



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Scantalk ApS TeamView Unified Operator 2.0 with Avaya Aura® Communication Manager 8.0 FP1 and Avaya Aura® Application Enablement Services 8.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Scantalk ApS TeamView Unified Operator 2.0 to interoperate with Avaya Aura® Communication Manager 8.0 FP1 and Avaya Aura® Application Enablement Services 8.0.

The compliance testing focused on the voice integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Telephony Services Application Programming Interface.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 configuration steps required for Scantalk ApS TeamView Unified Operator 2.0 to interoperate with Avaya Aura® Communication Manager 8.0 FP1 using Avaya Aura® Application Enablement Services 8.0.

TeamView Unified Operator is part of the TeamView Application Suite which provides switchboard users with information about different sources, including:

- PBXs, via Computer Telephony Integration (CTI).
- Directory information, via Microsoft Active Directory and LDAP.
- Calendar Information, via Microsoft Exchange and Lotus Notes.
- Presence, via Microsoft Skype4Business UCMA.

TeamView Unified Operator is a switchboard operator application which, using the Telephony Services Applications Programmers Interface (TSAPI) of Avaya Aura® Application Enablement Services, allows an attendant to monitor and manipulate calls and devices.

TeamView Unified Operator can also be used to log in as an Avaya Aura® Communication Manager Agent (using TSAPI functions).

## 2. General Test Approach and Test Results

The general test approach was to validate successful handling of inbound VDN calls using TeamView Unified Operator. This was performed by calling inbound to a VDN and/or outbound from the elite call center using TeamView Unified Operator to answer calls. Where applicable, agent actions were performed using the TeamView Unified Operator client.

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 this Application Note, the interface between Avaya systems and Scantalk TeamView Unified Operator did not include use of any specific encryption features as requested by Scantalk.

## 2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

- **Change Agent state** – Login, Ready, AUX, After Call Work using TeamView Unified Operator.
- **Inbound Calls** – Answer calls using TeamView Unified Operator.
- **Outbound Calls** – Make calls using TeamView Unified Operator.
- **Hold/Transfer**– Place callers on hold and transfer using TeamView Unified Operator.
- **Serviceability** - Verify the ability of TeamView Unified Operator to recover from disconnection and reconnection to the Avaya solution.

## 2.2. Test Results

All test cases were executed. The following were observations on TeamView Unified Operator from the compliance testing.

- TeamView Unified Operator software required to re-connect manually, after the connection to the Avaya solution was interrupted, by choosing **Connect** from the menu showing by right-click on the phone Icon in left bottom corner.
- TeamView Unified Operator does not support Conference.

## 2.3. Support

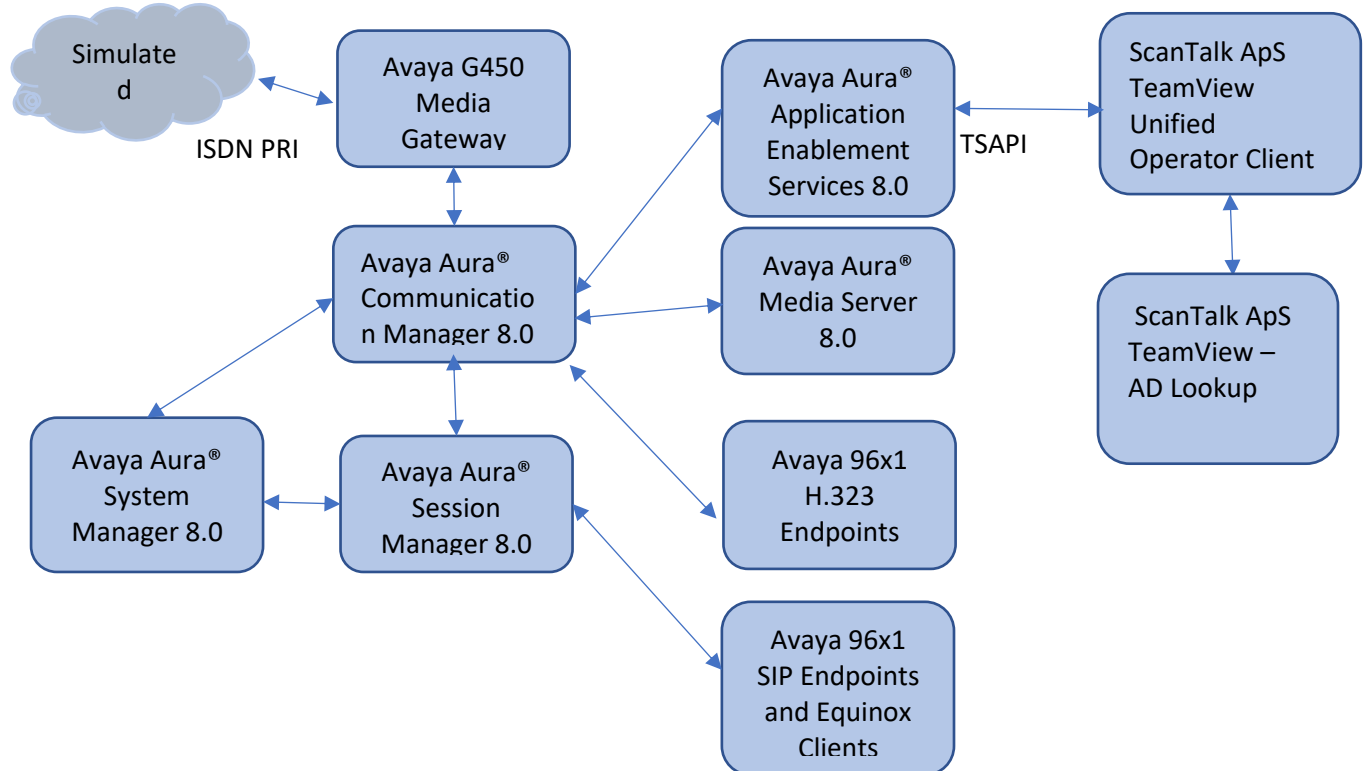
Technical support can be obtained for the TeamView Unified Operator solution as follows:

- Email: [support@scantalk.com](mailto:support@scantalk.com)
- Website: [www.scantalk.com](http://www.scantalk.com)
- Phone: +45 70 22 20 80

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services.

The devices used in the compliance testing are shown in the table below.



**Figure 1: Compliance Testing Configuration**

## 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 in Virtual Environment	8.0.1.0.0 (8.0 FP1)
Avaya G450 Media Gateway	40.10.1
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.0.1
Avaya Aura® Application Enablement Services TSAPI Client	8.0.1
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
ScanTalk ApS TeamView - Unified Operator Client	2.0.18.570
ScanTalk ApS TeamView – AD Lookup	3.2.193

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer vectors and VDNs

### 5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y		
Access Security Gateway (ASG)? n	Authorization Codes? y		
Analog Trunk Incoming Call ID? y	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n		
Answer Supervision by Call Classifier? y	Change COR by FAC? n		
ARS? y	<b>Computer Telephony Adjunct Links? y</b>		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y	DCS (Basic)? y		
ASAI Link Core Capabilities? y	DCS Call Coverage? y		
ASAI Link Plus Capabilities? y	DCS with Rerouting? y		
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y		
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y		
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y		
ATMS? y			
Attendant Vectoring? y			
(NOTE: You must logoff & login to effect the permission changes.)			

## 5.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 79999		
Type: ADJ-IP		
COR: 1		
Name: aes8		

## 5.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. The following sections give step by step instructions on how to add the following

- Hunt Group
- Agent

### 5.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **100** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

add hunt-group 2		Page 1 of 4
HUNT GROUP		
Group Number: 2		ACD? y
Group Name: Voice Service		Queue? y
Group Extension: 88100		Vector? y
Group Type: ucd-mia		
TN: 1		
COR: 1		MM Early Answer? n
Security Code:		Local Agent Preference? n
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:		Port:
Time Warning Threshold:		Port:

On **Page 2** ensure that **Skill** is set to **y** as shown below.

<b>add hunt-group 2</b>		Page 2 of 4
HUNT GROUP		
<b>Skill?</b> y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

### 5.3.2. Add Agent

To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent.

<b>add agent-loginID 80000</b>		Page 1 of 3
AGENT LOGINID		
Login ID: 80000	AAS? n	
Name: Voice Agent	AUDIX? n	
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	LWC Log External Calls? n	
	AUDIX Name for Messaging:	
	LoginID for ISDN/SIP Display? n	
	Password:	
	Password (enter again):	
	Auto Answer: station	
	MIA Across Skills: system	
	ACW Agent Considered Idle: system	
	Aux Work Reason Code Type: system	
	Logout Reason Code Type: system	
	Maximum time agent in ACW before logout (sec): system	
	Forced Agent Logout Time: :	
WARNING: Agent must log in again before changes take effect		

On **Page 2**, add the required skills. Note that the skill **2** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.



add agent-loginID 80000												Page 2 of 3		
												AGENT LOGINID		
Direct Agent Skill:												Service Objective? n		
Call Handling Preference: skill-level												Local Call Preference? n		
SN	RL	SL		SN	RL	SL		SN	RL	SL		SN	RL	SL
1: 2		1		16:				31:				46:		
2:				17:				32:				47:		
3:				18:				33:				48:		
4:				19:				34:				49:		
5:				20:				35:				50:		
6:				21:				36:				51:		
7:				22:				37:				52:		
8:				23:				38:				53:		
9:				24:				39:				54:		
10:				25:				40:				55:		
11:				26:				41:				56:		
12:				27:				42:				57:		
13:				28:				43:				58:		
14:				29:				44:				59:		
15:				30:				45:				60:		

## 5.4. Configure SIP Stations

To monitor the status of SIP endpoints in TeamView Unified Operator, the SIP station must be administered for 3<sup>rd</sup> Party Call Control. Enter the command **change station x**, where x is a SIP station, and navigate to **Page 6**. Set the **Type of 3PCC Enabled** to **Avaya**, as shown below. Perform this for every SIP station to be monitored by TeamView Unified Operator.

change station 1300										Page 6 of 6	
6											
STATION											
SIP FEATURE OPTIONS											
Type of 3PCC Enabled: Avaya											
SIP Trunk: 2											

## 5.5. Configure Directed Call Pickup Access Code

In order for operators to pick up calls ringing on other consoles, the Directed Call Pickup Access Code needs to be administered. Enter the command **change feature-access-codes**, on **Page 2** assign a code appropriate to the diaphan as the **Directed Call Pickup Access Code**.

<b>change feature-access-codes</b>	<b>Page 2 of</b>
10	
FEATURE ACCESS CODE (FAC)	
Contact Closure Pulse Code:	
Data Origination Access Code:	
Data Privacy Access Code:	
<b>Directed Call Pickup Access Code: *15</b>	
Directed Group Call Pickup Access Code:	
Emergency Access to Attendant Access Code:	
EC500 Self-Administration Access Codes:	
Enhanced EC500 Activation:	Deactivation:
Enterprise Mobility User Activation:	Deactivation:
Extended Call Fwd Activate Busy D/A All:	Deactivation:
Extended Group Call Pickup Access Code:	
Facility Test Calls Access Code:	
Flash Access Code:	
Group Control Restrict Activation:	Deactivation:
Hunt Group Busy Activation:	Deactivation:
ISDN Access Code:	
Last Number Dialed Access Code:	
Leave Word Calling Message Retrieval Lock:	
Leave Word Calling Message Retrieval Unlock:	

## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer Scantalk user
- Administer security database
- Administer ports
- Administer TCP settings
- Restart services
- Obtain Tlink name

### 6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.




### Application Enablement Services Management Console

A login form with a light gray background. It contains the text "Please login here:" followed by "Username" and a text input field. Below the input field is a button labeled "Continue".

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 15:47:40 ICT 2019  
HA Status: Not Configured

Home

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:


- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

## 6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 15:49:11 ICT 2019  
HA Status: Not Configured

Licensing

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
  - WebLM Server Address
  - WebLM Server Access**
  - Reserved Licenses
- ▶ Maintenance

### Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users and Device Media and Call Control**, as shown below. The TSAPI license is used for device monitoring and the DMCC license is used for the virtual IP softphones. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH**, which is needed for adjunct routing.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Licenses' selected. The main content area displays the 'View License Capacity' page for 'Application\_Enablement'. It shows the license installed on 'December 28, 2018 11:22:53 AM +07:00' and the 'License File Host IDs' as 'V0-55-3B-33-B4-26-01'. Below this is a table titled 'Licensed Features' showing 13 items. The table has columns for 'Feature (License Keyword)', 'Expiration date', and 'Licensed capacity'.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	1000
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	1000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	1000
DLG VALUE_AES_DLG	permanent	1000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 17:49:07 ICT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services


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

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<div>Add LinkEdit LinkDelete Link</div>				

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **CM8** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 17:58:54 ICT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services

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

Add TSAPI Links


Link1  
Switch ConnectionCM8  
Switch CTI Link Number1  
ASAI Link Version9  
SecurityUnencrypted  

Apply ChangesCancel Changes

## 6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “CM”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:01:53 ICT 2019  
HA Status: Not Configured

Communication Manager Interface | Switch Connections


Home | Help | Logout

- AE Services
- Communication Manager Interface
  - Switch Connections
  - Dial Plan
  - High Availability
  - Licensing
  - Maintenance
  - Networking

**Switch Connections**  
 

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> CM8	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case **10.30.5.93** as shown below. Click **Add Name or IP**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:04:25 ICT 2019  
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout


- AE Services
- Communication Manager Interface
  - Switch Connections
  - Dial Plan
  - High Availability
  - Licensing
  - Maintenance

**Edit H.323 Gatekeeper - CM8**  
   
Name or IP Address

## 6.5. Administer Scantalk 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.



**AVAYA** Application Enablement  
Services  
Management Console

Welcome: User cust  
Last login: Tue May 28 11:09:40 2019 from  
10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes95/10.30.5.95  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Jun 04 15:45:57 ICT 2019  
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with \* can not be empty.

\* User Idscantalk

\* Common Namescantalk

\* Surnamescantalk

\* User Password••••••••

\* Confirm Password••••••••

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle



## 6.6. Administer Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] to configure access privileges for the Scantalk user from **Section 6.5**.



### Application Enablement Services Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:29:44 ICT 2019  
HA Status: Not Configured

Security | Security Database | Control

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

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control

#### SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services


- ☐ Enable SDB for DMCC Service
- ☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

[Apply Changes](#)

## 6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2 :  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:32:41 ICT 2019  
HA Status: Not Configured

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**Ports**

CVLAN Ports

Unencrypted TCP Port

9999

Enabled Disabled

Encrypted TCP Port

9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port

450

Enabled Disabled

Local TLINK Ports

TCP Port Min

1024

TCP Port Max

1039

Unencrypted TLINK Ports

TCP Port Min

1050

TCP Port Max

1065

Encrypted TLINK Ports

TCP Port Min

1066

TCP Port Max

1081

DMCC Server Ports

Unencrypted Port

4721

Enabled Disabled

Encrypted Port

4722

Enabled Disabled

TR/87 Port

4723

Enabled Disabled

H.323 Ports

TCP Port Min

20000

TCP Port Max

29999

Local UDP Port Min


20000

Local UDP Port Max

29999

## 6.8. Administer TCP Settings

Select **Networking** → **TCP/TLS Settings** from the left pane, to display the **TCP/TLS Settings** screen in the right pane. For **TCP Retransmission Count**, select **TSAPI Routing Application Configuration (6)**, as shown below.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:34:19 ICT 2019  
HA Status: Not Configured

Networking | TCP / TLS SettingsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

TCP / TLS Settings

TLSv1 Protocol Configuration

☐ Support TLSv1.0 Protocol

☐ Support TLSv1.1 Protocol

☒ Support TLSv1.2 Protocol

TCP Retransmission Count

☐ Standard Configuration (15)

☒ TSAPI Routing Application Configuration (6)

Apply Changes

Restore Defaults

Cancel Changes

Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket.  
Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.

**Warning:** This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.

## 6.9. Restart Services

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



### Application Enablement Services Management Console

**Maintenance | Service Controller**

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

## 6.10. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring ContactPro

In this case, the associated Tlink name is **AVAYA#CM8#CSTA#AES8**. Note the use of the switch connection **CM8** from **Section 6.3** as part of the Tlink name.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Mar 26 14:26:05 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 15:26:16 ICT 2019  
HA Status: Not Configured

Security | Security Database | TlinksHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

Tlinks

Tlink Name

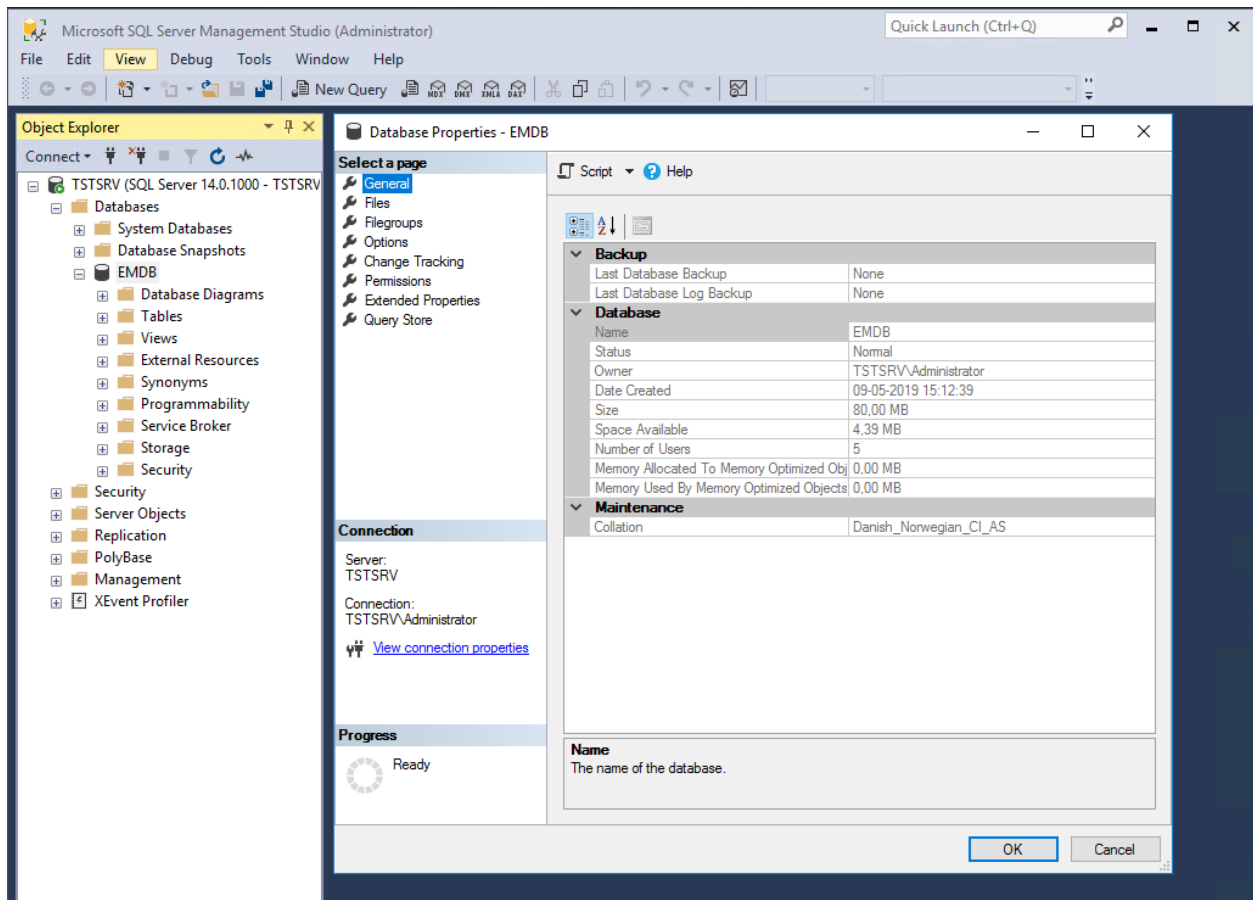
☒ AVAYA#CM8#CSTA#AES8

Delete Tlink

## 7. Configure Scantalk ApS TeamView Unified Operator

### 7.1. Configure Database and User

These Application Notes assume Microsoft SQL Server 2017 is already installed. SQL is used by TeamView Unified Operator for directory purposes. Documentation provided by Scantalk describes the method used to add a database, run the correct SQL script and add a user linked to the database. The screenshot below shows the **EMDB Database Properties** after being added to SQL, note the **Server** under the **Connection** section, this will be used in AD Lookup and in the TeamView Unified Operator configuration.



The screenshot below displays the **emdb** user administered.

**Login Properties - EMDB**

Select a page

- General
- Server Roles
- User Mapping
- Securables
- Status

Script ? Help

Login name:  Search...

☐ Windows authentication

☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☐ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential  Add

Mapped Credentials

Credential	Provider
------------	----------

Remove

Default database:

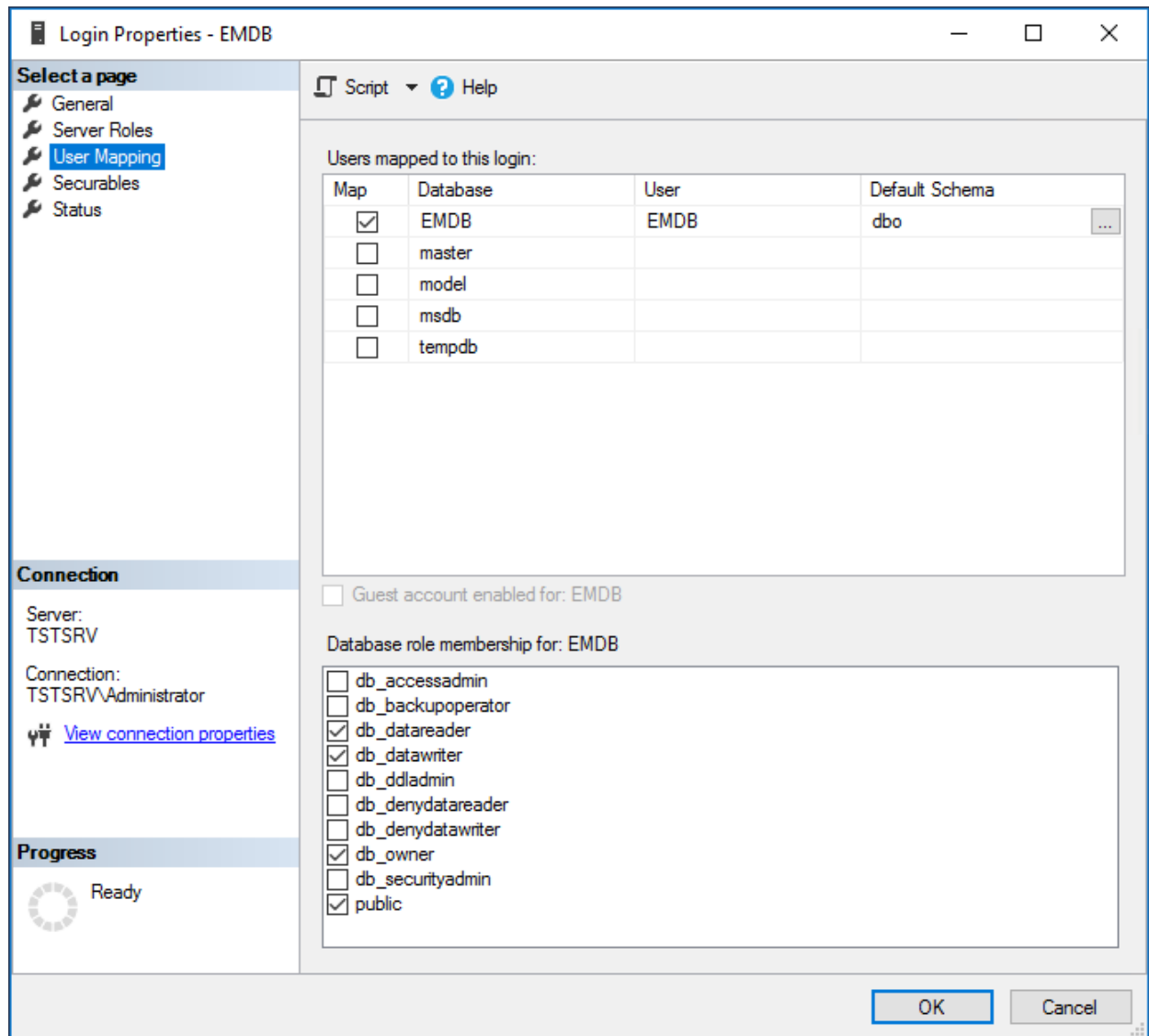
Default language:

Progress

Ready

OK Cancel

The emdb **User Mapping** and **Database Role** are shown below with regards to the EMDb database.





## 7.2. Configure Active Directory

The application note assumes active directory and a domain are already in place. The screenshot below displays an active directory user administered with a **Telephone Number**.

The screenshot shows the 'Quang Nguyen Properties' dialog box with the 'Account' tab selected. The 'First name' field is 'Quang', 'Last name' is 'Nguyen', and 'Display name' is 'Quang Nguyen'. The 'Telephone number' field is '70001'. There are 'Other...' buttons next to the 'Telephone number', 'E-mail', and 'Web page' fields. The dialog has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile	COM+	Attribute Editor		
General	Address	Account	Profile	Telephones
				Organization

Quang Nguyen

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

### 7.3. Configure TeamView AD Lookup

TeamView AD Lookup is used to extract user details administered in the corporate Microsoft Active Directory. For the purposes of this scenario, the AD Lookup application was configured as shown below. Where **Database Server** is the server connection details noted in the previous section, **Database** is the SQL database created earlier, the **User** and **Password** are those created in the previous section, the **Base/Domain** is the domain to which the both Active Directory Server and the machine on which the AD Lookup tool is run, belong. The **Filter** is the data in the Active Directory which will be extracted by the tool and added to the EMDB database.

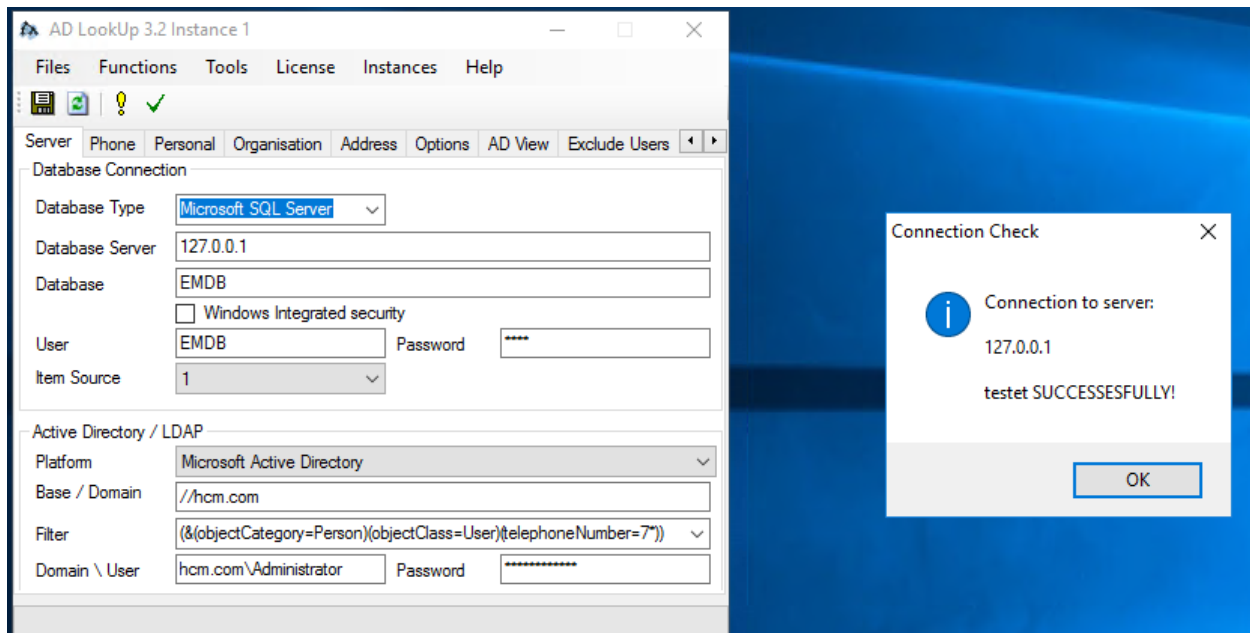
The screenshot shows the 'AD Lookup 3.2 Instance 1' application window. It has a menu bar with 'Files', 'Functions', 'Tools', 'License', 'Instances', and 'Help'. Below the menu bar is a toolbar with icons for saving, refreshing, help, and a status indicator. The main window is divided into two sections: 'Database Connection' and 'Active Directory / LDAP'. The 'Database Connection' section includes a 'Database Type' dropdown set to 'Microsoft SQL Server', a 'Database Server' text box with '127.0.0.1', a 'Database' text box with 'EMDB', a 'User' text box with 'EMDB', a 'Password' text box with masked characters, and an 'Item Source' dropdown set to '1'. The 'Active Directory / LDAP' section includes a 'Platform' dropdown set to 'Microsoft Active Directory', a 'Base / Domain' text box with '//hcm.com', a 'Filter' dropdown set to '(&(objectCategory=Person)(objectClass=User)(telephoneNumber=7\*))', and a 'Domain \ User' text box with 'hcm.com\Administrator' and a 'Password' text box with masked characters.

Database Connection	
Database Type	Microsoft SQL Server
Database Server	127.0.0.1
Database	EMDB
<input type="checkbox"/> Windows Integrated security	
User	EMDB
Password	*****
Item Source	1

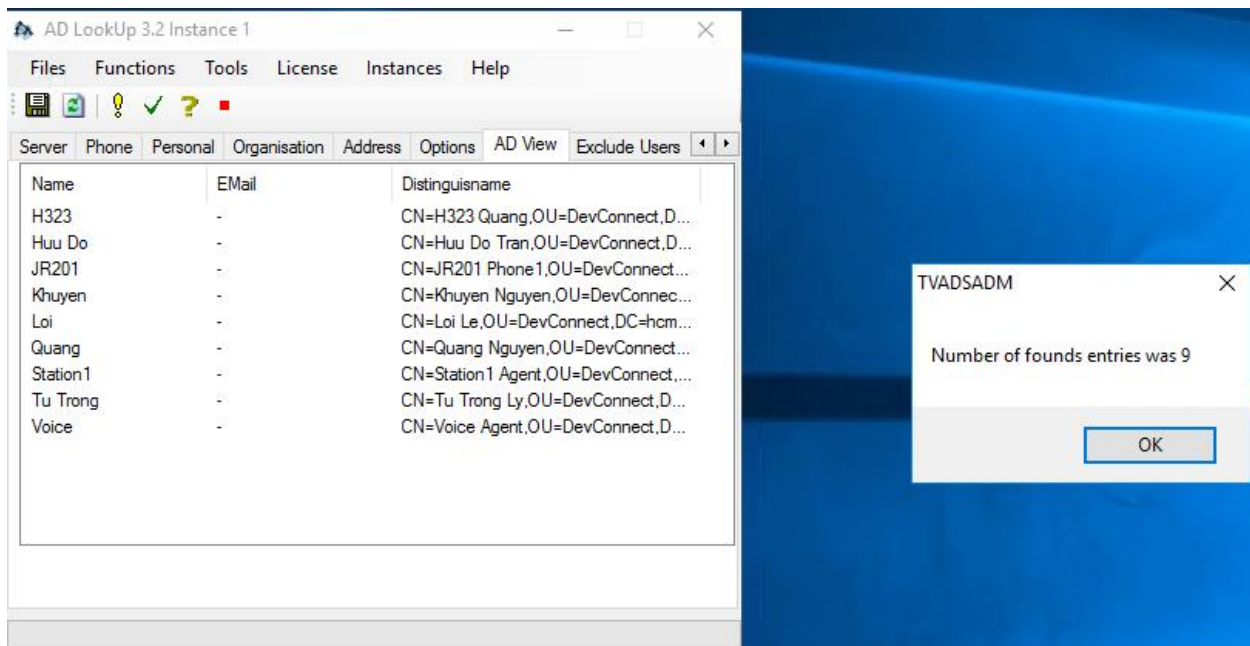
  

Active Directory / LDAP	
Platform	Microsoft Active Directory
Base / Domain	//hcm.com
Filter	(&(objectCategory=Person)(objectClass=User)(telephoneNumber=7*))
Domain \ User	hcm.com\Administrator
Password	*****

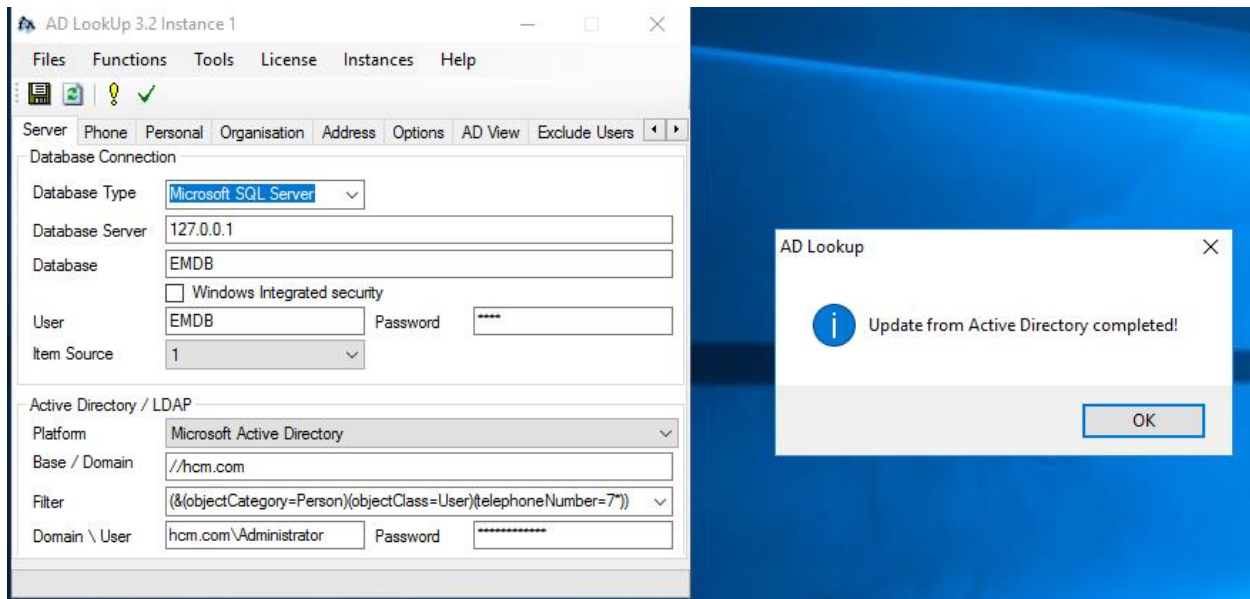
Check the connection to the SQL Server by clicking on  in the toolbar. The screenshot below shows confirmation of a successful connection.



Click the **AD View** tab and click on the yellow question mark. The screen below will display confirming entries found in Active Directory.



Return to the **Server** tab and click on the yellow exclamation mark, this will commit Active Directory entries into the EMDB database.



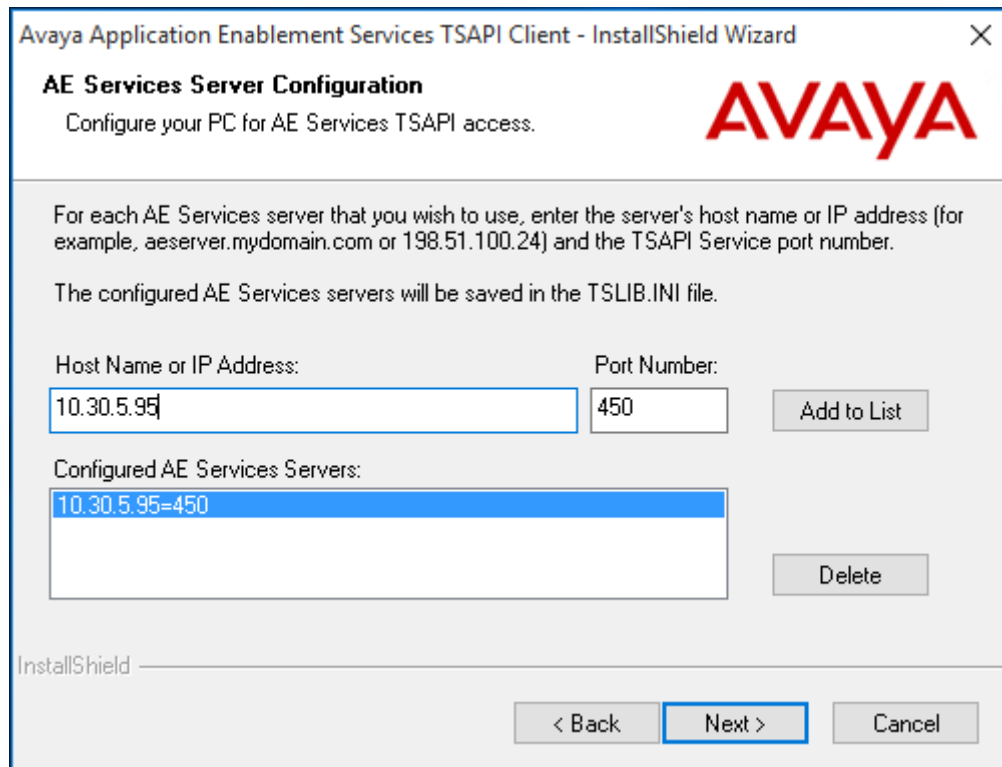
## 7.4. Configure Scantalk TeamView Unified Operator

The application note assumes that the default installation of TeamView Unified Operator software is performed. The following tasks are performed from the Windows PC on which TeamView Unified Operator is installed. Configuration can be separated into the following sections:

- Install Avaya TSAPI Client
- Install TeamView Unified Operator
- Configure TeamView Unified Operator

### 7.4.1. Install Avaya TSAPI Client

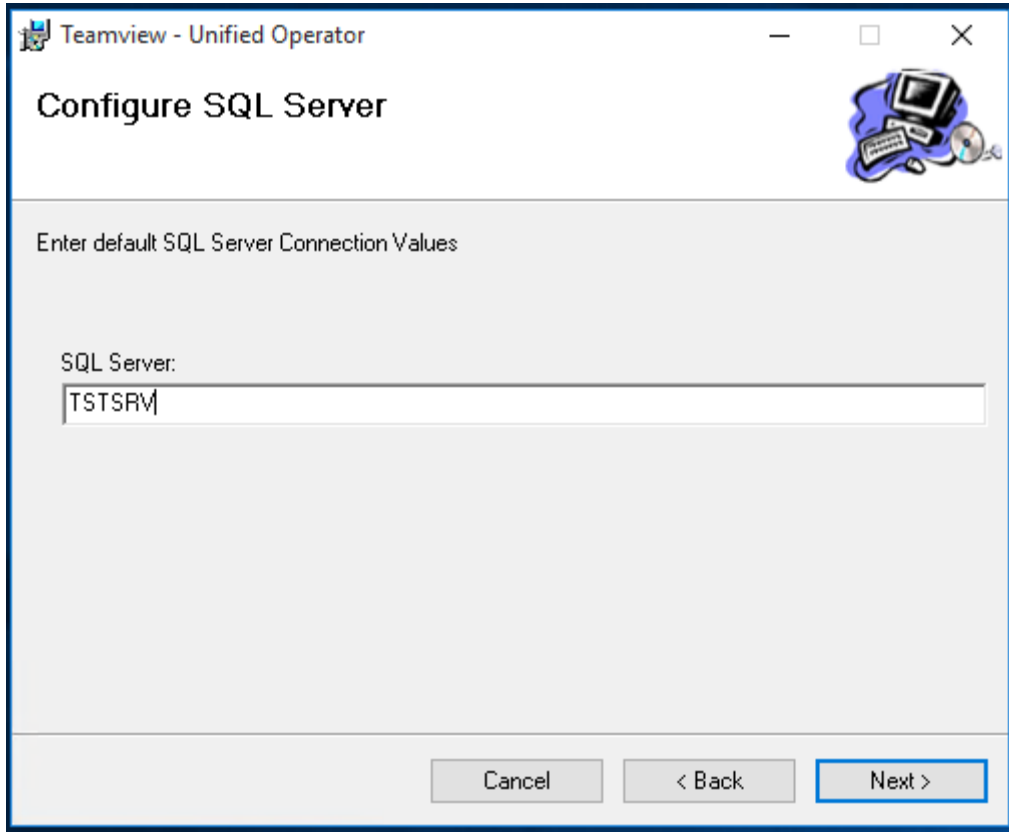
The Avaya TSAPI client is available for download from the DevConnect Support Site. Double click on the **setup** application and follow the intuitive instructions. When the **AE Services Server Configuration** screen is displayed, enter the **IP Address** of the Application Enablement Services Server, and **Port Number 450** and click **Add to List**, as shown below.



Click **Next** and follow the instructions to complete the installation of the TSAPI client.

### 7.4.2. Install Scantalk TeamView Unified Operator

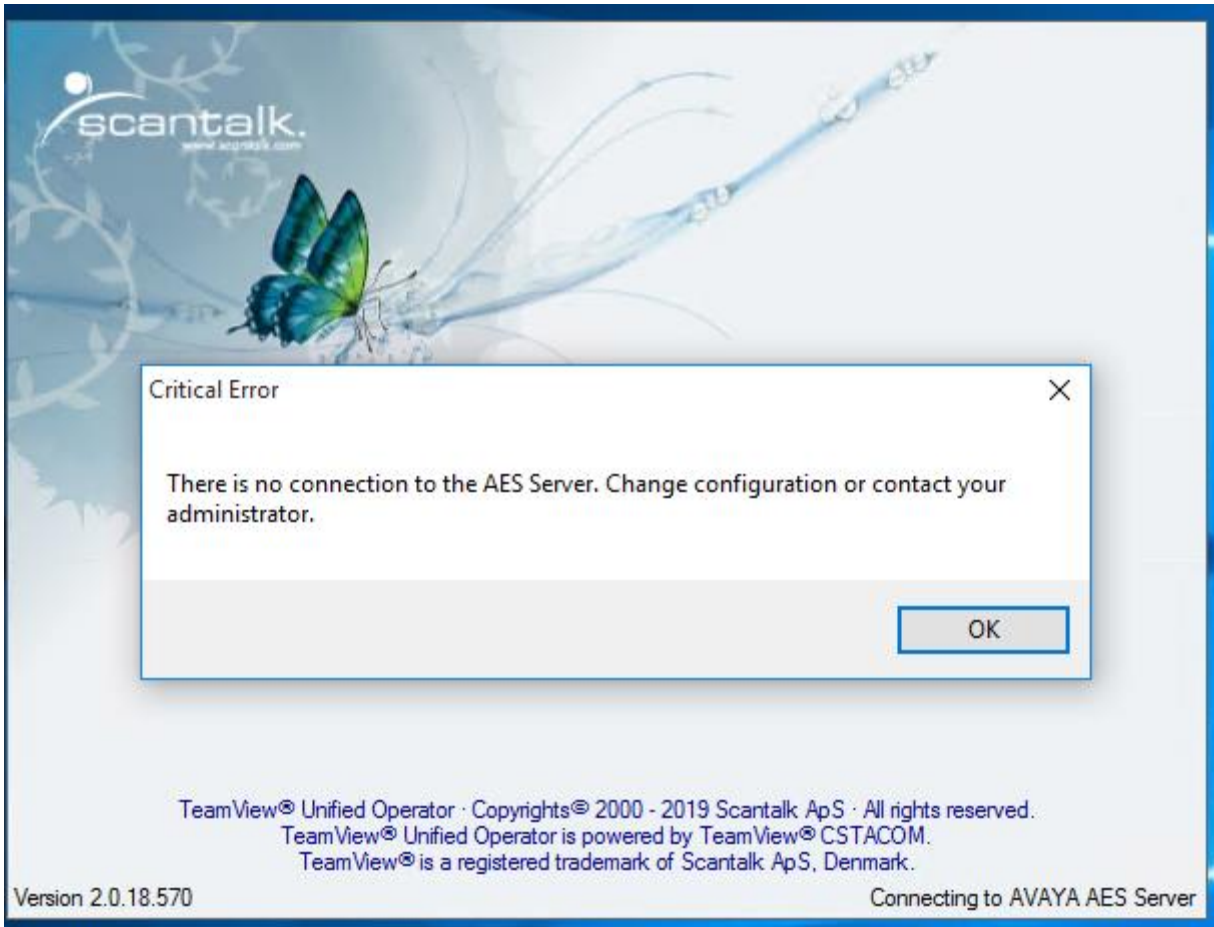
Complete a default installation of TeamView Unified Operator, by double clicking on **setup.exe** and following the self-explanatory setup wizard. When the **Configure SQL Server** screen is displayed, enter the **SQL Server**.



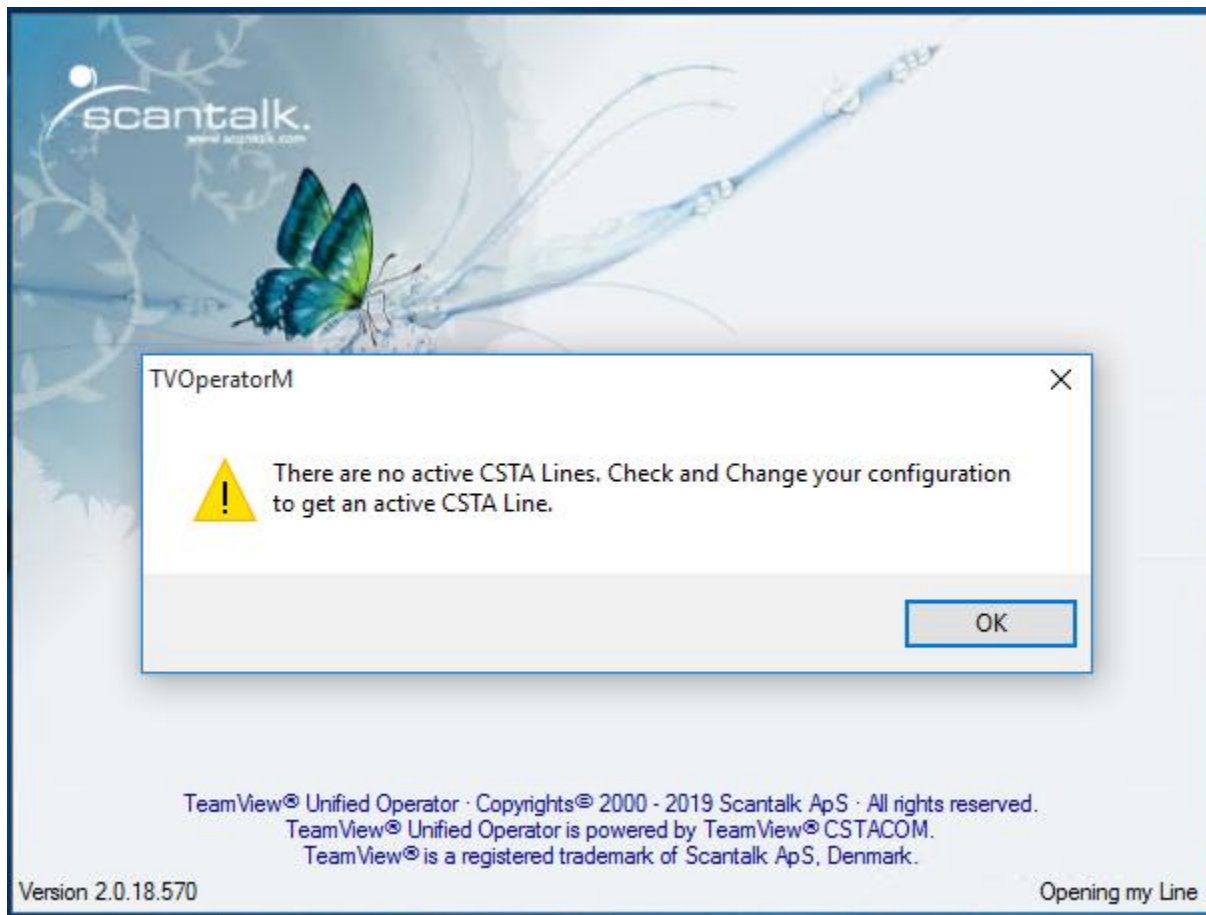
### 7.4.3. Configure Scantalk TeamView Unified Operator

Launch the TeamView Unified Operator application from the Windows Start menu, as shown below.

Upon the first run of the software, the screen below will be displayed advising **There is no connection to the AES server** administered, click **OK** to continue.



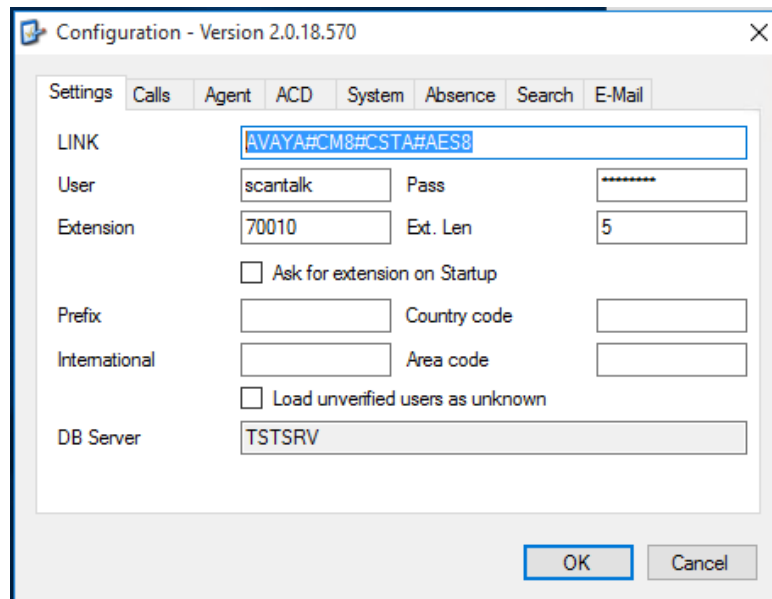
The screen below will now display advising **There are no active CSTA Lines** click **OK** to continue.





#### 7.4.4. Configure CTI, Agent, Database, System and phone parameters

The following screen will display showing the **Configuration** details. Enter the T-Link noted in **Section 6.3** as the **LINK**, the CTI User and **Password** administered in **Section 6.5**, the **Extension** you wish the operator to use, the **DB Server** as noted in **Section 7** and the extension length (**Ext. Len**) used on Communication Manager, as shown below.

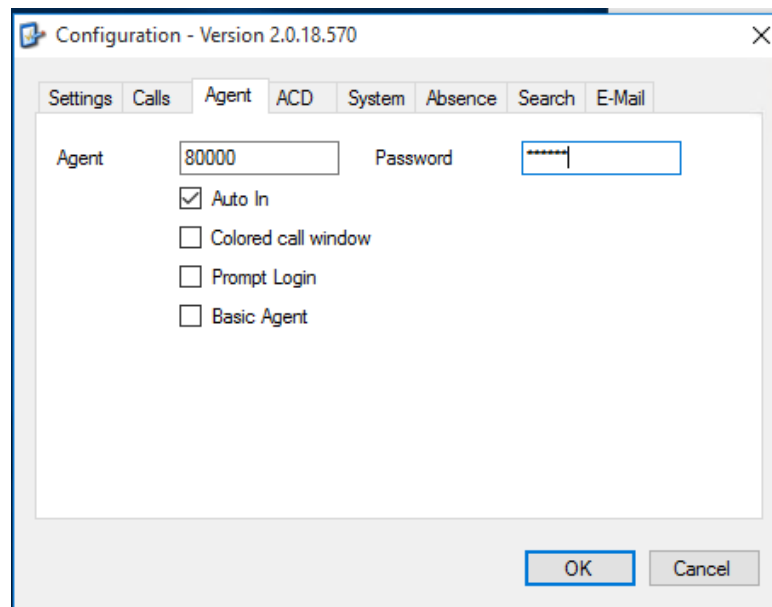


The image shows a dialog box titled "Configuration - Version 2.0.18.570" with a close button (X) in the top right corner. The "Settings" tab is selected, and the "Agent" sub-tab is active. The fields are as follows:

Field	Value
LINK	AVAYA#CM8#CSTA#AES8
User	scantalk
Pass	*****
Extension	70010
Ext. Len	5
Ask for extension on Startup	<input type="checkbox"/>
Prefix	
Country code	
International	
Area code	
Load unverified users as unknown	<input type="checkbox"/>
DB Server	TSTSRV

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

Click on the **Agent** tab and enter the **Agent** extension number and **Password** as configured in **Section 5.3**.



The image shows the same dialog box, but now the "Agent" sub-tab is selected. The fields are as follows:

Field	Value
Agent	80000
Password	*****
Auto In	<input checked="" type="checkbox"/>
Colored call window	<input type="checkbox"/>
Prompt Login	<input type="checkbox"/>
Basic Agent	<input type="checkbox"/>

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

Click on the **System** tab and configure the **Directed Call Pickup Access Code** configured in **Section 5.5** in the **Retrieve call** field as shown below. This is used in the event that calls are ringing on unattended consoles. Click **OK** when done.

The screenshot shows the 'Configuration - Version 2.0.18.570' dialog box with the 'System' tab selected. The 'System' section contains the following fields: 'HangOn' (empty), 'HangOn Return' (empty), 'Personal Park' (empty), '# Park Apprances' (3), and 'Retrieve call' (\*15N). The 'Calendar' section contains: 'Fix start to' (09), 'Calendar Offset' (0), and 'WEB Mail Url' (empty). The 'Debug logging' section contains 'Level' (4). The 'Language' section contains 'Danish'. The 'OK' and 'Cancel' buttons are at the bottom right.

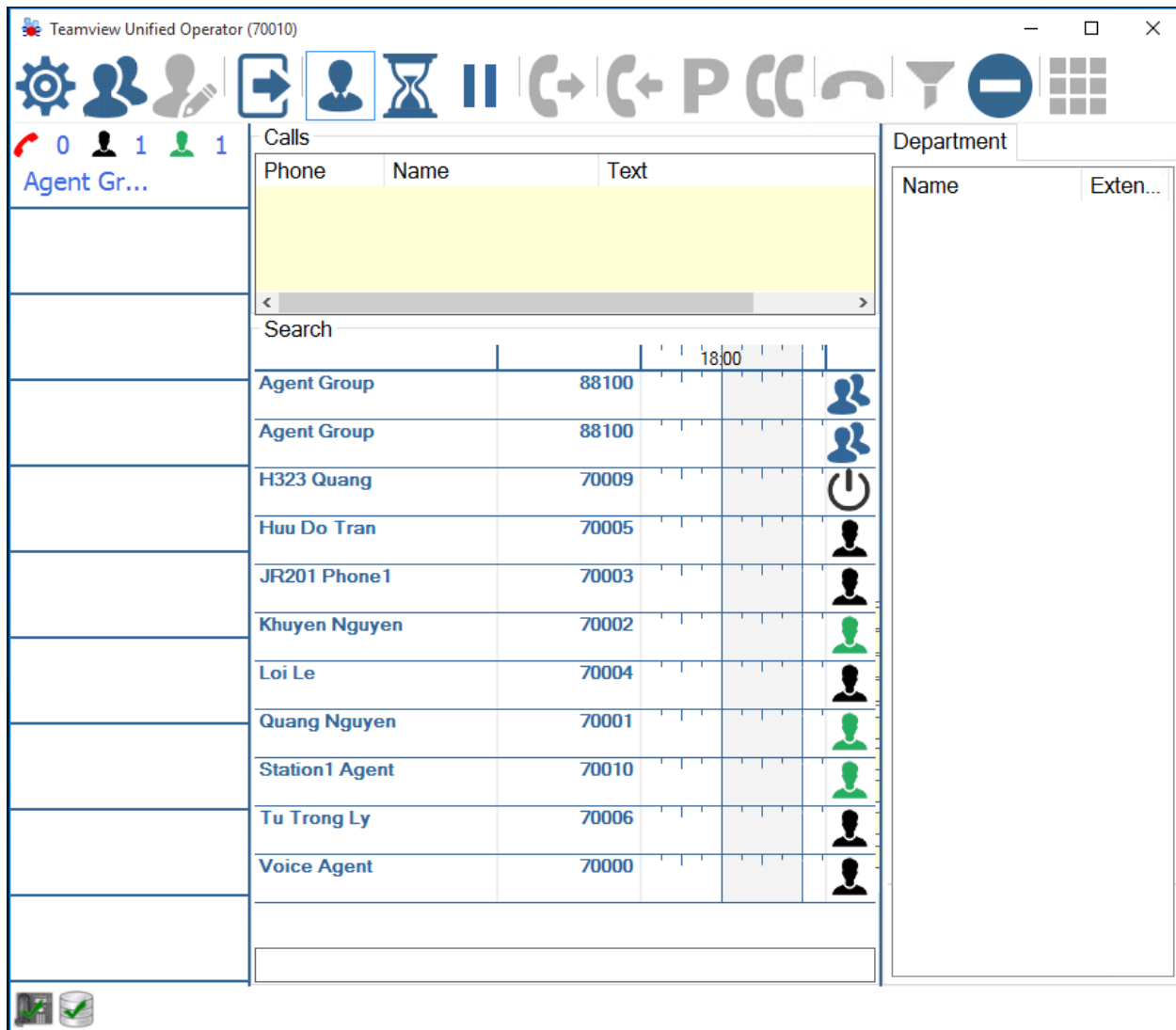
The prompt below will be displayed advising to restart the application. Click **OK**.

The screenshot shows the 'TVOperatorM' dialog box with the message 'You must restart the application to accept the changes.' and an 'OK' button at the bottom right.

Click **Yes** at the prompt shown below to close Unified Operator.

The screenshot shows the 'TVOperatorM' dialog box with the question 'Do you want to close Unified Operator?' and 'Yes' and 'No' buttons at the bottom.

Upon restart of the application, users added to the database in **Section 9** are shown. The details and status of each of these users is clearly displayed. The icons on the bottom left of the screenshot show that TeamView Unified Operator has successfully logged the agent onto the extension specified earlier in this section, as well as successful database connectivity. Click on the **Directory** icon as shown below.



Teamview Unified Operator (70010)

Agent Gr... 0 1 1

Calls

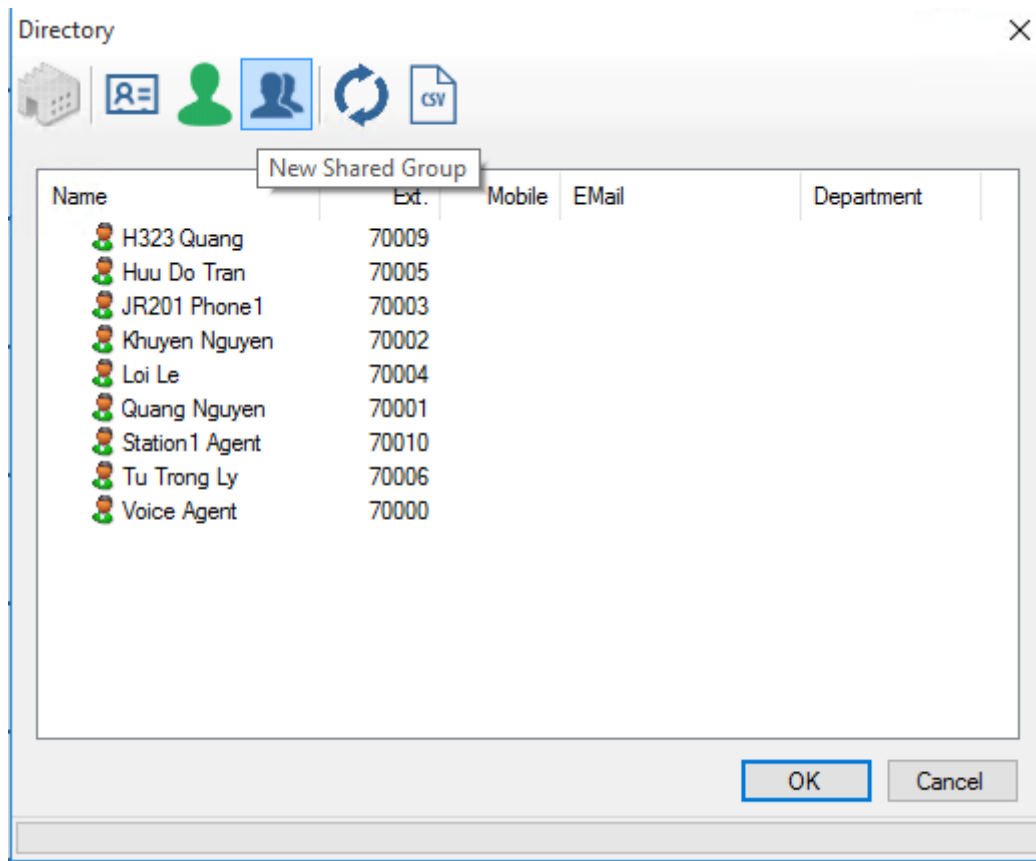
Phone	Name	Text
Search		
Agent Group	88100	18:00
Agent Group	88100	
H323 Quang	70009	
Huu Do Tran	70005	
JR201 Phone1	70003	
Khuyen Nguyen	70002	
Loi Le	70004	
Quang Nguyen	70001	
Station1 Agent	70010	
Tu Trong Ly	70006	
Voice Agent	70000	

Department

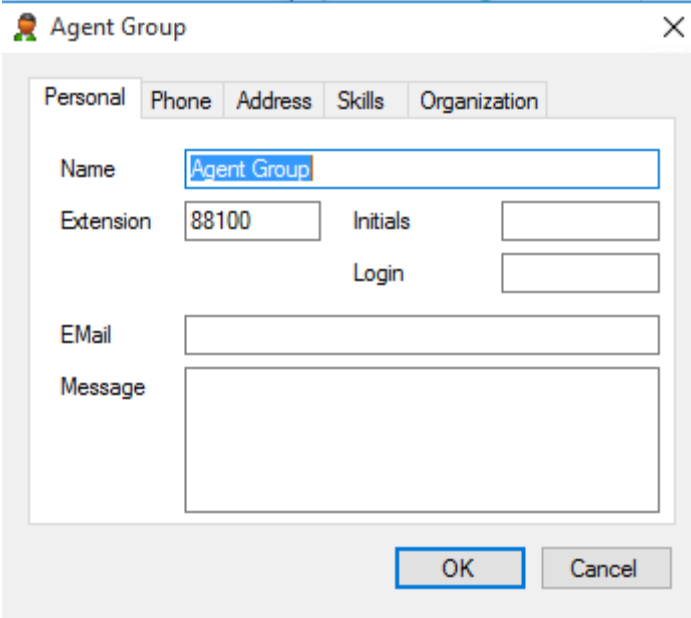
Name	Exten...
------	----------

### 7.4.5. Configure Operator Hunt Group Monitoring

Click on **New Shared Group** to add the Operator Hunt Group created in **Section 5.3.1**.

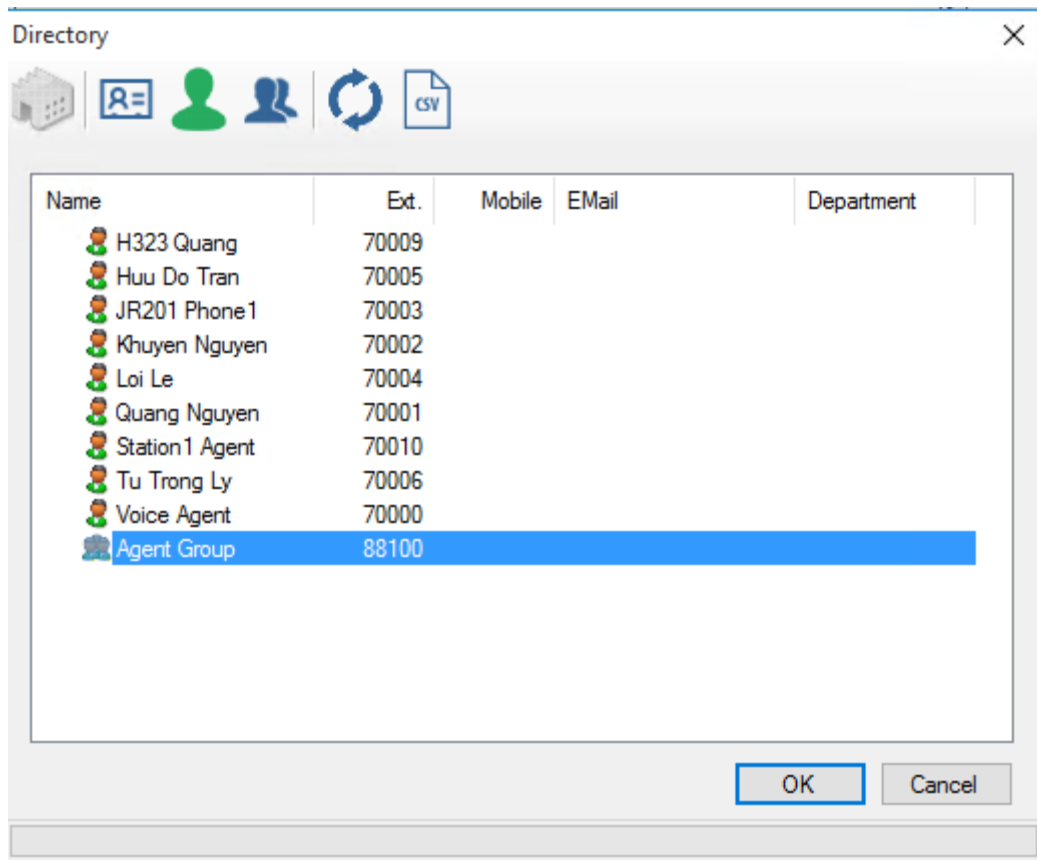


Assign the Shared Group an identifying **Name** and the **Extension** number assigned to the hunt group in **Section 5.3.1** and click **OK**.



The image shows a software window titled "Agent Group" with a close button (X) in the top right corner. The window contains several tabs: "Personal", "Phone", "Address", "Skills", and "Organization". The "Personal" tab is currently selected. Inside this tab, there are several input fields: a "Name" field containing the text "Agent Group", an "Extension" field containing "88100", an "Initials" field, a "Login" field, an "EMail" field, and a "Message" text area. At the bottom right of the window, there are two buttons: "OK" and "Cancel".

The new shared group will now appear in the directory with the other directory entries and is committed to the SQL Database for other operators to access.



Click **OK** and hit **Escape** on the keyboard to update the screen with the new shared group.

Search			18:00	
H323 Quang	70009			
Huu Do Tran	70005			
JR201 Phone1	70003			
Khuyen Nguyen	70002			
Loi Le	70004			
Quang Nguyen	70001			
Station1 Agent	70010			
Tu Trong Ly	70006			
Voice Agent	70000			
Agent Group	88100			

Click on the **Configuration** in the top left of the screen and select the **ACD** tab. From the first drop-down list select the shared group created previously, and click **OK**.

The screenshot shows a configuration window titled "Configuration - Version 2.0.18.570" with a close button (X) in the top right corner. The window has several tabs: Settings, Calls, Agent, ACD (selected), System, Absence, Search, and E-Mail. The ACD tab contains the following settings:

- ☐ Hide Queue Panel
- Agent Group: (Not Used) (dropdown menu)
- (Not Used) (dropdown menu)
- (Not Used) (dropdown menu)
- (Not Used) (dropdown menu)
- (Not Used) (dropdown menu)
- (Not Used) (dropdown menu)
- ☐ Alert when call queues
- Alert when calls in queue is: 1 (text input)
- Wallboard Server: (empty text input)

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

**Teamview Unified Operator (70010)**

Calls

Phone	Name	Text
<input type="text"/>		
Search		
H323 Quang	70009	18:00
Huu Do Tran	70005	
JR201 Phone1	70003	
Khuyen Nguyen	70002	
Loi Le	70004	
Quang Nguyen	70001	
Station1 Agent	70010	
Tu Trong Ly	70006	
Voice Agent	70000	
Agent Group	88100	

Department

Name	Exten...



## 8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Communication Manager, Application Enablement Services, and TeamView Unified Operator solution.

### 8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	9	no	aes8	established	14	14

Enter the command **list agent-loginID** verify that extension 70010 is logged into agent **80000** shown in **Section 5.4**.

```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name	Extension		Dir	Agt	AAS/AUD		COR Ag	Pr SO
		Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
80000	Voice Agent	70010						1	lvl
	2/01	/	/	/	/	/	/	/	

Enter the command **status station 70010** and on **Page 7** verify that the agent is logged-in to the appropriate skill.

```
status station 70010
```

ACD STATUS							Page 7 of 7
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
2/AI	/	/	/	/	/	/	On ACD Call? no

## 8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of agent, in this case “1”.

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	CM8	1	Talking	Mon May 20 18:12:03 2019	Online	18	1	6450	6461	30

For service-wide information, choose one of the following:

### 8.3. Verify Avaya Aura® Application Enablement Services TSAPI Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary → User Status**. The **Open Streams** section of this page displays open stream created by the **scantalk** user with the **Tlink**.

[Status](#) | [Status and Control](#) | [TSAPI Service Summary](#)[Home](#) | [Help](#) | [Logout](#)

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ [TSAPI Service Summary](#)

CTI User Status

☐ Enable page refresh every  seconds

CTI Users

Open Streams 3

Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Thu 06 Jun 2019 05:06:07 PM +07		AVAYA#CM8#CSTA#AES8
DMCCLCSUserDoNotModify	Thu 06 Jun 2019 05:06:07 PM +07		AVAYA#CM8#CSTA#AES8
scantalk	Thu 06 Jun 2019 05:07:30 PM +07		AVAYA#CM8#CSTA#AES8

## 8.4. Verify Scantalk TeamView Unified Operator Call Handling and User Status

Place a call from the operator to an extension in the directory. Confirm that the operator extension is shown as busy, the dialed extension is shown as busy, the correct extension details are displayed and the number of available agents available is decreased accordingly.

The screenshot displays the Teamview Unified Operator (70010) interface. At the top, there is a toolbar with various icons for settings, user management, call handling, and navigation. Below the toolbar, the 'Agent Gr...' section shows 0 red, 1 black, and 0 green status indicators. The main area is divided into two panes. The left pane, titled 'Calls', contains a table with columns 'Phone', 'Name', and 'Text'. The right pane, titled 'Department', contains a table with columns 'Name' and 'Exten...'. The 'Calls' table shows a single entry for extension 70002, which is highlighted in yellow. The 'Department' table is empty. Below the 'Calls' table, there is a search bar and a list of agents with their status icons.

Phone	Name	Text
70002	Nguyen, Khuyen	88100<--Nguyen, Khuyen

Name	Exten...
------	----------

Name	Exten...
H323 Quang	70009
Huu Do Tran	70005
JR201 Phone1	70003
Khuyen Nguyen	70002
Loi Le	70004
Quang Nguyen	70001
Station1 Agent	70010
Tu Trong Ly	70006
Voice Agent	70000
Agent Group	88100

## 9. Conclusion

These Application Notes describe the configuration steps required for the Scantalk ApS TeamView Unified Operator to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

This section references the Avaya and Scantalk product documentation that are relevant to these Application Notes.

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

1. *Administering Avaya Aura® Communication Manager, Release 8, Issue 2.0, Nov 2018*
2. *Administering Avaya Aura® Session Manager, Release 8, Issue 2, August 2018*
3. *Administering Avaya Aura® System Manager, Release 8, Issue 4, September 2018*
4. *Administering Avaya Aura® Application Enablement Services, Release 8.0.1, Issue 2, December 2018*

Product Documentation for TeamView - Unified Operator can be requested from Scantalk ApS found at <http://www.scantalk.com>.

5. *Unified Operator – TeamView – Unified Operator - install and Configuration*
6. *AD LookUp – TeamView – AD LookUp – Installation and Configuration*
7. *General – TeamView – Unified Operator – Prerequisites*

---

**©2019 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](mailto:devconnect@avaya.com).