



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Aura® Application Enablement Services R6.2 with Sikom AgentOne – Issue 1.0

Abstract

These Application Notes describe the steps to configure Sikom AgentOne to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services to provide IVR, ACD and call control functionality.

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

Sikom AgentOne is a universal event routing platform which can provide multiple functions such as IVR, ACD, Voicemail, Outbound Dialing and can handle multi-channel contact types such as Voice, Fax and email events.

Sikom AgentOne is fully scalable and has built in provisioning for Multisite, High Availability implementations and distributed architecture. In addition, Sikom AgentOne can manage connections to multiple PBX concurrently, using PRI, H.323 and SIP integration.

Monitoring, reporting, management and administration of Sikom AgentOne is driven through graphical and web based interfaces.

The Sikom CTI-Service and Sikom SIP Service are the conduit through which the Sikom AgentOne applications interoperate with Avaya Aura® Application Enablement Services using TSAPI and Avaya Aura® Session Manager using SIP respectively.

2. General Test Approach and Test Results

The general test approach was to validate the ability of AgentOne and the AgentOne client to correctly and successfully route, handle and control a variety of call scenarios in accordance with the relevant configuration.

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.

2.1. Interoperability Compliance Testing

Interoperability compliance testing consisted of successful routing, handling and control of a variety of call scenarios as follows:

- Incoming call from local/PSTN user direct to agent or through ACD
- Call Hangup by PSTN, local or agent user using AgentOne Client or deskphone
- Blind and Supervised call transfer
- Cancel of call transfer
- Call Conferencing
- Use of REFER for path-replacement
- Anchoring RTP for calls through AgentOne (without REFER)
- Verification of AgentOne Client call control options and appropriate availability of options
- Call toggling
- Recovery from outage of various solution components

2.2. Test Results

All test cases were executed successfully.

2.3. Support

Sikom shall provide Support Services between 08:00 am and 5:00 pm (Central European Time) Monday to Friday excluding public holidays in Germany. The standard reaction time during this support time is 4 (four) hours (only telephone tickets).

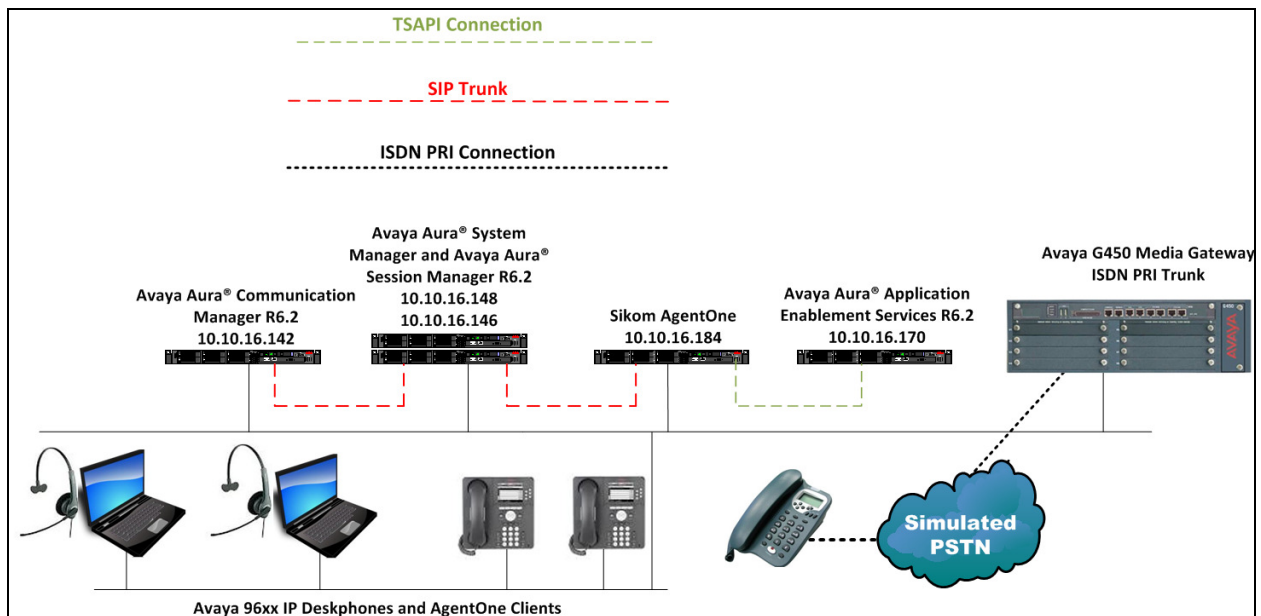
Perequisite is a valid service contract for a Sikom-system with the partner or end customer.

All charges are exclusive of all taxes and similar fees now in force or enacted in the future imposed on the delivery of services.

Hotline : a) during support times Germany 01805 008167 or support@sikom.de
 b) off support times: (via IVR)

3. Reference Configuration

An Avaya S8800 Server running Communication Manager R6.2 serving H.323 endpoints with a G450 Media Gateway was configured along with Application Enablement Services hosted on VMware providing a TSAPI interface to which the AgentOne CTI connector connects. Session Manager hosted on an S8800 Server provides a SIP interface to which both Communication Manager and Sikom are connected over SIP trunks. Session Manager also provides the point of registration for Avaya SIP endpoints. System Manager hosted on an S8800 Server provides a means to manage and configure Session Manager.



Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services with Sikom AgentOne Solution

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP5 build R016x.02.0.823.0-20396
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.2 patch 1
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP4
Avaya G450 Media Gateway <ul style="list-style-type: none">• MM710	32.24.0 <ul style="list-style-type: none">• HW5 FW22
Avaya 9630 IP Deskphone	<ul style="list-style-type: none">• H323 3.2• SIP 2.6.8.4
Sikom AgentOne running on Windows Server	<ul style="list-style-type: none">• Windows 2008 R2 SP1• Sikom HST SaphirVOIP 3.1.1304.119• Avaya Application Enablement Services TSAPI Windows Client 6.2• Sikom AgentOne (Common) Cti Proxy 5.2.1304.3• Sikom AgentOne Server (SkCcServer.exe) 5.1.1304.102• Sikom Voiceman 7.5.1201.283
Sikom AgentOne Client running on Windows XP Machine	<ul style="list-style-type: none">• 5.1.1304.92

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using Communication Manager System Access Terminal (SAT). 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 as referenced in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Configure Interface to Avaya Aura® Application Enablement Services
- Configure aar
- Configure 3rd Party Control for SIP Endpoints

5.1. Configure Interface to Avaya Aura® Application Enablement Services

Enter the node **Name** and **IP Address** for the Application Enablement Server, in this case **aes62vm** and **10.10.16.170** respectively. Take a note of the **procr** node **Name** and **IP Address** as it is used later in this section.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
default	0.0.0.0	
aes62vm	10.10.16.170	
procr	10.10.16.142	

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

add cti-link 1		Page 1 of 3
		CTI LINK
CTI Link: 1		
Extension: 5899		
Type: ADJ-IP		
Name: aes62vm		COR: 1

Configure IP-Services for the **AESVCS** service using the **change ip-services** command. Using the procr node name as noted above i.e. **procr**, ensure **Enabled** is set to **y**.

change ip-services					Page 1 of 4
IP SERVICES					
Service	Enabled	Local	Local	Remote	Remote
Type		Node	Port	Node	Port
AESVCS	y	procr	8765		

Navigate to **Page 4**, set the **AE Services Server** node-name and the **Password** the AES Server will use to authenticate with Communication Manager, ensure **Enabled** is set to **y**..

change ip-services					Page 4 of 4
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes62vm	Avaya1234567	y	in use	

5.2. Configure aar

The aar table must be configured with the relevant routing entry for calls to AgentOne. In this instance trunk-group one is already configured as the SIP trunk to Session Manager and route-pattern 1 is configured to route calls over this trunk group. Enter the command **change aar analysis 0**, in the **Dialed String** column enter the digits which will be dialed to reach AgentOne, in this case **57**, set the **Total Min** and **Max** value to **4** , and configure the **Route Pattern** as **1**. When a 4 digit string is dialed beginning with 57, the call will route to Session Manager, the Session Manager configuration later in this document explains how the call is then routed to AgentOne.

change aar analysis 0							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							
Percent Full: 0							
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
13	4	4	4	aar		n	
2	4	4	1	unku		n	
3	11	11	1	unku		n	
4	4	4	1	aar		n	
402	4	4	4	aar		n	
57	4	4	1	aar		n	
5999	4	4	1	unku		n	
6	4	4	1	unku		n	

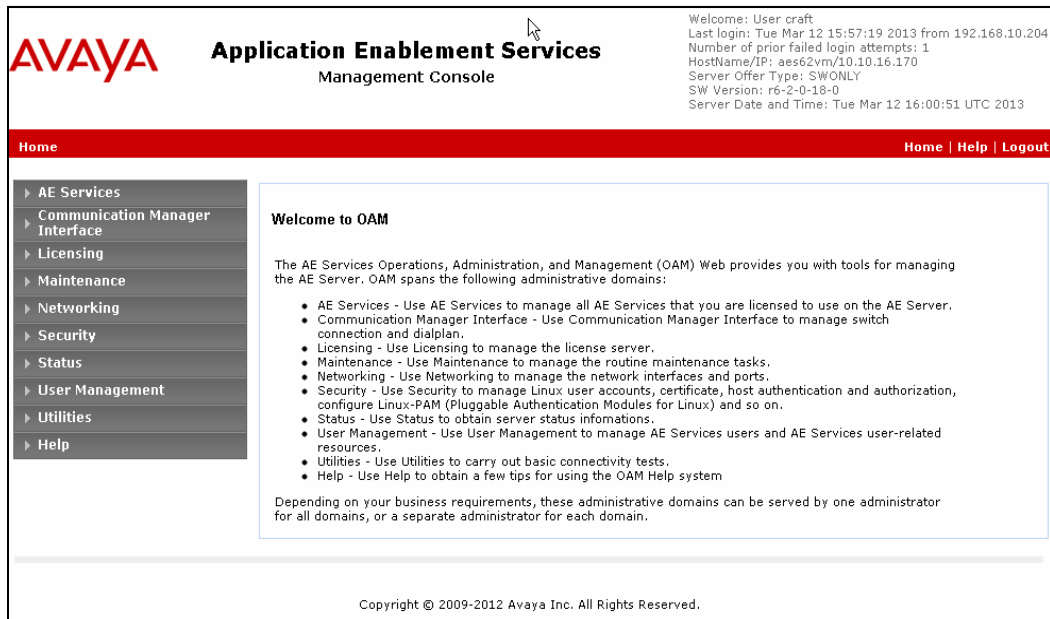
5.3. Configure 3rd Party Control for SIP Endpoints

In order that SIP endpoints can be controlled by the AgentOne CTI-Service, enter the command **change station x** where **x** is a relevant SIP extension configured on Communication Manager, navigate to **Page 6** and set **Type of 3PCC Enabled:** to **Avaya**.

change station 6003	Page 6 of 6
STATION	
SIP FEATURE OPTIONS	
Type of 3PCC Enabled: Avaya	
SIP Trunk: aar	

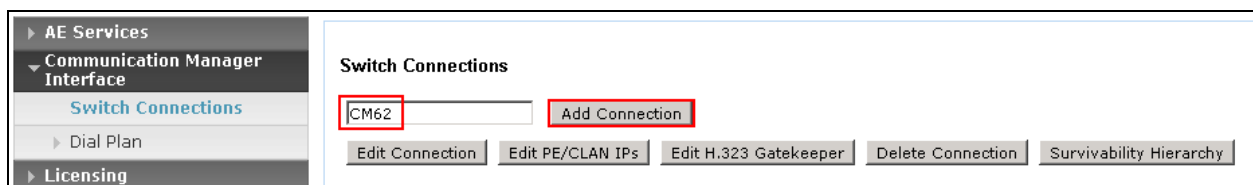
6. Configure Avaya Aura® Application Enablement Services

Configuration of Application Enablement Services is performed from the OAM web pages. Navigate to the URL of the AES OAM, in this case <https://10.10.16.170/index.jsp> and login using the appropriate credentials (not shown). Upon successful login the screen below will appear.



6.1. Configure Switch Connection

To establish the connection between Communication Manager and AE Services, click **Communication Manager Interface → Switch Connections**. In the field next to **Add Connection** enter **CM62** and click on **Add Connection**.



The following screen is displayed. Complete the configuration as shown and enter the password specified in **Section 5.1** when configuring AESVCS in ip-services. Click on **Apply** when done.

Connection Details - CM62

Switch Password: [Masked Password]

Confirm Switch Password: [Masked Password]

Msg Period: 30 Minutes (1 - 72)

SSL: ☒

Processor Ethernet: ☒

Apply Cancel

The following screen will be shown displaying the newly added switch connection, click **Edit PE/CLAN IPs**.

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM62	Yes	30	0

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

Enter the IP Address of the procr noted in **Section 5.1** and click **Add/Edit Name or IP**.

Edit Processor Ethernet IP - CM62

10.10.16.142 Add/Edit Name or IP

Name or IP Address

Back

The following screen will appear showing the newly added procr IP address, click **Back**.

Name or IP Address	Status
10.10.16.142	Idle

The newly added **Switch Connection** will appear once more.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM62	Yes	30	0

6.2. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, click **Add Link**.

Link	Switch Connection
Add Link	Edit Link

Configure the TSAPI Link using the newly configured **Switch Connection** as shown below and click **Apply Changes**.

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ TWS
- ▶ Communication Manager Interface

Add TSAPI Links

Link: 1

Switch Connection: CM62

Switch CTI Link Number: 1

ASAI Link Version: 4

Security: Both

Apply Changes Cancel Changes

The screen below will be displayed with instructions to restart the TSAPI Server. Click **Apply** taking note of the instructions given.

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.

⚠ Please use the Maintenance -> Service Controller page to restart the TSAPI server.

Apply Cancel

The screen below will appear displaying the newly added TSAPI link.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM62	1	4	Both

Add Link Edit Link Delete Link

6.3. Restart TSAPI Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service** box, and click **Restart Service**.

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

6.4. Administer Sikom CTI User

Select **User Management** → **User Admin** → **Add User** from the left pane to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown).

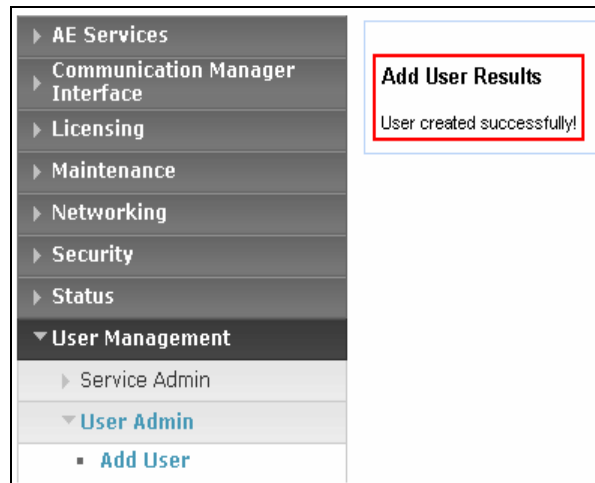
User Management | User Admin | Add User

Add User

Fields marked with * can not be empty.

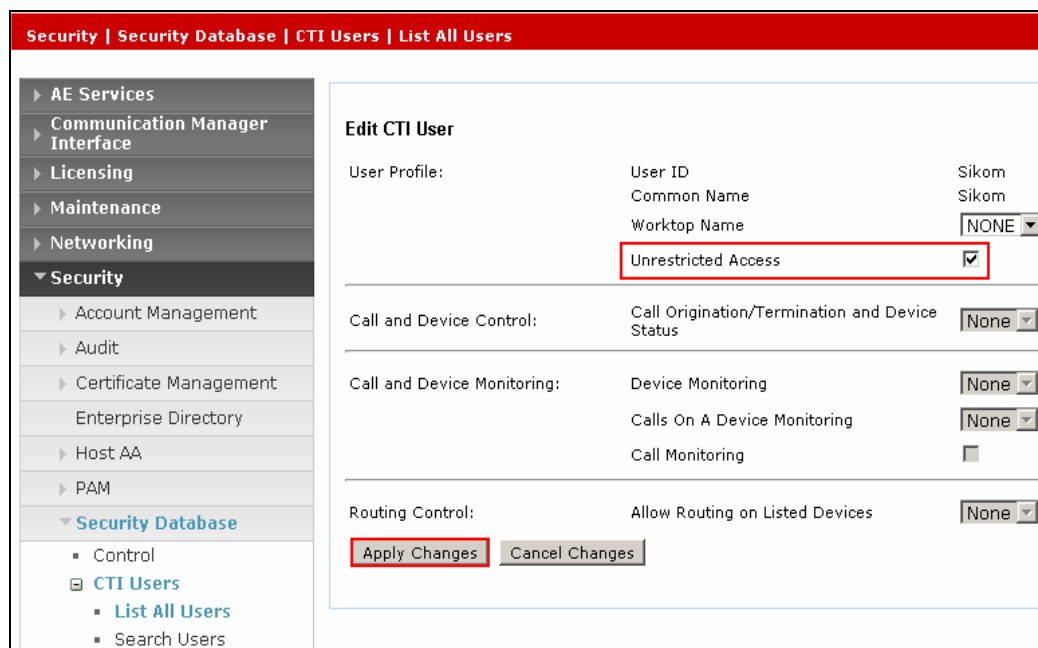
* User Id	<input type="text" value="Sikom"/>
* Common Name	<input type="text" value="Sikom"/>
* Surname	<input type="text" value="Sikom"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>

The following screen will appear confirming the succesful creation of the new user.



6.5. Configure User Unrestricted Access

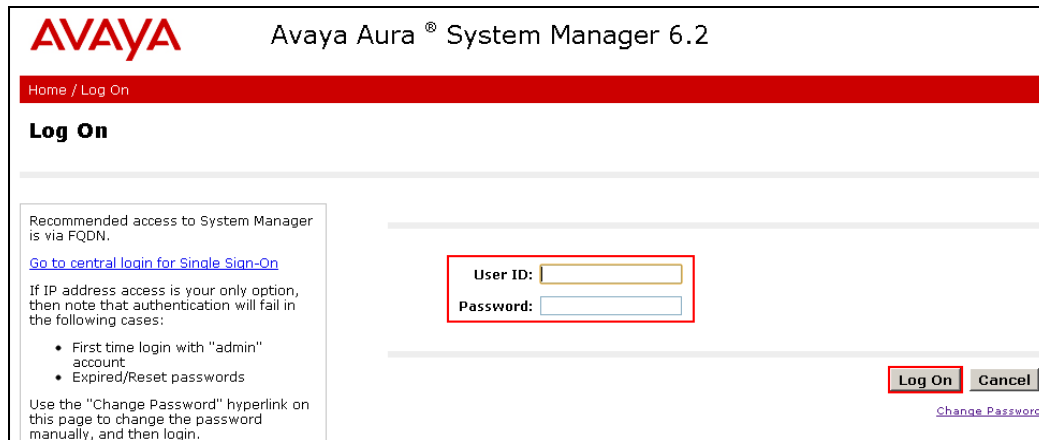
Select **Security**→ **Security Database** → **CTI Users** → **List All Users** from the left pane, click on the radio button beside the user created above, in this case, **sikom** and click **Edit** (not shown). Place a tick in the box next to **Unrestricted Access**, as shown in the image below. Click **Apply Changes** when done.



7. Configure Avaya Aura® Session Manager

This section illustrates relevant aspects of the Session Manager configuration required for interoperating with AgentOne.

Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button



The screenshot shows the Avaya Aura System Manager 6.2 Log On page. The header includes the Avaya logo and the text "Avaya Aura® System Manager 6.2". Below the header is a red bar with "Home / Log On". The main heading is "Log On". On the left, there is a section titled "Recommended access to System Manager is via FQDN." with a link "Go to central login for Single Sign-On". Below this, it states "If IP address access is your only option, then note that authentication will fail in the following cases:" followed by a bulleted list: "First time login with 'admin' account" and "Expired/Reset passwords". It also mentions "Use the 'Change Password' hyperlink on this page to change the password manually, and then login." On the right, there are input fields for "User ID:" and "Password:", both highlighted with red boxes. Below these fields are "Log On" and "Cancel" buttons, with "Log On" also highlighted with a red box. A "Change Password" link is at the bottom right.

It is assumed that the Domains, Locations, SIP entities for Session Manager and Communication Manager and corresponding Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured.

7.1. Configure AgentOne SIP Entity

A SIP Entity must be created for the AgentOne SIP interface. Click **Routing** → **SIP Entities** → **New**, assign an identifying **Name**, the **FQDN or IP Address** for the AgentOne SIP interface, set the **Type** to **SIP Trunk**, and click **Commit** when done.



The screenshot shows the Avaya Aura System Manager 6.2 SIP Entity Details page. The left sidebar has a menu with "Routing" selected, and "SIP Entities" is highlighted in blue. The main heading is "Home / Elements / Routing / SIP Entities". Below the heading is "SIP Entity Details" and "General". On the right, there are "Commit" and "Cancel" buttons, with "Commit" highlighted with a red box. The main content area has three fields: "Name:" with the value "SIKOM", "FQDN or IP Address:" with the value "10.10.16.184", and "Type:" with a dropdown menu showing "SIP Trunk". The "Name" and "FQDN or IP Address" fields are highlighted with red boxes.

7.2. Configure Entity Link

The configuration of an Entity Link connects the Session Manager SIP Entity with the AgentOne SIP Entity. Click **Routing → Entity Links → New**, assign an identifying **Name**, choose the entity assigned to the preconfigured Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **UDP**, enter **5060** for the Port, choose the AgentOne SIP entity as **SIP Entity 2** and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop down box. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to AgentOne.

Home / Elements / Routing / Entity Links

Entity Links

Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
ToSikom	SM62	UDP	5060	SIKOM	5060	Trusted

7.3. Create Routing Policy

A routing entity must be configured to route the required dialed calls to AgentOne. Click **Routing → Routing Policies → New**, assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select**.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

* Name: ToSikom

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

Choose the AgentOne Entity configured in **Section 7.1** and click **Select**.

Home / Elements / Routing / Routing Policies

SIP Entity List Select Cancel

SIP Entities

16 Items | Refresh Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	CM62	10.10.16.142	CM	
<input type="radio"/>	CMM62	10.10.16.142	CM	
<input checked="" type="radio"/>	SIKOM	10.10.16.184	SIP Trunk	

Review the configuration and click **Commit** when done.

Home / Elements / Routing / Routing Policies

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SIKOM	10.10.16.184	SIP Trunk	

7.4. Administer Dial Patterns

Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate destination. In **Section 5.2** Communication Manager is configured to route 4 digit strings beginning with 57 to Session Manager. To create a Dial Pattern to route these digits from Session Manager to AgentOne click **Routing → Dial Patterns → New**. Under **General** enter the numbers presented to Session Manager by Communication Manager in the **Pattern** box. Set the **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**. In the **Originating Locations and Routing Policies** section of the web page, click **Add**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Place a tick in the **Apply The Selected Routing Policies to All Originating Locations** tick box, and select the **Routing Policy** created in **Section 7.3**. Click **Select** when done

Home / Elements / Routing / Dial Patterns

Originating Location and Routing Policy List

SelectCancel

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

1 Item | Refresh

Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	DevConnectLab	

Select : All, None

Routing Policies

12 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ToCM6.2	<input type="checkbox"/>	CM62	
<input type="checkbox"/>	ToCMM62	<input type="checkbox"/>	CMM62	
<input checked="" type="checkbox"/>	ToSikom	<input type="checkbox"/>	SIKOM	

Review the configuration and click **Commit** when done.

Home / Elements / Routing / Dial Patterns

[Help ?](#)

Dial Pattern Details

Commit **Cancel**

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

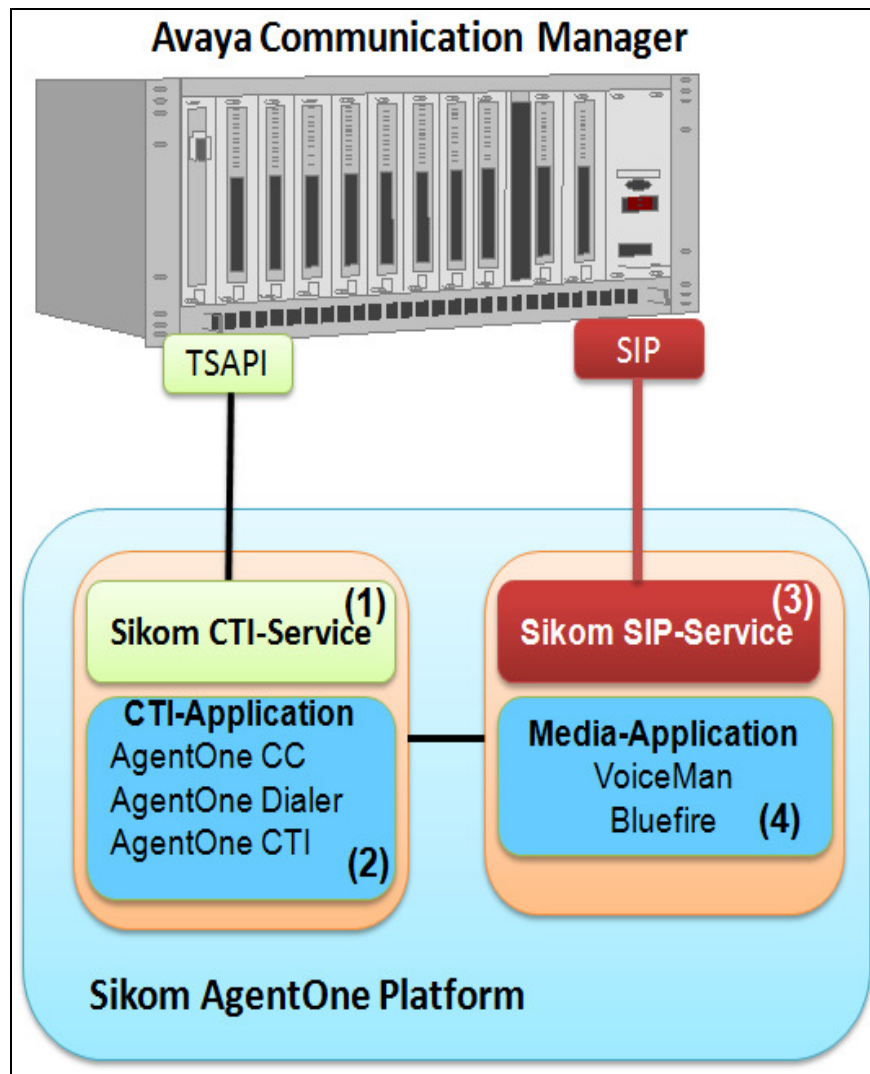
Add **Remove**

1 Item | [Refresh](#) Filter: [Enable](#)

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

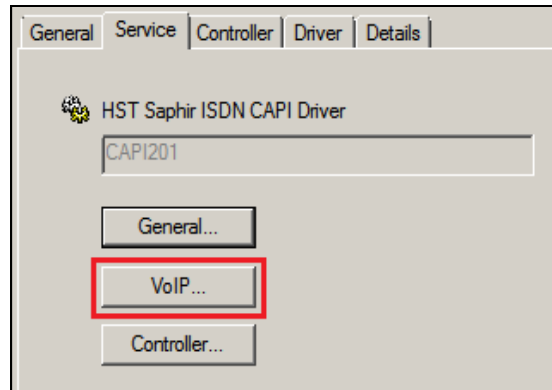
8. Configure Sikom AgentOne

AgentOne comprises of several components and services which can be distributed in a survivable, distributed and scalable architecture. For the purposes of the compliance test a single server was used on which all the required services were installed, configured and running. The configuration relevant to the interoperability with the Avaya platform is detailed in this section. The overview below provides a simplified demonstration of the AgentOne solution architecture where the Sikom CTI-Service and Sikom SIP-Service acts as a conduit to the Avaya solution for Sikom AgentOne Platform Applications.

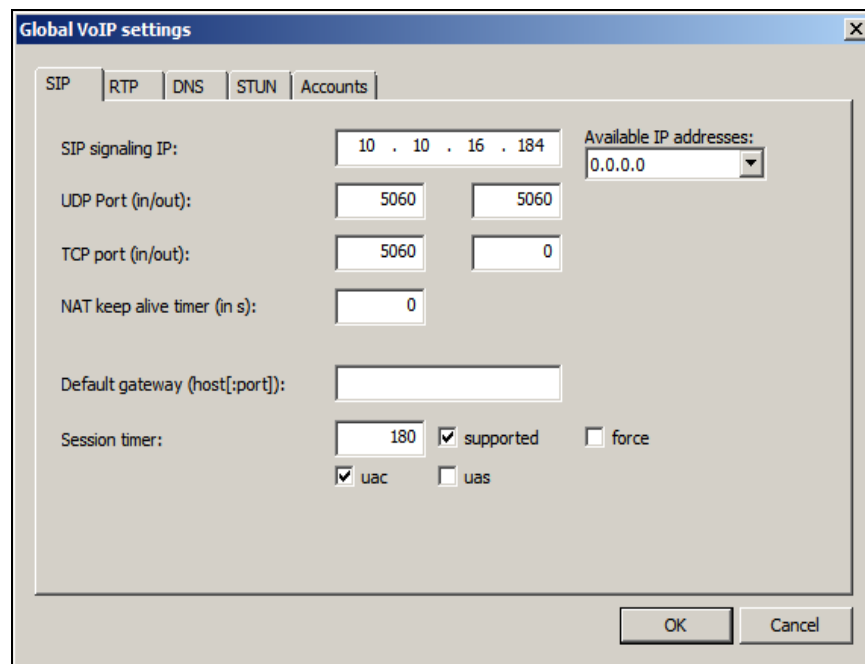


8.1. Configure SIP Stack

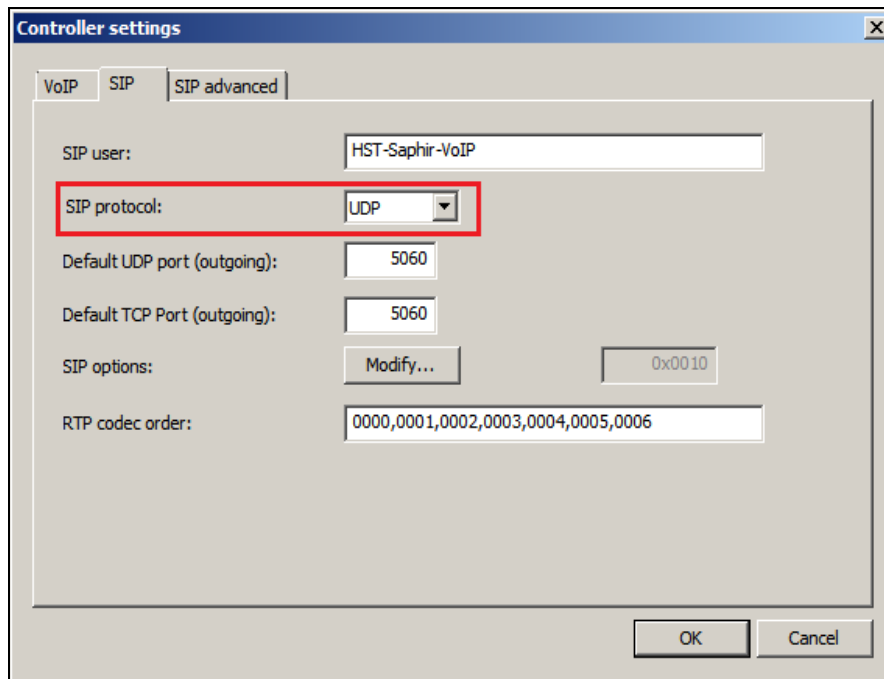
Enter the Windows Device Manager and right click the **HST SaphirVOIP** icon  under Network Adaptors and click on **Properties**. Under the **Service** tab click **VoIP**.



Under the **SIP** tab enter the IP address used for the AgentOne SIP interface and the **UDP Port** to be used. Set the **Session Timer** to **180** seconds and place a check in the **supported** and **uac** boxes to enable a session expiry value in the SIP signaling.



Click on the **Accounts** tab and click **VoIP**, the screen below will appear; under the **SIP** tab ensure **SIP Protocol** is set to **UDP**.



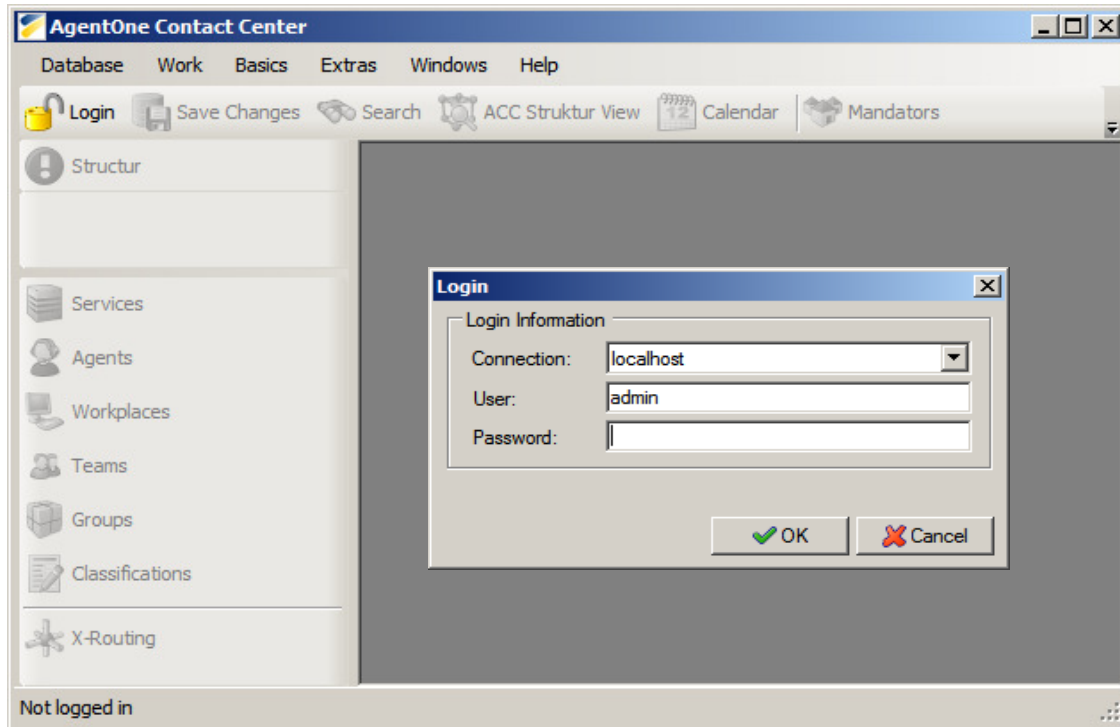
The image shows a 'Controller settings' dialog box with three tabs: 'VoIP', 'SIP', and 'SIP advanced'. The 'SIP' tab is selected. The 'SIP user' field contains 'HST-Saphir-VoIP'. The 'SIP protocol' dropdown menu is set to 'UDP' and is highlighted with a red rectangle. Below this, the 'Default UDP port (outgoing)' and 'Default TCP Port (outgoing)' are both set to '5060'. The 'SIP options' field has a 'Modify...' button and a value of '0x0010'. The 'RTP codec order' field contains the string '0000,0001,0002,0003,0004,0005,0006'. At the bottom right are 'OK' and 'Cancel' buttons.

Controller settings		
VoIP	SIP	SIP advanced
SIP user:	HST-Saphir-VoIP	
SIP protocol:	UDP	
Default UDP port (outgoing):	5060	
Default TCP Port (outgoing):	5060	
SIP options:	Modify...	0x0010
RTP codec order:	0000,0001,0002,0003,0004,0005,0006	
OK		Cancel

8.2. Configure Workplaces

Workplaces must be configured. A Workplace defines the telephone which will be used for the speech path.

Start the AgentOne Administration: **START→All Programs→Sikom→AgentOne→Administrator**. Click **Login** and the Login Window will appear. Type **admin** for **User** and click **OK**.



After Login click **Workplaces** on the left side and the **Workplace Manager Window** appears. Add, edit or delete Workplaces using the intuitive icons and menu options. The screenshot below shows Workplace with a **Name**, **PC-Name** and **Dialnumber** of **6003** and a **Type** of **CTI**. The **CTI-Interface** is set to **COM1 (1)**. Click **OK**.

The screenshot shows a window titled "Edit Workplace" with a close button (X) in the top right corner. The window is divided into two main sections: "Settings" and "Information".

Settings Section:

- Name:** Text box containing "6003".
- PC-Name:** Text box containing "6003".
- Dialnumber:** Text box containing "6003".
- Type:** Dropdown menu showing "CTI".
- CTI-Interface:** Dropdown menu showing "COM1 (1)".
- Priority:** Text box containing "0".
- Active:** A checked checkbox.

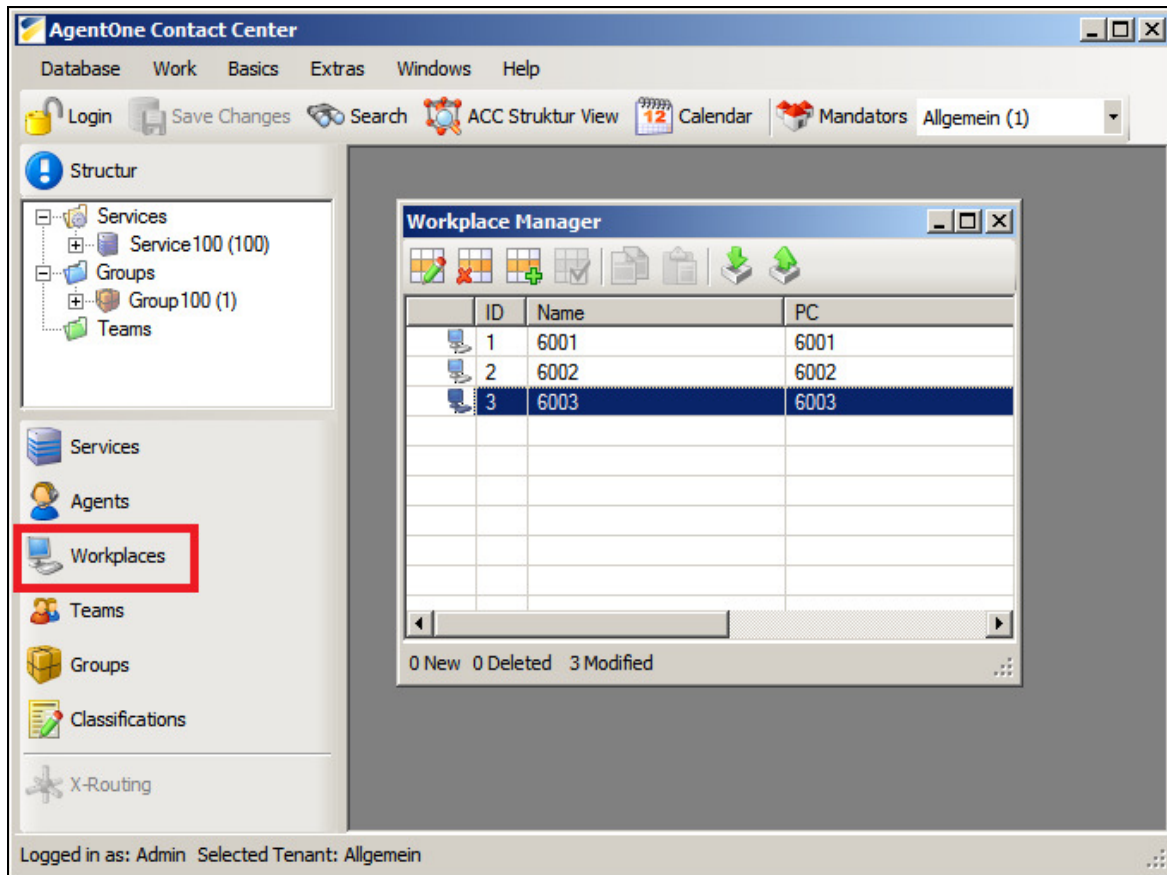
Information Section:

A large empty text area for additional information.

Buttons:

At the bottom right, there are two buttons: "OK" (with a green checkmark icon) and "Cancel" (with a red X icon).

The screen shot below shows workplaces 6001 to 6003 administered.



8.3. Configure Services

Click **Services** on the left side and **Service Manager Window** will appear. Click on **Add Service** to add a new service and enter the values as shown below where:

- **Name** – enter a descriptive name
- **Dialnumber** – enter a dial string appropriate to the dial plan in order to access this service. In this case **5704**

The screenshot shows the 'Edit Service' dialog box with the following fields and values:

- General Tab:**
 - ID:** 100
 - Name:** Service 100
 - Priority:** 5
 - Routing:** Servicebased (dropdown)
 - Team:** (empty dropdown)
 - ☐ Lastagent Routing
 - ☐ Client invisible
 - ☐ Personal Services
 - ☐ Ignore Grouptimes if no Group active
- Call Tab:**
 - Dialnumber:** 5704
 - Emergency Call:** (empty field)
- Mail Tab:**
 - E-Mail Address:** (empty field)
 - E-Mail Target:** (empty field)
 - Reminder Priority:** 0
- Information Tab:** (empty text area)

At the bottom right, there are **OK** and **Cancel** buttons.

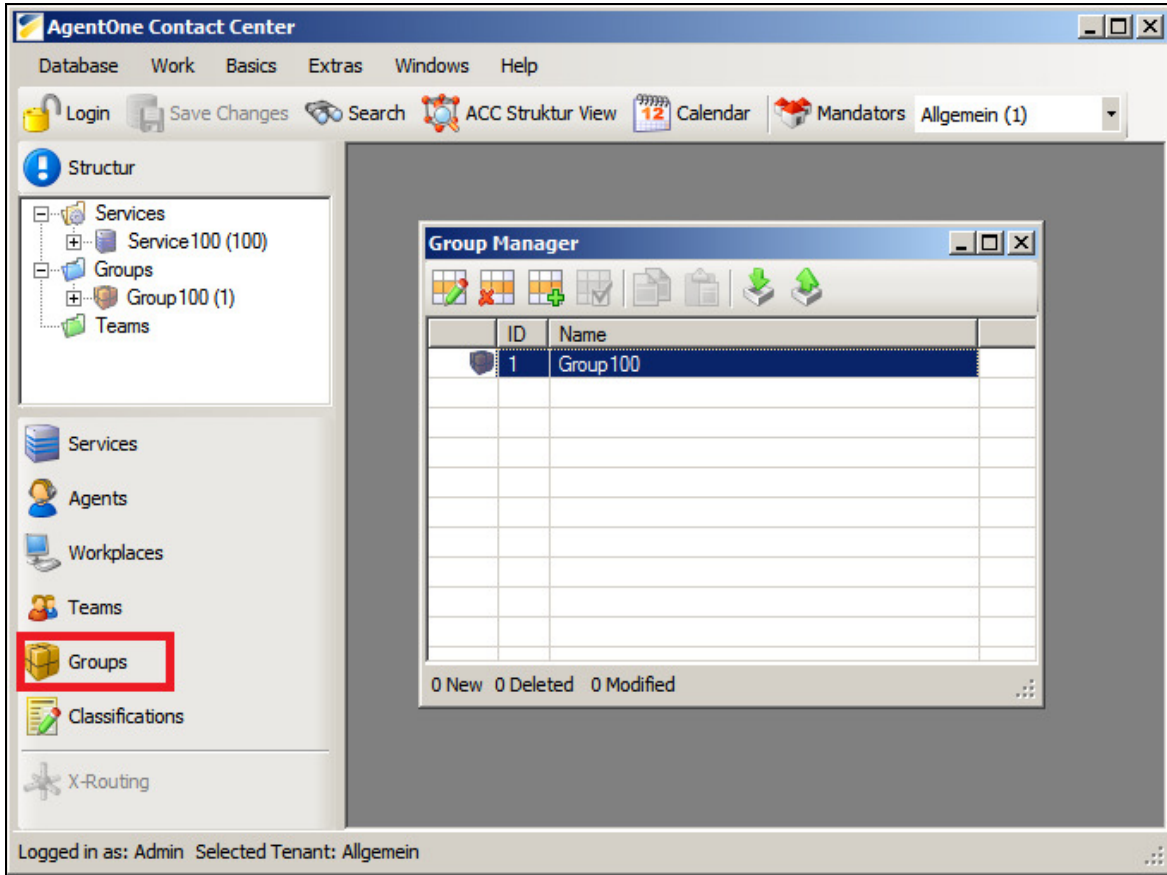
Click the **Extended** tab and enter the values shown in the window below. In this case the Service is routing to a preconfigured **Callflow** named **SkAvScript**. Click **OK** to save.

The screenshot shows the 'Edit Service' dialog box with the 'Extended' tab selected. The dialog has three tabs: 'General', 'Member', and 'Extended'. The 'Extended' tab contains several sections: 'Timer' with four input fields (Service Level, Max. Ringingtime, Max. Afterworktime, and Reminder Timeout) all set to '0'; 'Recording' with two checkboxes ('Recording active' and 'Autostart Recording') both unchecked; 'Silent Monitoring' with two checkboxes ('Auditor' and 'Training') both unchecked; 'Scriptfile' with an empty text box and a browse button (...); and 'Callflow' with a text box containing 'SkAvScript'. At the bottom right are 'OK' and 'Cancel' buttons.

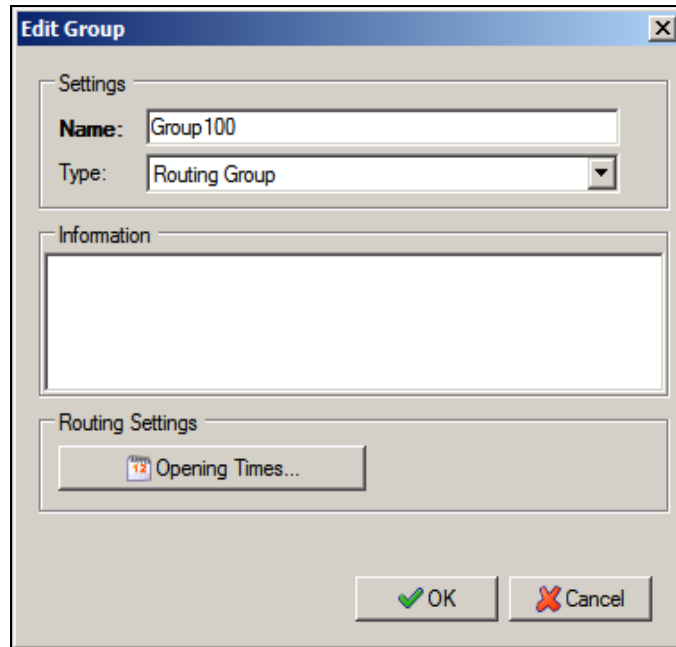
Section	Field	Value
Timer	Service Level:	0
	Max. Ringingtime:	0
	Max. Afterworktime:	0
	Reminder Timeout:	0
Recording	<input type="checkbox"/> Recording active	Unchecked
	<input type="checkbox"/> Autostart Recording	Unchecked
Silent Monitoring	<input type="checkbox"/> Auditor	Unchecked
	<input type="checkbox"/> Training	Unchecked
Scriptfile	Text box	
Callflow	Text box	SkAvScript

8.4. Configure Groups

Close Service Manager and click **Groups** on the left side of the window to add or edit routing groups using the intuitive menu bar icons.



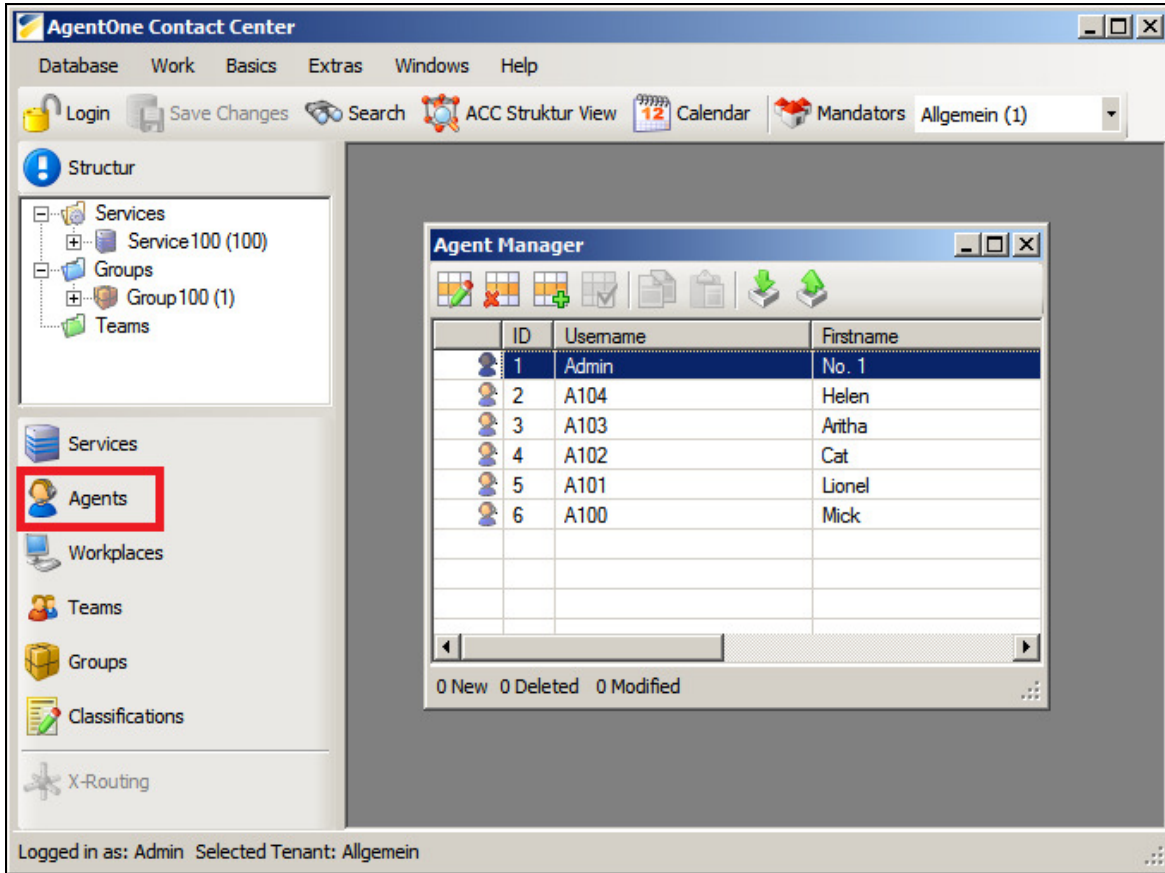
The screenshot below shows a new group with a Group **Name** of **Group 100** and a type **Routing Group**. Set the **Opening Times** for this Group as required and click **OK**,



The screenshot shows a dialog box titled "Edit Group". It contains three main sections: "Settings", "Information", and "Routing Settings". In the "Settings" section, the "Name" field is set to "Group 100" and the "Type" dropdown is set to "Routing Group". The "Information" section is currently empty. In the "Routing Settings" section, there is a button labeled "Opening Times...". At the bottom of the dialog, there are two buttons: "OK" (with a green checkmark icon) and "Cancel" (with a red X icon).

8.5. Configure Agents

Click **Agents** on the left side of the window and use the intuitive menu icons to add or edit Agents.



The screenshot below shows newly administered agent **A100** and corresponding credentials and **Agent Information**.

The screenshot displays a Windows-style dialog box titled "Edit Agent" with a close button (X) in the top right corner. The dialog has three tabs: "General", "Agent Details", and "Member". The "General" tab is currently selected. It is divided into three sections: "Login Settings", "Agent Information", and "Information".

Login Settings:

- User Name:** A100
- Password:** [Redacted with dots]
- Password (again):** [Redacted with dots]
- PIN:** [Redacted with dots]
- ☐ Supervisor

Agent Information:

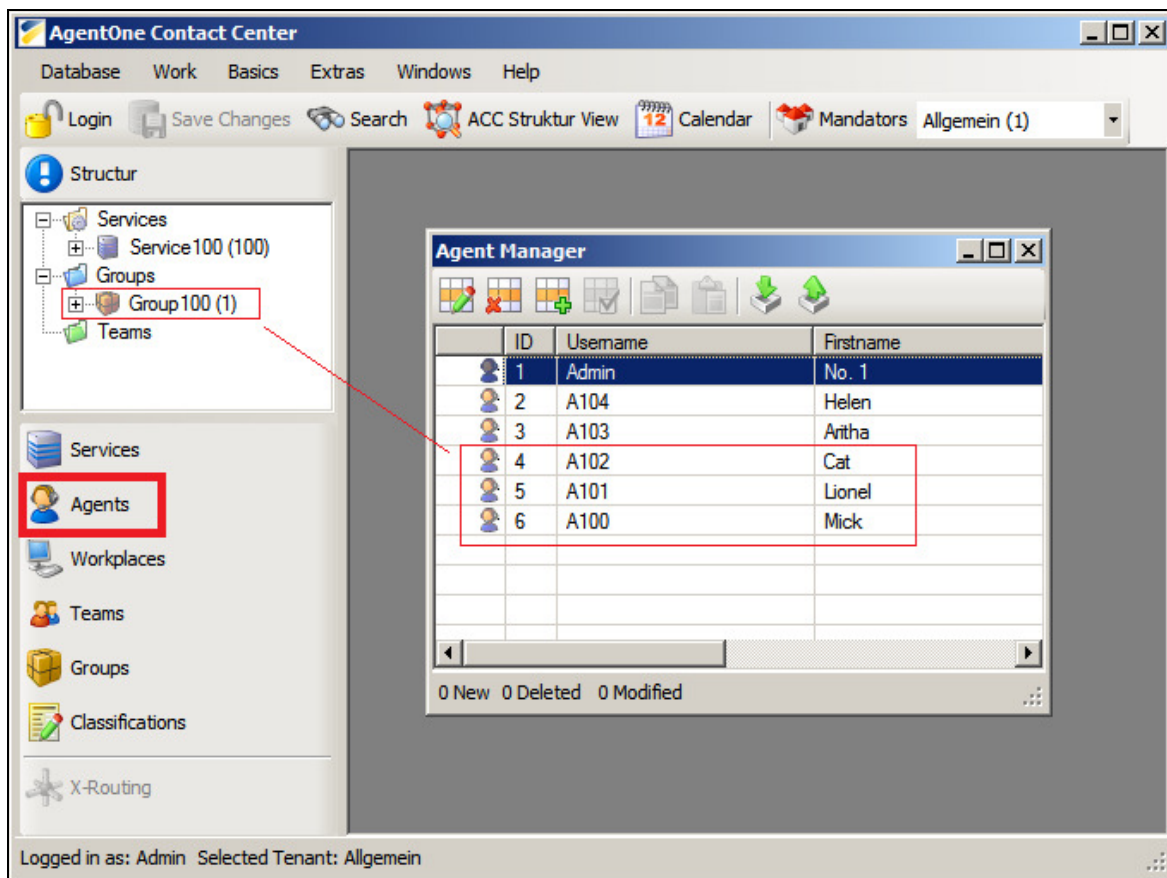
- First Name:** Mick
- Last Name:** Jagger
- Alias:** [Empty text box]
- Sex:** male (dropdown menu)

Information:

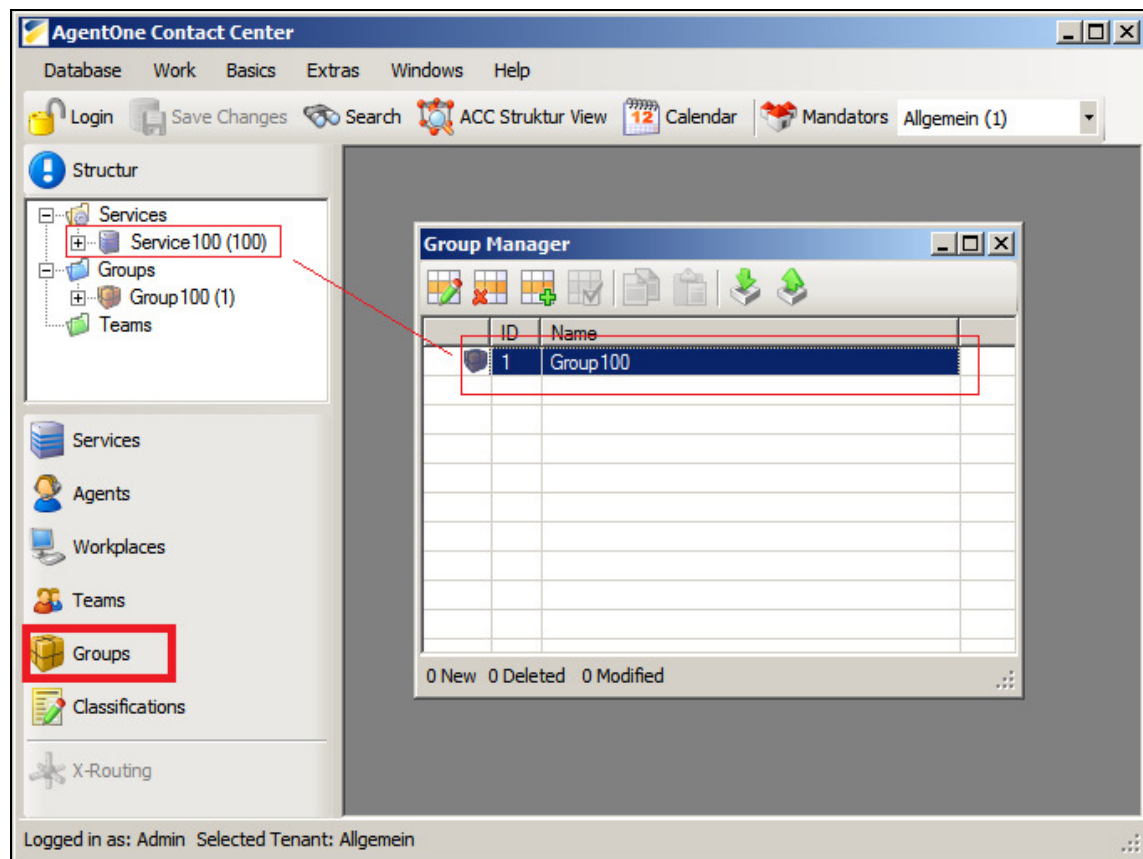
[Large empty text area]

At the bottom right, there are two buttons: "OK" (with a green checkmark icon) and "Cancel" (with a red X icon).

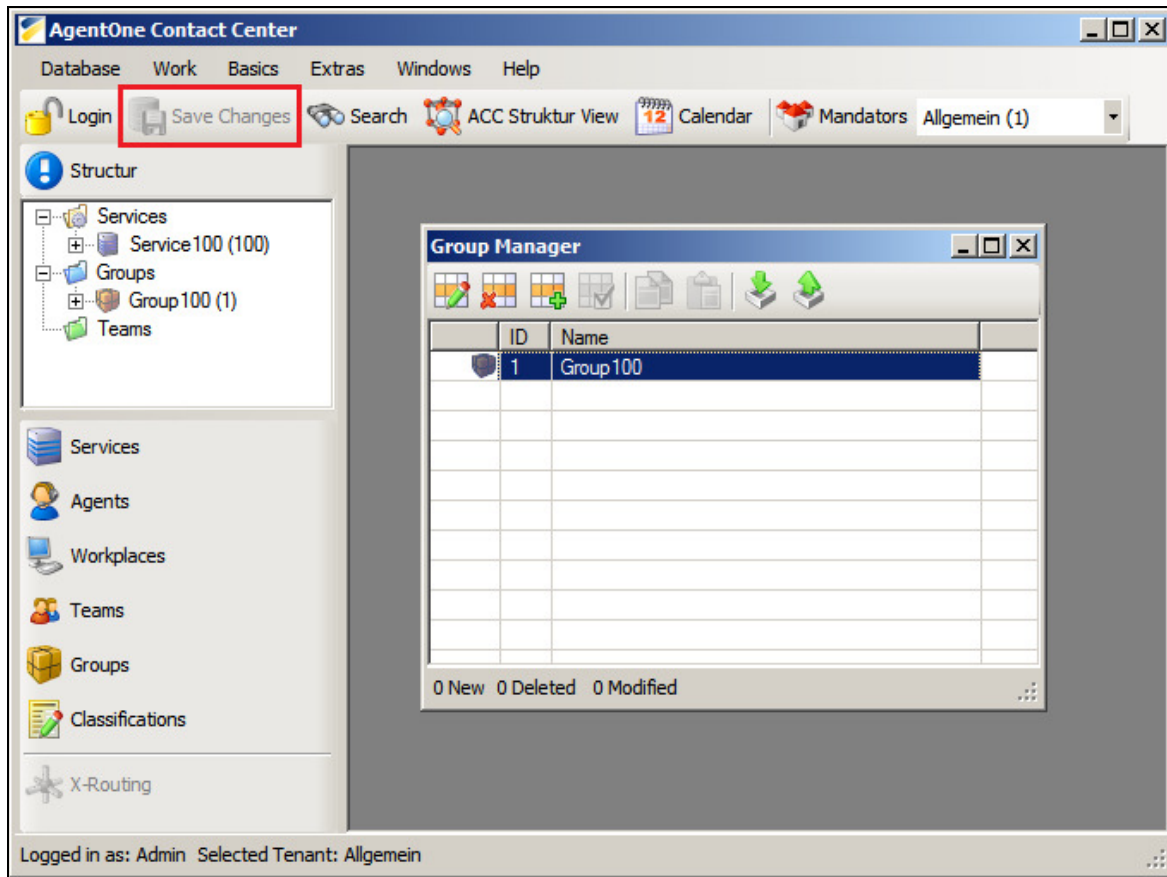
The screenshot below shows newly administered agents. Within **Agent Manager** select the appropriate agents and drag and drop them to the left side (tree) to newly administered Group, in this case **Group 100**.



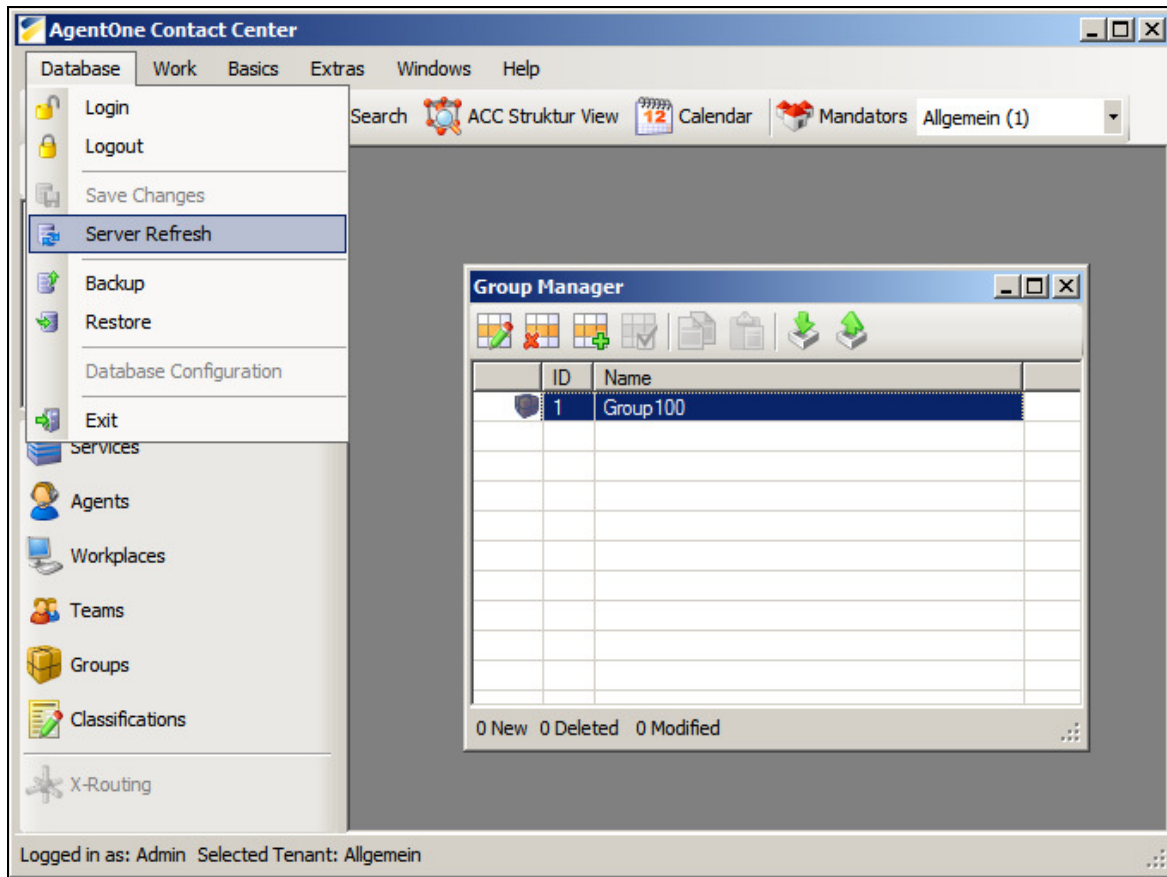
After assignment, close the Agent Manager window and open once more the Group Manager. Select the administered group, in this case **Group100** and drag and drop it to the newly administered Service, in this case **Service100** on left side of the main window.



Click **Save Changes** when done.

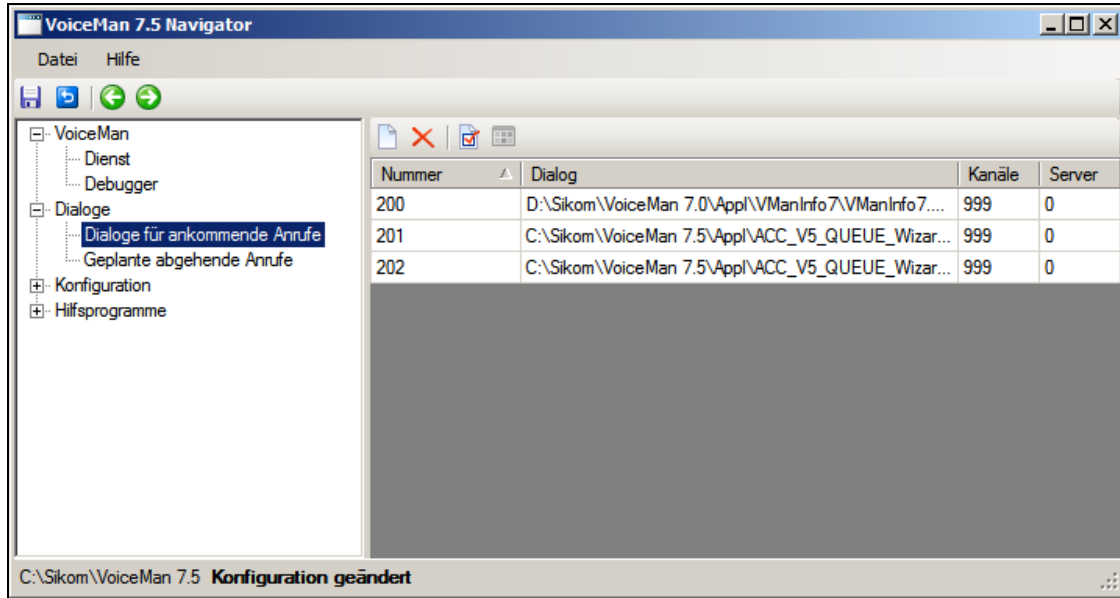


Click **Database** → **Server Refresh** to activate the new configuration.

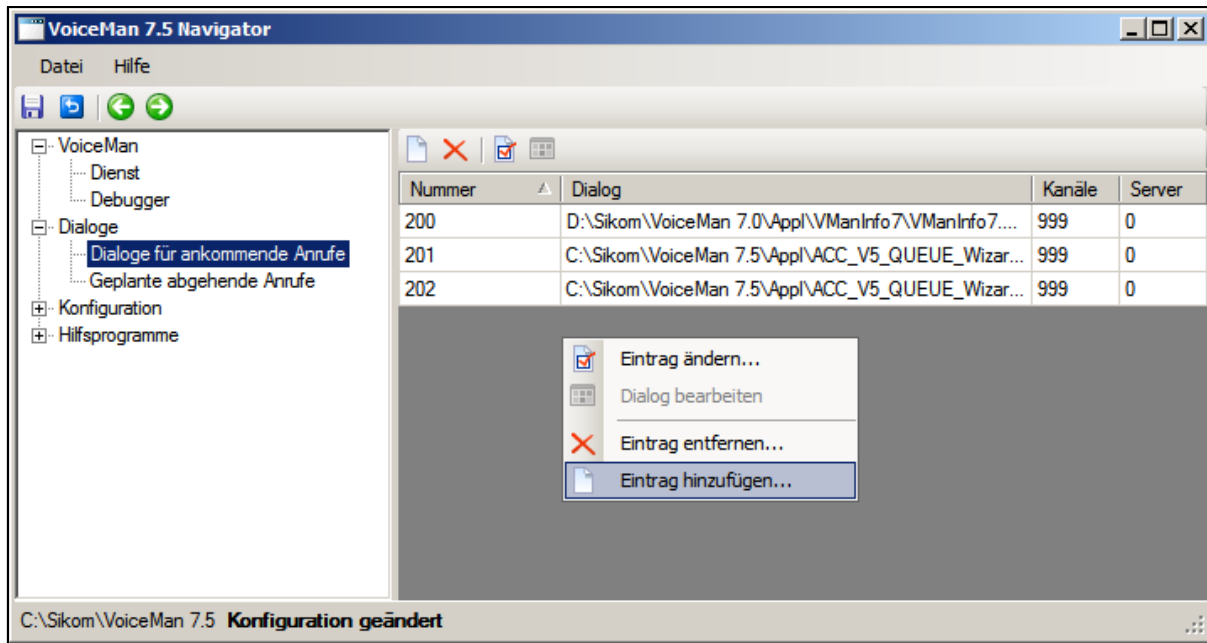


8.6. Configure IVR Application

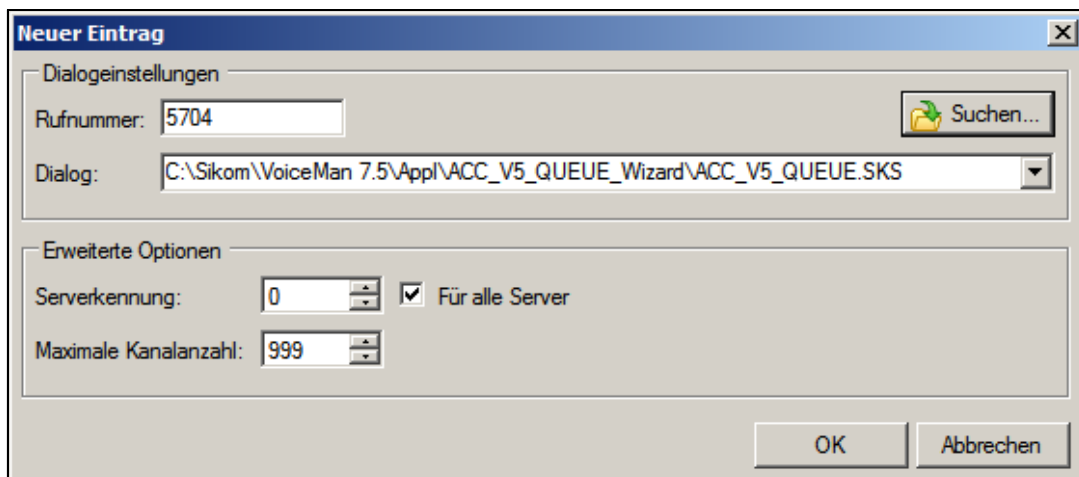
Double click on the Voiceman Navigator icon on the Gateway PC. If the Application has started, click **Dialoge**→**Dialoge für ankommende Anrufe** in the tree on left side.



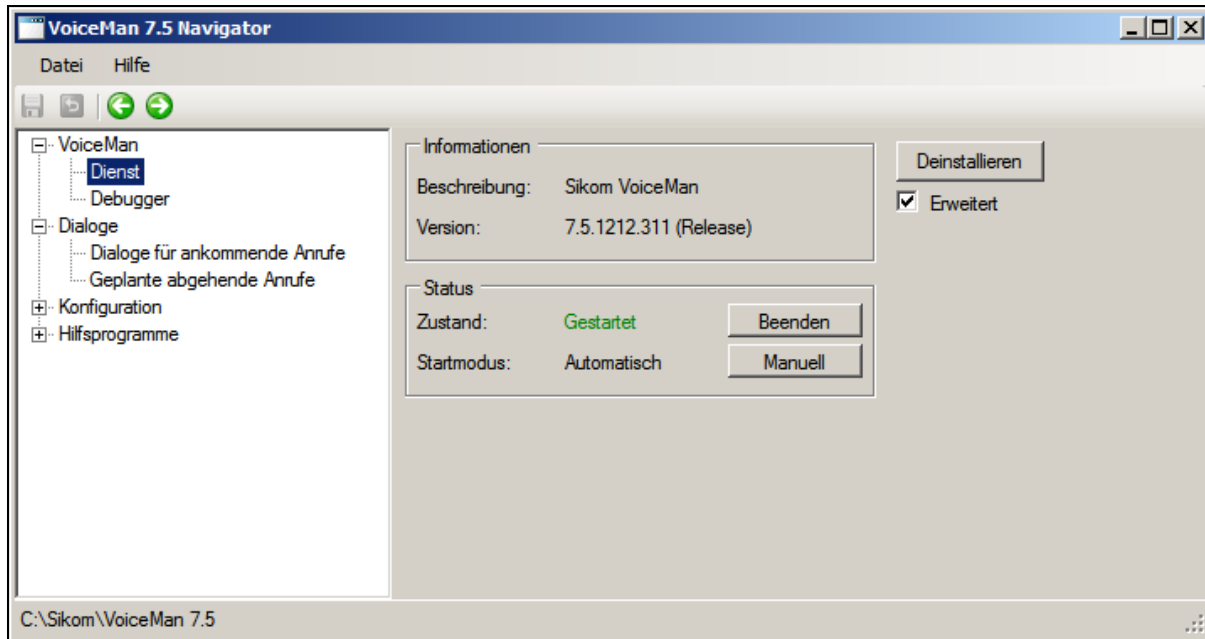
Right click in the right table and click **Eintrag hinzufügen**.



In the **Rufnummer** field, enter the Service **Dial Number** administered in **Section 8.3**, enter the path to an appropriate application file: In this case preconfigured **ACC_V5_QUEUE.SKS** was used. Click **OK** when done.



Click **Dienst** in the left hand pane and ensure IVR Service Sikom Voiceman is running whereby **Zustand** shows **Gestartet**.



8.7. Configure Refer

AgentOne can be configured so that the signaling and speech path are either routed through the AgentOne server, or once routed to the appropriate agent, the speech path and signaling are switched back to the PBX. This uses the SIP REFER signaling method. To switch call handling concerning REFER, navigate to the path of the Voiceman installation and open the file:

Acc51_Config.js with an appropriate text editor.

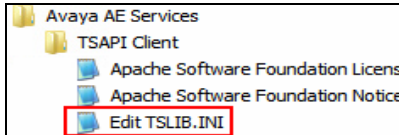
Edit accordingly whereby:

```
var AgentPR = 1           REFER is active
var AgentPR = 0           REFER inactive
```

This change can be made without requiring a restart of Voiceman.

8.8. Configure Avaya AE Services TSAPI Client

From the AgentOne server click on **Start → All Programs → Avaya AE Services → TSAPI Client → Edit TSLIB.ini**.

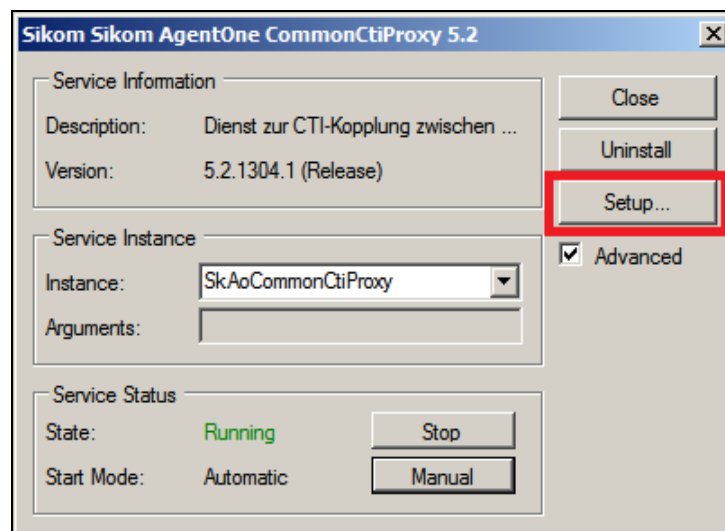


Under the **Telephony Servers** section enter the IP address assigned to AES.

```
; TSLIB.INI - Windows Telephony Services Library Configuration File  
  
; Blank lines and lines beginning with ";" are ignored.  
  
;-----  
[Telephony Servers]  
10.10.16.170=450
```

8.9. Configure Sikom CTI - Service

To configure Sikom CTI-Service navigate to the path of the CTI-Service installation and double click the Application named **Sikom.AgentOne.CtiProxy.exe** and click **Setup...**



Enter the CTI User credentials created in **Section 6.4** and the TSAPI Link string created in **Section 6.2** and click **OK**. Restart the service as necessary.

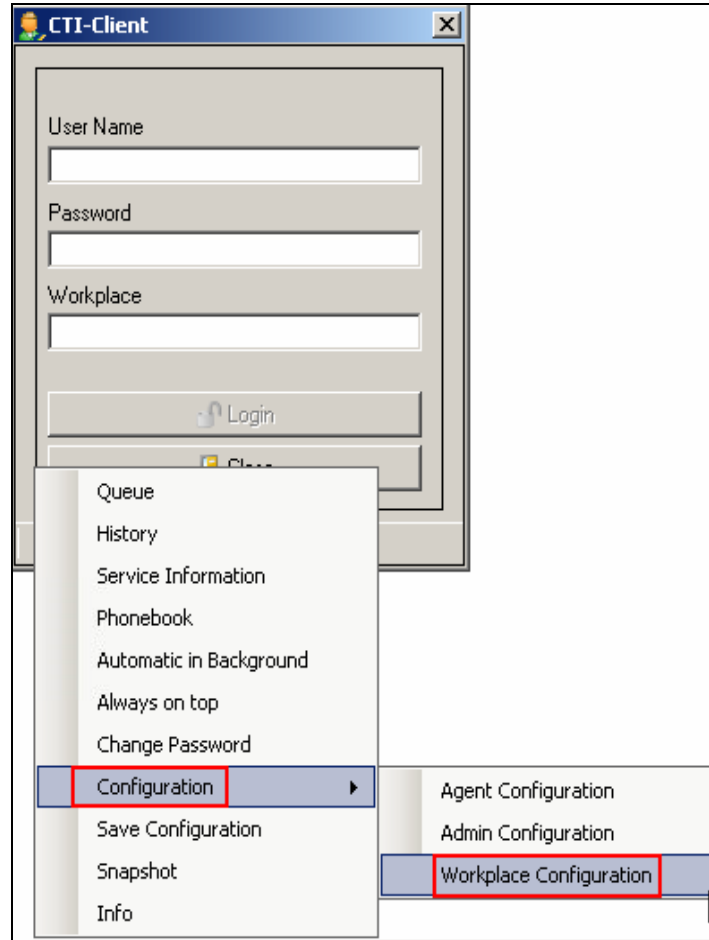
Sonstiges	
AOneCtiPort	2104
AOneDBConStr	MySQL;Database=sk_acc_v5;User Id=acca
AOneServerAdr	127.0.0.1
CommonCtiProxyKey	Software\Sikom\AgentOne\V5\CommonCti
CreateInAndOutboundForAgentCalls	True
PbxLoginId	Sikom
PbxPassword	Sikom 123!
PbxServerId	AVAYA#CM62#CSTA#AES62VM


AOneCtiPort
Port der AgentOne CTI-Schnittstelle

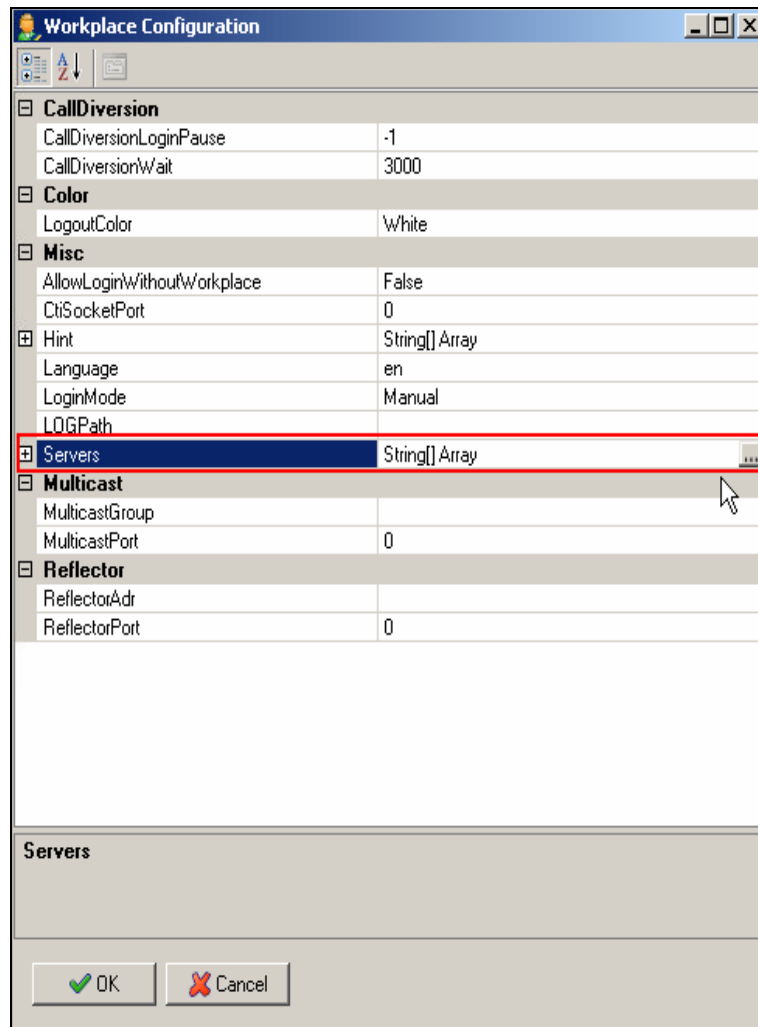
OK Abbrechen

8.10. Configure AgentOne Client

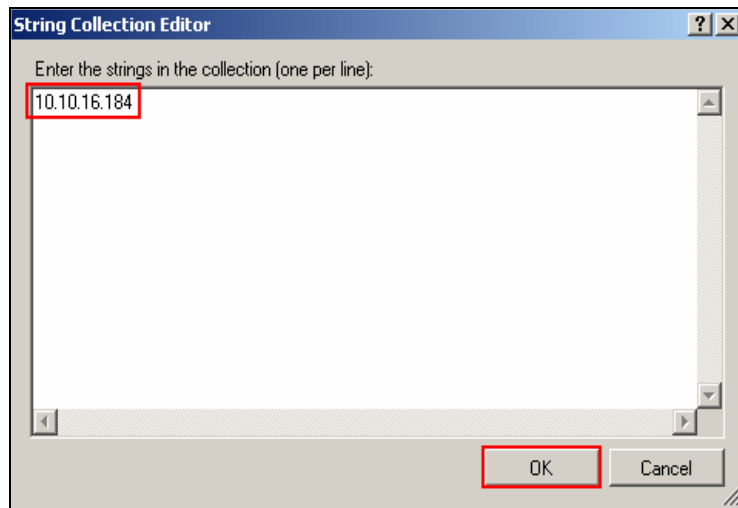
Double click on the AgentOne Client icon on the agent PC and right click on the **CTI-Client** login screen to display the menu, click **Configuration** → **Workplace Configuration**



In the **Workplace Configuration** screen, click on **String[] Array** next to **Servers** and click the  icon.



In the **String Collection Editor** screen enter the IP address assigned to the AgentOne server and click **OK** and OK again on the **Workplace Configuration Screen**.



The CTI-Client screen will re-appear and the status bar at the bottom will display **Connect**. Enter the appropriate AgentOne credentials and in the **Workplace** field enter the extension number for the Communication Manager endpoint which will be controlled by AgentOne Client and be used for the agent speech-path and click **Login**.



9. Verification Steps

The correct configuration of the solution can be verified as follows:

9.1. Verify Entity Link to AgentOne

From the System Manager web interface click **Home → Session Manager → System Status → SIP Entity Monitoring**. Click on the entity configured in **Section 7.1** and confirm the **Conn. Status** is **Up**, the **Reason Code** is **200 OK** and the **Link Status** is **Up**.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	SM62	10.10.16.184	5060	UDP	Up	200 OK	Up

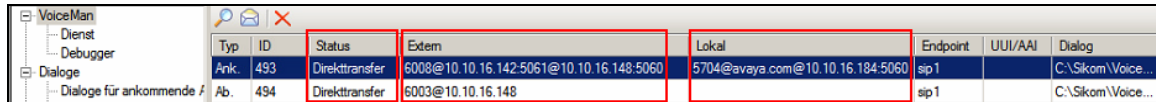
9.2. Verify TSAPI Connection Status

Using the Application Enablement Services web interface click **Status → Status and Control → TSAPI Service Summary → User Status** and under the **Name** column ensure the AgentOne CTI User configured in **Section 6.4** is shown with the corresponding **Tlink Name**.


Name	Time Opened	Time Closed	Tlink Name
Sikom	Fri 03 May 2013 07:48:06 PM UTC		AVAYA#CM62#CSTA#AES62VM
DMCCLCSUserDoNotModify	Thu 02 May 2013 09:52:51 AM UTC		AVAYA#CM62#CSTA#AES62VM

9.3. Verify SIP Call Status on AgentOne and AgentOne Client CTI Control

Dial an appropriately configured number on the AgentOne platform which routes to an endpoint controlled by an AgentOne Client. Using VoiceMan 7.5 Navigator click on VoiceMan at the top of the hierarchy and verify the **Status**, **Extern** and **Lokal** details are accurate. In the example shown below the dialogue used when 5704 was dialed created a direct transfer of an inbound call from extension 6008 to extension 6003.

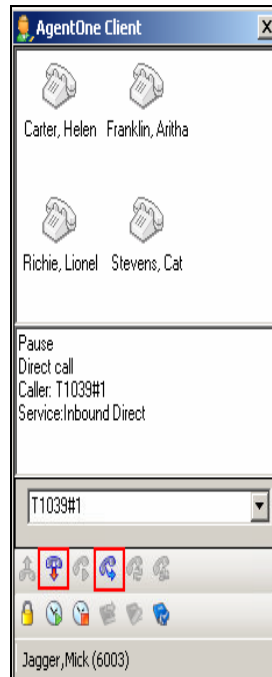




Typ	ID	Status	Extern	Lokal	Endpoint	UUI/AAI	Dialog
Ank.	493	Direkttransfer	6008@10.10.16.142:5061@10.10.16.148:5060	5704@avaya.com@10.10.16.184:5060	sip1		C:\Sikom\Voice...
Ab.	494	Direkttransfer	6003@10.10.16.148		sip1		C:\Sikom\Voice...

Where the AgentOne Client is configured with a Workstation of 6003 verify that the incoming call information is displayed accordingly and click on the  to answer the call



Verify that the call is answered on endpoint 6003 and the additional call control options are available on the AgentOne Client.



Repeat as necessary using an ACD dialogue configured on the AgentOne server and verify that the AgentOne Client agent status icons   can be used to control the status of the agent and appropriately affect the delivery of ACD routed calls.

10. Conclusion

These Application Notes describe the compliance testing of Sikom AgentOne with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. All test cases were executed successfully with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 6.2, 03-300509, Issue 7, December 2012

©2013 Avaya Inc. All Rights Reserved.

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

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