Avaya Solution & Interoperability Test Lab

Application Notes for Vision 80/20 from Enghouse Interactive AB with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using a SIP Trunk Connection - Issue 1.0

Abstract

These Application Notes describe how to configure Avaya Aura® Communication Manager and Avaya Aura® Session Manager to interface with Vision 80/20, which is operating as an attendant answering position. Vision 80/20 is a software application from Enghouse Interactive AB installed on a number of Linux and Windows servers that interface with Avaya Aura® Communication Manager 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 how to configure Avaya Aura® Communication Manager R8.0 and Avaya Aura® Session Manager R8.0 to interface with Vision 80/20 (hereafter referred to as Vision) release 3.1, which is operating as an attendant answering position. Vision 80/20 is a software application from Enghouse Interactive AB installed on a number of Linux and Windows servers that interface with Avaya Aura® Communication Manager 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. The application also uses Avaya Aura® Application Enablement Services to provide operators with a method to remotely redirect calls to the attendant when users are away from their phone for lunch, breaks or similar absences.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using Communication Manager and Session Manager. The Vision server uses a SIP trunk connection to Session Manager. See **Figure 1** for a network diagram. An incoming call handling rule was created 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 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.

In order to enable the attendant to set a user's status when away from the phone, the solution uses Avaya Aura® Application Enablement Services to perform a TSAPI function to route all calls to the attendant.

A variety of Avaya telephones were used for both the attendant position, and the users as described in **Section 4**.

Note: The Vision server places a call to the attendant's deskphone. When the attendant is called, the Vision server calls the attendant's 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 systems 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
- Remotely monitoring user status and setting call forwarding to the attendant
- Ability to recover following network outages between Session Manager and Application Enablement Services and the Vision systems

2.2. Test Results

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

It should be noted that Vision uses Application Enablement Services to set a redirect on Avaya phones when the user will be away for breaks, etc. This method does not work on SIPCC phones but does work on all other phone types. This is an Avaya limitation, but the target audience for the Vision 80/20 solution is typically not a call center environment.

2.3. Support

For technical support for Enghouse Interactive AB products, please use the following web link.
https://mysupport.enghouse.com

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 Vision 80/20 server connects to Session Manager using a SIP Trunk. A variety of Avaya deskphones were used as Vision 80/20 Attendant telephones during compliance testing. A PRI/T1 trunk on a Media Gateway was configured to connect to the PSTN. SIP calls originating from Vision were routed through Session Manager to Communication Manager and then to Avaya phones or the PSTN.

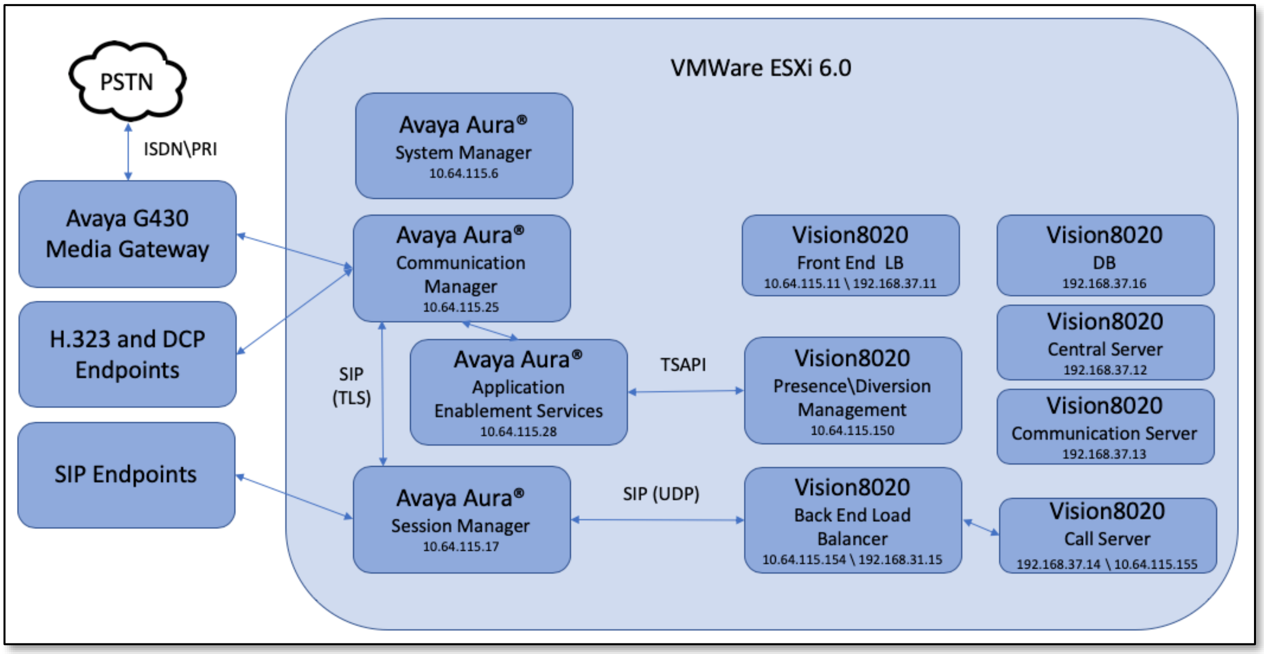


Figure 1: Enghouse Vision 80/20 Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on VMWare ESXi 6.0	R8.0.0.0.098174
Avaya Aura® Session Manager running on VMWare ESXi 6.0	R8.0.0.0.800035
Avaya Aura® Communication Manager running on VMWare ESXi 6.0	R.018x.00.0.822.0 (R8.0GA)
Avaya Aura® Application Enablement Services running on VMWare ESXi 6.0	R8.0.0.0.0.6-0
Avaya Phones • 9611 (H.323) • 9650 (H.323) • 6408D+ (DCP) • 9641G (SIP) • J169 (SIP) • J179 (SIP)	 6.6506 3.280A N/A 7.1.1.09 3.0.0.1.6 3.0.0.1.6
Avaya G430 Media Gateway	40.10.0/1
Enghouse Vision 8020 – CentOS on ESXi 6.0	R3.1
Enghouse Vision 8020 – Windows 2012R2 on ESXi 6.0	R3.1

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using an SSH System Access Terminal (SAT) session. The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows:

- Verify License
- Administer SIP Trunk Group
- Administer SIP Signaling Group
- Administer SIP Trunk Group Members
- Administer IP Network Region
- Administer IP Codec Set
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan
- Administer Uniform Dial Plan
- Administer AAR Analysis

5.1. Verify License

Verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "**display system-parameters customer-options**" command. 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.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 1000  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 1000  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 1000  0
                       Maximum Administered SIP Trunks: 4000  20
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

5.2. Administer SIP Trunk Group

An existing SIP Trunk was used for this testing, the following values demonstrate the settings.

- **Group Type:** *sip*
- **Group Name:** A descriptive name
- **TAC:** An available trunk access code
- **Service Type:** *tie*

```
change trunk-group 10                                           Page   1 of   4
                                TRUNK GROUP

Group Number: 10                   Group Type: sip           CDR Reports: y
  Group Name: ToSM2                       COR: 1        TN: 1        TAC: 110
   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:
                                                    Number of Members:
```

Navigate to **Page 3** and enter *private* for **Numbering Format**.

```
change trunk-group 10                                           Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no





 Show ANSWERED BY on Display? y

 DSN Term? n
```

5.3. Administer SIP Signaling Group

An existing SIP Signaling Group was used for this testing, the following values demonstrate the settings.

- **Group Type:** *sip*
- **Transport Method:** *tls*
- **Near-end Node Name:** An existing C-LAN node name or *procr*
- **Far-end Node Name:** The existing node name for Session Manager
- **Near-end Listen Port:** An available port for integration with Session Manager
- **Far-end Listen Port:** The same port number as used in **Section 6.6**
- **Far-end Network Region:** An existing network region to use with Session Manager
- **Far-end Domain:** The applicable domain name for the network
- **Direct IP-IP Audio Connections:** *y*

```
change signaling-group 10                                       Page   1 of   3
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                      Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                   Far-end Node Name: sildvsm2
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1

Far-end Domain: sildenver.org
                                             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? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                   Alternate Route Timer(sec): 6
```

5.4. Administer SIP Trunk Group Members

Use the "**change trunk-group n**" command, where "**n**" is the trunk group number from **Section 5.2**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.3**.
- **Number of Members:** The desired number of members, in this case *10*.

```
change trunk-group 10                                              Page   1 of   4
                                TRUNK GROUP

Group Number: 10                   Group Type: sip           CDR Reports: y
  Group Name: ToSM2                       COR: 1        TN: 1        TAC: 110
   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: 10
                                                     Number of Members: 10
```

5.5. Administer IP Network Region

Use the "**change ip-network-region n**" command, where "**n**" is the existing Far-end Network Region number used by the SIP signaling group from **Section 5.3**.

For **Authoritative Domain**, enter the applicable domain for the network as configured in **Section 5.3**. Enter a descriptive **Name**. Enter *yes* for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Vision 80/20.

```
change ip-network-region 1                                         Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: sildenver.org
    Name: SM                    Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   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
```

Navigate to **Page 4**, and specify this codec set to be used for calls with network regions used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region *1* was used by the Avaya endpoints and by the trunk to the PSTN.

```
change ip-network-region 1                                          Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                                all
 2    1     y    NoLimit                                             n       t
 3
```

5.6. Administer IP Codec Set

Use the "**change ip-codec-set n**" command, where "**n**" is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. The codec shown below was used in the compliance testing.

```
change ip-codec-set 1                                               Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A           n         2        20
 2: G.722-64K                  2        20
 3: G.711MU          n         2        20
 4:
 5:
 6:
 7:

     Media Encryption                    Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: aes
 3: none
 4:
```

5.7. Administer Route Pattern

Use the "**change route-pattern n**" command, where "**n**" is an existing route pattern number to be used to reach Vision 80/20, in this case "10". Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.2**.
- **FRL:** A level that allows access to this trunk, with *0* being least restrictive.
- **Numbering Format:** lev0-pvt (private numbering) was used to ensure 5-digit extensions appeared on both ends.

```
change route-pattern 10                                         Page   1 of   4
                    Pattern Number: 10     Pattern Name: toSM2
    SCCAN? n    Secure SIP? n     Used for SIP stations? y
    Primary SM: sildvsm2        Secondary SM: sildvsm3
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 10   0                                                             n   user
 2: 11   0                                                             n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               lev0-pvt  next
 2: y y y y y n  n            rest                               lev0-pvt  rehu
 3: y y y y y n  n            rest                                         none
```

5.8. Administer Private Numbering

Use the "**change private-numbering 0**" command, to define the calling party number to send to Vision 8020. Add an entry for the trunk group defined in **Section 5.20**. In the example shown below, all calls originating from a 5-digit extension beginning with **3** and routed to any trunk group will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

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

Ext Ext               Trk        Private          Total
Len Code              Grp(s)     Prefix           Len
 5  3                                             5  Total Administered: 1
                                                        Maximum Entries: 540
```

5.9. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 45xx to Vision 80/20. Use the "**change dialplan analysis 0**" command and add an entry to specify the use of digits pattern **4**, as shown below.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
 0             1  attd
 1             3  dac
 1             4  udp
 1             11 udp
 3             5  ext
 4             4  aar
 4             5  ext
 5             5  ext
 8             1  fac
 9             1  fac
 *             3  fac
```

5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits **45**xx to Vision 80/20. Note, other routing methods may be used. Use the "**change uniform-dialplan 0**" command and add an entry to specify the use of AAR for routing of digits 45xx, as shown below.

```
change uniform-dialplan 0                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0
  Matching                          Insert                Node
  Pattern             Len Del       Digits       Net Conv Num
 1                    4   0                      aar n
 1                    11  0                      ars n
 31111                5   5                      aar n
 45                   4   4                      aar n
```

5.11. Administer AAR Analysis

Use the "**change aar analysis 0**" command and add an entry to specify how to route calls to 45xx. In the example shown below, calls with digits 45xx will be routed as an AAR call using route pattern *10* from **Section 5.7**.

```
AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 2
          Dialed          Total     Route    Call   Node  ANI
          String        Min  Max   Pattern   Type   Num   Reqd
    1                   4    4      10       aar          n
    2                   7    7      254      aar          n
    3                   5    5      10       aar          n
    31111               5    5      10       aar          n
    4                   7    7      254      aar          n
    45                  4    4      10       aar          n
```

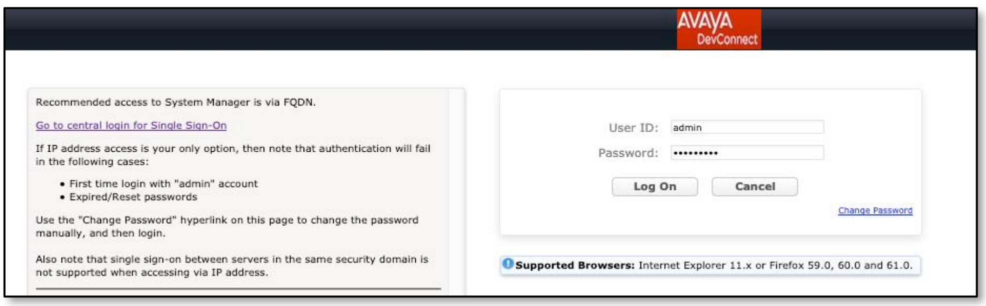
6. Configure Avaya Aura® Session Manager

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

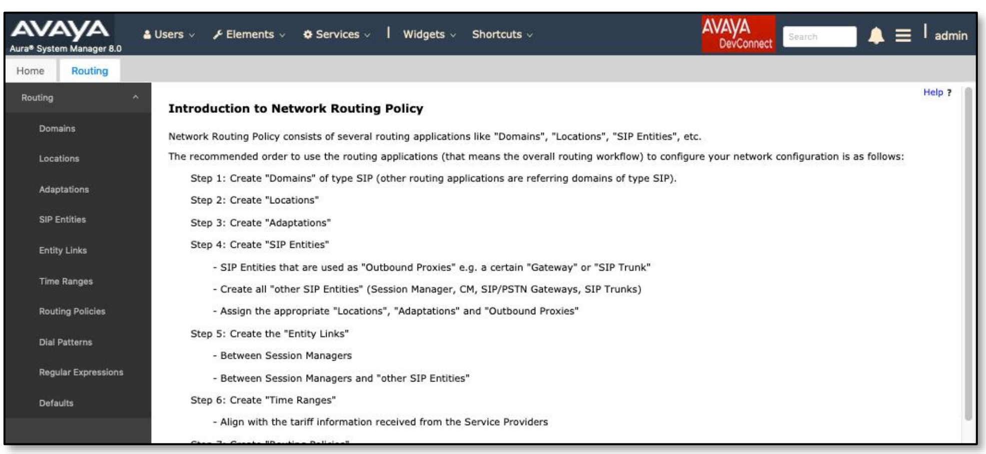
6.1. Launch System Manager

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 or Fully Qualified Domain Name of System Manager. Log in using the appropriate credentials.

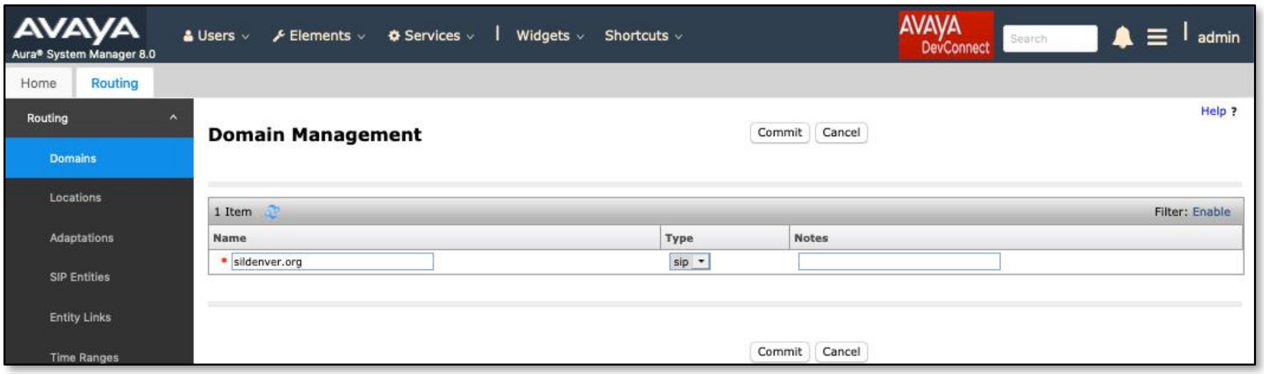


6.2. Administer Domain

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.



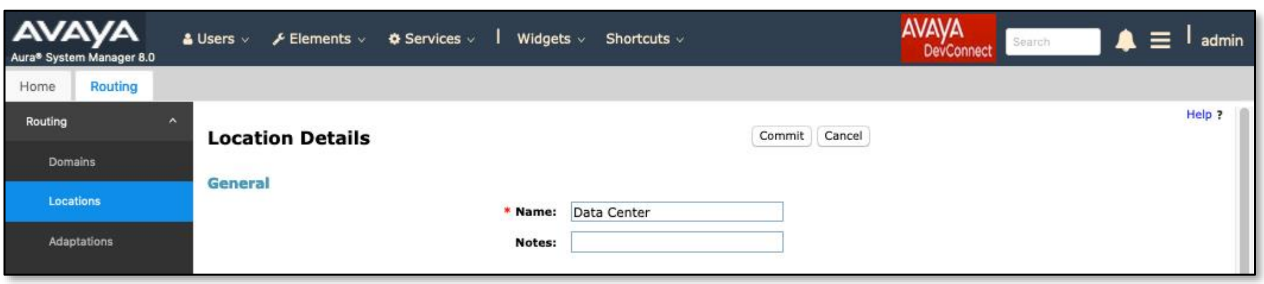
The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select *sip* from the **Type** drop down menu and provide any optional **Notes**.



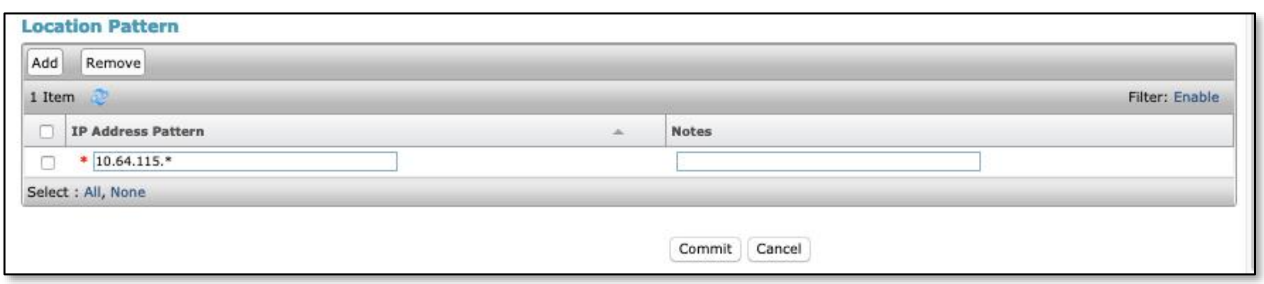
6.3. Administer Locations

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

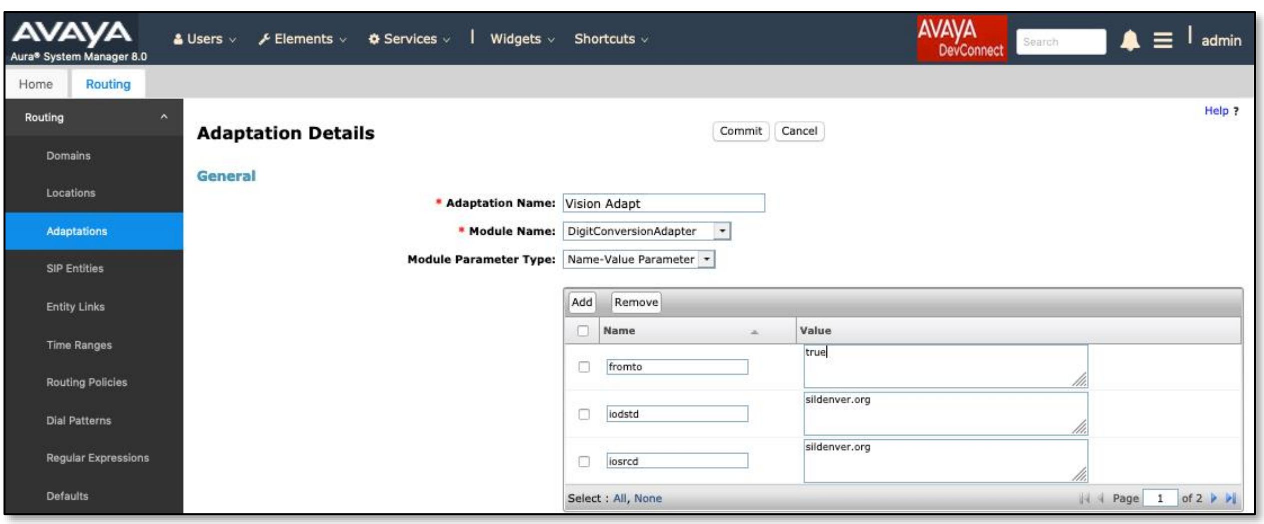
During compliance testing, in order to make the call from and to Communication Manager via Session Manager, an Adaptation to translate IP address into domain name is used for the Vision SIP entity. Here are the steps on how to create the Adaptation. Select **Adaptations** on the left panel menu and then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

- **Adaptation Name** An informative name (e.g., **Vision Adapt**)
- **Module Name** Select **DigitConversionAdapter**
- **Module Parameter Type** Select Name-Value Parameter

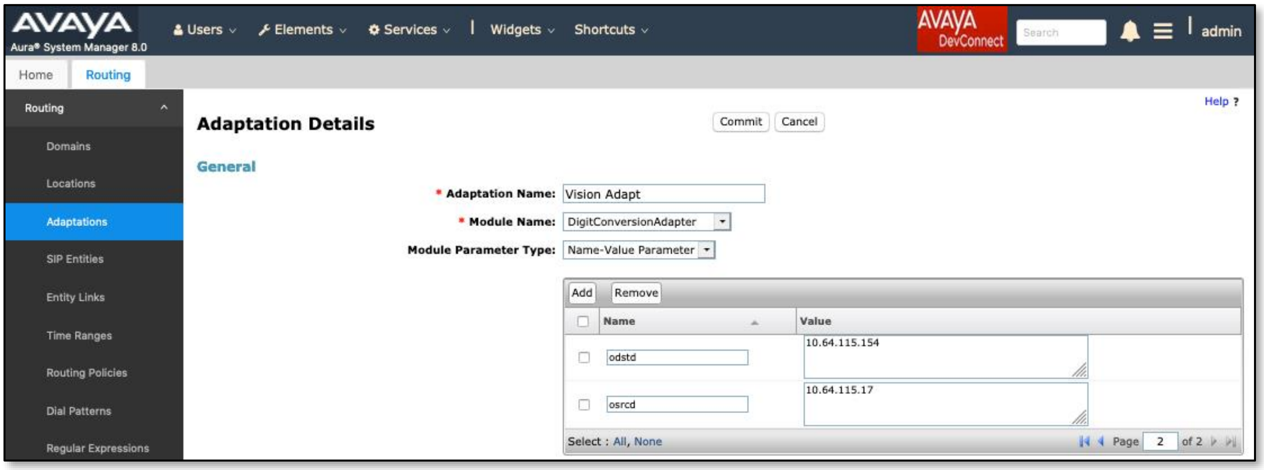
Click **Add** to add a new row for the following values as shown below table:

Name	Value
fromto	true
iodstd	Enter the domain name of system, eg: **sildenver.org**
iosrcd	Enter the domain name of system, eg: **sildenver.org**
odstd	Enter IP address of Vision, eg: **10.164.115.154**
osrcd	Enter IP Address of Session Manager, eg: **10.64.115.17**

Once complete, click the **Commit** button. Here is the screenshot showing the Adaptation.



(Continue) the screenshot showing the Adaptation:



6.5. Administer SIP Entities

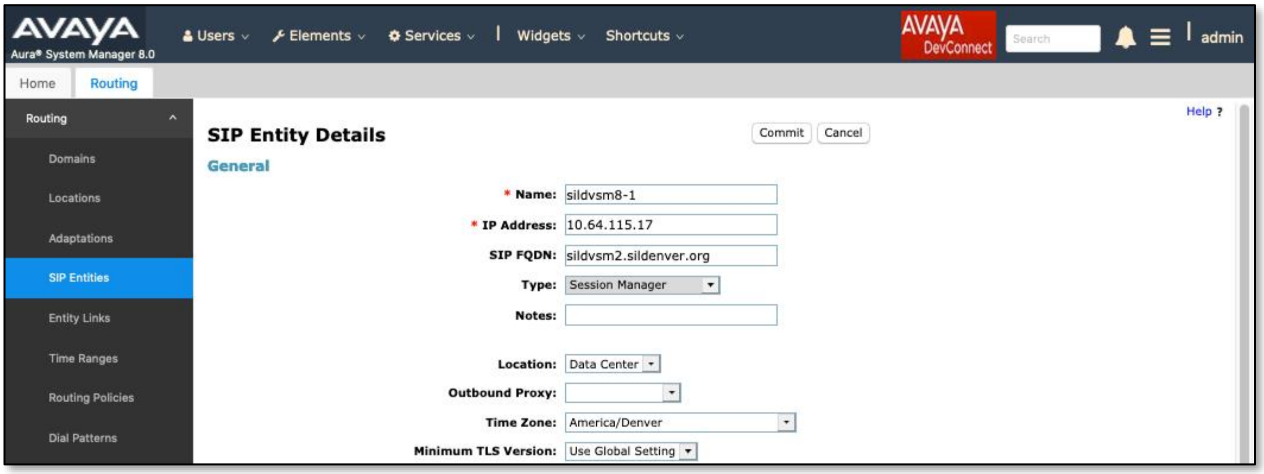
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and Vision.

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.
- **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.

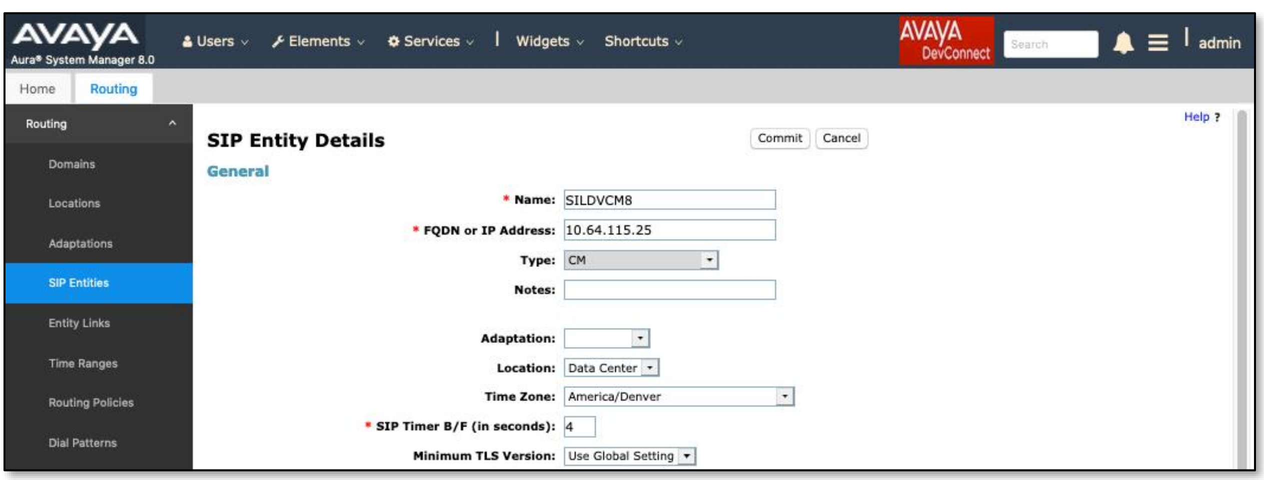
The following screen shows the addition of the ***Session Manager*** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.



6.5.2. SIP Entity for Communication Manager

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 Manager. 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 Manager as mentioned in **Section 5.3**.
- **Type:** Select "CM" in the dropdown list.
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

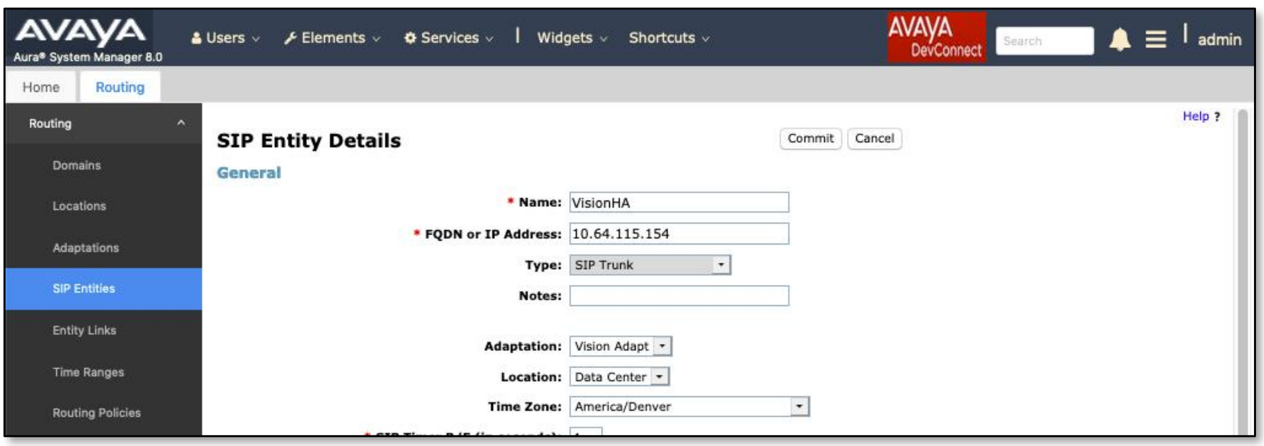


6.5.3. SIP Entity for Vision

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.

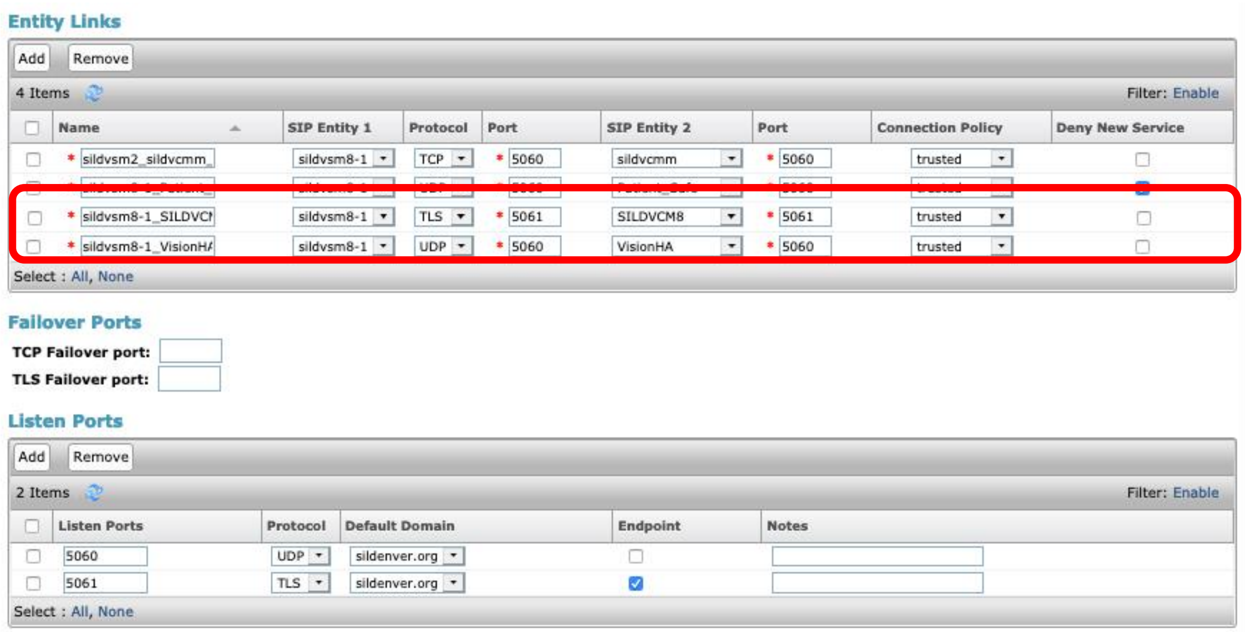


6.6. Administer Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were used; one to the Communication Manager 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 Links to Communication Manager and Vision. During the compliance test, **TLS** transport with port **5061** was used between Session Manager and Communication Manager. **UDP** transport and port **5060** was used between Session Manager and Vision.



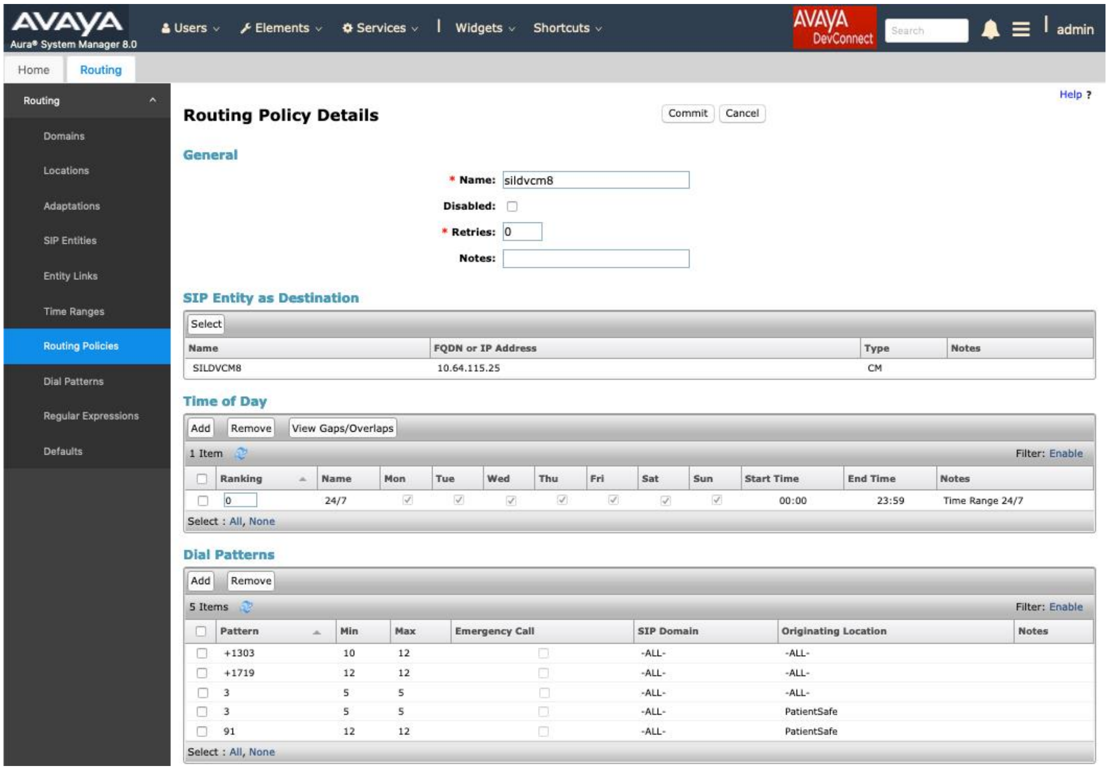
Also, enable **Listen Ports** on Session Manager to open ports **5060** and **5061** for incoming messages.

6.7. Administer Routing Policies

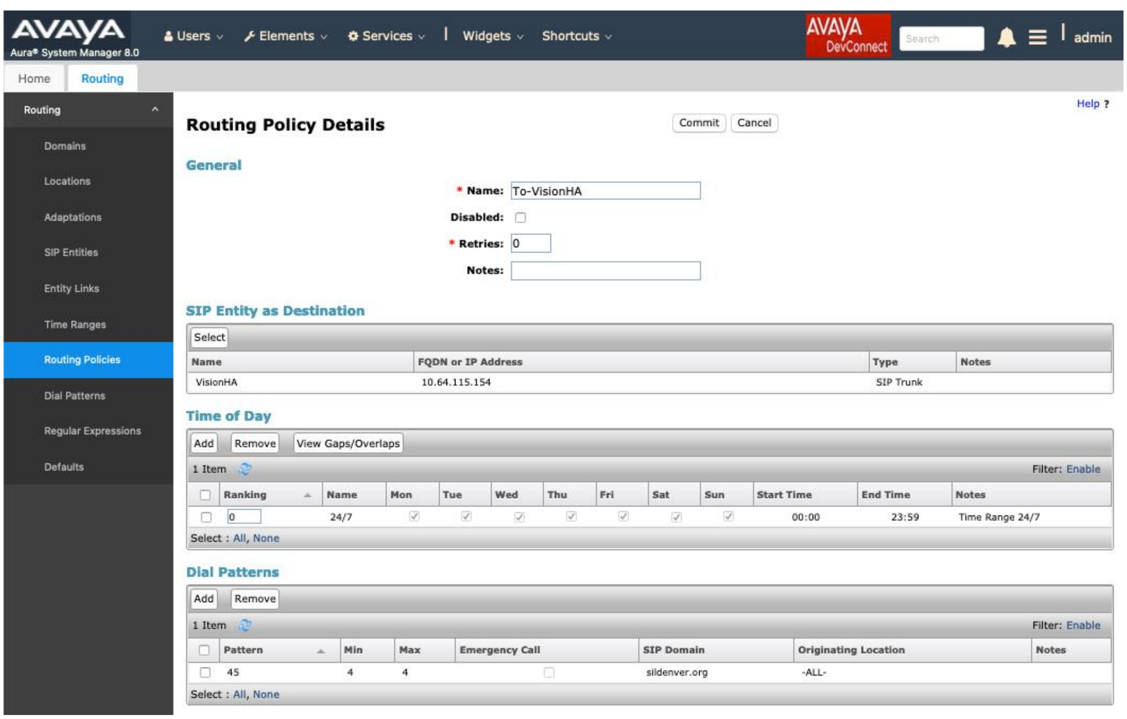
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: a policy with Communication Manager as the destination, and a policy with Vision as the destination. To add a routing policy, select to **Routing → 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 Manager.



The following screens show the **Routing Policy** for Vision.



6.8. Administer Dial Patterns

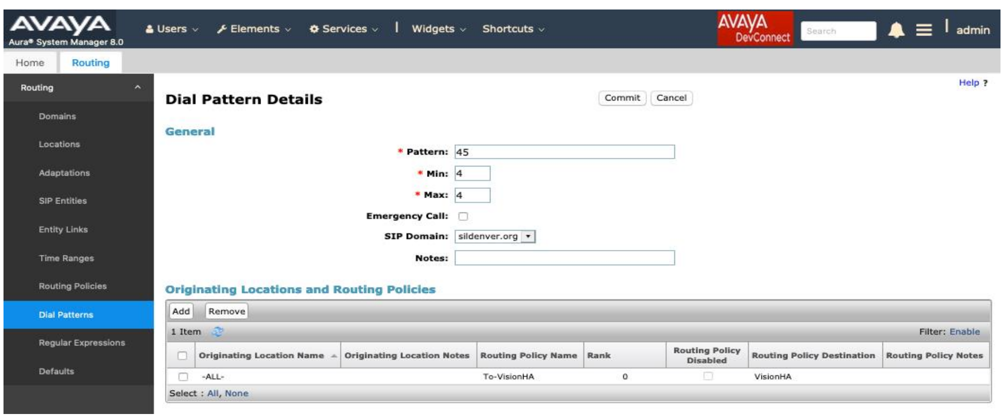
Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Vision and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination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

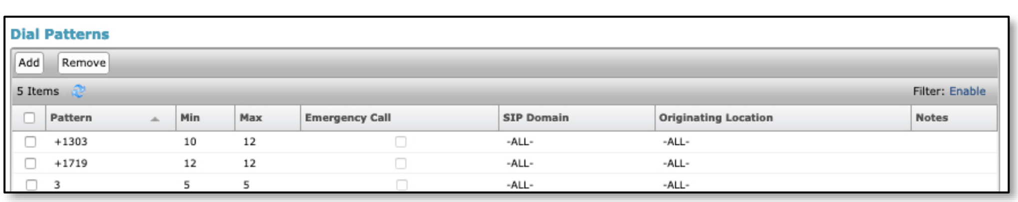
- **Pattern:** A dial pattern to match, in this case "45".
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 6.2**.

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 Manager endpoints in all locations using the SIP Domain "sildenver.org".



6.8.2. Dial Pattern for Communication Manager

Following the same process of creating a Dial Pattern for Vision, digits **3**xxx, **+1719**, and **+1303** were created to route any calls with these digit patterns to Communication Manager. The +1 numbers were used to route **12**-digit calls to Communication Manager, which in turn routed them over PRI trunks to the PSTN.



Dial Patterns

Add | Remove

5 Items — Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
+1303	10	12		-ALL-	-ALL-	
+1719	12	12		-ALL-	-ALL-	
3	5	5		-ALL-	-ALL-	

7. Configure Enghouse Vision 80/20

This section shows how to configure Vision 80/20 to successfully connect to Session Manager. The installation of the Vision software is assumed to be completed and the correct license is installed.

For reference, the servers comprising the Vision 80/20 solution used in testing were as follows, note that some of the servers had additional virtual IP interfaces for back end communications, these addresses are not described fully in the Application Notes.

OS	Function	Vswitch IP	Public IP
CentOS	Callserver	192.168.37.14	10.64.115.155
CentOS	Back-End load balancer	192.168.37.15	10.64.115.154
CentOS	Central server	192.168.37.12	N/A
CentOS	Communication server	192.168.37.13	N/A
CentOS	Database	192.168.37.16	N/A
CentOS	Front-End load balancer	192.168.37.11	10.64.115.151
Windows	Presence/Diversion management	192.168.37.17	10.64.115.150

7.1. Configuring SIP trunk for Avaya SM

On the Back-End load balancer server, use SSH to login to the command line and edit /usr/local/etc/kamailio/kamailio.cfg with the following settings, then reboot the server:

```
#!define VU_PBX_IP                    "10.64.115.17"     <- SM IP
#!define VU_PBX_PORT                  "5060"             <- Port
#!define VU_PBX_PROTO                 "udp"              <- Protocol
```

7.2. Configure SIP properties on the Call Server

On the Call Server, use SSH to login to the command line and edit /etc/asterisk/sip.conf with the following settings, then reboot the server:

```
type=peer
host=192.168.37.35
disallow=all
allow=alaw
allow=ulaw
nat=no
canreinvite=yes
qualify=no
alwaysauthreject=no
dtmfmode=rfc2833
fromdomain=xyz.se
usereqphone=yes
```

7.3. Configure TSAPI on the Presence Server

On the Presence Server, open \conf\ppbx1.xml and provide the TSAPI login credentials created in <Section Reference> and the VDN that Avaya phones will use to cover to the attendant.

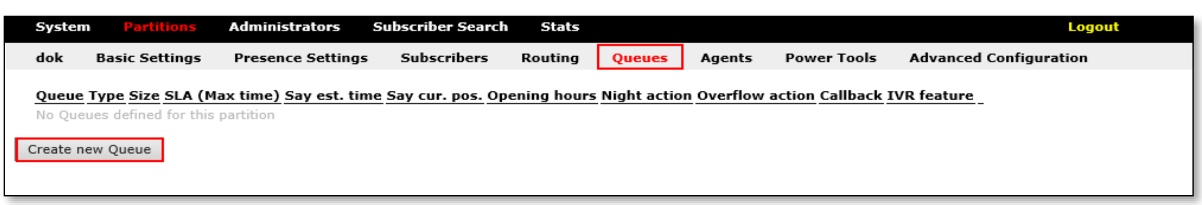
```
<xml>
   <settings>
      <PBXLogon>enghouse</PBXLogon>
      <PBXPassword>Avaya123!</PBXPassword>
      <SaveDiversion>False</SaveDiversion>
      <DefaultOrsKod>0</DefaultOrsKod>
      <OrsKodLength>1</OrsKodLength>
      <CSTAServer>AVAYA#SILDVCM8#CSTA#SILDVAES8</CSTAServer>
      <SimpleRoutingDevice>31501</SimpleRoutingDevice>
   </settings>
</xml>
```

7.4. Configure Operator queue

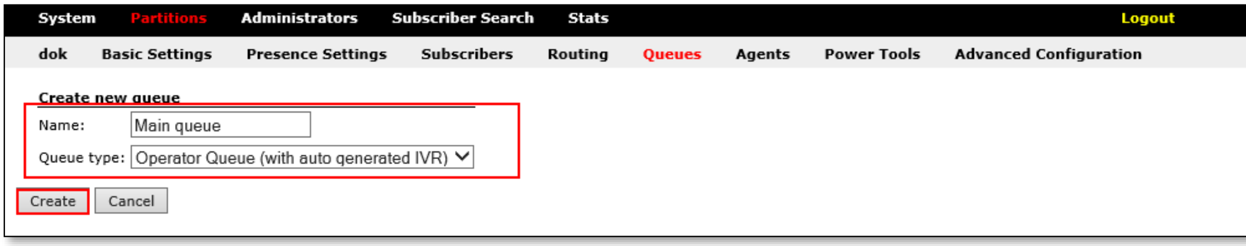
Log on to the partition manager and go to the "**Basic Settings**" tab.

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

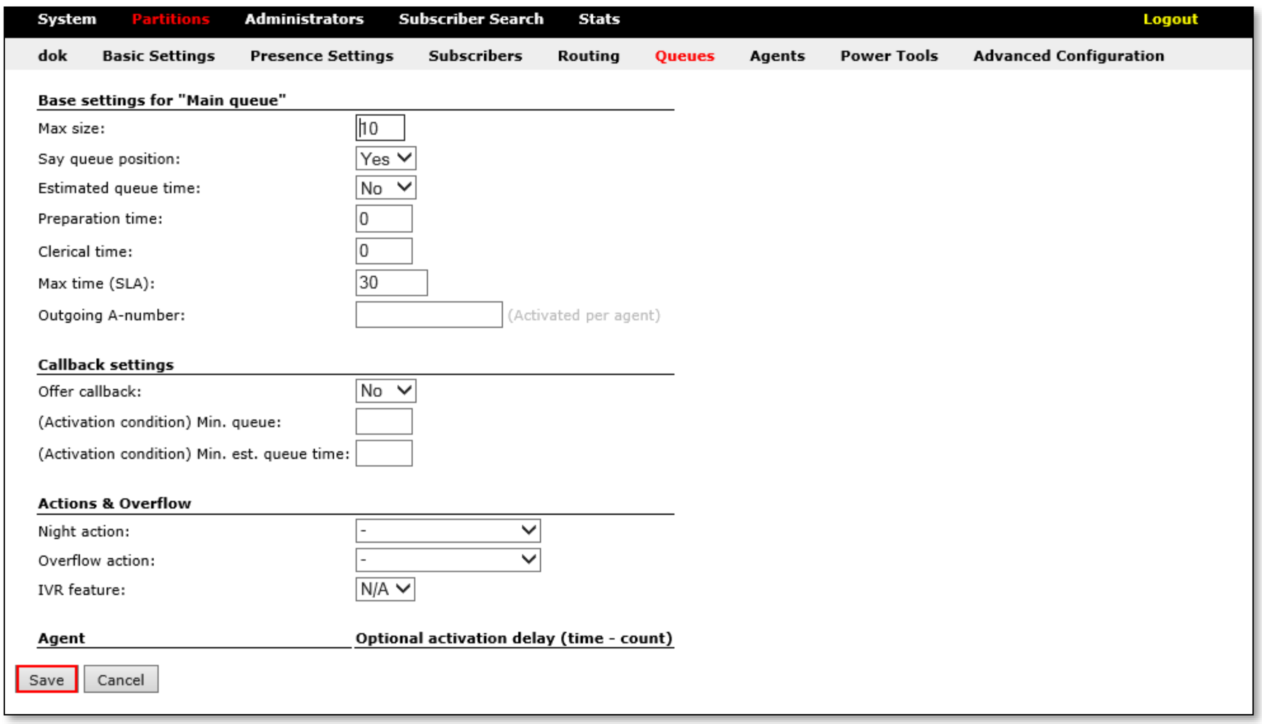
Browse to the "**Queues**" tab and select to create a new queue.



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

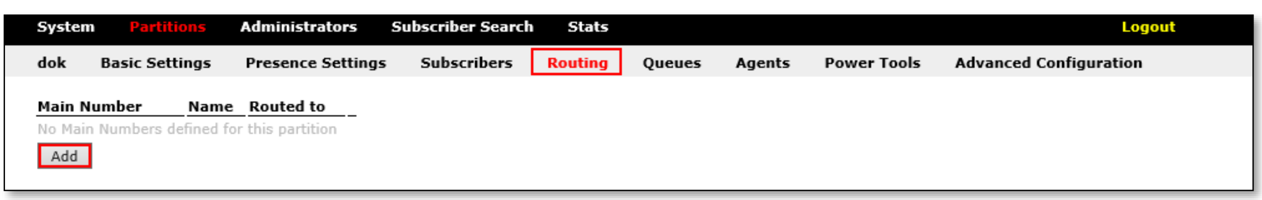


Set the queue preferences and click **Save**.

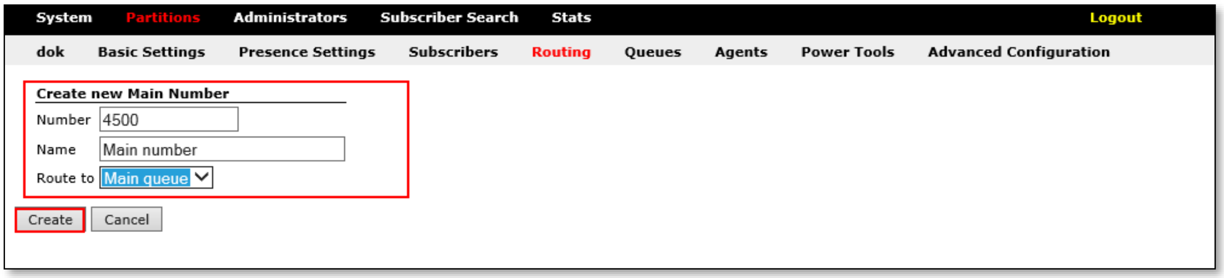


7.5. Configure routing to queue

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

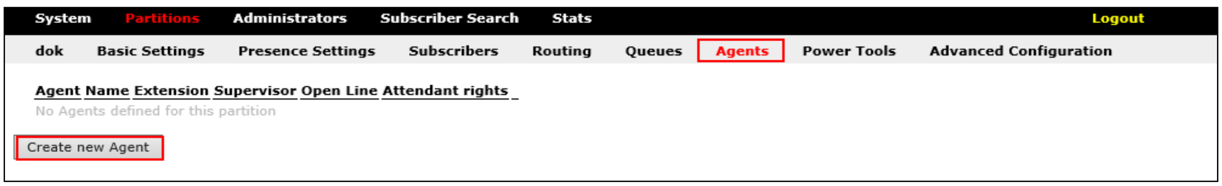


Enter the number to route, give the route a suitable name and select where to route the call. In this scenario number **4500** is given the name "**Main number**" and is routed to the "**Main queue**". Click **Create** when done.



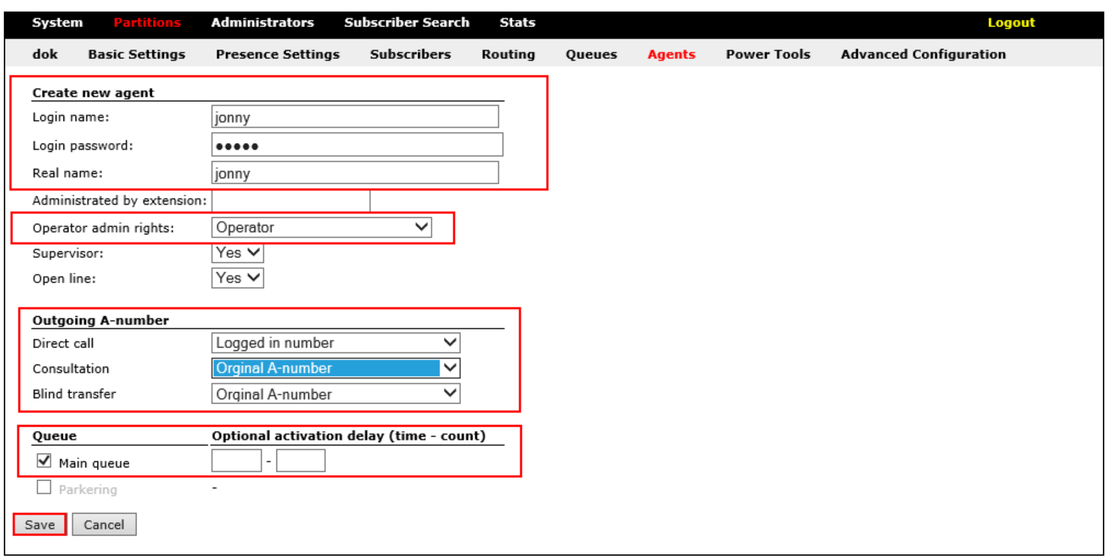
7.6. Setting up attendant

Go to the "**Agents**" tab and click **Create new Agent**.



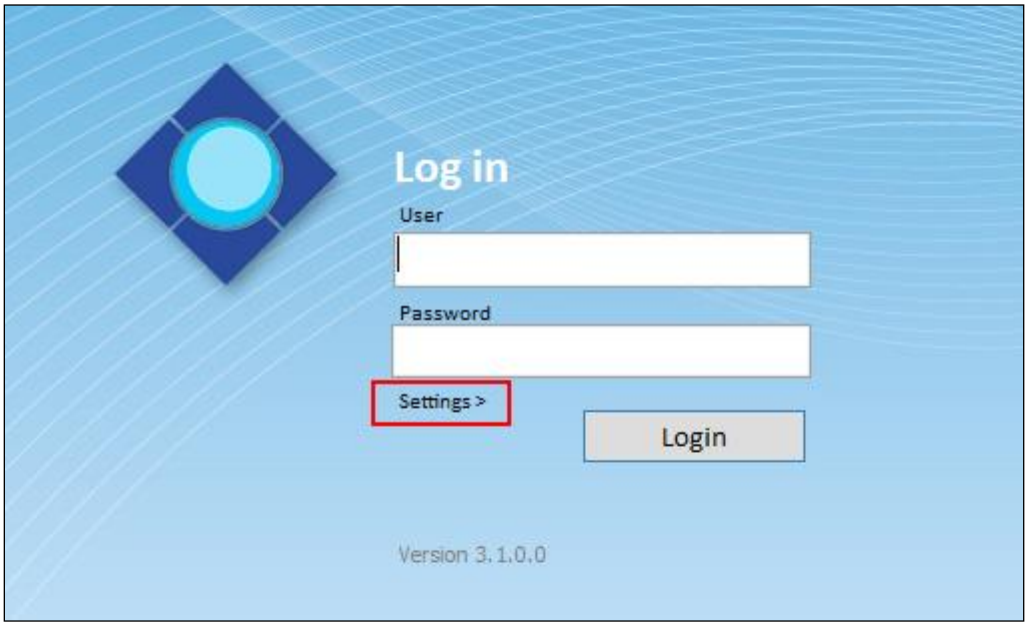
In the **Create new agent** section, enter the attendant a login name in the **Login name** field, in this scenario "**jonny**" and enter the attendant a password in the **Login password** field. Select the rights to "**Operator**" in the **Operator admin rights** dropdown menu.

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.

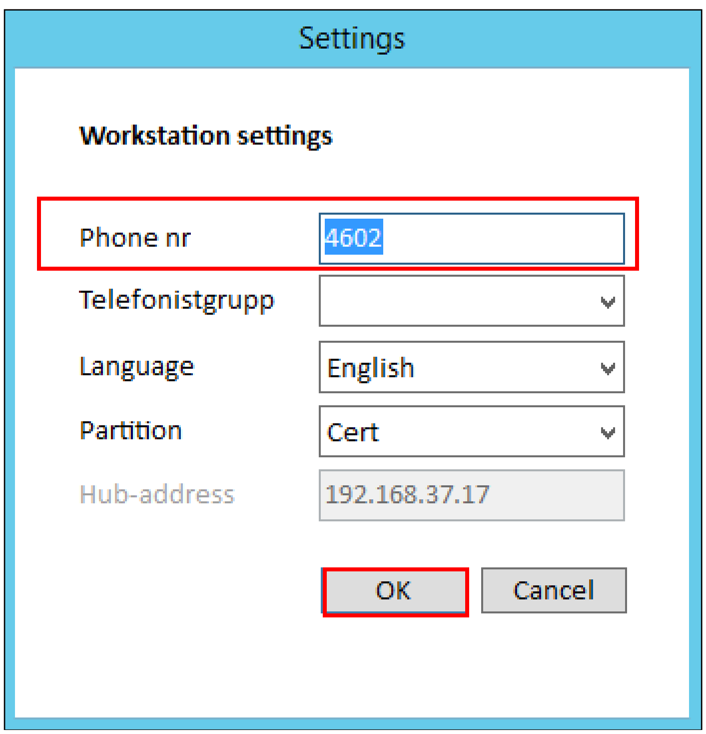


7.7. Running the attendant client

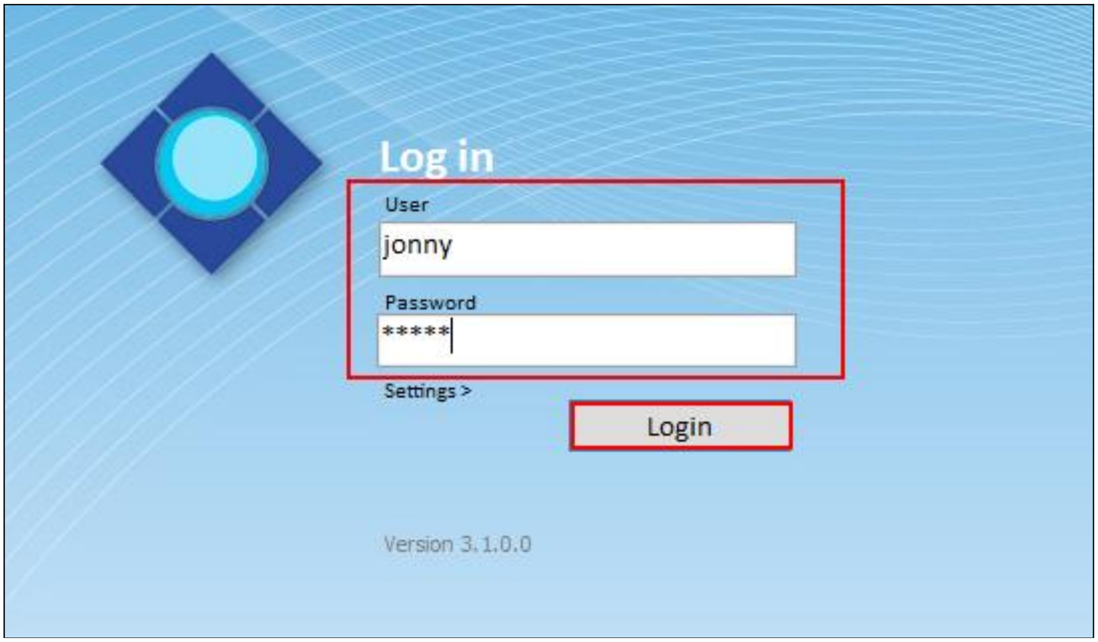
Start the “svara” application and click **Settings**.



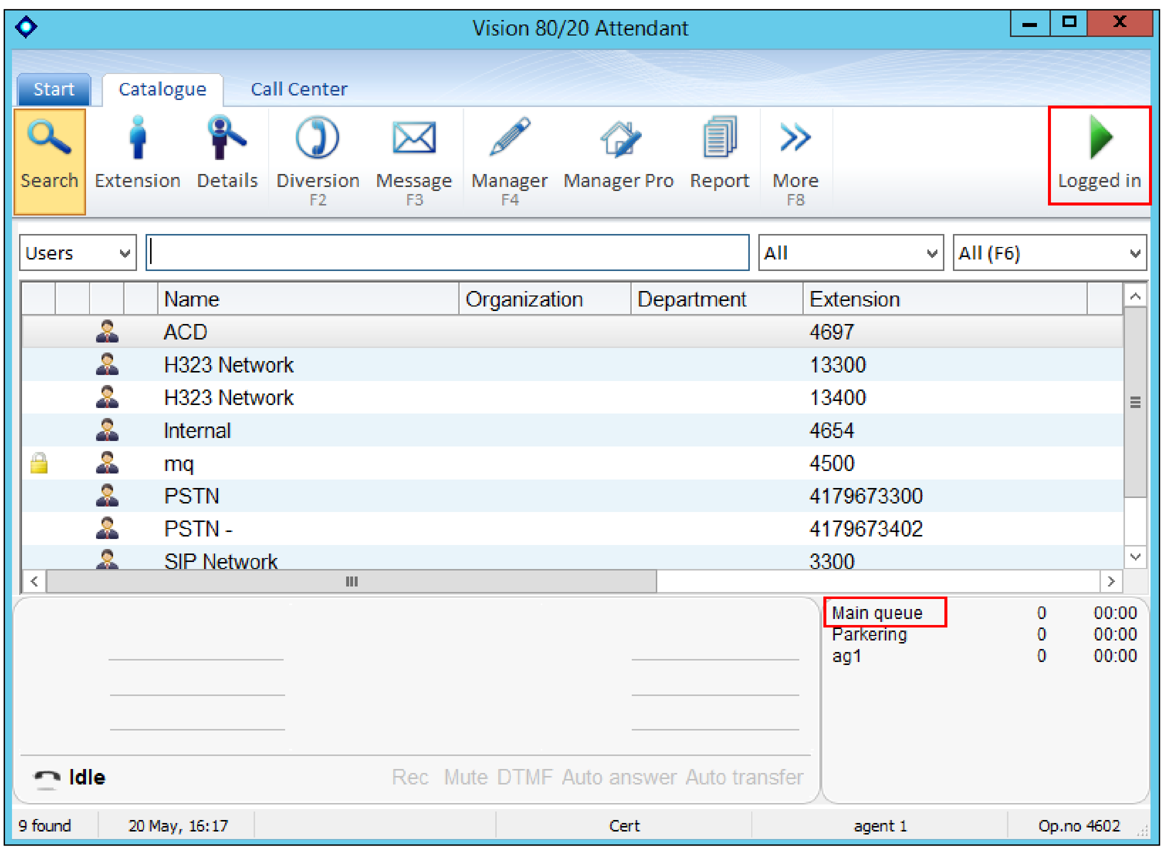
Select which telephone number on Communication Manager is to be used as the attendant phone in this case the number is **4602** and click **OK**.



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



When logged in, the queue that the attendant is servicing should be visible.



8. Verification Steps

With a call placed to the attendant and connected to a trunk and\or internal station, use the status station command as shown below to verify connectivity and media properties. In the screenshot below, the H.323 phone (**30004**) is at **10.64.115.31** and is using **G.729a** with SRTP for its connection to the G430 Gateway (**10.64.115.2**). The Vision 80/20 server connection from the G430 Gateway to **10.64.115.155** is transcoded to **G.711** with no encryption.

For SIP endpoints, use the **status trunk 10** command to locate the port the call is connected on then use status trunk 0010/0001 to see the connection properties for each port the call is connected to on the SIP Trunk (not shown).

```
status station 30004                                                Page   8 of   9
                              SRC PORT TO DEST PORT TALKPATH
src port: S00008
S00008:TX:10.64.115.31:2658/g729a/20ms/1-srtp-aescm128-hmac80
001V011:RX:10.64.115.2:2054/g729/20ms/1-srtp-aescm128-hmac80:TX:ctxID:180
001V011:RX:ctxID:180:TX:10.64.115.2:2060/g711u/20ms
T00002:RX:10.64.115.155:12980/g711u/20ms









dst port: T00002


ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

9. Conclusion

These Application Notes describe the configuration steps required for Vision from Enghouse Interactive AB to successfully interoperate with Avaya Aura® Communication Manager 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.

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. *Administering Avaya Aura® Communication Manager*, Release 8.0.x Issue 4, May 2019
2. *Administering Avaya Aura® Session Manager*, Release 8.0.1 Issue 3, December 2018
3. *Administering Avaya Aura® System Manager for Release 8.0.1*, Release 8.0.x Issue 8, April 2019

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.