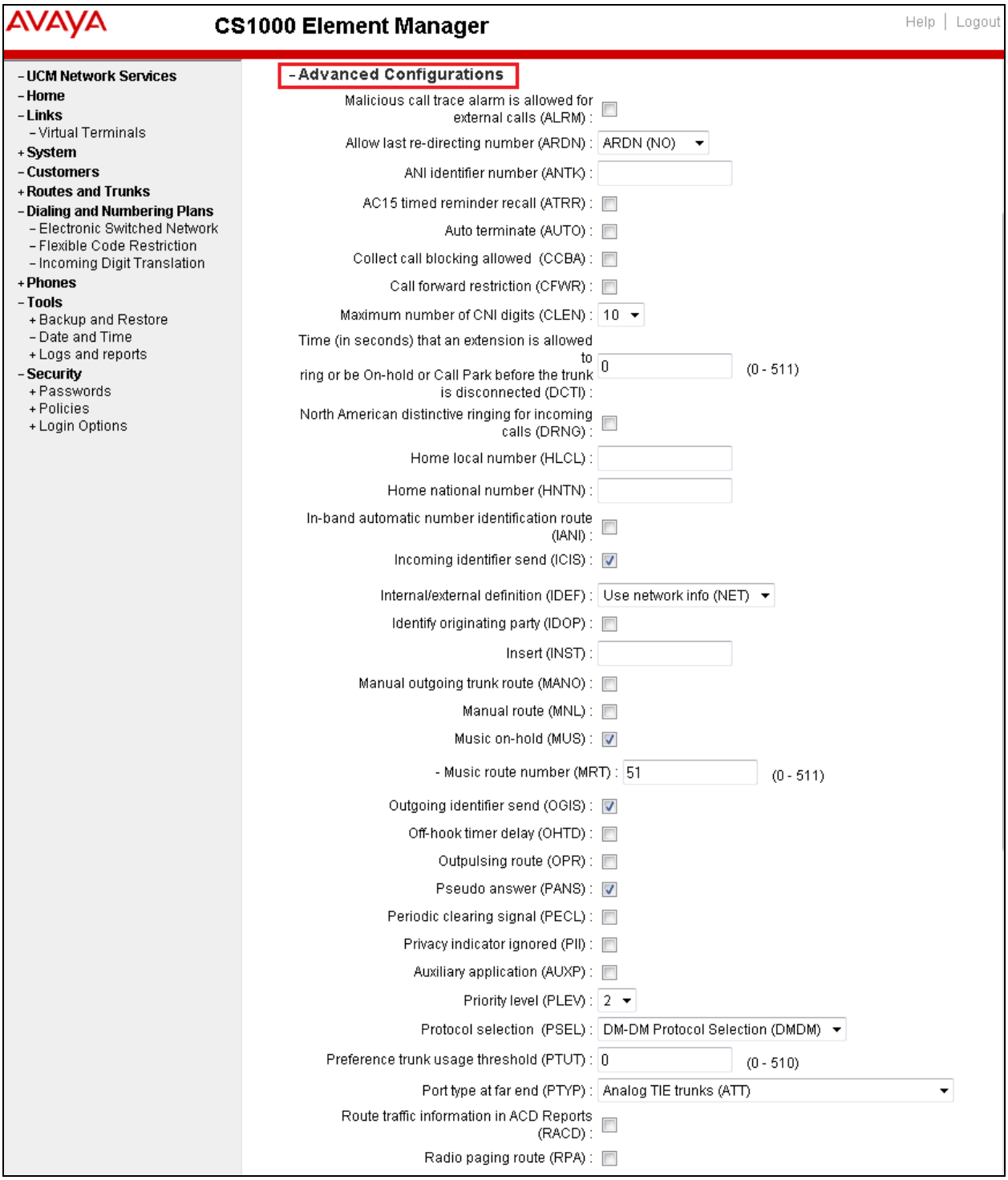
Click on **Edit** button on the route **101** to show the configuration of this route. All necessary parameters of the **Basic Configuration** section are shown in the screenshot below.



Keep all values at default for the **Basic Route Options**, **Network Options**, **General Option**s, and **Advanced Configurations** sections as shown in the screenshots below.

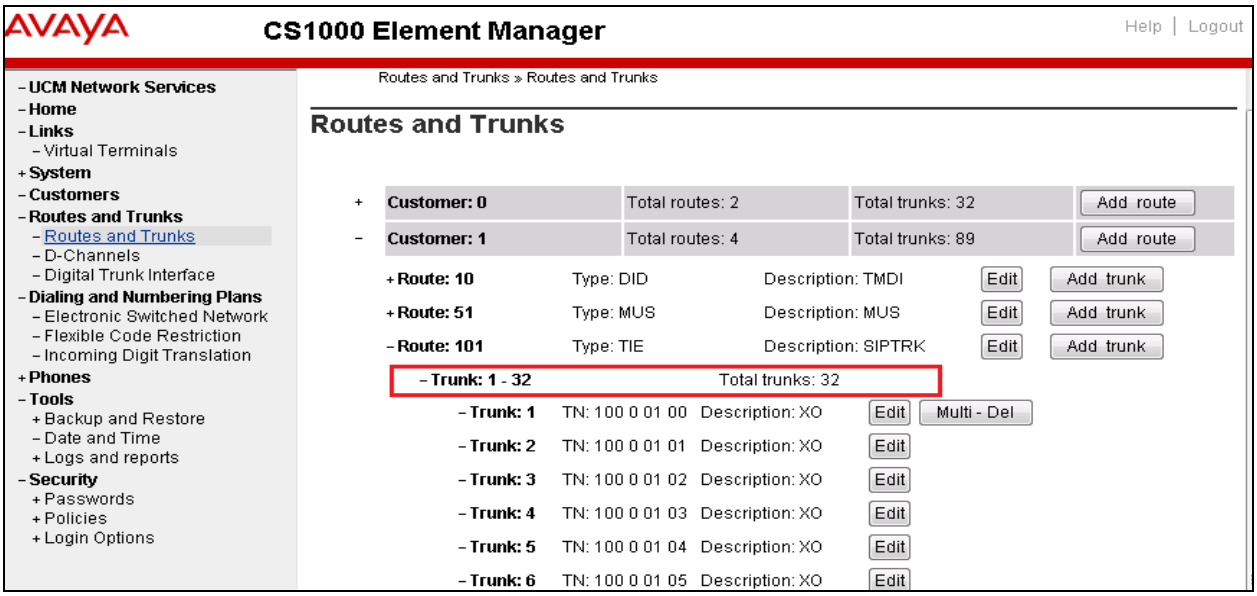


The screen below shows the parameters of the **Advanced Configurations** section of the route **101**.

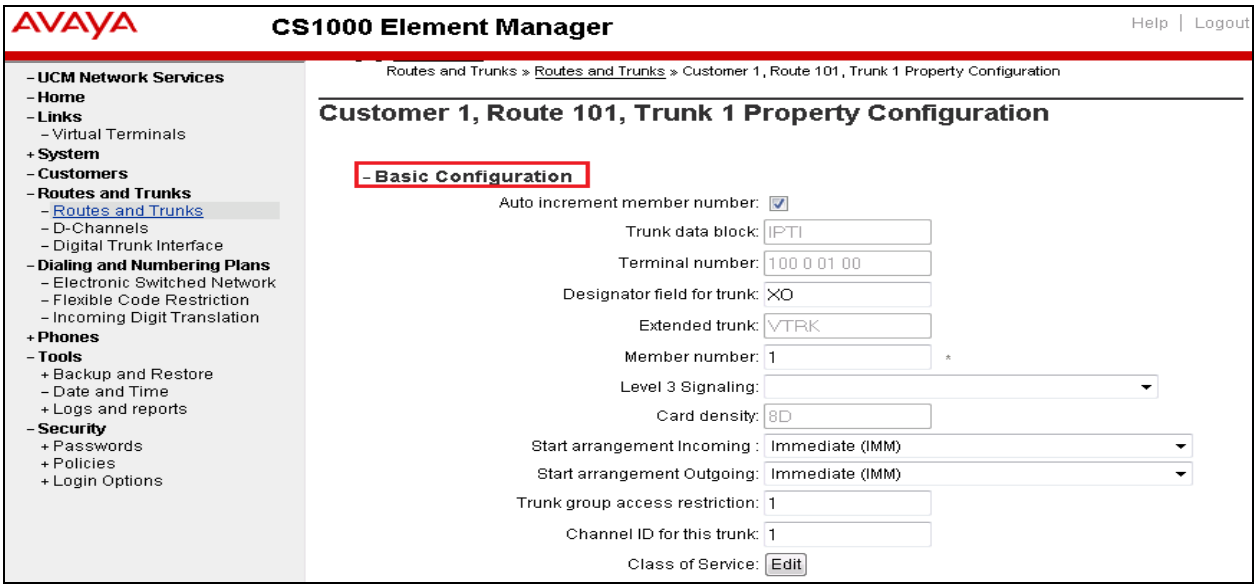


5.6. Administer SIP Trunks

To configure SIP trunks, from the homepage of Element Manager, navigate to **Routes and Trunks → Routes and Trunks**. The **Routes and Trunks** page is displayed in the right-hand side. In the compliance test, the route and trunks were created in the **Customer 1**. Expand the **Customer: 1** and the SIP route **101** there are 32 SIP trunks already created as shown below.



Click on **Edit** button on **Trunk: 1** to show configuration of this SIP trunk. The configuration of the trunk 1 is the same for the rest of SIP trunks. The screen below shows the **Basic Configuration** of the SIP trunk. Keep all values at default for the **Advance Trunk Configurations** section.

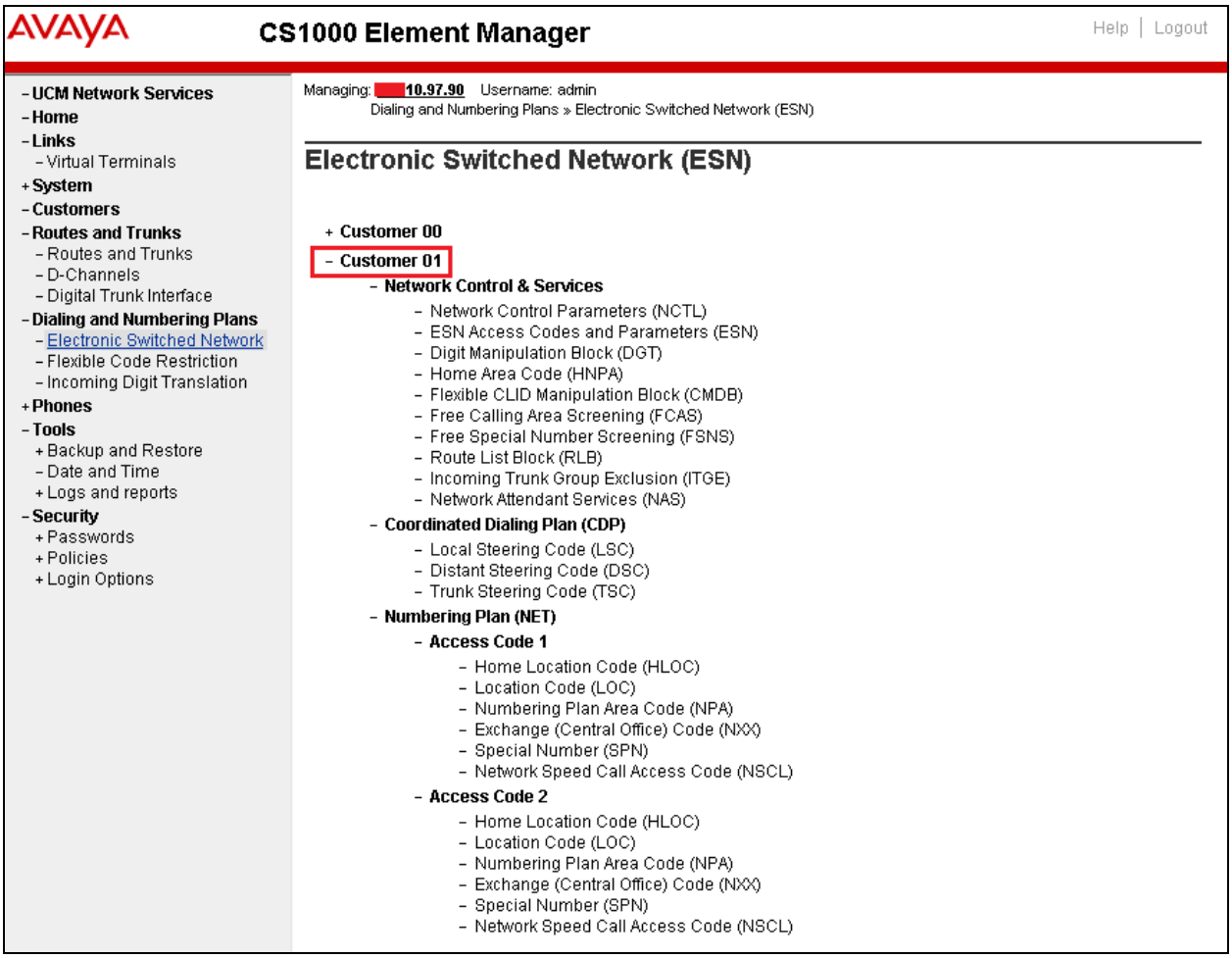


5.7. Administer CDP Dialing Plan

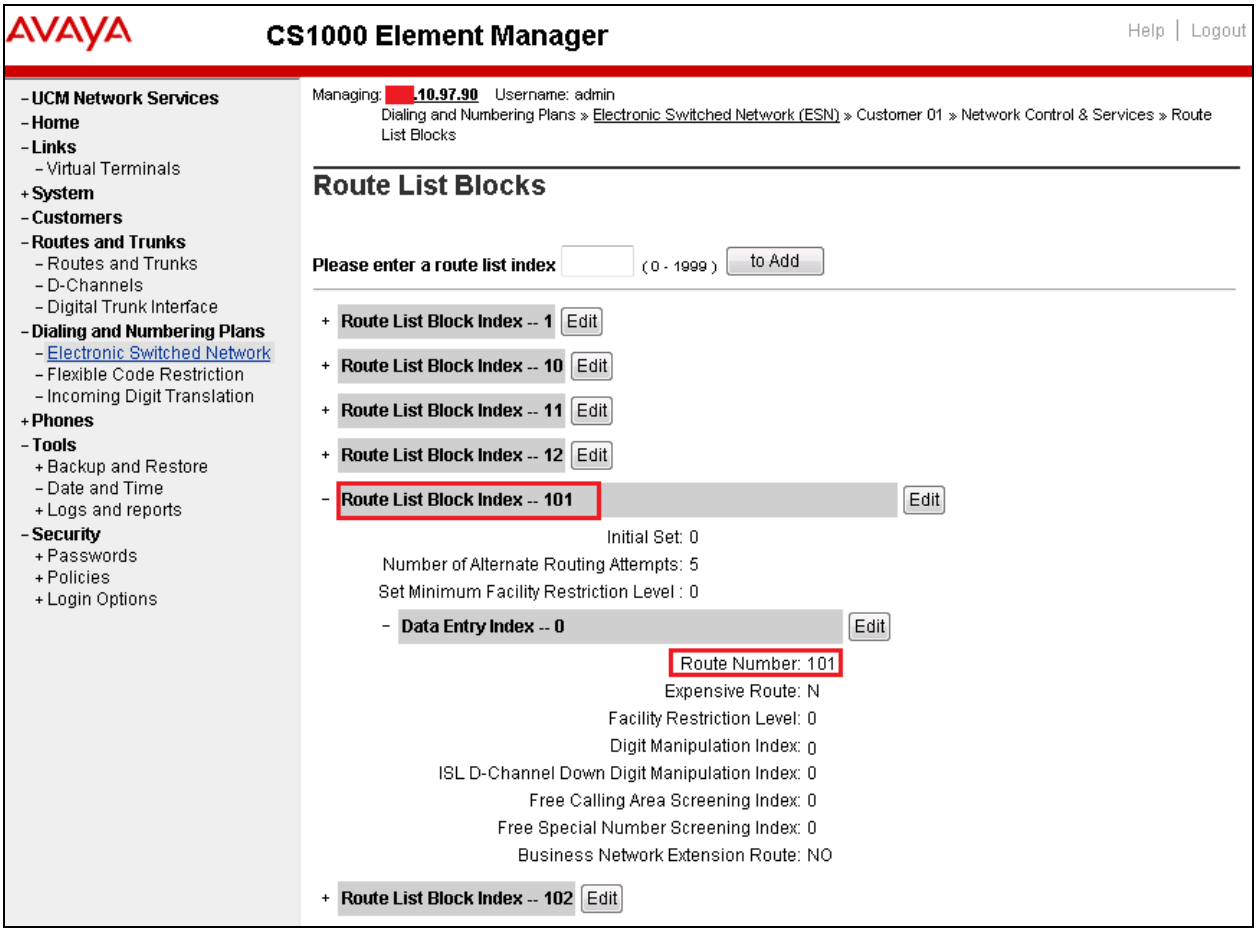
This section provides the steps on how to create a new Route List Index (RLI) and a new Distant Steering Code (DSC) for the Coordinated Dialing Plan (CDP) dialing plan.

5.7.1. Configure Route List Index (RLI)

To configure Route List Index, from the home page of Element Manger, navigate to **Dialing and Numbering Plan → Electronic Switched Network**. The **Electronic Switched Network (ESN)** page is displayed; expand the **Customer 01** which the RLI will be created.

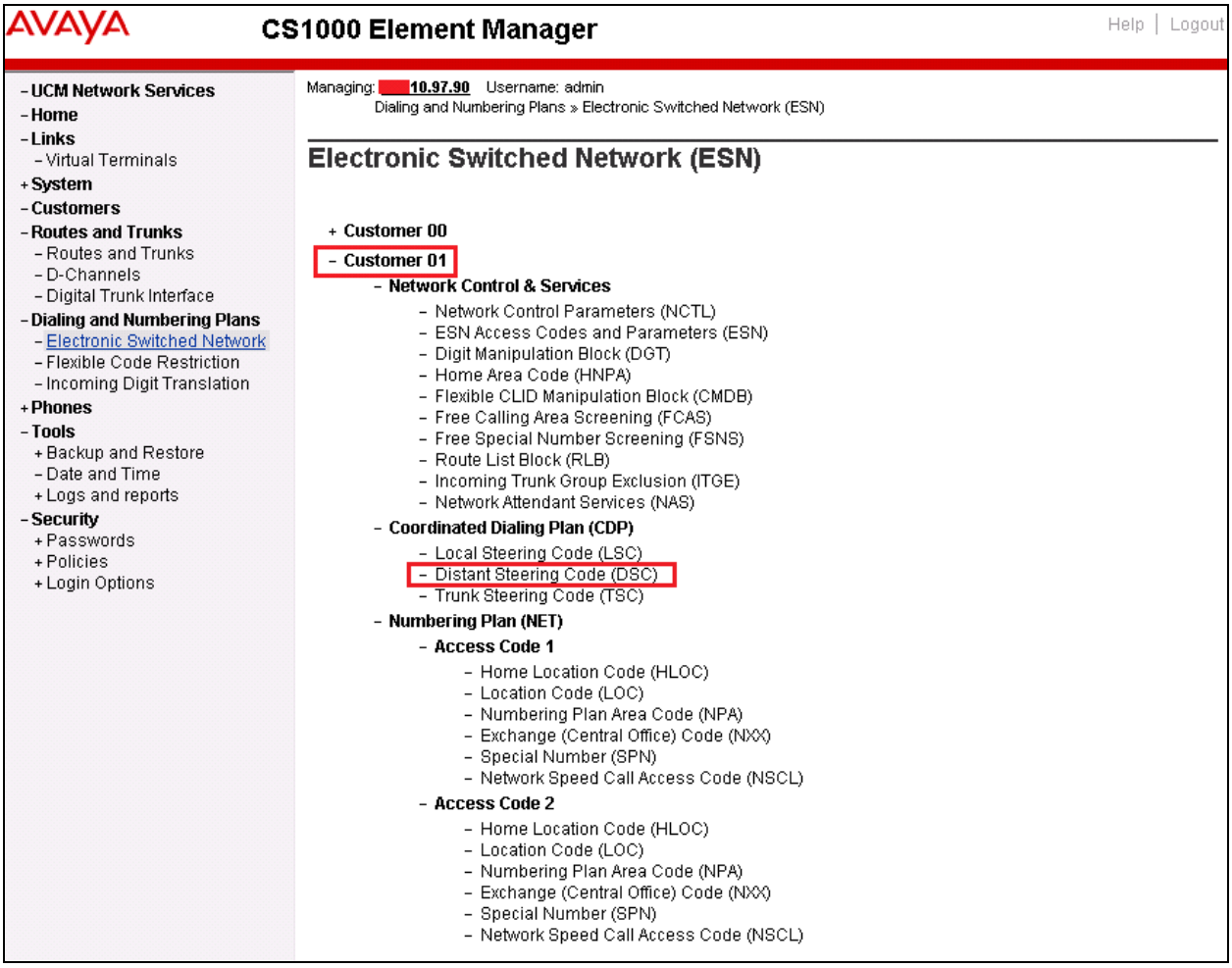


Click on the **Route List Block** (**RLB)** link, the **Route List Blocks** page is displayed as the screen below. In the testing, the Route Link Block Index **101** was created and used the route **101** as configured in **Section 5.5**.

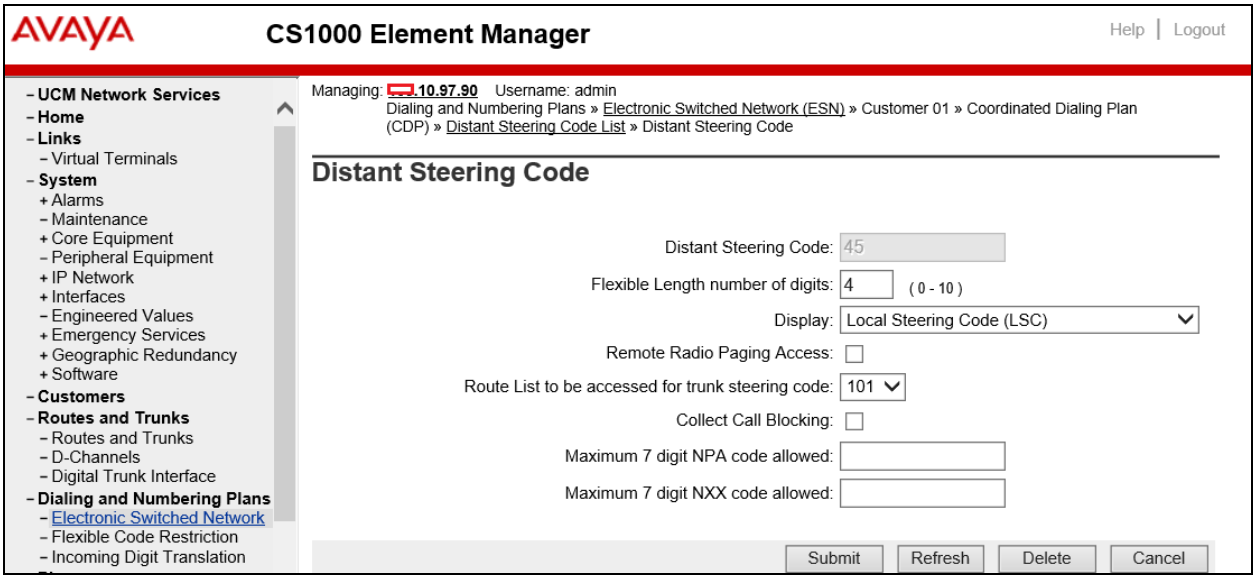


5.7.2. Create a Distant Steering Code (DSC)

In the **Customer 01** of the Electronic Switch Network (ESN) page, select **Distant Steering Code (DSC)** under **Coordinated Dialing Plan (CDP)**. .



The **Distant Steering Code List** page is displayed. In the testing, the distant steering code **45** was configured for routing call from CS 1000 to Vision. The distant steering code contains 4 digits and used the route list index **101** as configured in **Section 5.7.1** above.



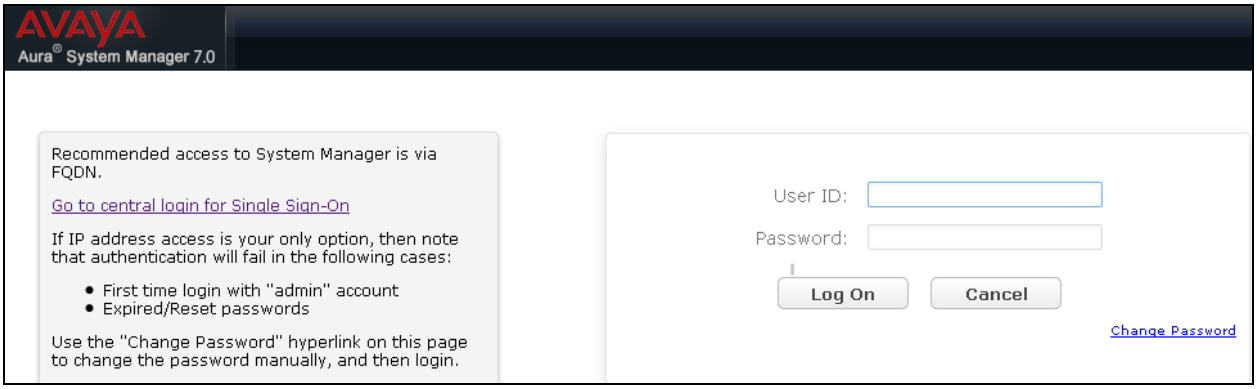
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer Domain
- Administer locations
- Administer Adaptation
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

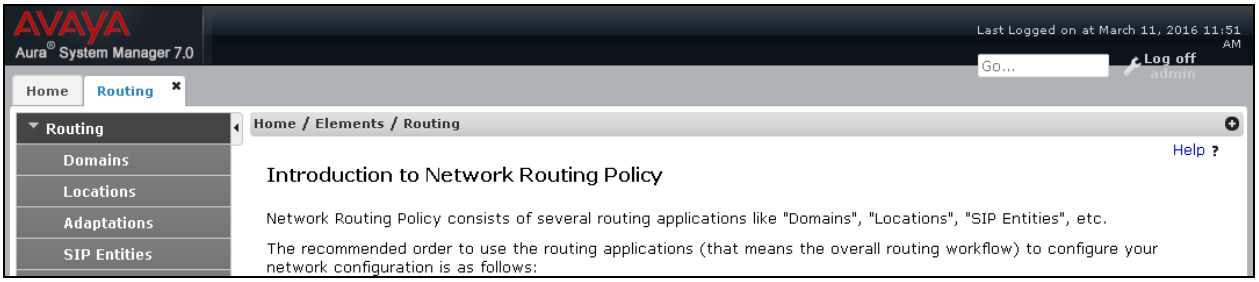
6.1. Launch System Manager

Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.

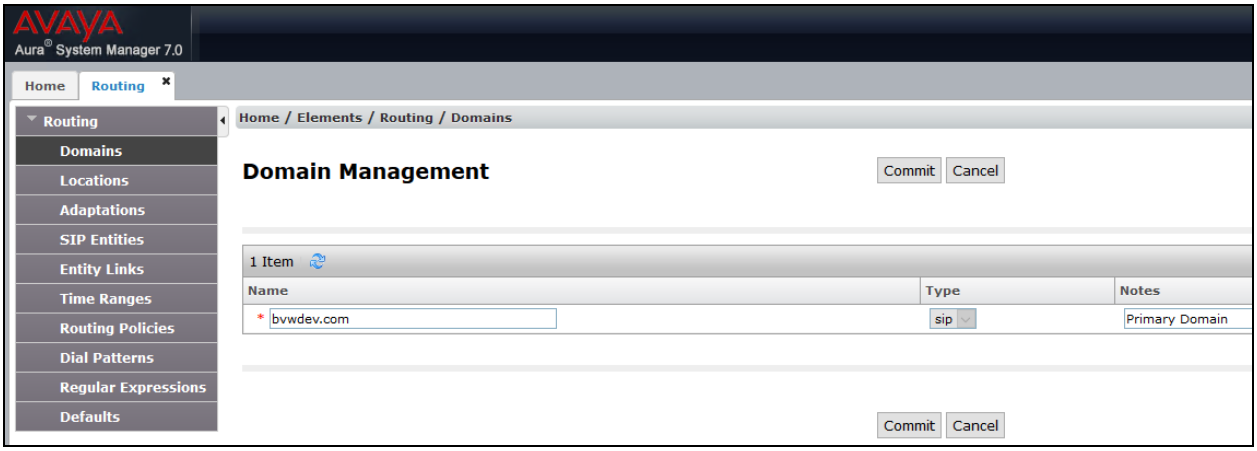


6.2. Administer Domain

In the subsequent screen (not shown), select **Elements → Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing → Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new domain



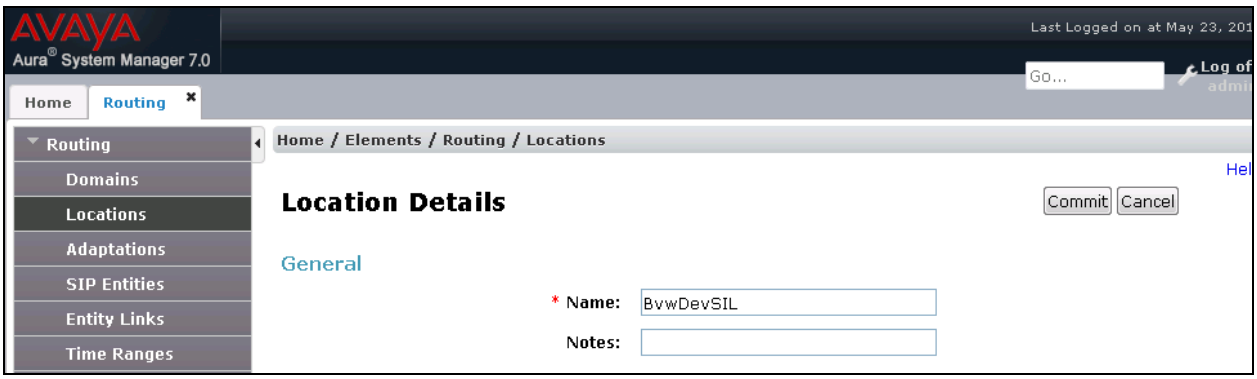
The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select *sip* from the **Type** drop down menu and provide any optional **Notes**.



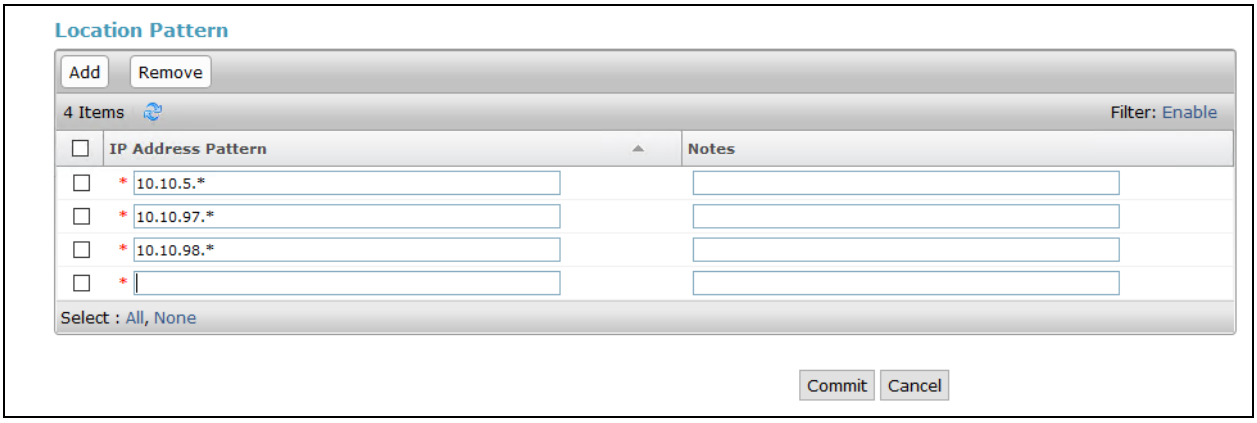
6.3. Administer Locations

Select **Routing → Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for Vision.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.



Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.



6.4. Administer Adaptation

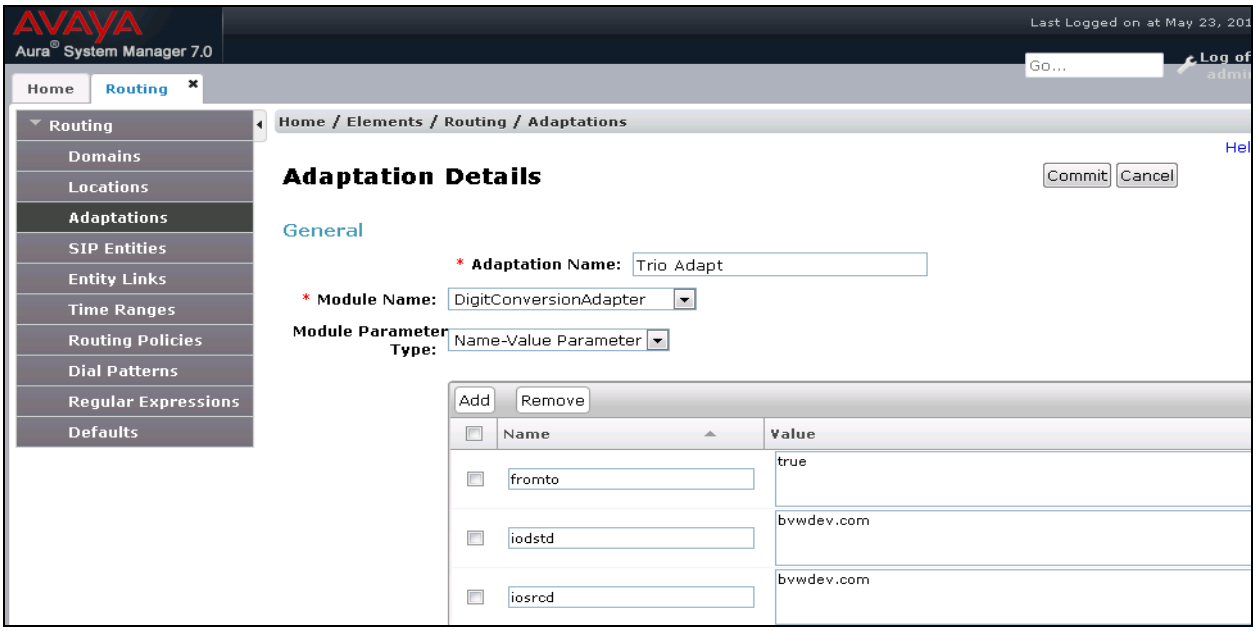
During compliance test, in order to make the call from and to Communication Server 1000 via Session Manager, Adaptation to translate IP address into domain name is used for Trio SIP entity. Here is step on how to create Adaptation. Select **Adaptations** on the left panel menu and then click on the **New** button in the main window (not shown). Enter the following for the Trio Adaptation.

- **Adaptation Name** An informative name (e.g., **change IP to Domain Trio**)
- **Module Name** Select **DigitConversionAdapter**
- **Module Parameter Type** Select Name-Value Parameter

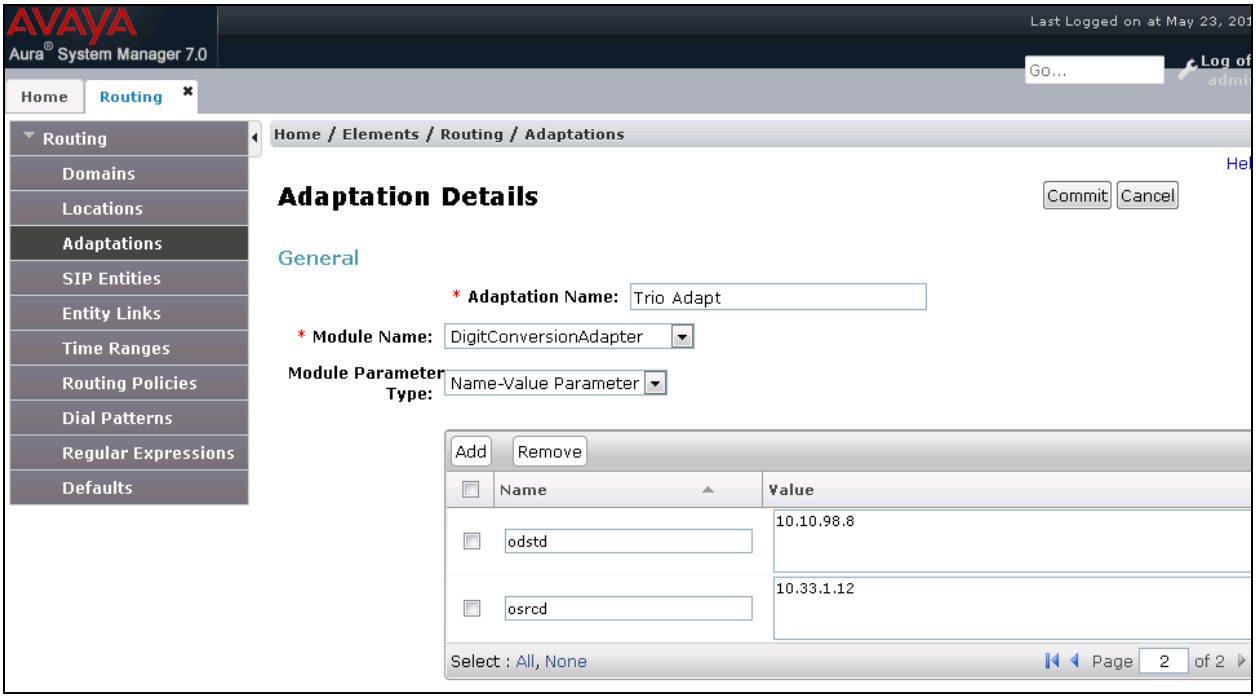
Click **Add** to add a new row for the following values as shown below table:

Name	Value
fromto	true
iodstd	Enter the domain name of system, ex: **bvwdev.com**
iosrcd	Enter the domain name of system, ex: **bvwdev.com**
odstd	Enter IP address of Trio, ex: **10.10.98.8**
osrcd	Enter IP Address of Session Manager, ex: **10.33.1.12**

Once the correct information is entered click the **Commit** button. Here is the screenshot show Adaptation created for Trio.



(Continue) the screenshot show Adaptation created for Trio:



6.5. Administer SIP Entities

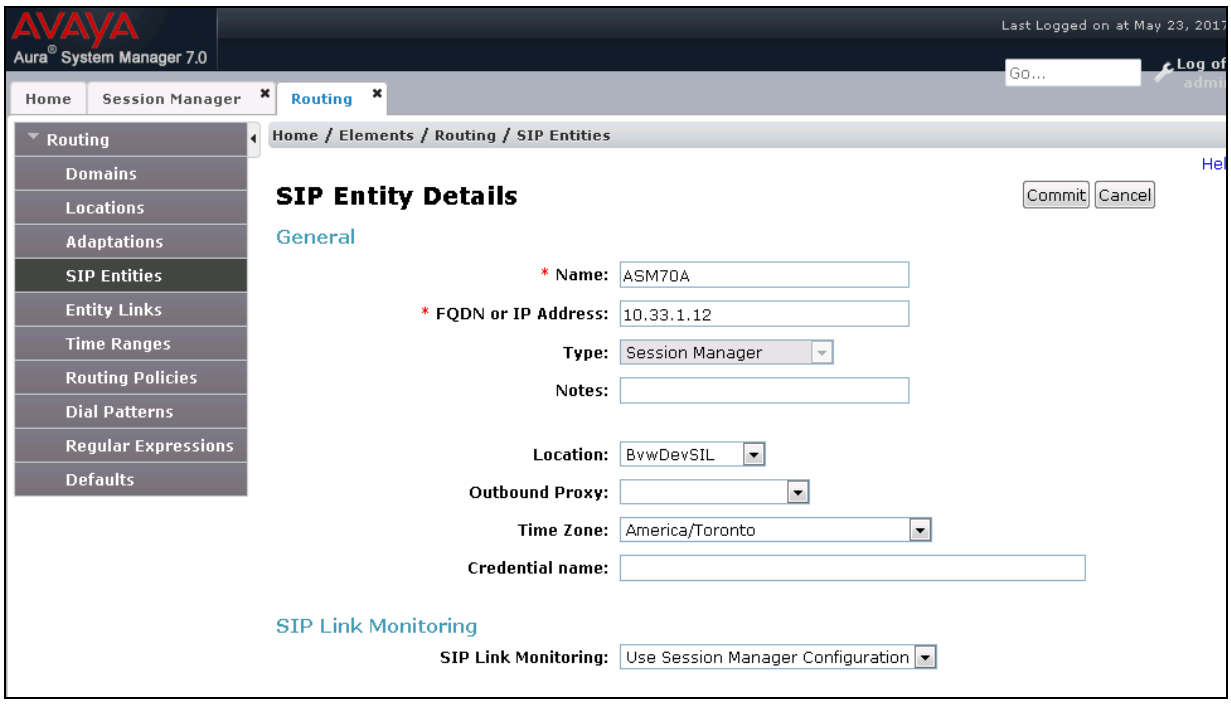
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Server 1000 and Vision.

6.5.1. SIP Entity for Session Manager

Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select ***Session Manager*** for Session Manager.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager** if Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the ***Session Manager*** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

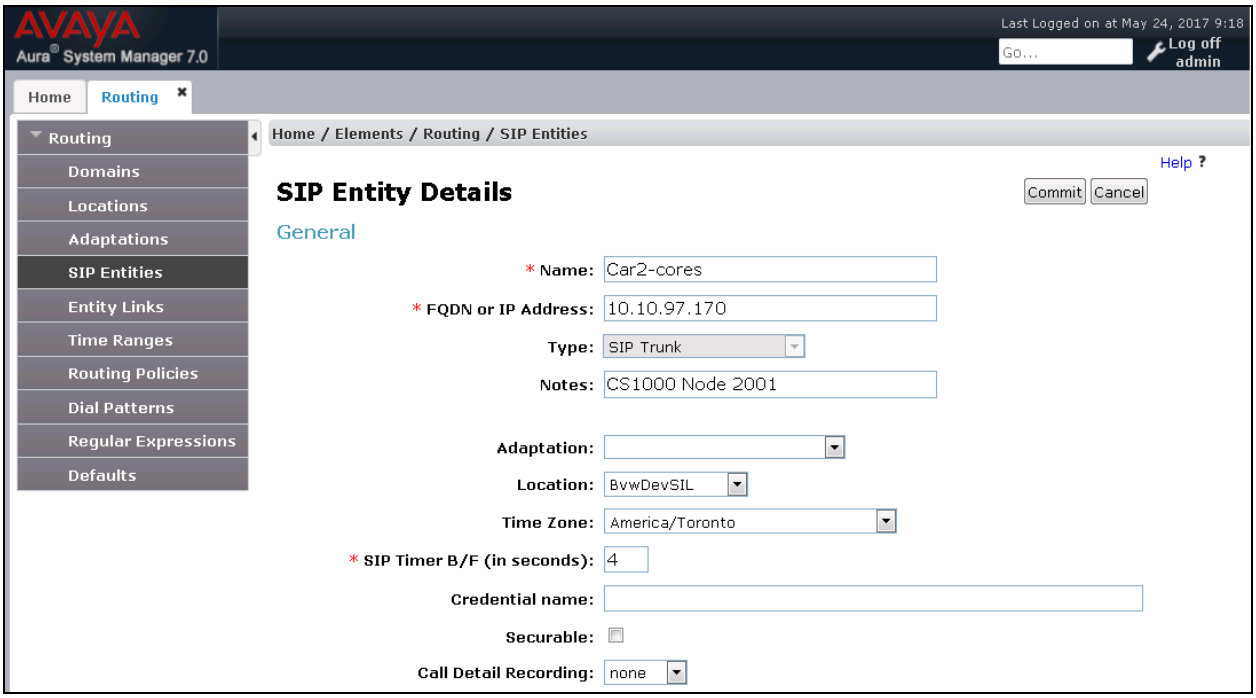


6.5.2. SIP Entity for Communication Server 1000

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Server 1000. Note that this SIP entity is used for integration with Vision.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The node IP address of Communication Server 1000 SIP Gateway as mentioned in **Section 5.2**.
- **Type:** Select "SIP Trunk" in the dropdown list.
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Server 1000.
- **Time Zone:** Select the applicable time zone.

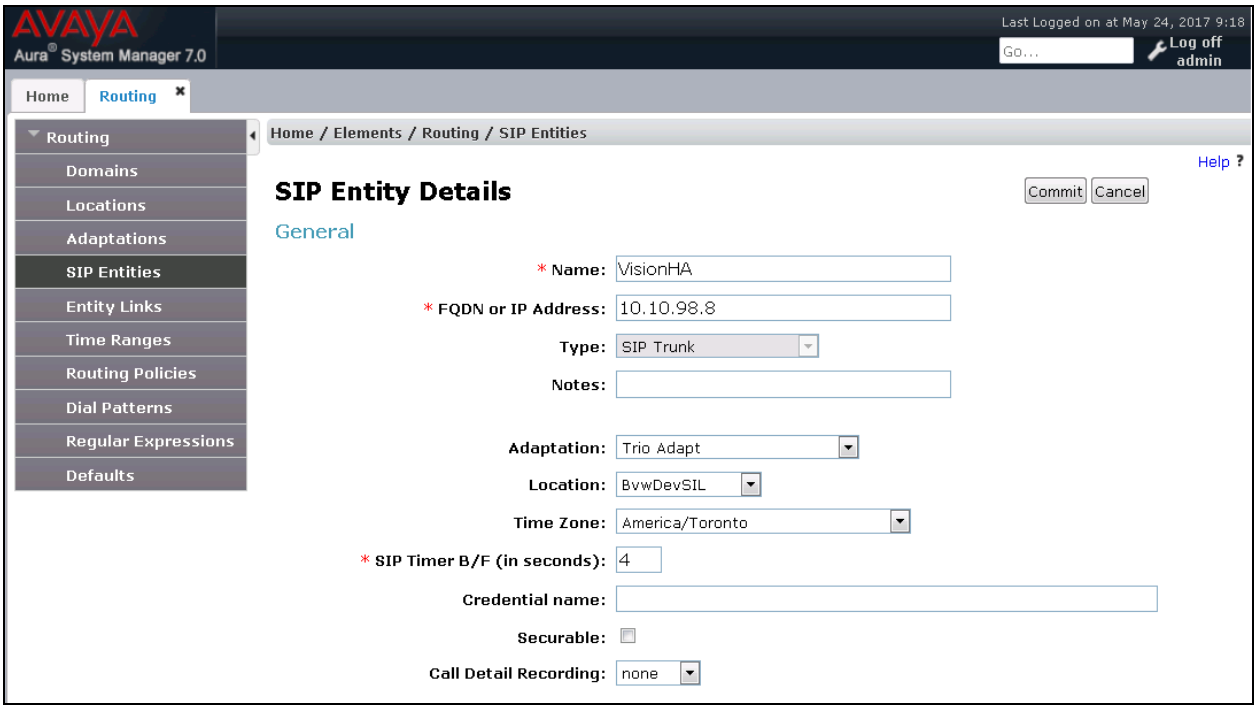


6.5.3. SIP Entity for Vision

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Vision.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Vision server.
- **Type:** Select "SIP Trunk" in the dropdown list.
- **Notes:** Any desired notes.
- **Adaptation:** Select the adaptation configured in **Section 6.4**
- **Location:** Select the applicable location from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.

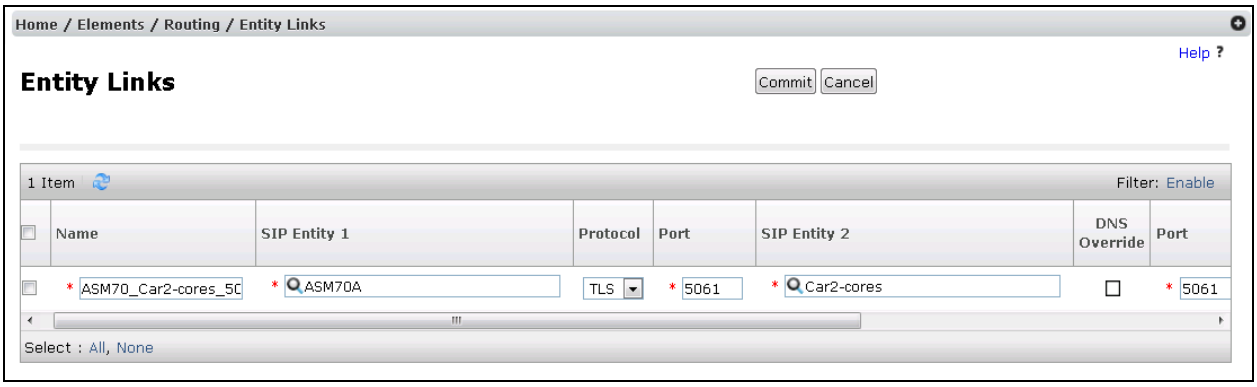


6.6. Administer Entity Links

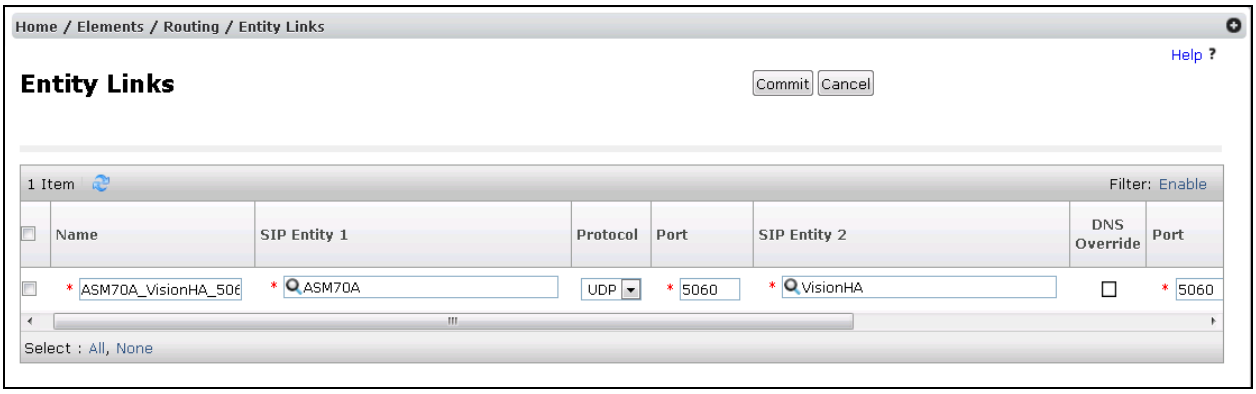
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Server 1000 and one to Vision. To add an Entity Link, select to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select applicable transport protocol.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other systems from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

The screens below show the Entity Link to Communication Server 1000 and Vision. During the compliance test, **TLS** transport with port **5061** was used between Session Manager and Communication Server 1000.



The Entity Link to Vision is shown below; **UDP** transport and port **5060** were used.

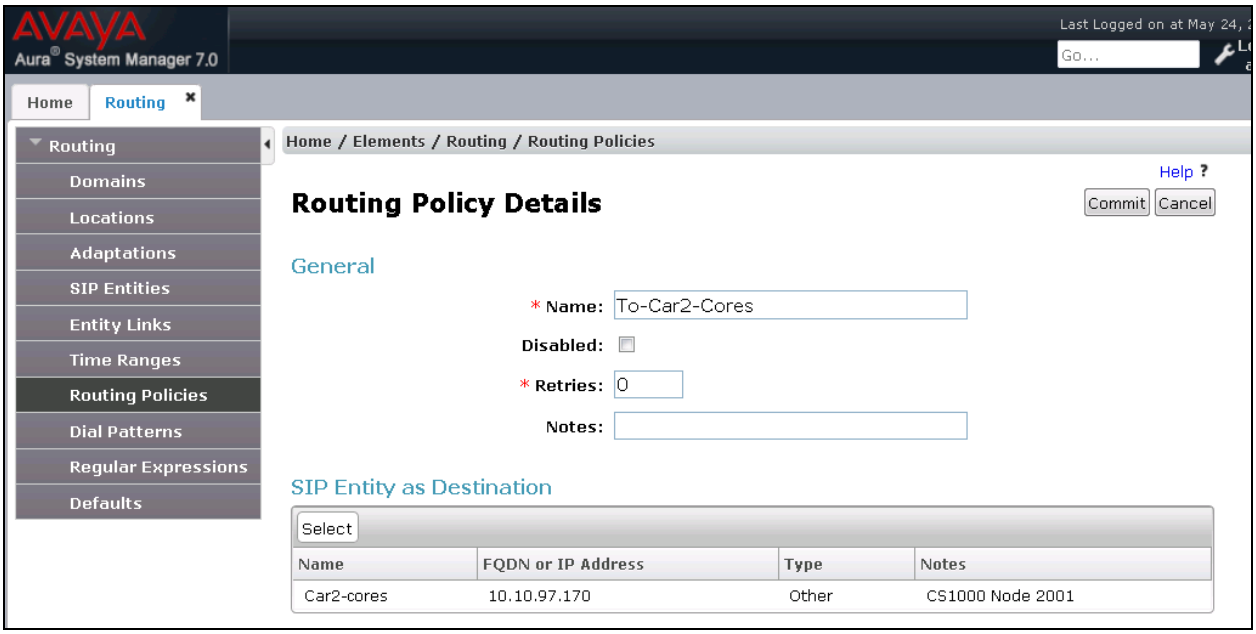


6.7. Administer Routing Policies

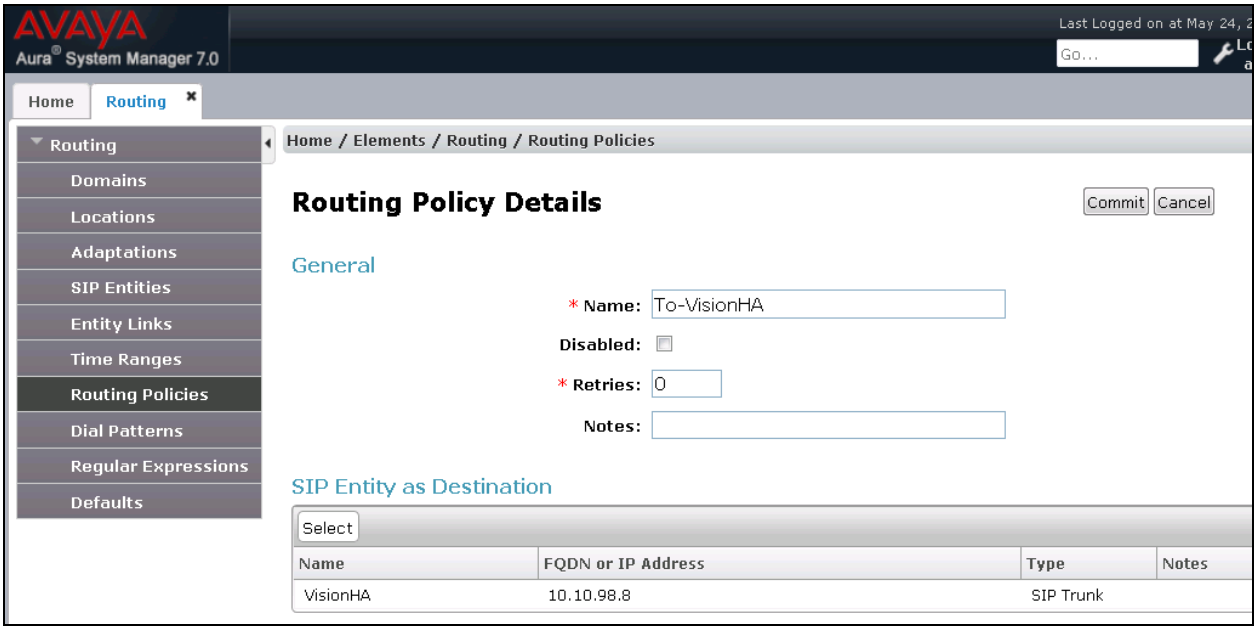
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Server 1000 as the destination, and an incoming policy to Vision. To add a routing policy, select to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policy for Communication Server 1000.



The following screens show the Routing Policy for Vision.



6.8. Administer Dial Patterns

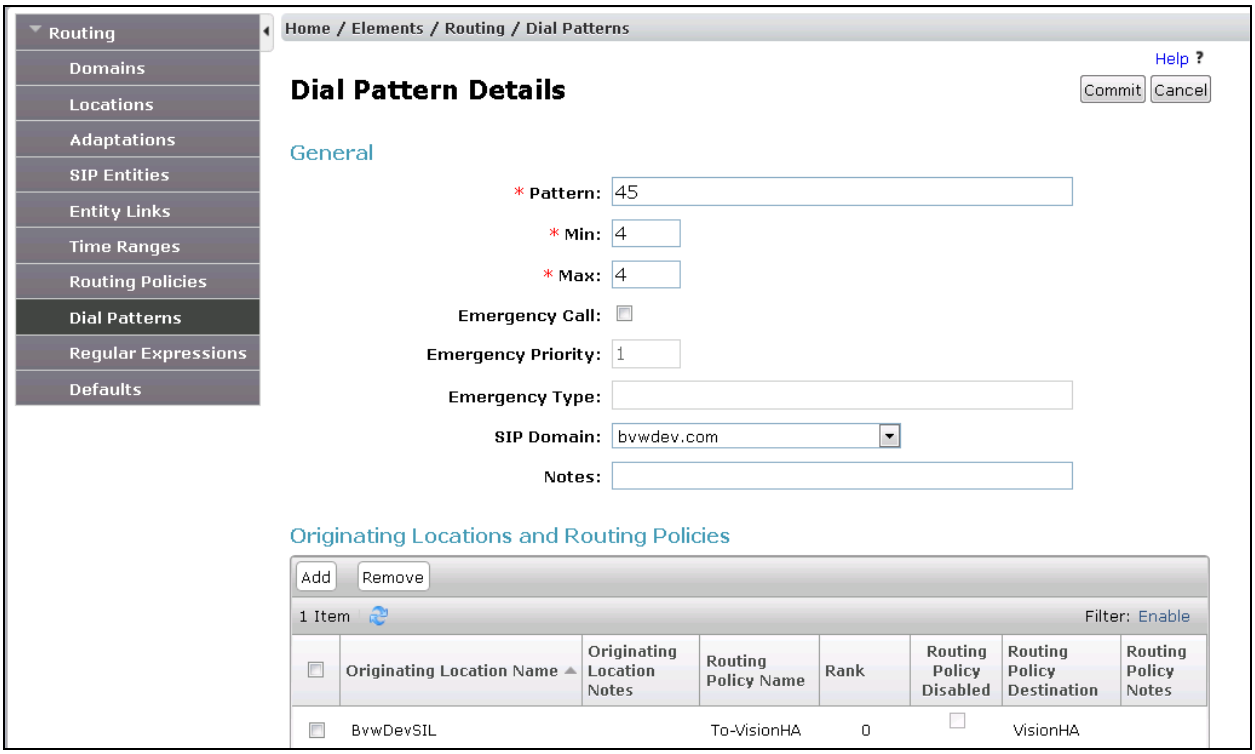
Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Server 1000 to Vision and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location.

6.8.1. Dial Pattern for Vision

Select **Routing → Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Vision. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case "45".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 6.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Vision. In the compliance testing, the entry allowed for call originations from all Communication Server 1000 endpoints in the location "BvwDevSIL". The Vision routing policy from **Section 6.7** was selected as shown below.

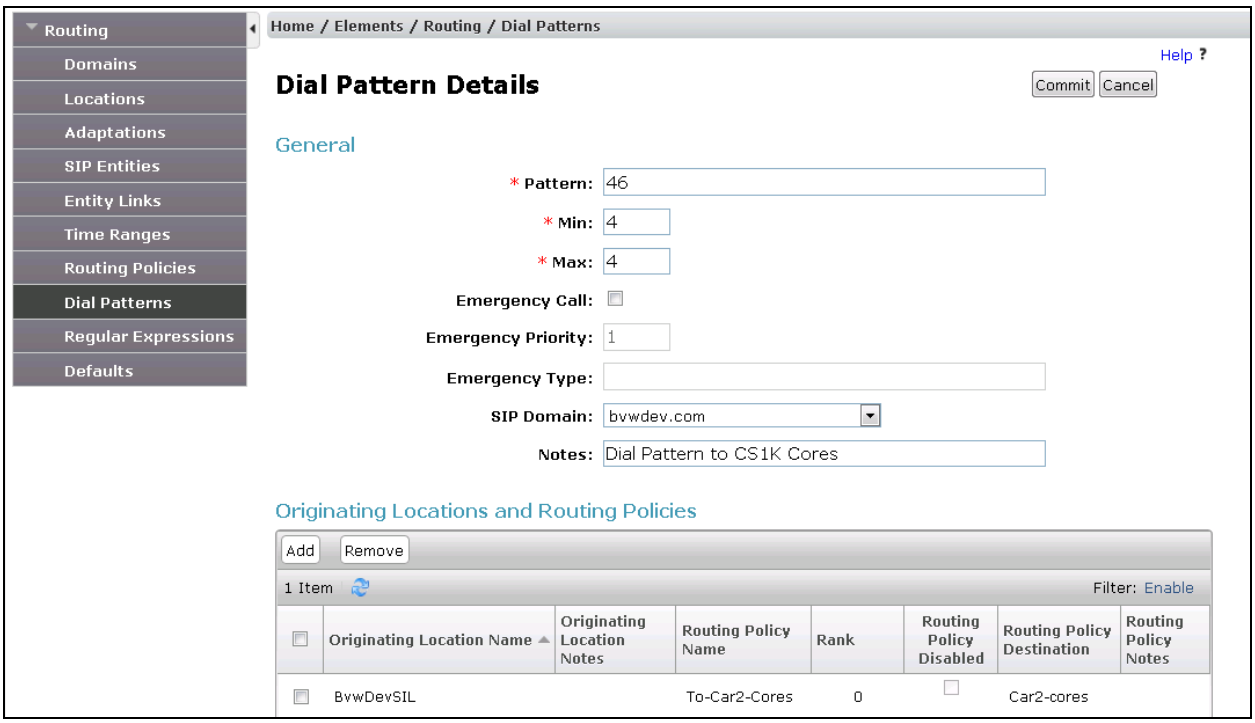


6.8.2. Dial Pattern for Communication Server 1000

Select **Routing → Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Communication Server 1000. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case "46".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 6.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Server 1000. In the compliance testing, the entry allowed for call originations from all Vision endpoints in locations "BvwDevSIL". The Communication Server 1000 routing policy from **Section 6.5** was selected as shown below.

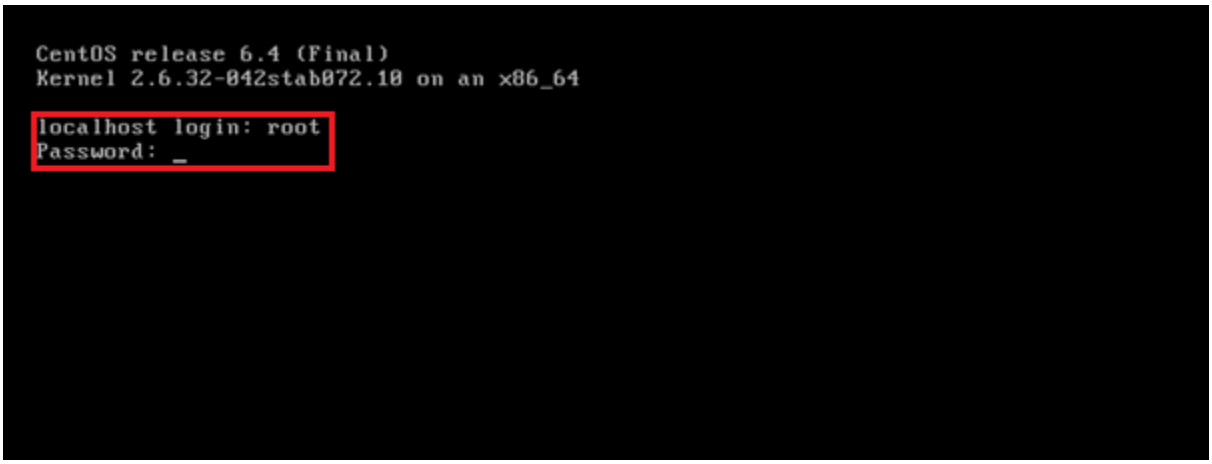


7. Configure Enghouse Vision 8030HA

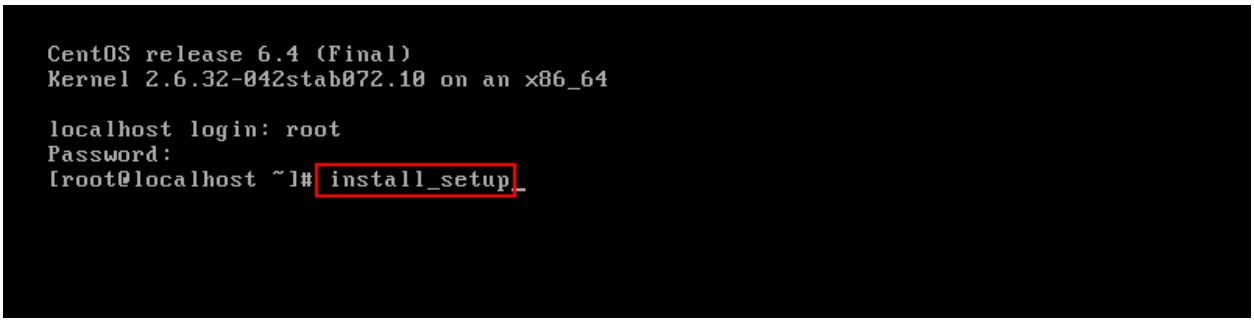
This section shows how to configure Vision 8030HA to successfully connect to Session Manager. The installation of the Vision 8030HA software is assumed to be completed and the correct licence is installed.

7.1. Configure SIP Trunk

Using SSH connect to the Vision 8030HA server and login with as root with the appropriate password.



At the **root@**localhost prompt start the configuration program using the **install_setup** command.



Select option **4** to configure the **SIP trunk**.

```
---- System Settings ----

1. General

2. Current DHCP Network

3. Current DHCP DNS

4. SIP trunk

5. Additional features

6. Update/Import

Change section 1-6 or (E)xit: 4_
```

Select option 1

```
---- SIP Trunk Settings ----

1. T1 PBX IP addr: 1.2.3.4
2. T1    PBX port: 5060
3.     SIP domain:

Change 1-3 or (B)ack: 1_
```

Enter the signaling IP address of Session Manager.

```
---- SIP Trunk Settings ----

1. T1 PBX IP addr: 1.2.3.4
2. T1    PBX port: 5060
3.     SIP domain:

Change 1-3 or (B)ack: 1

  IP or name: 10.33.1.12_
```

Select option 3.

```
---- SIP Trunk Settings ----

1. T1 PBX IP addr: 10.33.1.12
2. T1    PBX port: 5060
3.     SIP domain:

Change 1-3 or (B)ack: 3_
```

Enter the SIP domain **bvwdev.com** as configured in **Section 6.2**.

```
---- SIP Trunk Settings ----

1. T1 PBX IP addr: 10.33.1.12
2. T1    PBX port: 5060
3.     SIP domain:

Change 1-3 or (B)ack: 3

    SIP domain: bvwdev.com_
```

Return back to the previous menu.

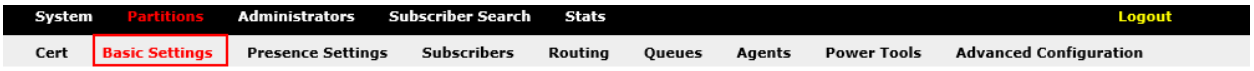
```
---- SIP Trunk Settings ----

1. T1 PBX IP addr: 10.33.1.12
2. T1    PBX port: 5060
3.     SIP domain: bvwdev.com

Change 1-3 or (B)ack: b_
```

Exit from the setup and reboot the server.

```
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# shutdown -r now
```

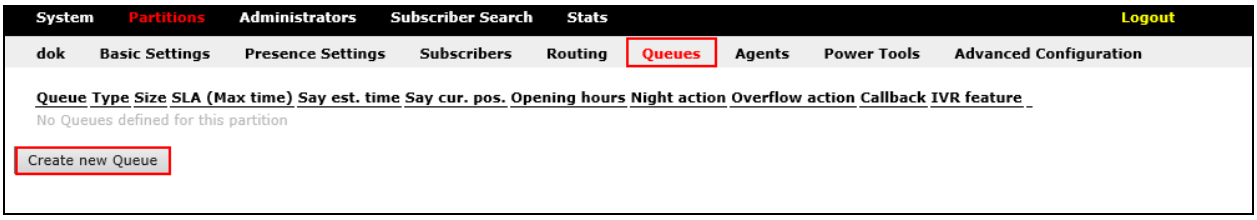
7.2. Configure Operator queue

Log on to the partition manager and go to the "Basic Settings" tab.

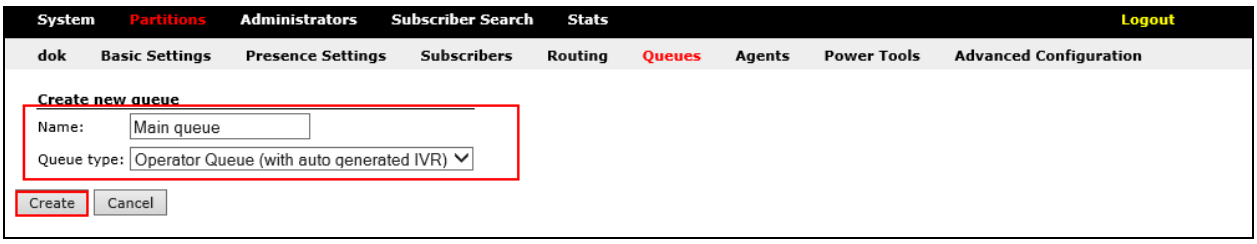


Enter the queue number, in this scenario the queue number was **4500**. Click **Save** when done.

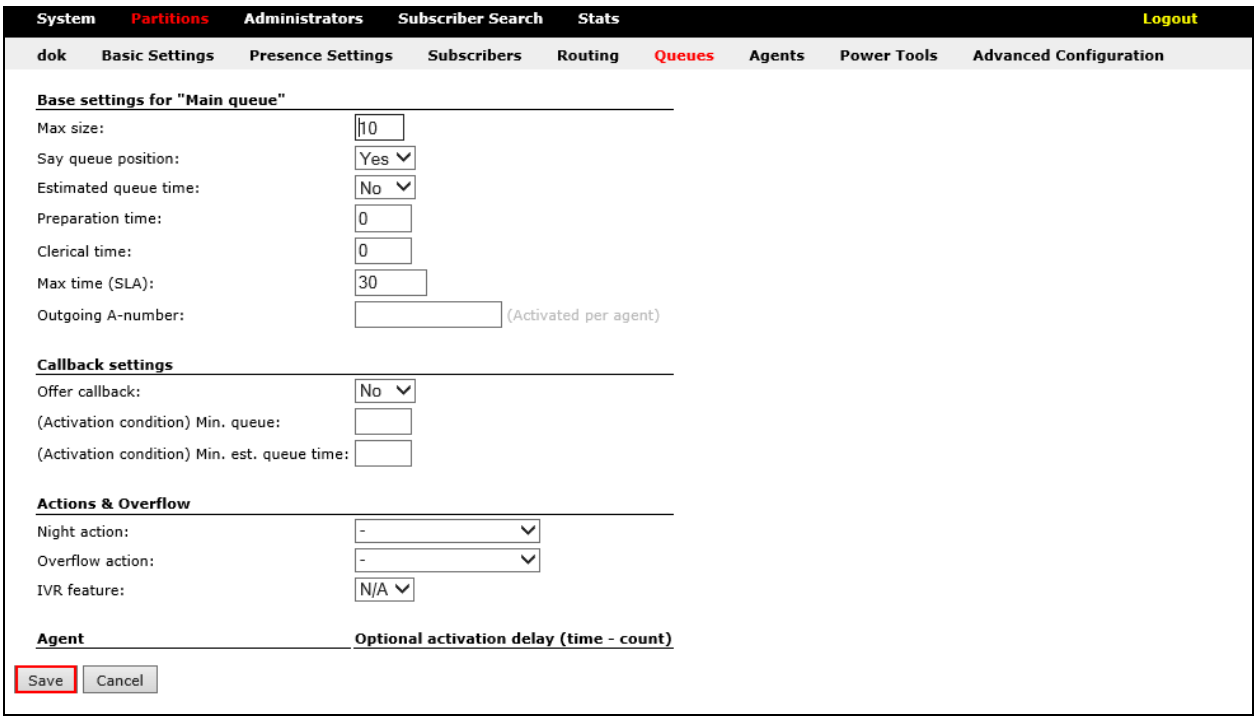
Browse to the "Queues" tab and select to create a new queue.



Give the queue a suitable name, and select queue type "Operator Queue". Click **Create** when done.

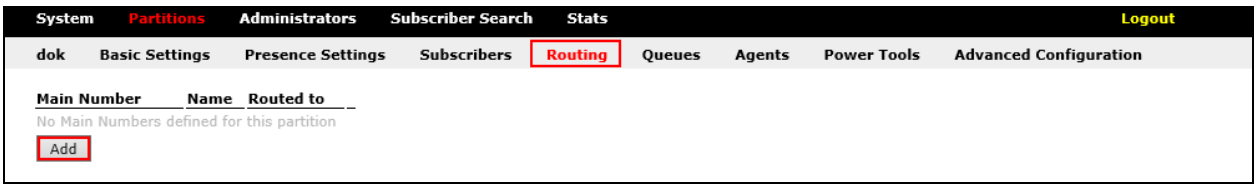


Set the queue preferences and click **Save**.

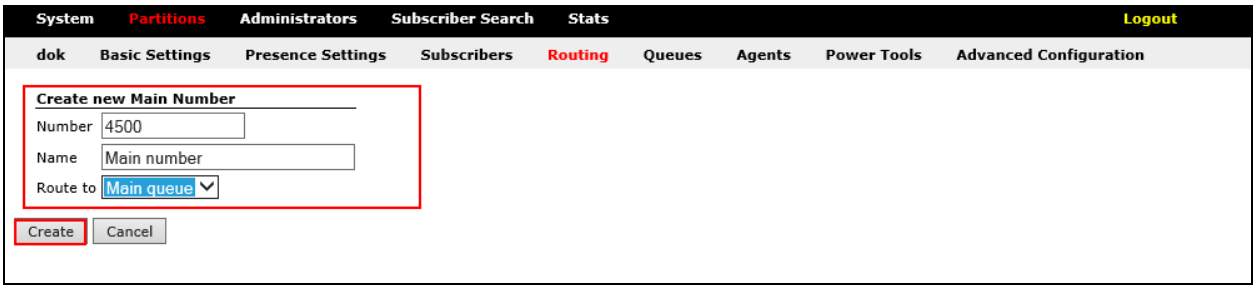


7.3. Configure routing to queue

Go to the "Routing" tab and select **Add**.

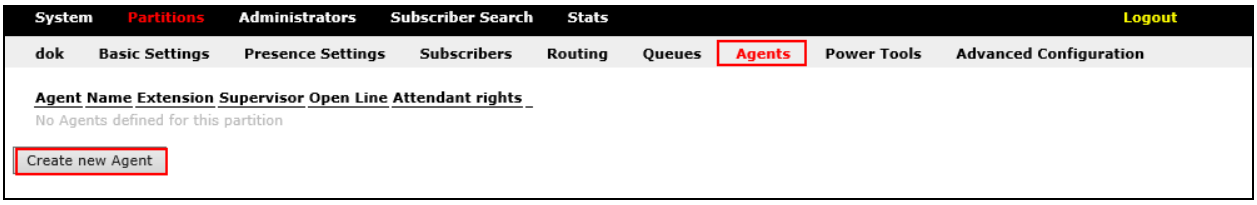


Enter the number to route, give the route a suitable name and select where to route the call. In this scenario number 4500 is given the name "Main number" and is routed to the "Main queue". Click **Create** when done.



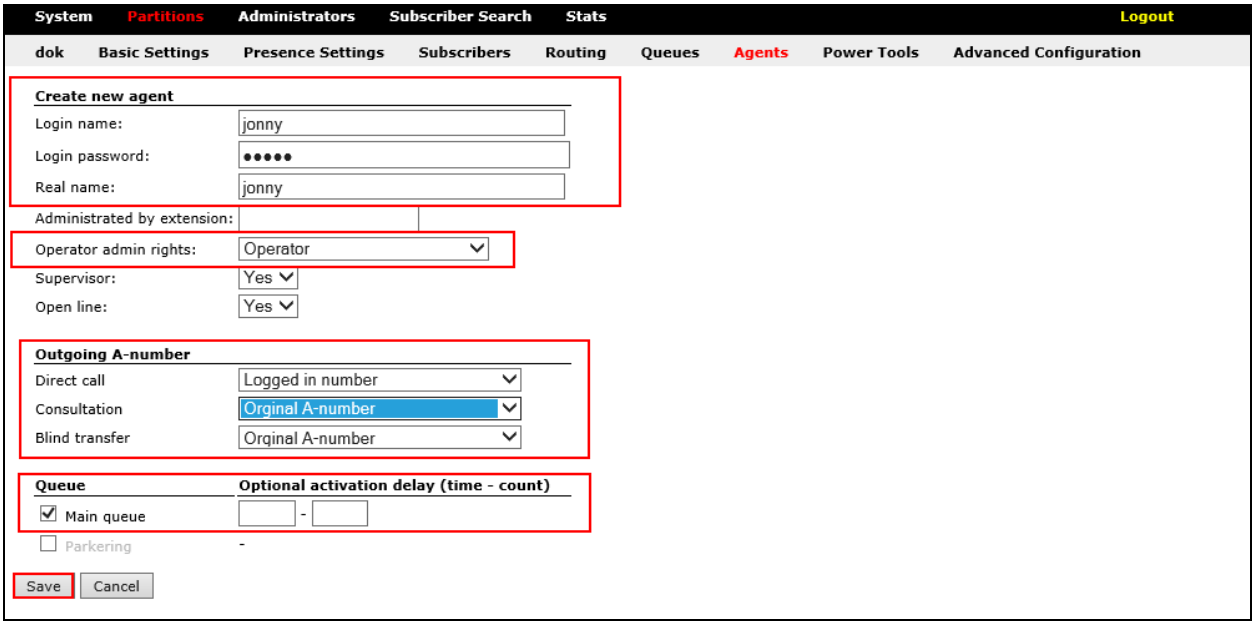
7.4. Setting up attendant

Go to the “Agents tab and select to create a new agent.



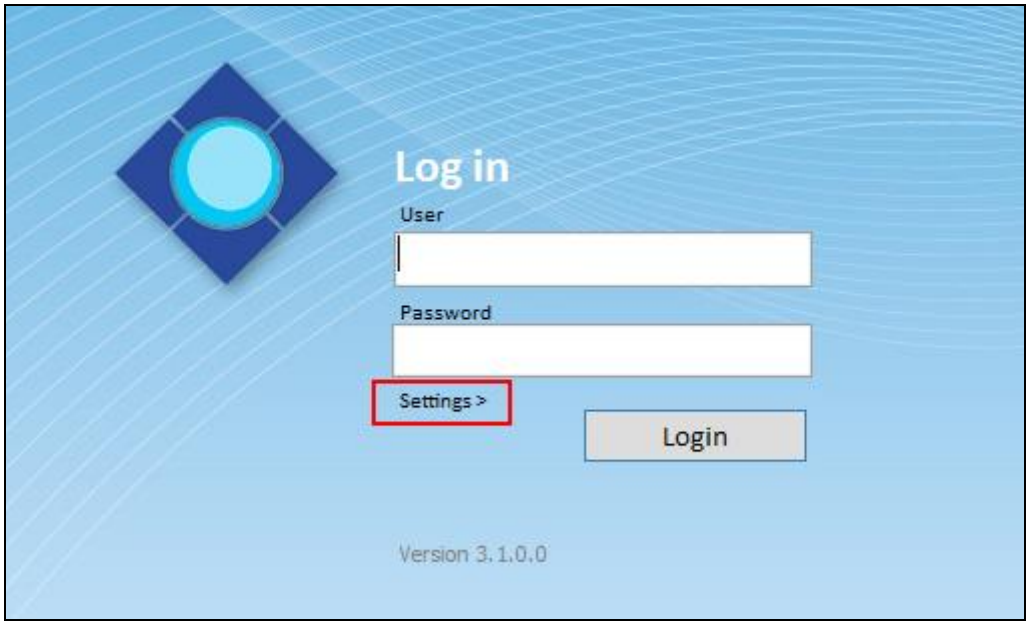
In the **Create new agent** section, enter the attendant a login name in the **Login name** field, in this scenario “jonny” and enter the attendant a password in the **Login password** field. Select the rights to “Operator” in the **Operator admin rights** dropdown menu.

In the **Outgoing A-number** section, specify A-number settings in this scenario attendant uses logged in number for spontaneous calls and original a-number for transfers. Select which queue the attendant will service, in this scenario “Main queue”. Click **Save** when done.

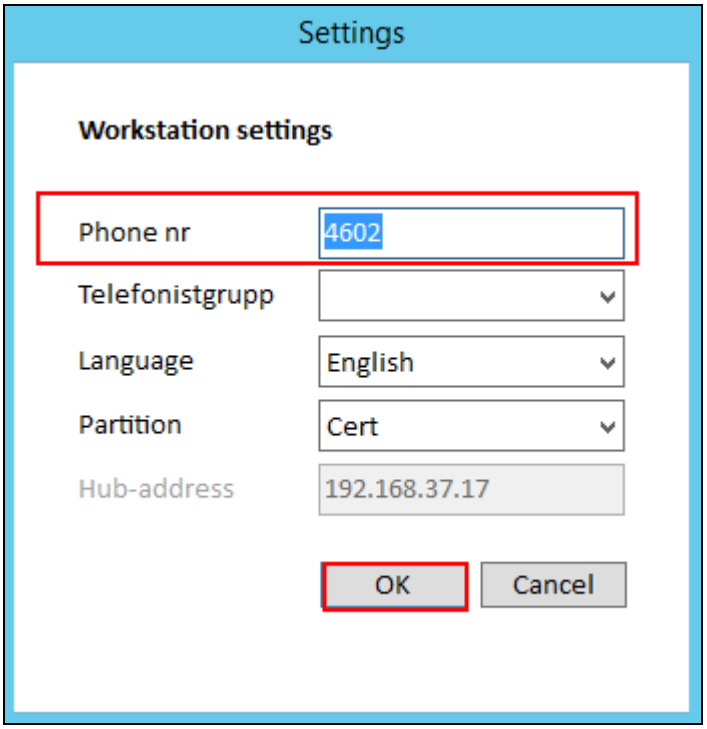


7.5. Running the attendant client

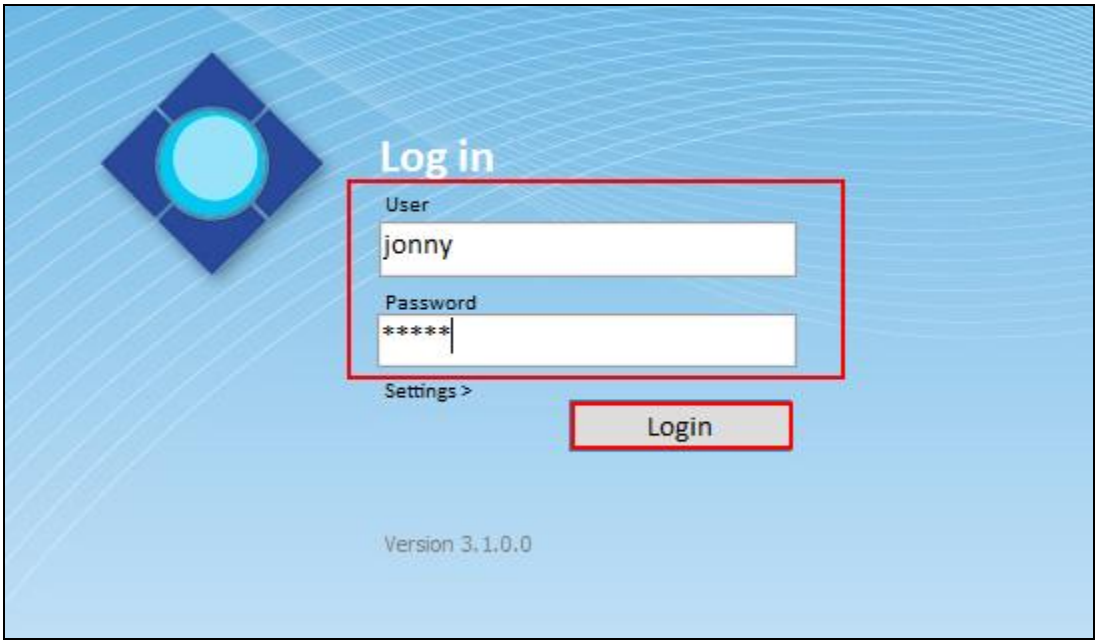
Start the “svara” application and click settings.



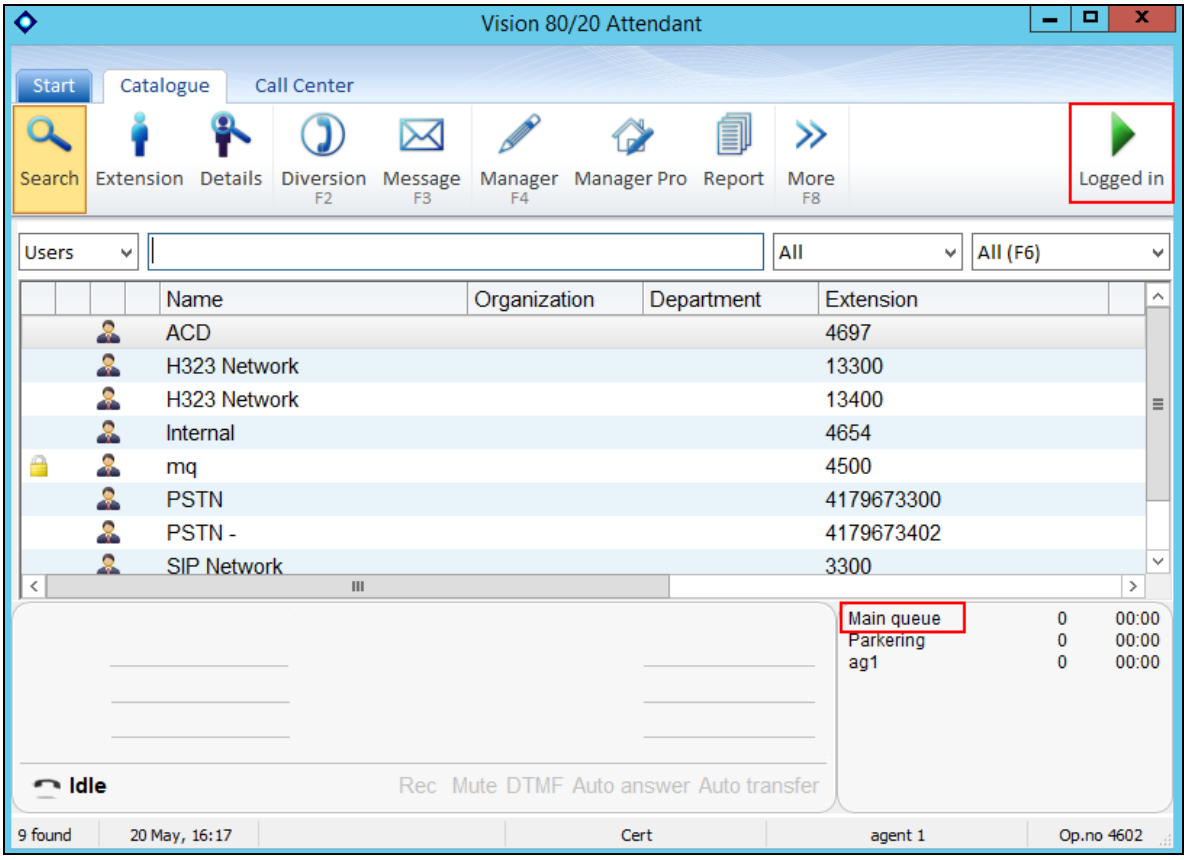
Select which telephone number in the Communication Server 1000 to be used as attendant phone in this case the number is **4602**, and click **OK**.



Enter the credentials as configured in the step above and click **Login**.



When logged in it should be able to see which queue the attendant is servicing

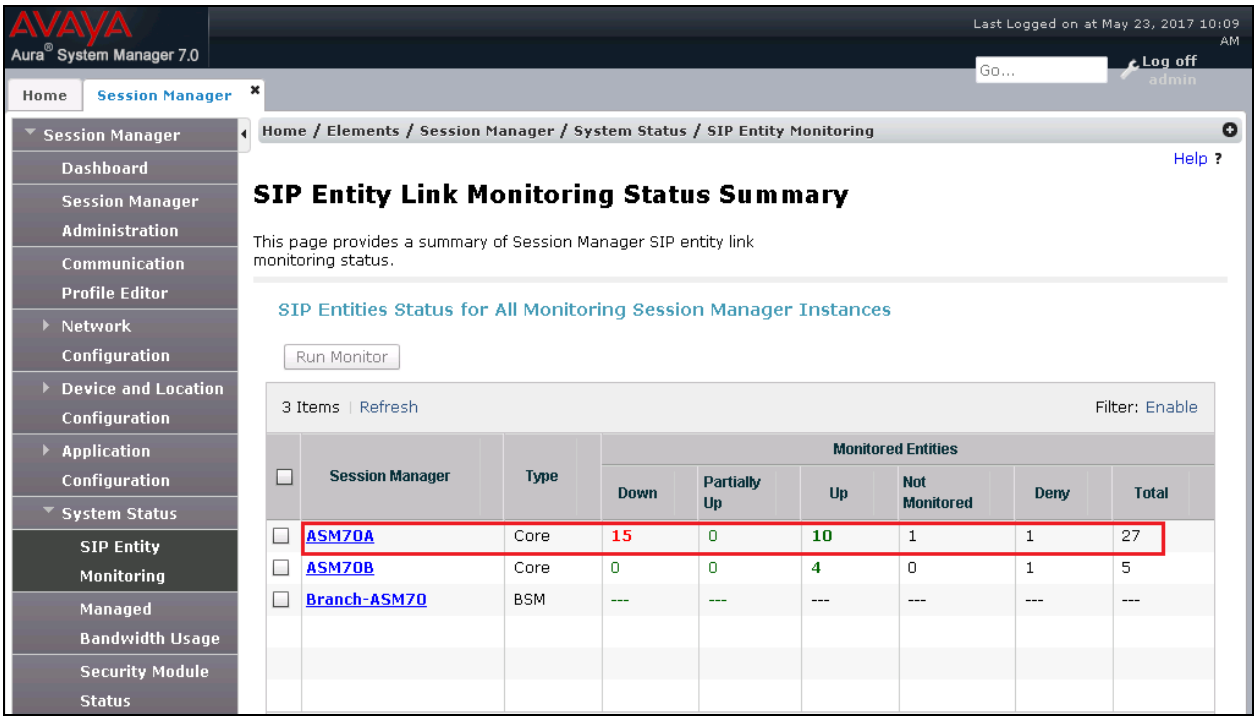


8. Verification Steps

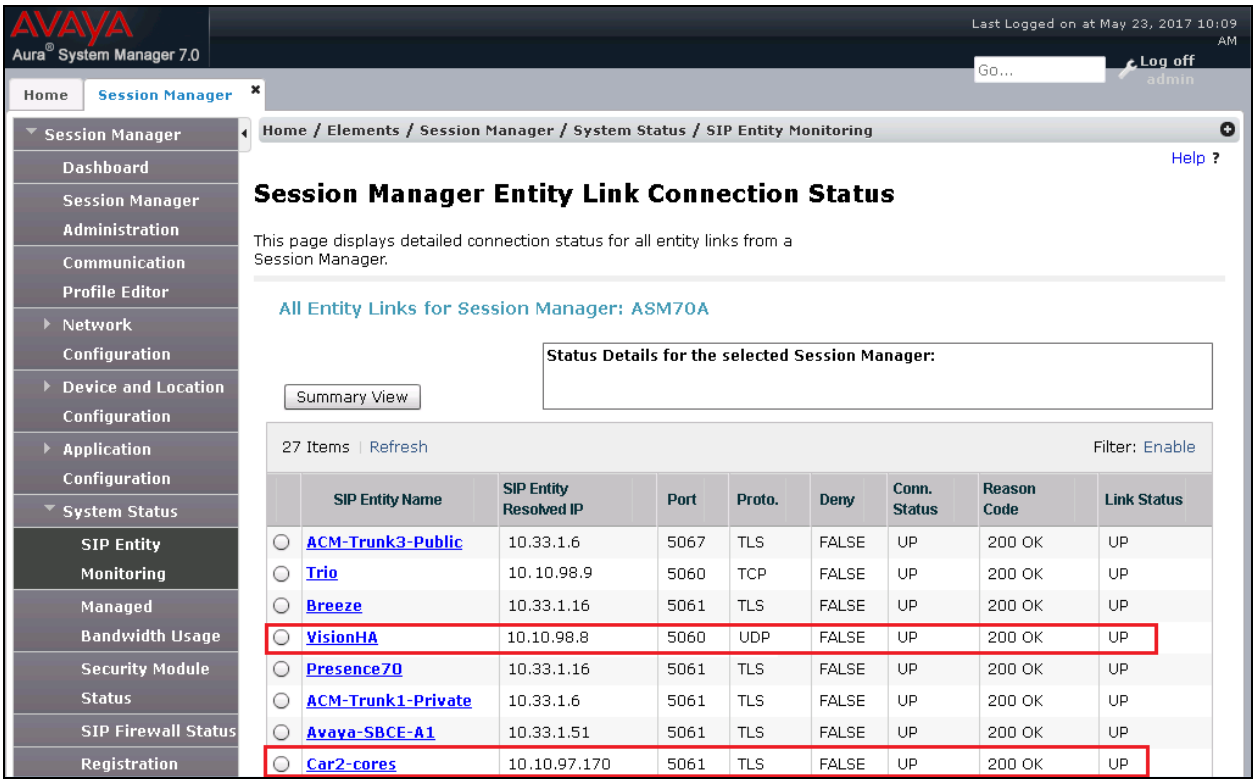
This section provides the tests that can be performed to verify correct configuration of Communication Server 1000 and Vision with Session Manager.

8.1. Verify Session Manager

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Click the Session Manager instance (***ASM70A*** in the example below).



Verify that the state of the Session Manager links to Communication Server 1000 and Vision under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
ACM-Trunk3-Public	10.33.1.6	5067	TLS	FALSE	UP	200 OK	UP
Trio	10.10.98.9	5060	TCP	FALSE	UP	200 OK	UP
Breeze	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
VisionHA	10.10.98.8	5060	UDP	FALSE	UP	200 OK	UP
Presence70	10.33.1.16	5061	TLS	FALSE	UP	200 OK	UP
ACM-Trunk1-Private	10.33.1.6	5061	TLS	FALSE	UP	200 OK	UP
Avaya-SBCE-A1	10.33.1.51	5061	TLS	FALSE	UP	200 OK	UP
Car2-cores	10.10.97.170	5061	TLS	FALSE	UP	200 OK	UP

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements → Session Manager →System Tools → Call Routing Test**. Enter the requested data to run the test.

9. Conclusion

These Application Notes describe the configuration steps required for Vision 2020 3.1HA from Enghouse Interactive AB to successfully interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager using SIP trunks. Vision passed all compliance testing successfully; please see **Section 2.2** of these Application Notes for results and observations if any.

10. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at http://support.avaya.com.

Avaya:

1. *Communication Server 1000E Installation and Commissioning*, Release 7.6, NN43041-310
2. *Element Manager System Reference – Administration - Avaya Communication Server 1000*, Release 7.6, NN43001-632.
3. *Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals* Release 7.6, *NN43001*-509.
4. *Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals* -, Release 7.6, NN43001-116.
5. *Avaya Communication Server 1000 - Software Input Output Reference — Administration* Release 7.6, NN43001-611.
6. *Avaya Communication Server 1000 - ISDN Primary Rate Interface Installation and Commissioning*, Release 7.6, NN43001-301.
7. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
8. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
9. *Deploying Avaya Aura® System Manager*, Release 7.0.
10. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.

All information on the product installation and configuration Vision Server can be found at http://enghouseinteractive.com

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.