DevConnect Program

Application Notes for Xima Chronicall 4.4 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Xima Chronicall 4.4 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1.

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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required for Xima Chronicall 4.4 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1.

In the compliance testing, Chronicall used the System Management Services (SMS) and Java Telephony Application Programming Interface (JTAPI) from Application Enablement Services to provide real-time agent status monitoring and cradle to grave reporting.

The SMS interface is used by Chronicall to obtain configured call center resources on Communication Manager via Application Enablement Services to facilitate configuration of Chronicall.

The JTAPI interface is used by Chronicall to monitor VDNs, skills, agent and supervisor stations. The received JTAPI events are used to provide real-time agent status monitoring and cradle to grave reporting.

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Chronicall, the application automatically sent SMS requests to obtain configured agents, skill groups, stations, uniform dial plan, VDNs, vectors, and sent JTAPI/TSAPI requests to monitor VDNs, skills, agent and supervisor stations.

For the manual part of the testing, calls were made from the PSTN and from internal users. Necessary actions such as hold/reconnect were performed from the agent telephones to generate events for the various call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the Chronicall server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and Chronicall did not include use of any specific encryption features as requested by Xima.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Chronicall:

- Use of SMS to obtain configuration data associated with the following SMS objects: Agent, Hunt Group, Station, Uniform Dial Plan, VDN, and Vector.

- Use of JTAPI/TSAPI in areas of event notifications and value queries.

- Handling of JTAPI/TSAPI events for proper reflection of activities in agent timeline and cradle to grave reporting for various call scenarios including internal, external, inbound, outbound, drop, hold/resume, transfer, conference, voicemail coverage, voicemail retrieval, queuing, service observing, long duration, simultaneous agents, simultaneous calls, and abandon calls.

The serviceability testing focused on verifying the ability of Chronicall to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to the Chronicall server.

2.2. Test Results

All test cases were executed. All test cases were executed, and the following were observations on Chronicall:

- By design, all VDNs obtained from the SMS connection are monitored by Chronicall.
- This release of Chronicall does not provide full agent timeline reflection and cradle to grave report support for service observing scenarios.
- For blind conference scenarios, one of the three reported cradle to grave entries contained the conference-to agent as both the calling and receiving party.
- By design, when an agent has two calls at the telephone, the agent timeline reflects the status of the call that the user is active on.
- A call that was abandoned by the calling party while waiting in queue was reported with Receiving Drop in cradle to grave.
- A call that covered to voicemail was not reflected with Voicemail in agent timeline and cradle to grave.
- A call that traversed through two VDNs and vectors only reflected one vector in cradle to grave.
- After a busy out and release of CTI link commands on Communication Manager, active device monitors were removed on Communication Manager and Application Enablement Services and were not re-established by Chronicall. The workaround for this release of Chronicall is for the administrator to manually restart the Chronicall Server service.
- When the Chronicall server experienced a 60 seconds Ethernet disruption, the first new call post recovery was not reflected in agent timeline but was reflected in cradle to grave without agent information. Subsequent calls were reflected in both agent timeline and cradle to grave.

2.3. Support

Technical support on Chronicall can be obtained through the following:

- **Phone:** (888) 944-XIMA
- **Email:** support@ximasoftware.com
- **Web:** http://www.ximasoftware.com/support

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, Session Manager, and of call center devices are not the focus of these Application Notes and will not be described. The call center devices used in the compliance testing are shown in the table below.

Device Type	Extension
VDN	60001-2
Skill Group	61001-2
Supervisor Station	65000 (H.323)
Agent Station	65001-2 (H.323), 66002 & 66006 (SIP)
Agent ID	65881-4

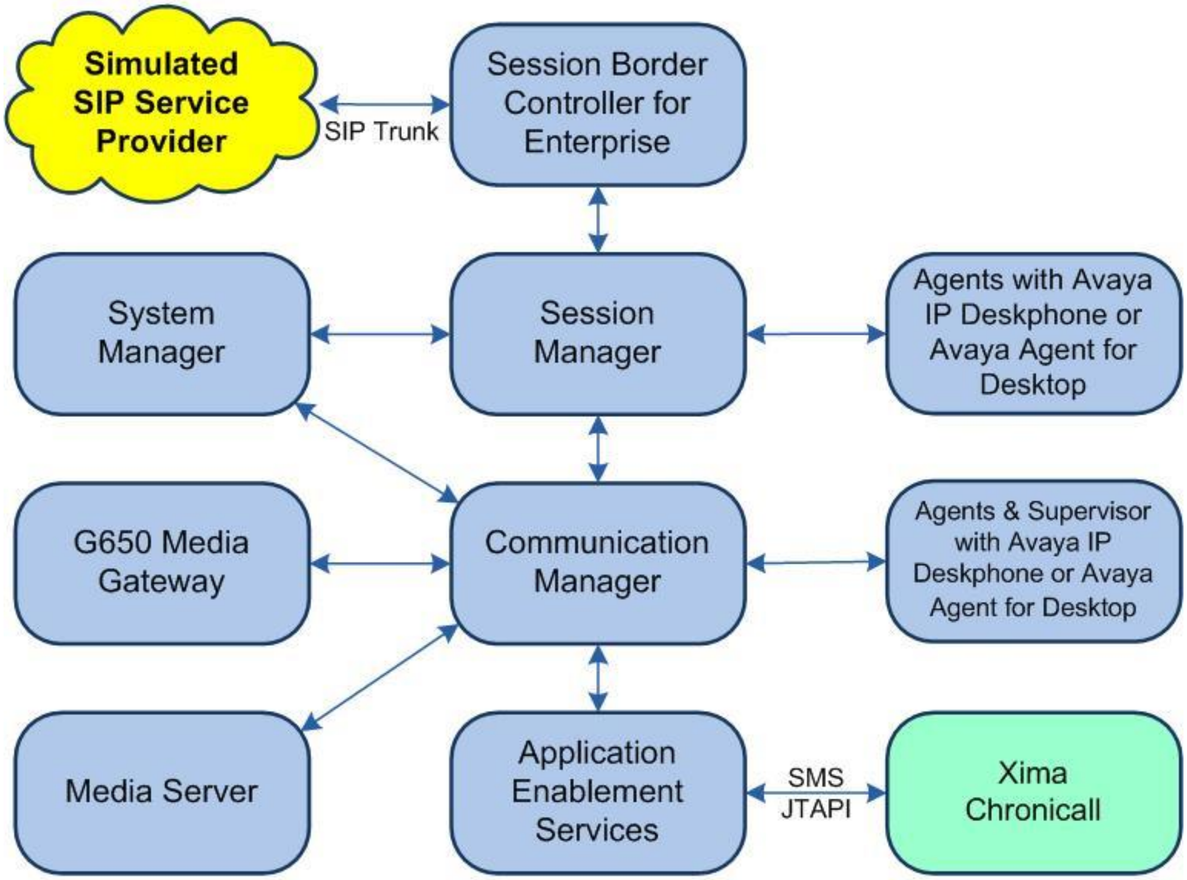

Simulated SIP Service Provider
SIP Trunk
Session Border Controller for Enterprise
System Manager
Session Manager
Agents with Avaya IP Deskphone or Avaya Agent for Desktop
G650 Media Gateway
Communication Manager
Agents & Supervisor with Avaya IP Deskphone or Avaya Agent for Desktop
Media Server
Application Enablement Services
SMS
JTAPI
Xima Chronicall

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	10.1.3 (10.1.3.0.1.974.27893)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	Virtual Environment 10.1 (10.1.0.154)
Avaya Aura® Application Enablement Services in Virtual Environment	10.1.3 (10.1.3.0.0.11-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.3 (10.1.3.0.1013007)
Avaya Aura® System Manager in Virtual Environment	10.1.3 (10.1.3.0.0715713)
Avaya Session Border Controller in Virtual Environment	10.1 (10.1.2.0-64-23285)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G IP Deskphone (H.323)	6.8.5.3.2
Avaya J169 IP Deskphone (SIP)	4.0.13.0.6
Xima Chronicall on Windows Server 2019 • Avaya JTAPI Windows Client (ecsjtapia.jar)	4.4 Standard 6.3.3.26
Xima Chronicall Desktop on Windows 10 Pro	4.4

5. Configure Avaya Aura® Communication Manager (for example)

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

- Verify license
- Administer CTI link
- Obtain reason codes
- Administer accounts

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  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      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
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? Y
```

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: 60111
     Type: ADJ-IP
                                                                     COR: 1
     Name: AES CTI Link
Unicode Name? n
```

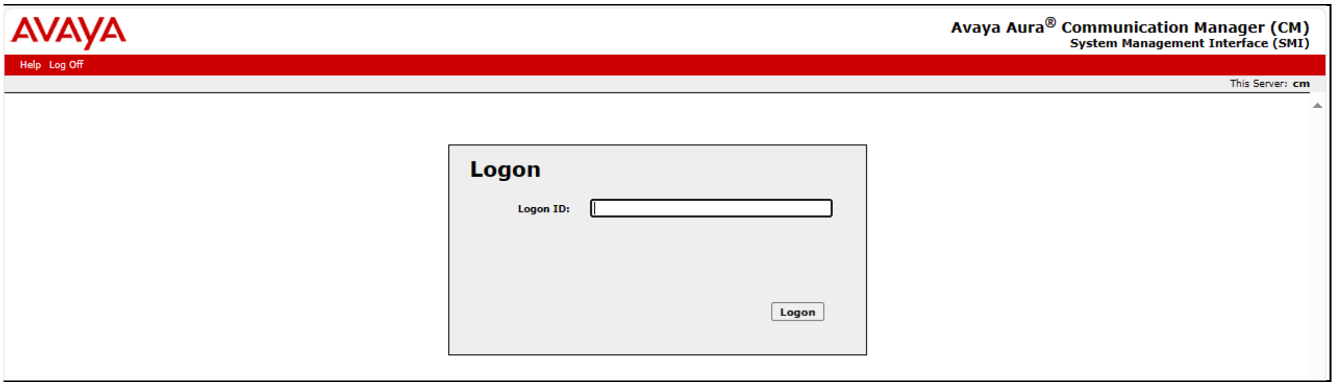
5.3. Obtain Reason Codes

For call centers that use reason codes for aux work mode, enter the “display reason-code-names” command to display the configured reason codes. Make a note of the reason codes for aux work, which will be used later to configure Chronicall.

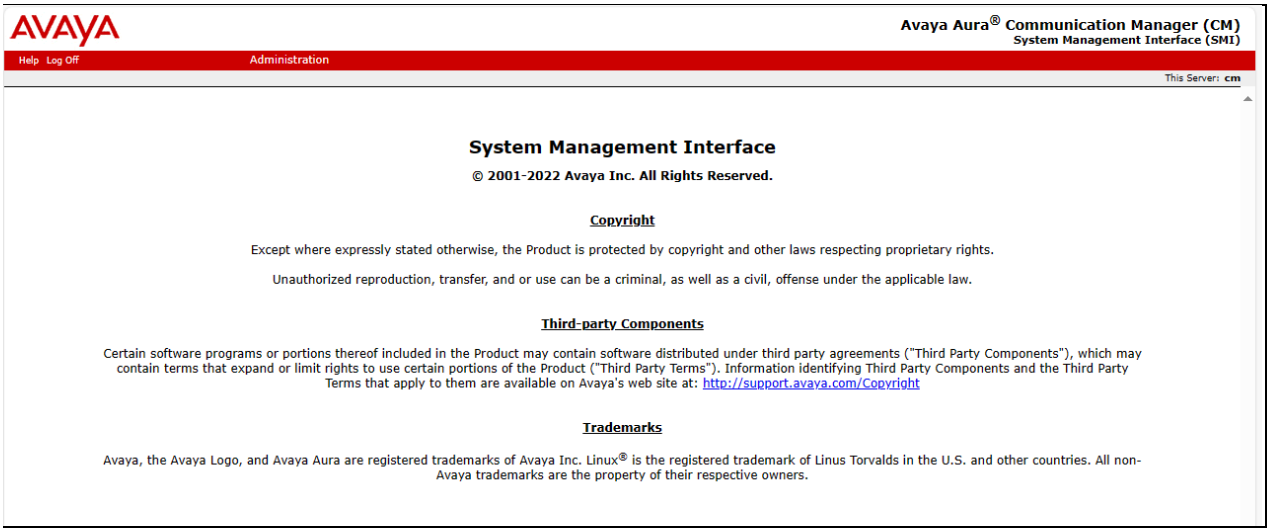
```
display reason-code-names                                       Page   1 of   1

                                REASON CODE NAMES

                           Aux Work/            Logout
                        Interruptible?

        Reason Code 1: Meeting         /n
        Reason Code 2: Lunch           /n
        Reason Code 3: Break           /n
        Reason Code 4: Sleep           /n
        Reason Code 5:                 /n
        Reason Code 6:                 /n
        Reason Code 7:                 /n  Other
        Reason Code 8:                 /n
        Reason Code 9:                 /n

  Default Reason Code:
```

5.4. Administer Accounts

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


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: cm
Logon
Logon ID:
Logon

The **System Management Interface** screen is displayed next. Select **Administration → Server (Maintenance)** from the top menu.



AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
Administration
This Server: cm

System Management Interface

© 2001-2022 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

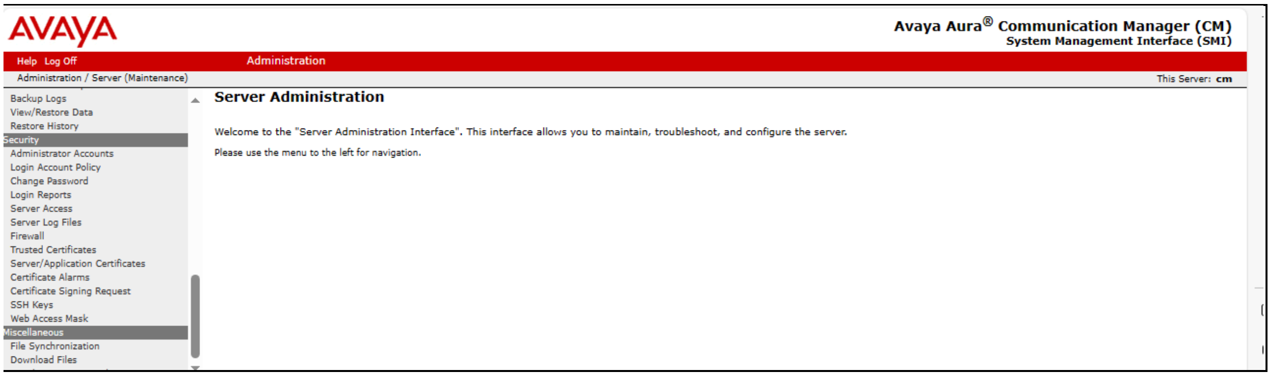
Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/Copyright

Trademarks

Avaya, the Avaya Logo, and Avaya Aura are registered trademarks of Avaya Inc. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All non-Avaya trademarks are the property of their respective owners.

The **Server Administration** screen is displayed. Scroll the left pane as necessary and select **Security → Administrator Accounts**.

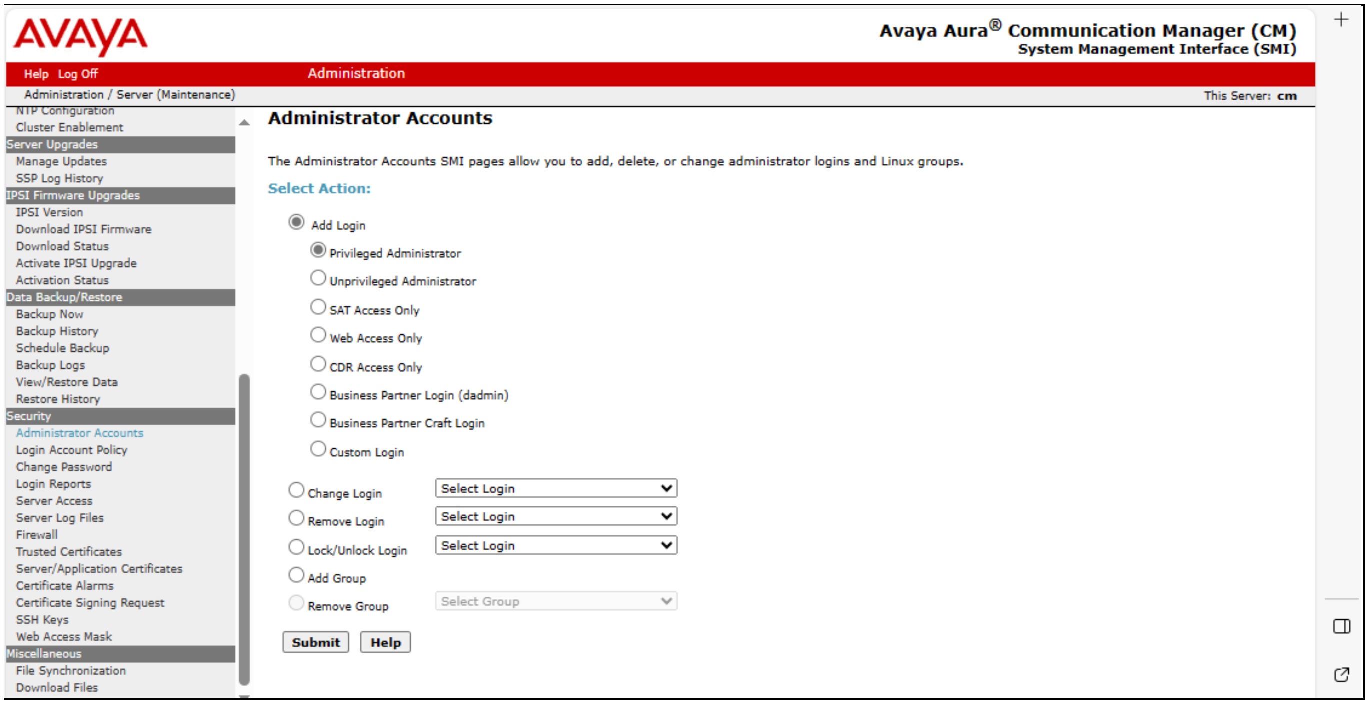


Server Administration

Welcome to the "Server Administration Interface". This interface allows you to maintain, troubleshoot, and configure the server.

Please use the menu to the left for navigation.

The **Administrator Accounts** screen is displayed next. Select **Add Login** and **Privileged Administrator**, as shown below.



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

● Add Login

  ● Privileged Administrator

  ○ Unprivileged Administrator

  ○ SAT Access Only

  ○ Web Access Only

  ○ CDR Access Only

  ○ Business Partner Login (dadmin)

  ○ Business Partner Craft Login

  ○ Custom Login

○ Change Login Select Login

○ Remove Login Select Login

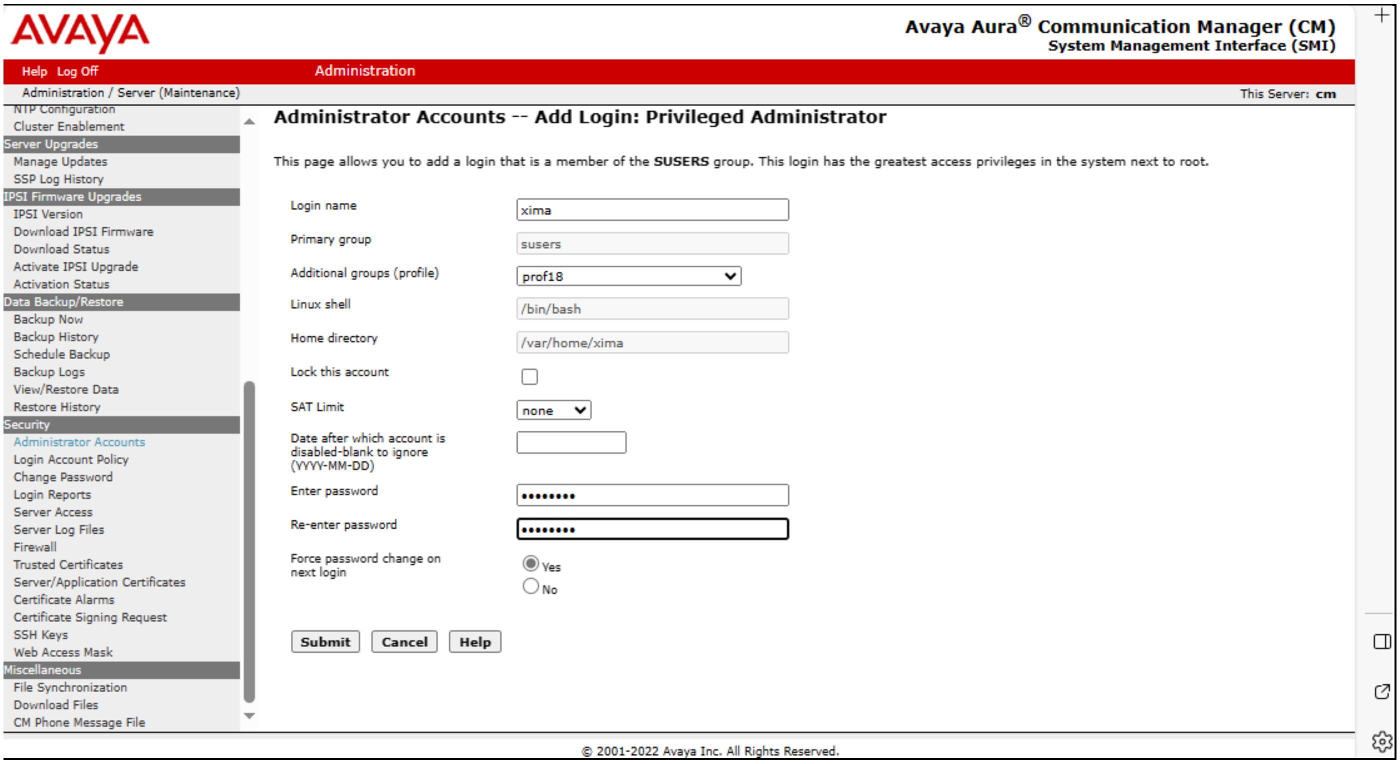
○ Lock/Unlock Login Select Login

○ Add Group

○ Remove Group Select Group

The **Administrator Accounts** screen is updated. Enter the desired credentials for **Login name**, **Enter password**, and **Re-enter password**. Retain the default values in the remaining fields.

Make a note of the account credentials, which will be used later to configure Chronicall.



Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	xima
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/xima
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	••••••••
Re-enter password	••••••••
Force password change on next login	● Yes ○ No

.

6. Configure Avaya Aura® Application Enablement Services

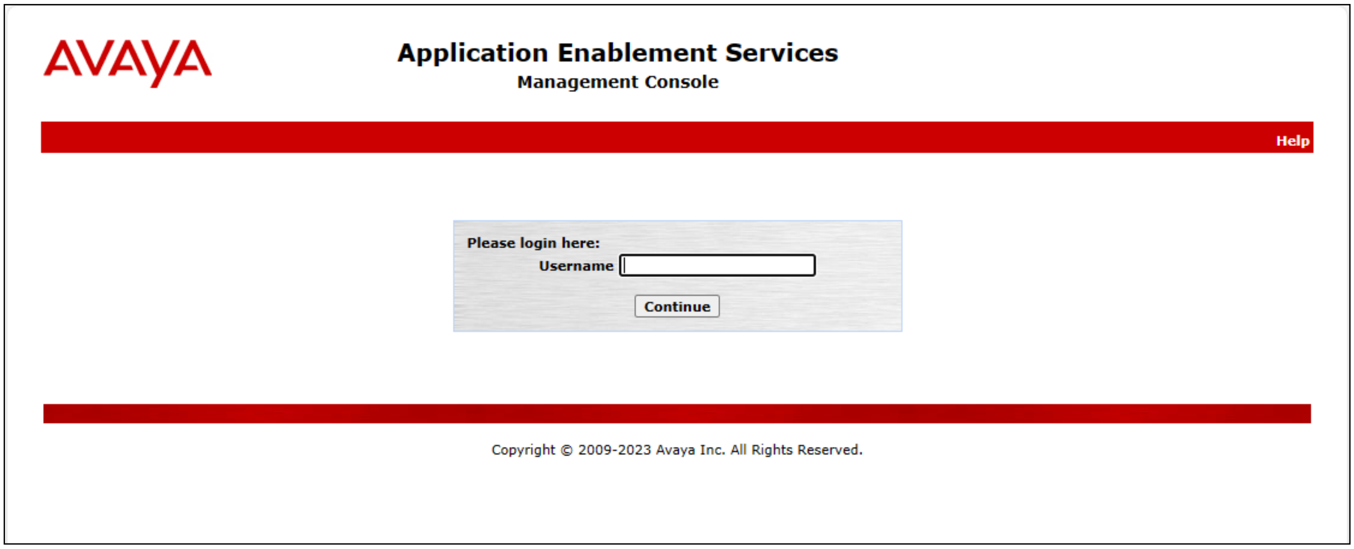
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Chronicall user
- Administer security database
- Restart TSAPI service
- Obtain Tlink name
- Administer ports
- Administer SMS properties

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 screen below is displayed. Log in using the appropriate credentials.



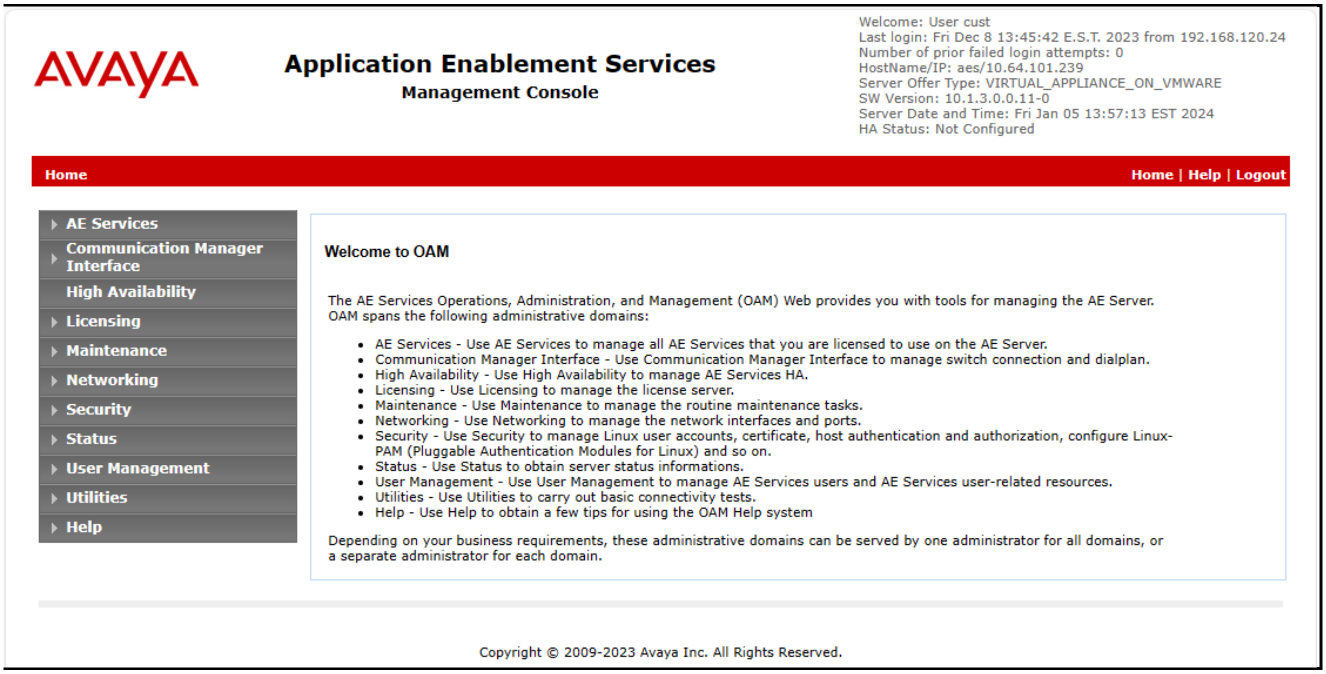
Application Enablement Services

Management Console

Please login here:

Username

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



AVAYA **Application Enablement Services** Management Console

Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 13:57:13 EST 2024
HA Status: Not Configured

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:

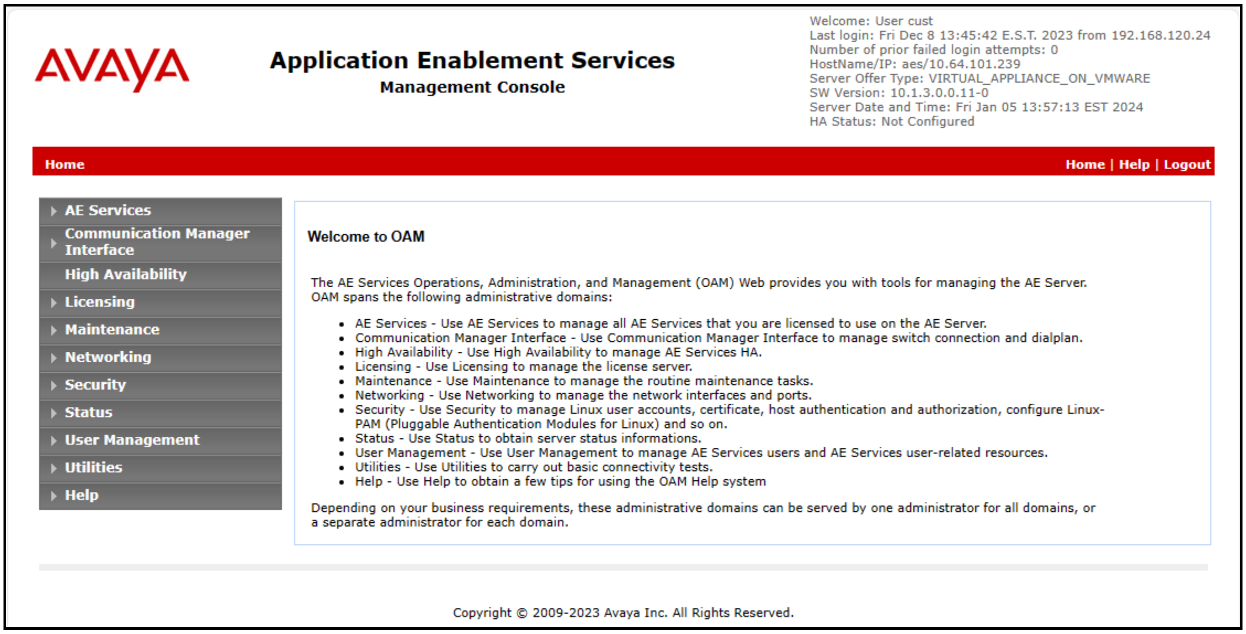
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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 © 2009-2023 Avaya Inc. All Rights Reserved.

6.2. Verify License

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



AVAYA **Application Enablement Services** Management Console

Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 13:57:13 EST 2024
HA Status: Not Configured

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:

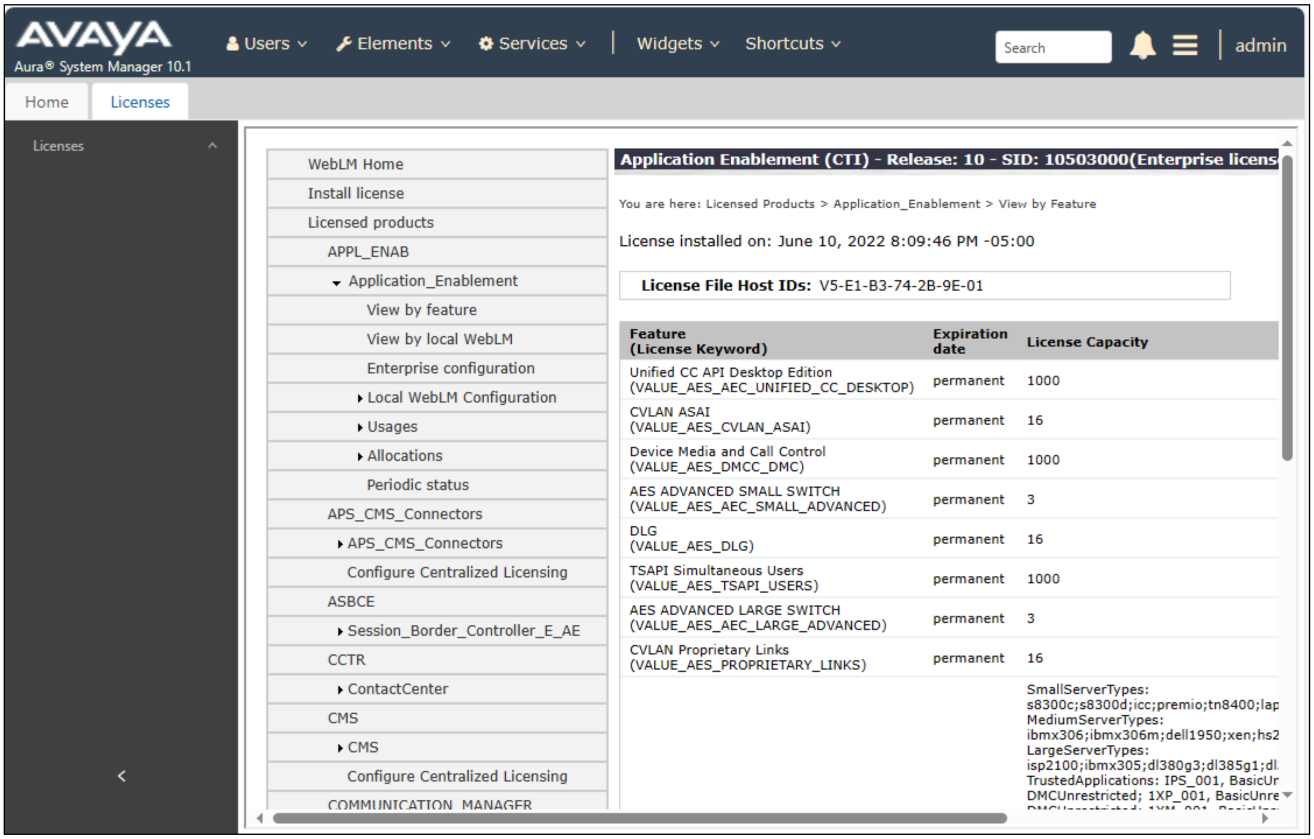
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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 © 2009-2023 Avaya Inc. All Rights Reserved.

Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.



Application Enablement (CTI) - Release: 10 - SID: 10503000(Enterprise licens

You are here: Licensed Products > Application_Enablement > View by Feature

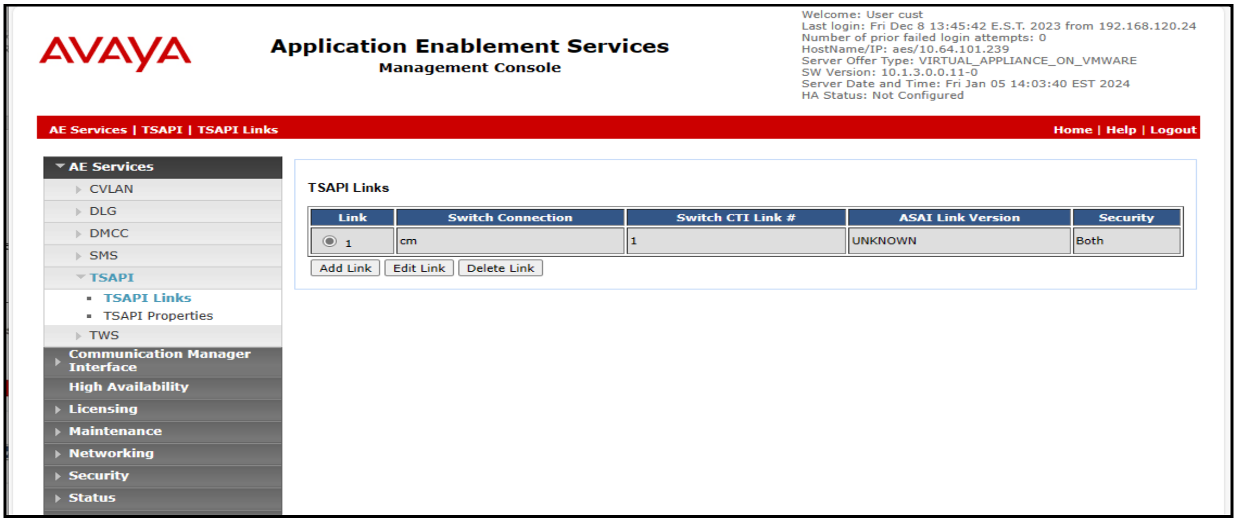
License installed on: June 10, 2022 8:09:46 PM -05:00

License File Host IDs: V5-E1-B3-74-2B-9E-01

Feature (License Keyword)	Expiration date	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3
DLG (VALUE_AES_DLG)	permanent	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16
		SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;lap MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs2 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl TrustedApplications: IPS_001, BasicUr DMCUnrestricted; 1XP_001, BasicUnre

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**.



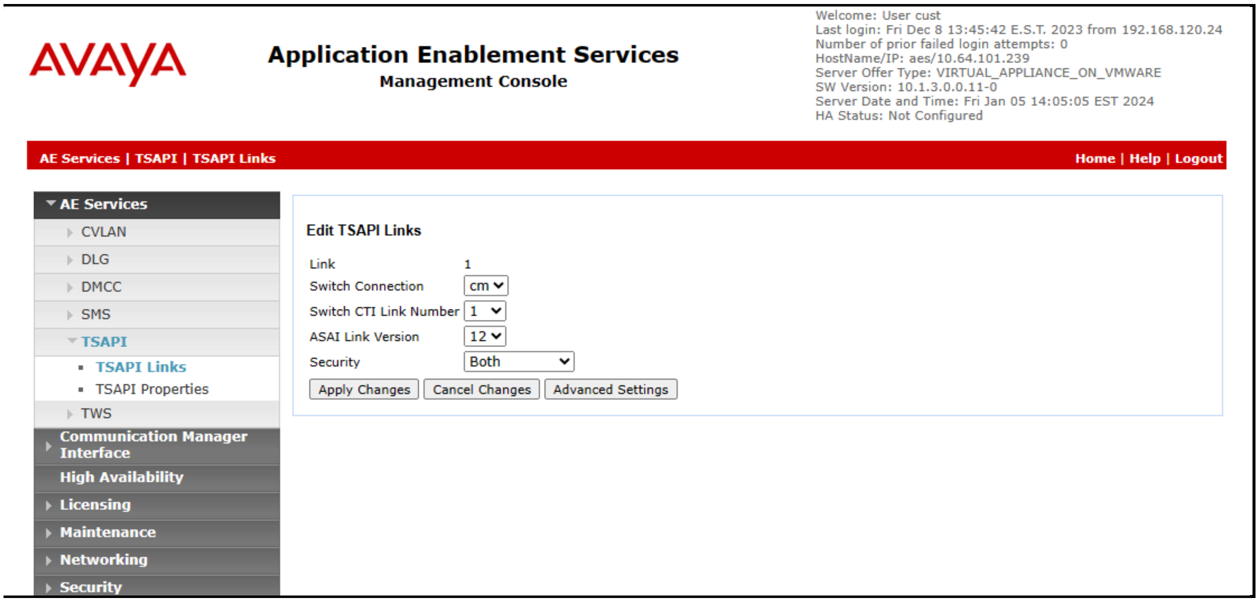
Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:03:40 EST 2024
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm	1	UNKNOWN	Both

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 “cm” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 0**. Retain the default values in the remaining fields.



Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:05:05 EST 2024
HA Status: Not Configured

Edit TSAPI Links

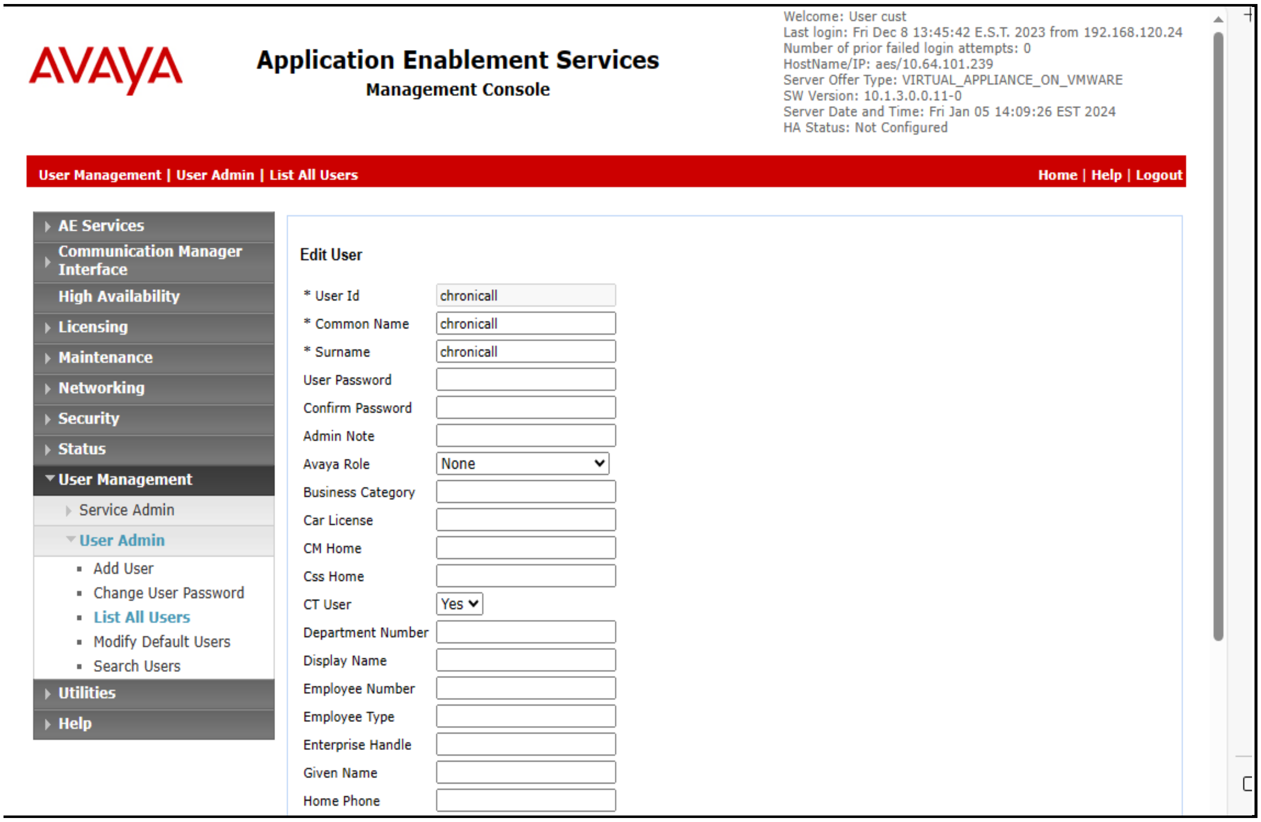
Link	1
Switch Connection	cm
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

6.4. Administer Chronicall 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.

Make a note of the user credentials, which will be used later to configure Chronicall.



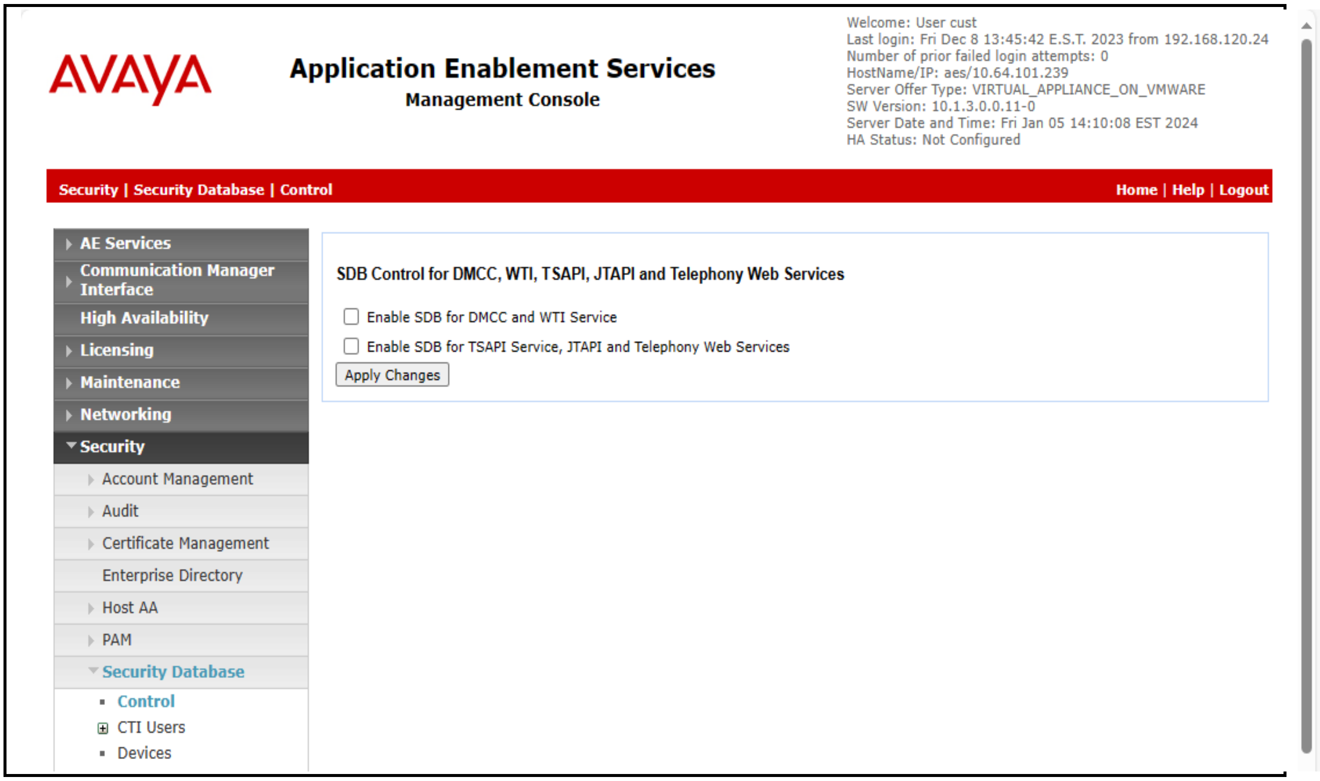
Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:09:26 EST 2024
HA Status: Not Configured

Edit User

* User Id	chronicall
* Common Name	chronicall
* Surname	chronicall
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	

6.5. 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. Make certain both parameters are unchecked, as shown below.



Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:10:08 EST 2024
HA Status: Not Configured

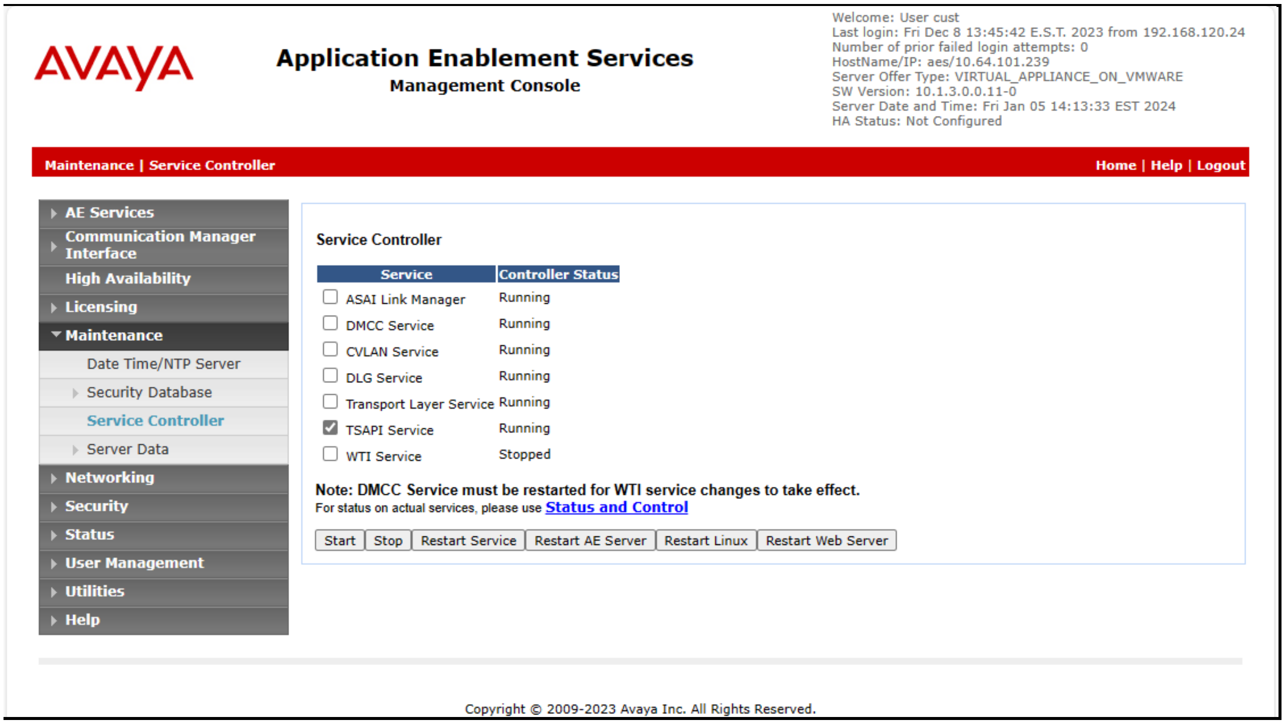
SDB Control for DMCC, WTI, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC and WTI Service

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

6.6. Restart TSAPI Service

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**.



Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:13:33 EST 2024
HA Status: Not Configured

Service Controller

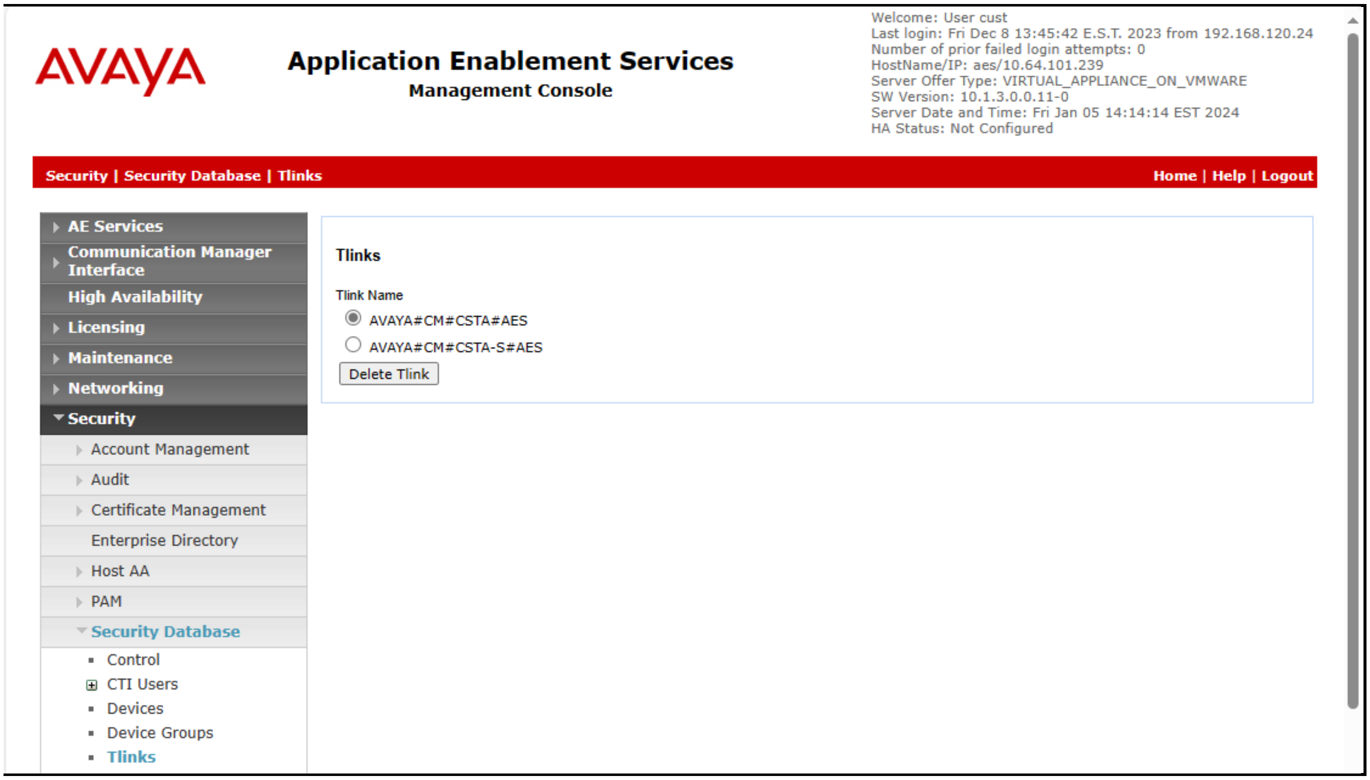
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running
□ WTI Service	Stopped

Note: DMCC Service must be restarted for WTI service changes to take effect.
For status on actual services, please use Status and Control

6.7. 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 Chronicall.

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



Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:14:14 EST 2024
HA Status: Not Configured

Tlinks

Tlink Name

● AVAYA#CM#CSTA#AES

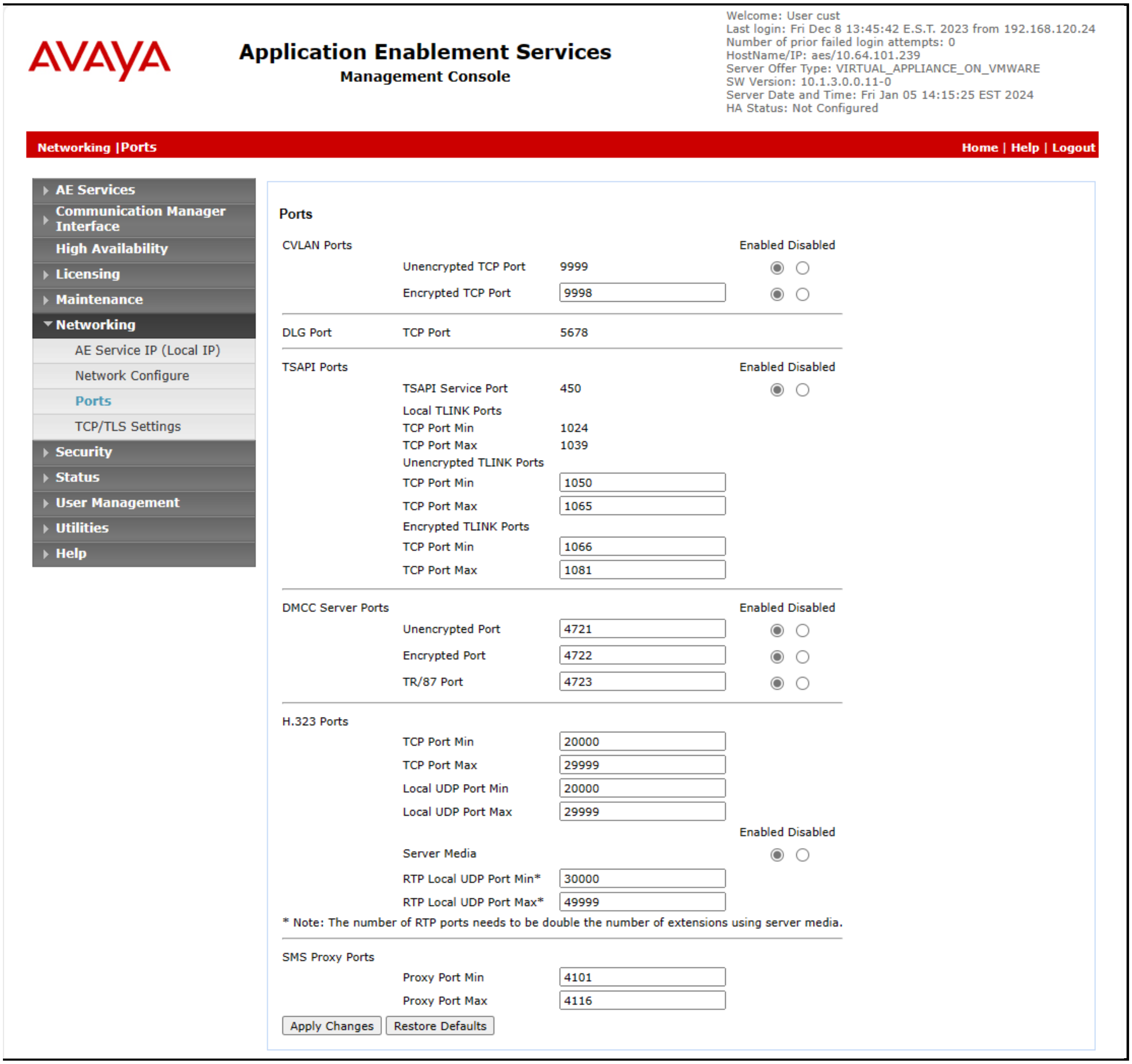
○ AVAYA#CM#CSTA-S#AES

Delete Tlink

6.8. Administer Ports

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

Scroll down to the **SMS Proxy Ports** sub-section and set **Proxy Port Min** and **Proxy Port Max** to the desired values. Note that SMS can use up to 16 ports, and the compliance testing used the default ports "4101-4116" as shown below.



Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:15:25 EST 2024
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	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			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○
H.323 Ports				
	TCP Port Min	20000		
	TCP Port Max	29999		
	Local UDP Port Min	20000		
	Local UDP Port Max	29999		
			Enabled	Disabled
	Server Media		●	○
	RTP Local UDP Port Min*	30000		
	RTP Local UDP Port Max*	49999		

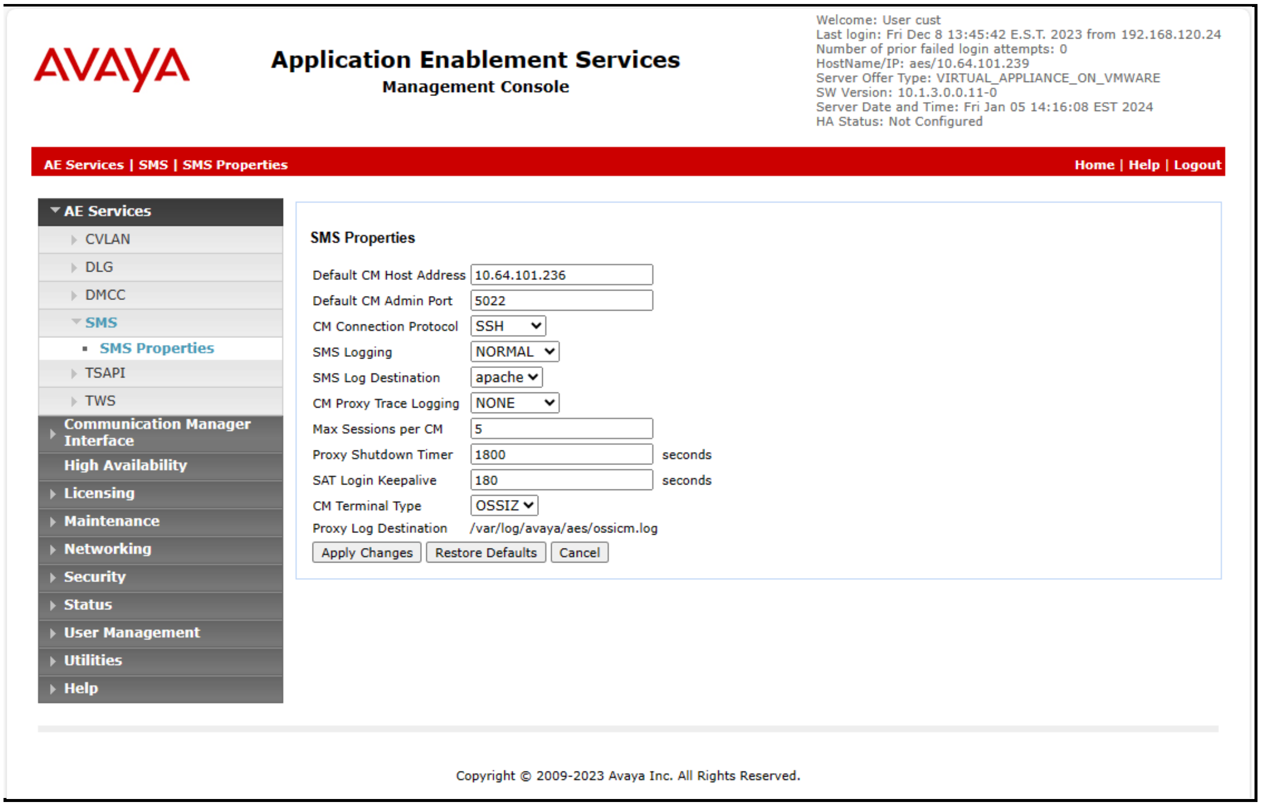
* Note: The number of RTP ports needs to be double the number of extensions using server media.

SMS Proxy Ports		
	Proxy Port Min	4101
	Proxy Port Max	4116

6.9. Administer SMS Properties

Select **AE Services** → **SMS** → **SMS Properties** from the left pane, to display the **SMS Properties** screen in the right pane.

For **Default CM Host Address**, enter the IP address of Communication Manager, in this case "10.64.101.236". Retain the default values for the remaining fields.



Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:16:08 EST 2024
HA Status: Not Configured

SMS Properties

Default CM Host Address	10.64.101.236
Default CM Admin Port	5022
CM Connection Protocol	SSH
SMS Logging	NORMAL
SMS Log Destination	apache
CM Proxy Trace Logging	NONE
Max Sessions per CM	5
Proxy Shutdown Timer	1800 seconds
SAT Login Keepalive	180 seconds
CM Terminal Type	OSSIZ
Proxy Log Destination	/var/log/avaya/aes/ossicm.log

Copyright © 2009-2023 Avaya Inc. All Rights Reserved.

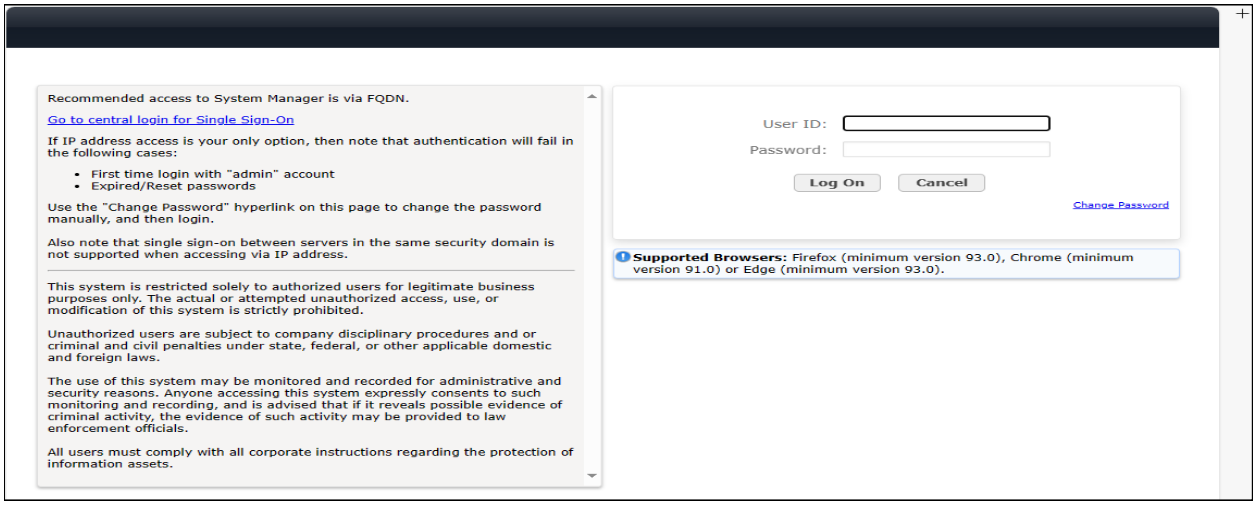
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

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



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

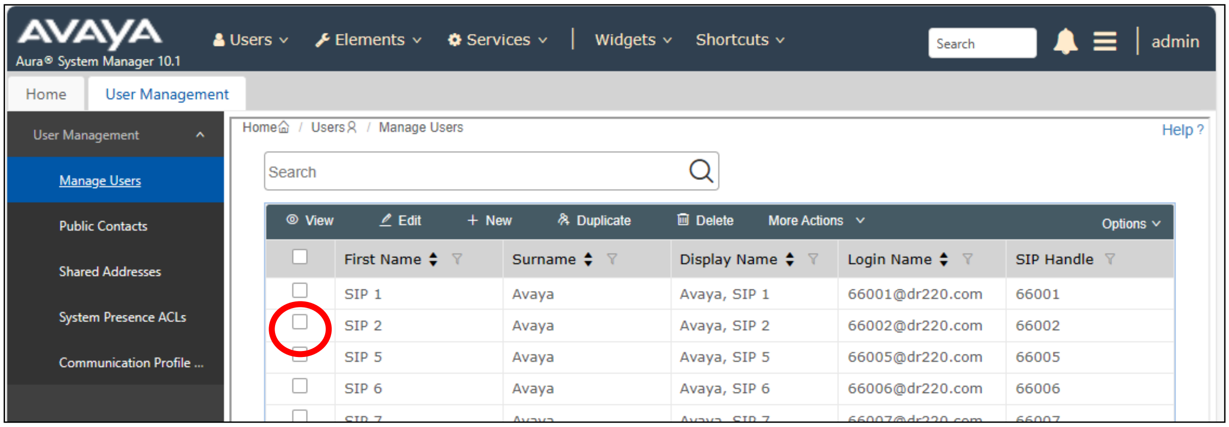
All users must comply with all corporate instructions regarding the protection of information assets.

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

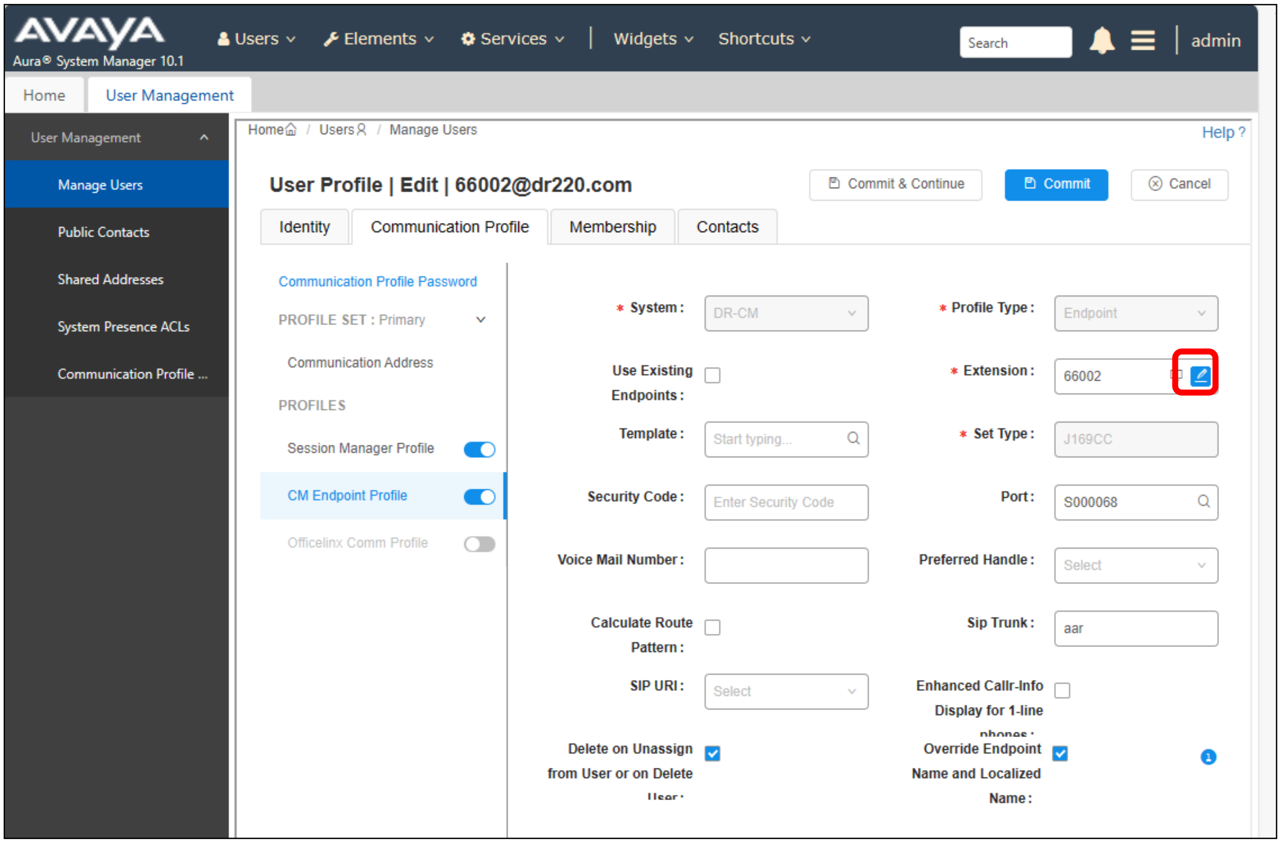
Select the entry associated with the first SIP agent station from **Section** Error! Reference source not found., in this case “66002”, and click **Edit**.



□	First Name	Surname	Display Name	Login Name	SIP Handle
□	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001
□	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
□	SIP 5	Avaya	Avaya, SIP 5	66005@dr220.com	66005
□	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006
□	SIP 7	Avaya	Avaya, SIP 7	66007@dr220.com	66007

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

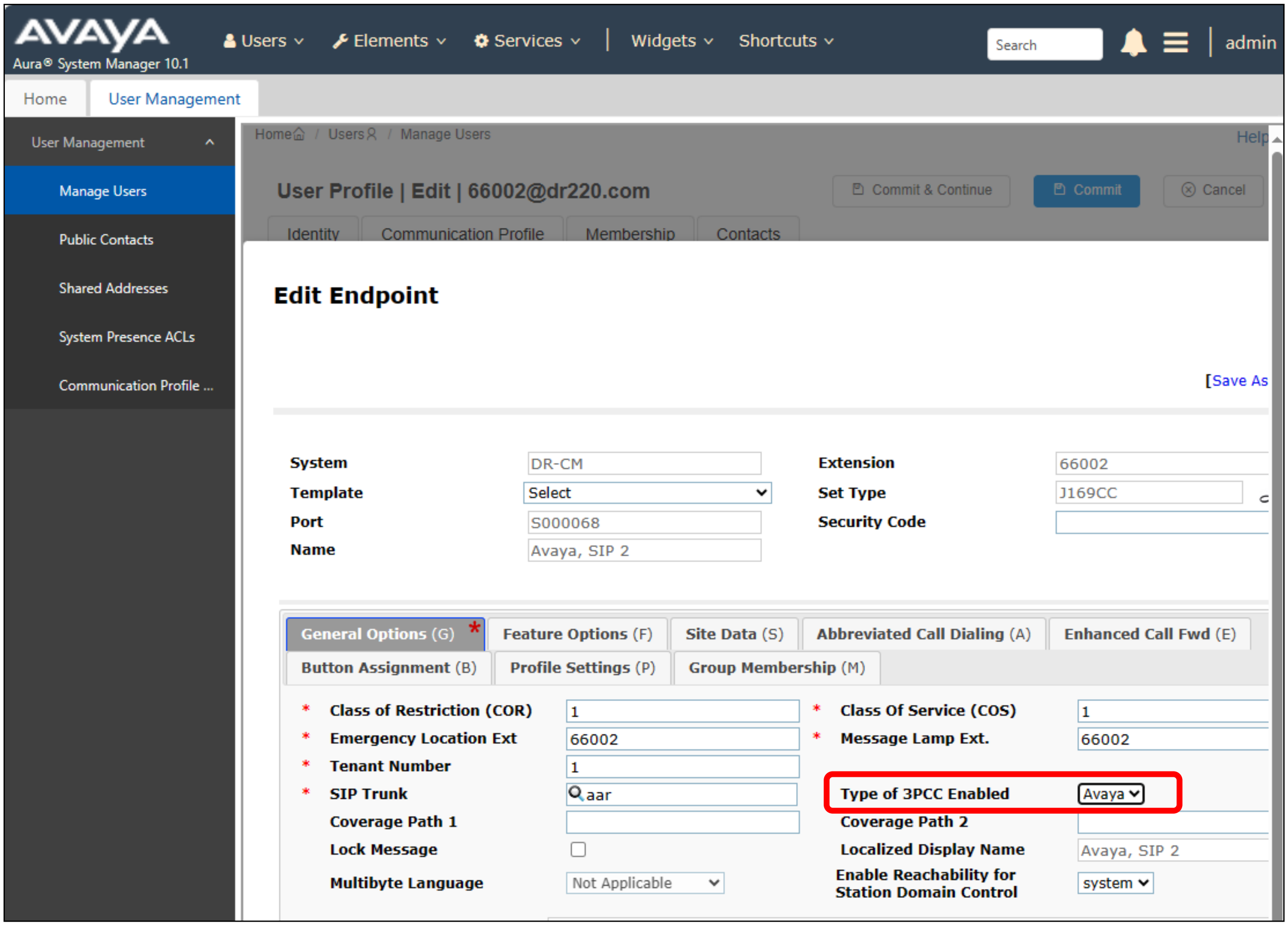


User Profile | Edit | 66002@dr220.com

* System :	DR-CM	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	66002
Template :	Start typing...	* Set Type :	J169CC
Security Code :	Enter Security Code	Port :	S000068
Voice Mail Number :		Preferred Handle :	Select
Calculate Route Pattern :	□	Sip Trunk :	aar
SIP URI :	Select	Enhanced Callr-Info Display for 1-line phones :	□
Delete on Unassign from User or on Delete User :	☑	Override Endpoint Name and Localized Name :	☑

The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select "Avaya" as shown below.

Repeat this section for all SIP agent users from **Section** Error! Reference source not found.. In t he compliance testing, two SIP agent users 66002 and 66006 were configured.



User Profile | Edit | 66002@dr220.com

Edit Endpoint

System	DR-CM	Extension	66002
Template	Select	Set Type	J169CC
Port	S000068	Security Code	
Name	Avaya, SIP 2		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 2
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

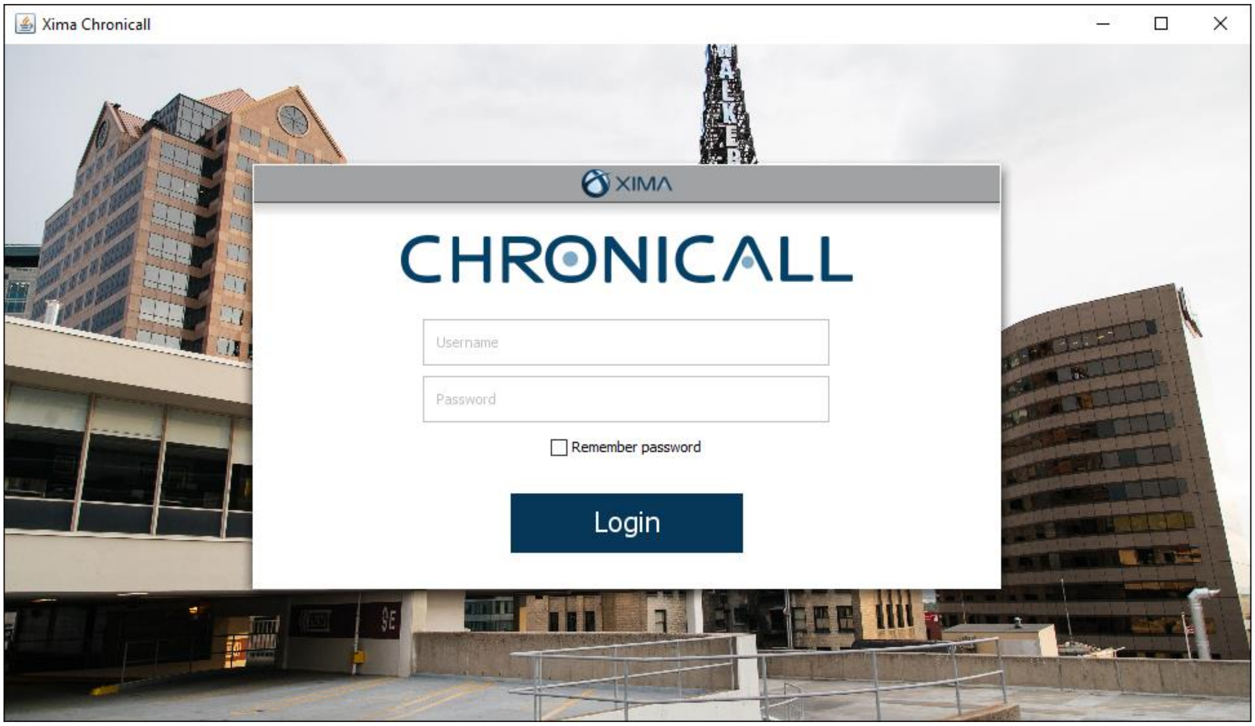
8. Configure Xima Chronicall

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

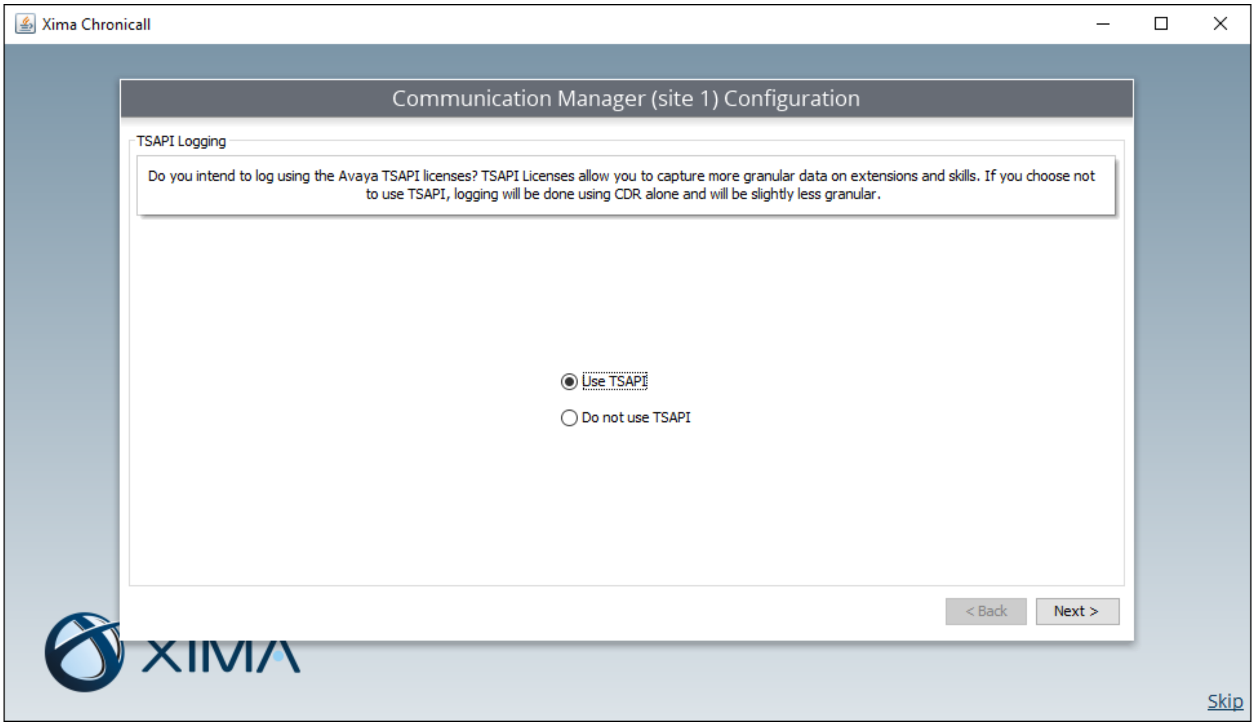
- Launch Chronicall Desktop
- Administer SMS settings
- Administer TSAPI settings
- Administer seat assignment
- Administer license assignments
- Administer voicemail group
- Administer reason codes
- Administer realtime seat assignment
- Administer dashboards seat assignment

8.1. Launch Chronicall Desktop

From a PC where Chronicall Desktop is installed, select **Start → Xima Software → Chronicall Desktop** to launch the client application, and sign in with the appropriate credentials.



Upon initial access post installation, the following **TSAPI Logging** screen from the setup wizard is displayed. Select **Use TSAPI**.



Do you intend to log using the Avaya TSAPI licenses? TSAPI Licenses allow you to capture more granular data on extensions and skills. If you choose not to use TSAPI, logging will be done using CDR alone and will be slightly less granular.

● Use TSAPI

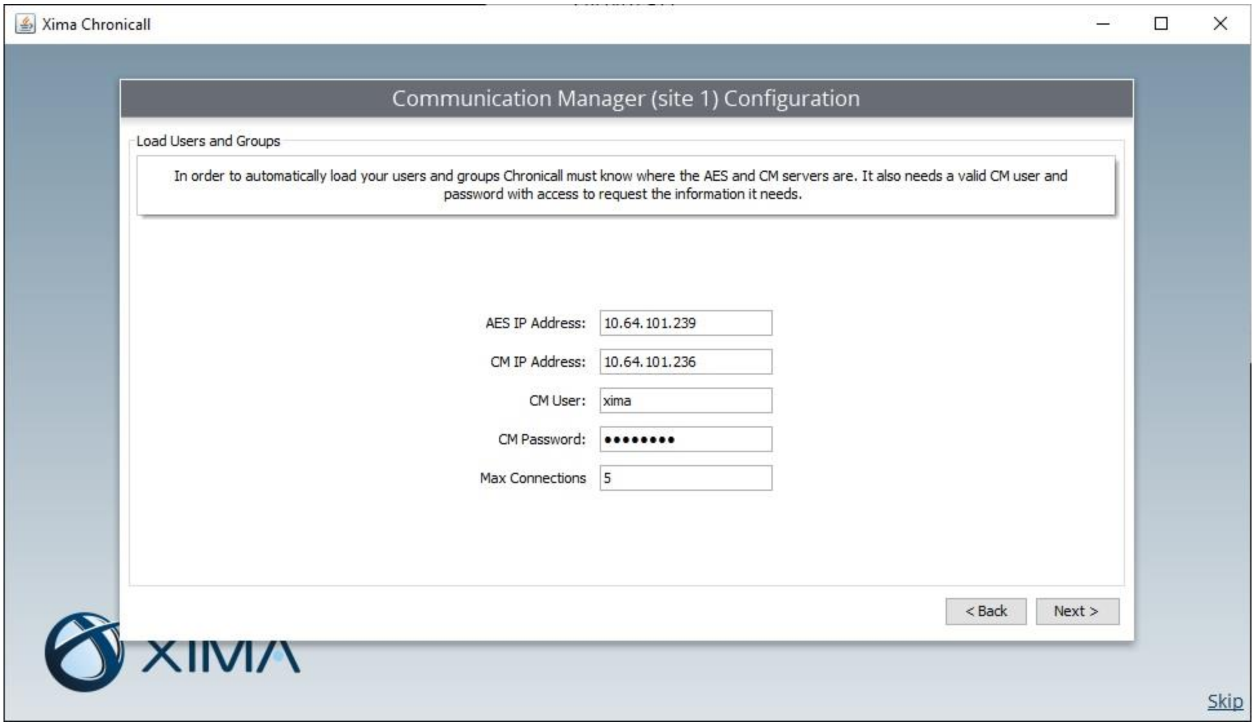
○ Do not use TSAPI

8.2. Administer SMS Settings

The **Load Users and Groups** screen is displayed next. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **AES IP Address:** The IP address of Application Enablement Services.
- **CM IP Address:** The IP address of Communication Manager.
- **CM User:** The Communication Manager account login name from **Section 0**.
- **CM Password:** The Communication Manager account password from **Section 0**.

After configuring the parameters and clicking **Next**, Chronicall automatically tests the SMS connection to Application Enablement Services and obtains configured resources on Communication Manager.



Communication Manager (site 1) Configuration

Load Users and Groups

In order to automatically load your users and groups Chronicall must know where the AES and CM servers are. It also needs a valid CM user and password with access to request the information it needs.

AES IP Address: 10.64.101.239

CM IP Address: 10.64.101.236

CM User: xima

CM Password: ••••••••

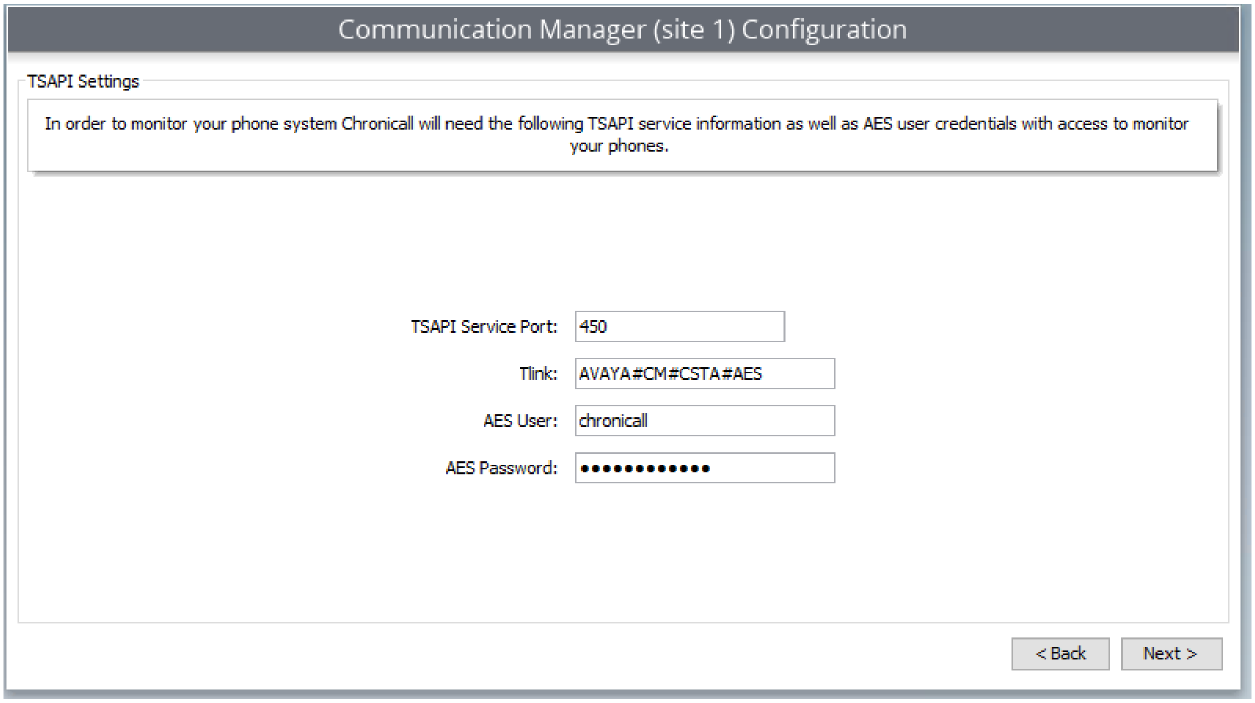
Max Connections 5

8.3. Administer TSAPI Settings

The **TSAPI Settings** screen is displayed next. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Tlink:** The Tlink name from **Section 6.7**.
- **AES User:** The Chronicall user credentials from **Section 6.4**.
- **AES Password:** The Chronicall user credentials from **Section 6.4**.

After configuring the parameters and clicking **Next**, Chronicall automatically tests the JTAPI/TSAPI connection to Application Enablement Services.



Communication Manager (site 1) Configuration

TSAPI Settings

In order to monitor your phone system Chronicall will need the following TSAPI service information as well as AES user credentials with access to monitor your phones.

TSAPI Service Port: 450

Tlink: AVAYA#CM#CSTA#AES

AES User: chronicall

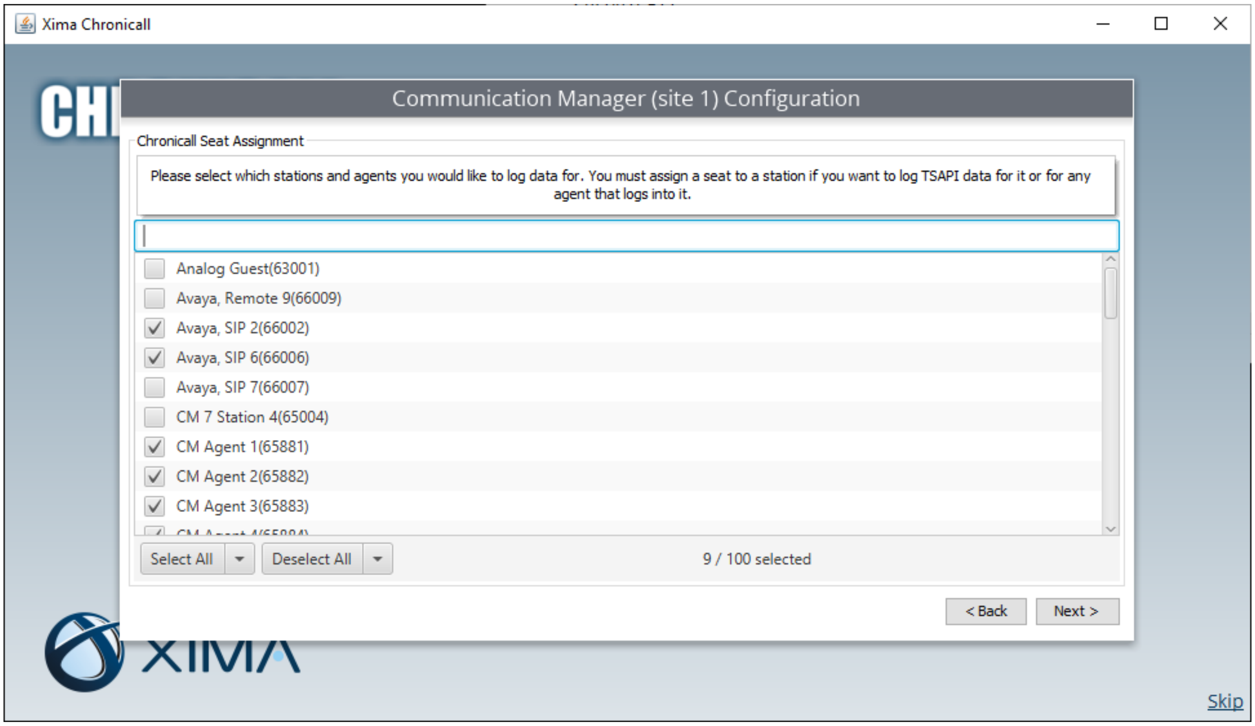
AES Password: ●●●●●●●●●●●●

8.4. Administer Seat Assignment

The **Chronicall Seat Assignment** screen is displayed next, showing a list of stations and agent IDs obtained via the SMS connection to Application Enablement Services.

Scroll the screen as necessary and select all desired stations and agent IDs for Chronicall to log data for.

In the compliance testing, all stations and agent IDs from **Section** Error! Reference source not f ound. were selected, as partially shown below.



Xima Chronicall
Communication Manager (site 1) Configuration
Chronicall Seat Assignment

Please select which stations and agents you would like to log data for. You must assign a seat to a station if you want to log TSAPI data for it or for any agent that logs into it.

- □ Analog Guest(63001)
- □ Avaya, Remote 9(66009)
- ☑ Avaya, SIP 2(66002)
- ☑ Avaya, SIP 6(66006)
- □ Avaya, SIP 7(66007)
- □ CM 7 Station 4(65004)
- ☑ CM Agent 1(65881)
- ☑ CM Agent 2(65882)
- ☑ CM Agent 3(65883)
- ☑ CM Agent 4(65884)

9 / 100 selected

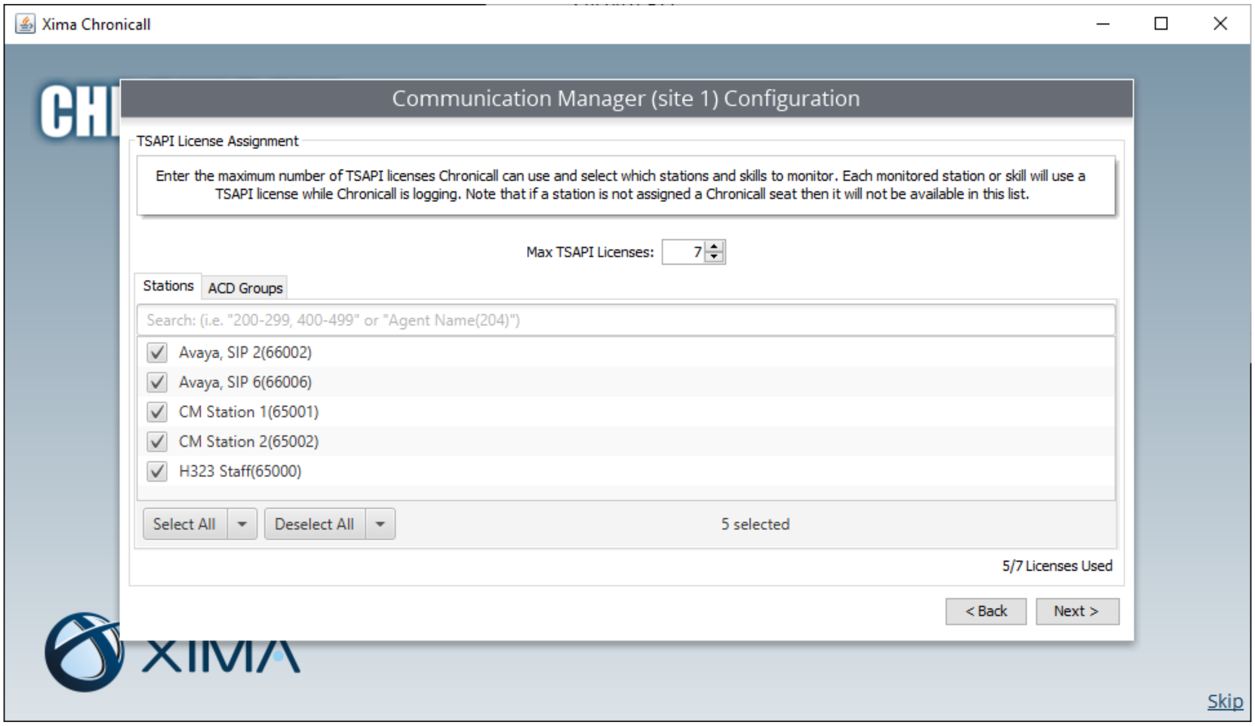
Select All
Deselect All
< Back
Next >
Skip

8.5. Administer License Assignment

The **TSAPI License Assignment** screen is displayed next. For **Max TSAPI Licenses**, select the maximum number of stations and skills to be monitored by Chronicall, in this case “7”.

Select the **Stations** tab to display a list of stations with seat assignments that were configured in **Section 8.4**. Select the desired stations to monitor.

In the compliance testing, all five stations from **Section** Error! Reference source not found. were s elected, as shown below.



Communication Manager (site 1) Configuration

TSAPI License Assignment

Enter the maximum number of TSAPI licenses Chronicall can use and select which stations and skills to monitor. Each monitored station or skill will use a TSAPI license while Chronicall is logging. Note that if a station is not assigned a Chronicall seat then it will not be available in this list.

Max TSAPI Licenses: 7

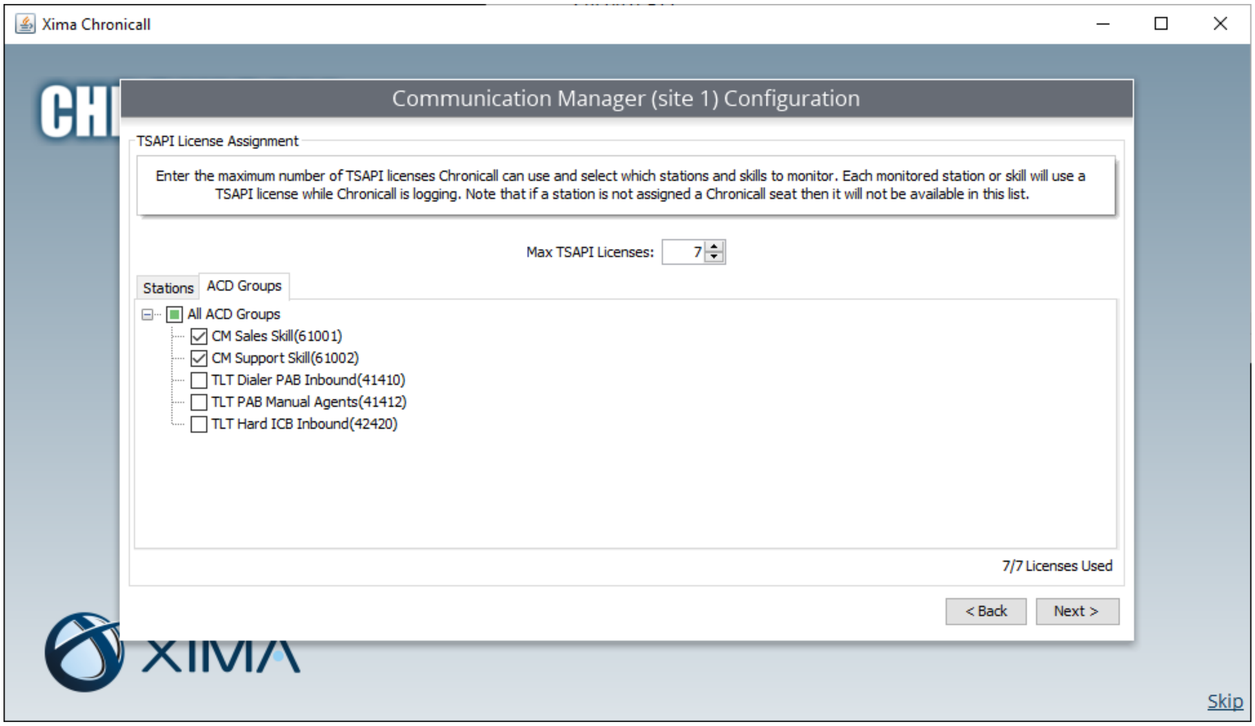
☑ Avaya, SIP 2(66002)
☑ Avaya, SIP 6(66006)
☑ CM Station 1(65001)
☑ CM Station 2(65002)
☑ H323 Staff(65000)

5 selected

5/7 Licenses Used

Select the **ACD Groups** tab to display a list of groups that were obtained from Application Enablement Services via the SMS connection. Select the desired skill groups to monitor.

In the compliance testing, two skill groups from **Section** Error! Reference source not found. were s elected, as shown below.



Enter the maximum number of TSAPI licenses Chronicall can use and select which stations and skills to monitor. Each monitored station or skill will use a TSAPI license while Chronicall is logging. Note that if a station is not assigned a Chronicall seat then it will not be available in this list.

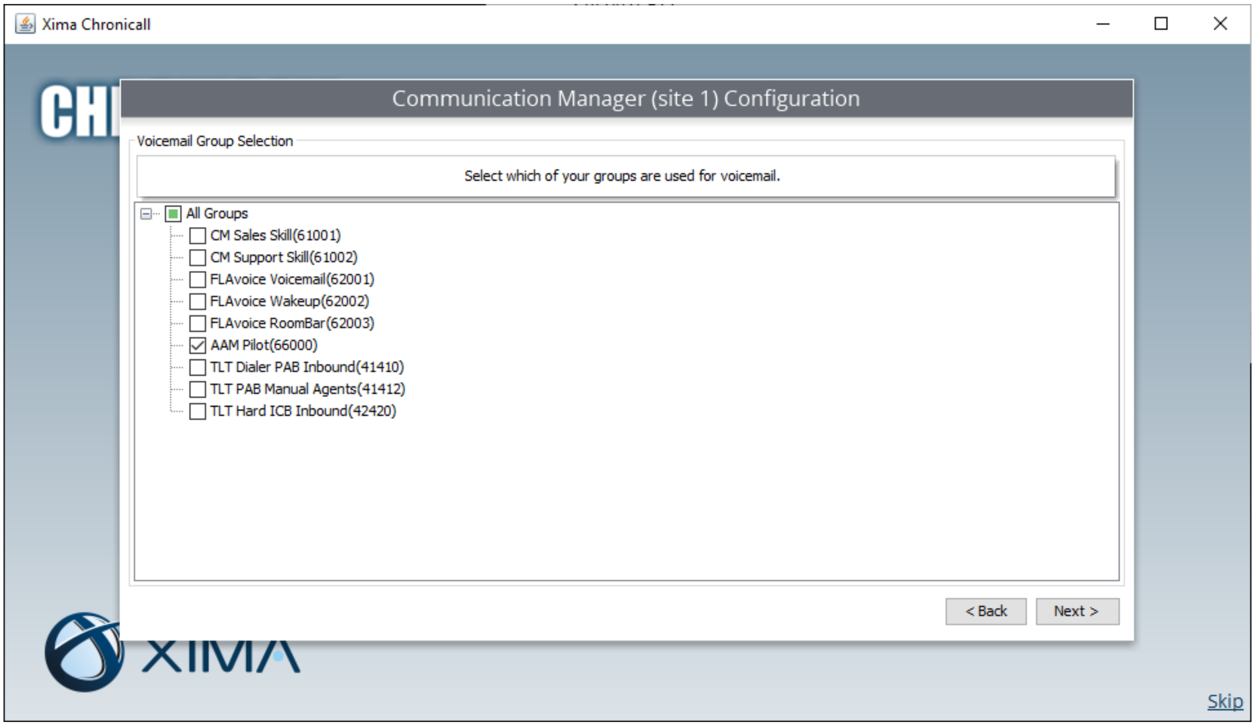
Max TSAPI Licenses: 7

- ▣ All ACD Groups
  - ☑ CM Sales Skill(61001)
  - ☑ CM Support Skill(61002)
  - ☐ TLT Dialer PAB Inbound(41410)
  - ☐ TLT PAB Manual Agents(41412)
  - ☐ TLT Hard ICB Inbound(42420)

7/7 Licenses Used

8.6. Administer Voicemail Group

The **Voicemail Group Selection** screen is displayed next, showing a list of groups obtained via the SMS connection to Application Enablement Services. Select the group used for voicemail if any, in this case “66000”. This enables calls to voicemail to be identified as such.


Xima Chronicall
Communication Manager (site 1) Configuration
Voicemail Group Selection
< Back
Next >
Skip

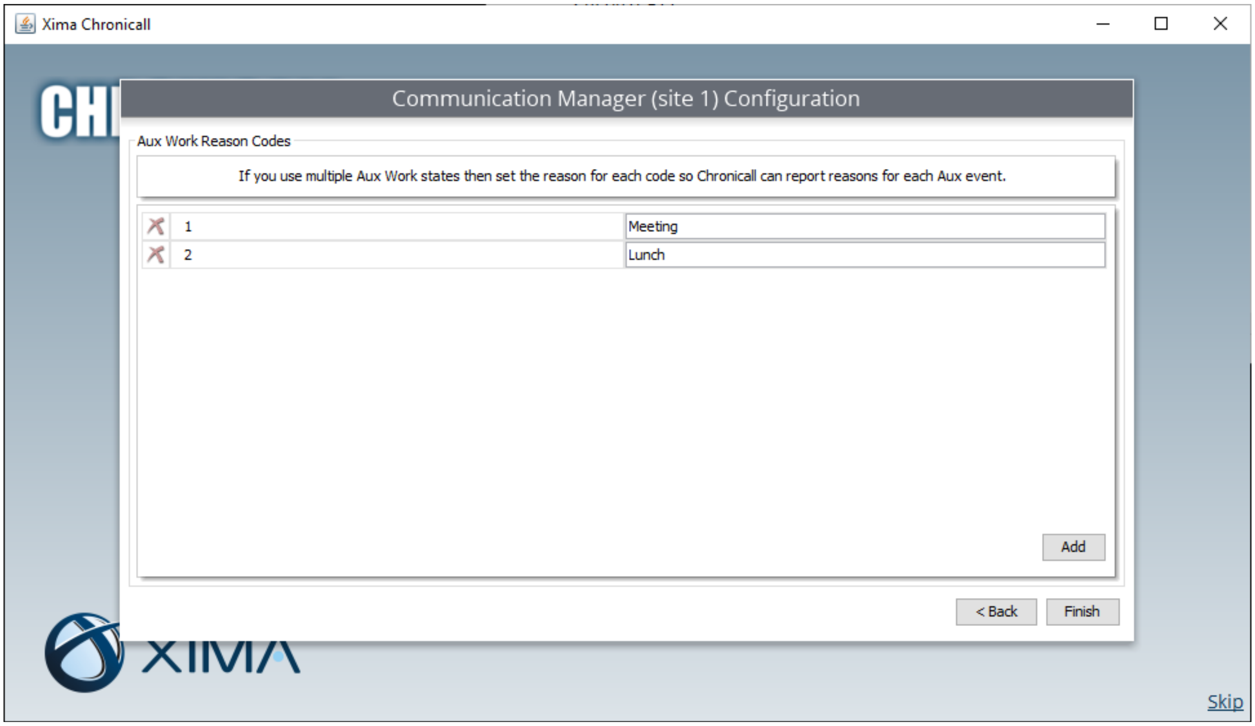
Select which of your groups are used for voicemail.

- All Groups
  - ☐ CM Sales Skill(61001)
  - ☐ CM Support Skill(61002)
  - ☐ FLAvoice Voicemail(62001)
  - ☐ FLAvoice Wakeup(62002)
  - ☐ FLAvoice RoomBar(62003)
  - ☑ AAM Pilot(66000)
  - ☐ TLT Dialer PAB Inbound(41410)
  - ☐ TLT PAB Manual Agents(41412)
  - ☐ TLT Hard ICB Inbound(42420)

8.7. Administer Reason Codes

The **Aux Work Reason Codes** screen is displayed next. For call centers that use reason codes for aux work, click **Add** to configure an entry for each aux work reason code from **Section 5.3**.

In the compliance testing, two reason codes were created, as shown below.



Communication Manager (site 1) Configuration

Aux Work Reason Codes

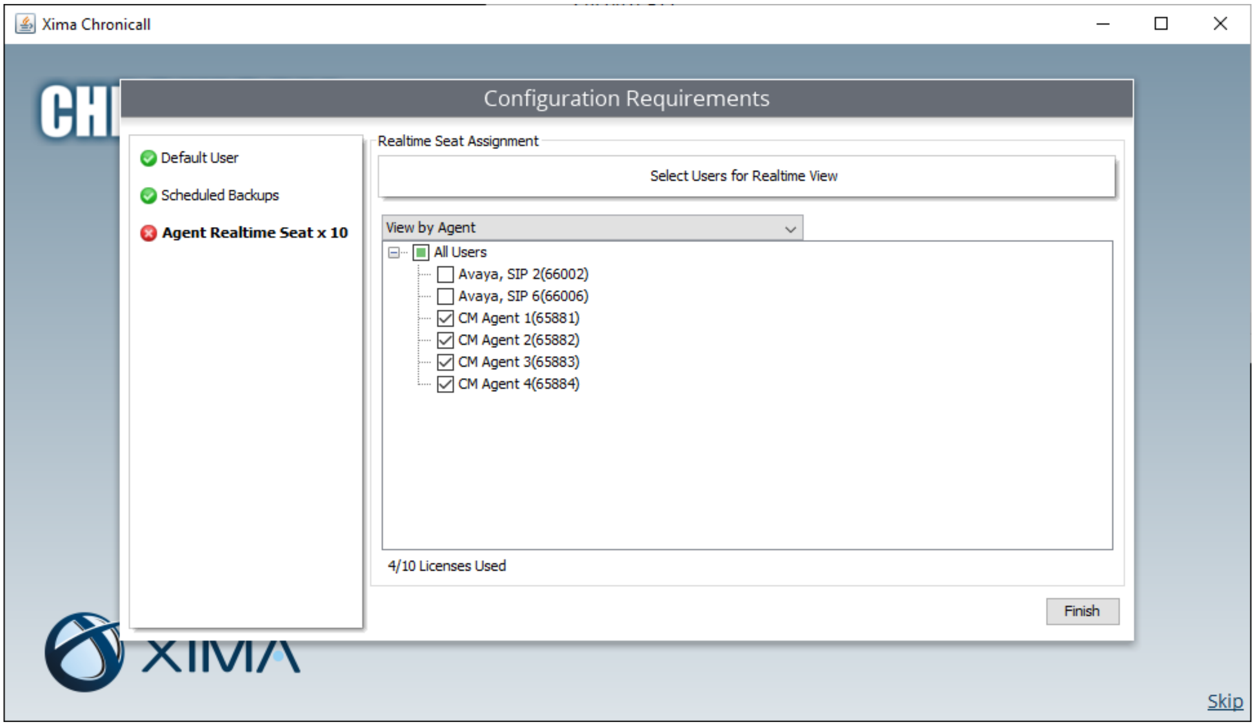
If you use multiple Aux Work states then set the reason for each code so Chronicall can report reasons for each Aux event.

1	Meeting
2	Lunch

8.8. Administer Realtime Seat Assignment

For deployments with Chronicall Realtime licenses, the **Configuration Requirements** screen is displayed next. Continue to the **Realtime Agent Assignment** screen and select all desired agent IDs to monitor.

In the compliance testing, four agents IDs were selected, as shown below.



Configuration Requirements

- ✓ Default User
- ✓ Scheduled Backups
- ☒ **Agent Realtime Seat x 10**

Realtime Seat Assignment

Select Users for Realtime View

View by Agent

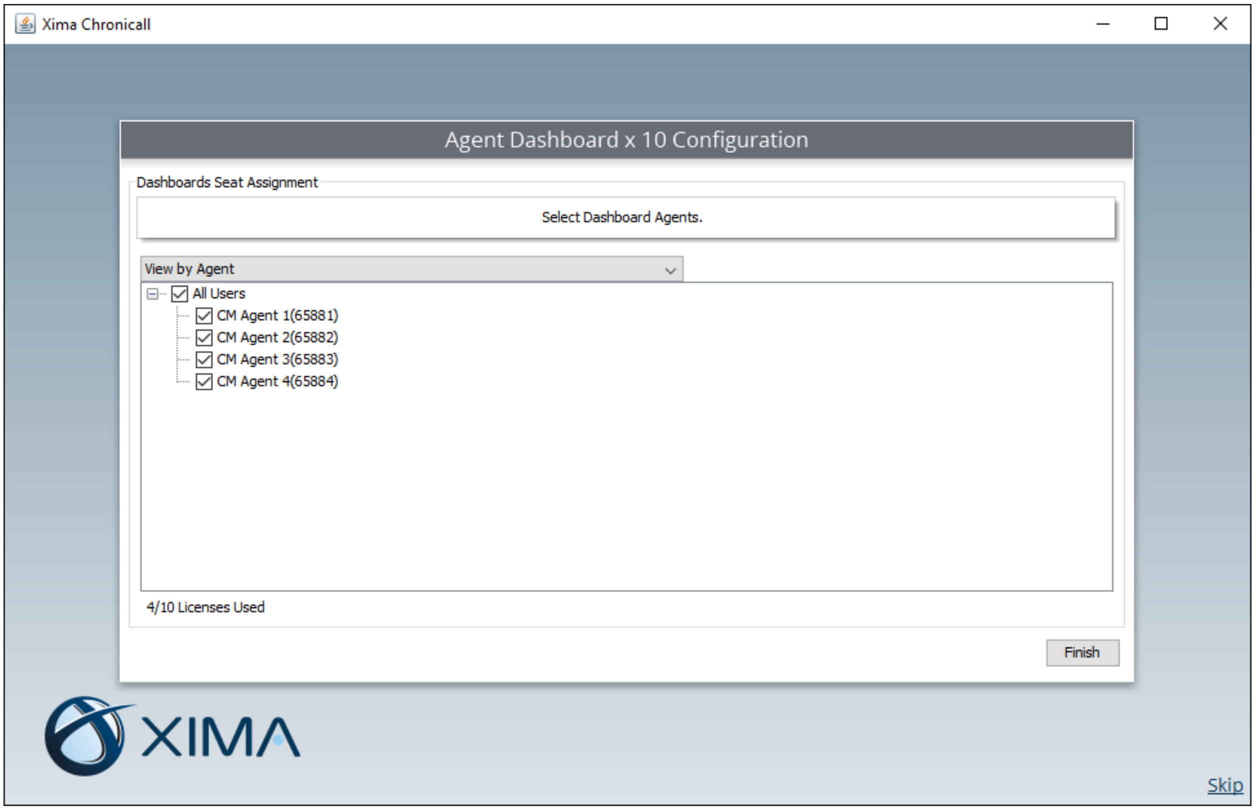
- ⊟ 🟩 All Users
  - □ Avaya, SIP 2(66002)
  - □ Avaya, SIP 6(66006)
  - ☑ CM Agent 1(65881)
  - ☑ CM Agent 2(65882)
  - ☑ CM Agent 3(65883)
  - ☑ CM Agent 4(65884)

4/10 Licenses Used

8.9. Administer Dashboards Seat Assignment

For deployments with Chronicall Realtime licenses, the **Dashboards Seat Assignment** screen is displayed next, listing all selected agent IDs from **Section 8.8**. Select all desired agent IDs to display on dashboard.

In the compliance testing, four agent IDs from **Section** Error! Reference source not found. were s elected, as shown below.



9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Chronicall.

9.1. Verify Avaya Aura® Communication Manager

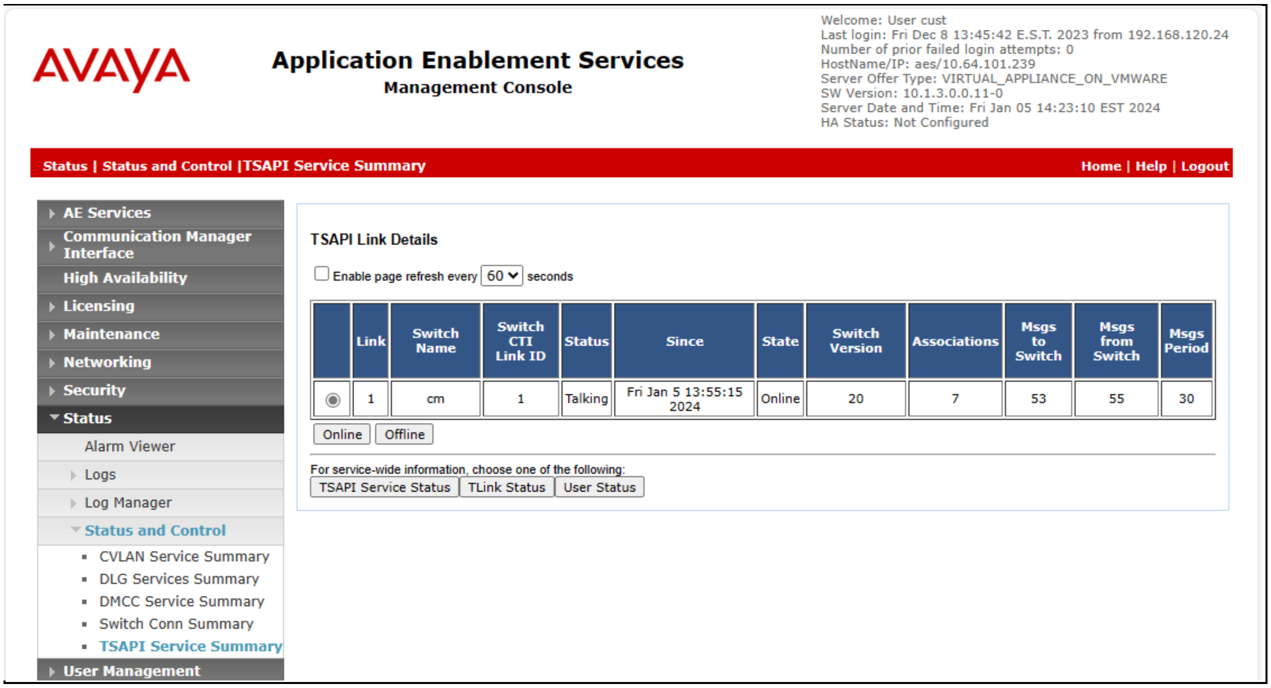
On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 0**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     12       no    aes              established   288      302
```

9.2. 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 (not shown). The **TSAPI Link Details** screen is displayed.

Prior to logging in any agents, verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored VDNs, skill groups, agent and supervisor stations, in this case "20".



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Dec 8 13:45:42 E.S.T. 2023 from 192.168.120.24
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Fri Jan 05 14:23:10 EST 2024
HA Status: Not Configured

Status | Status and Control |TSAPI Service Summary

TSAPI Link Details

□ Enable page refresh every 60 seconds

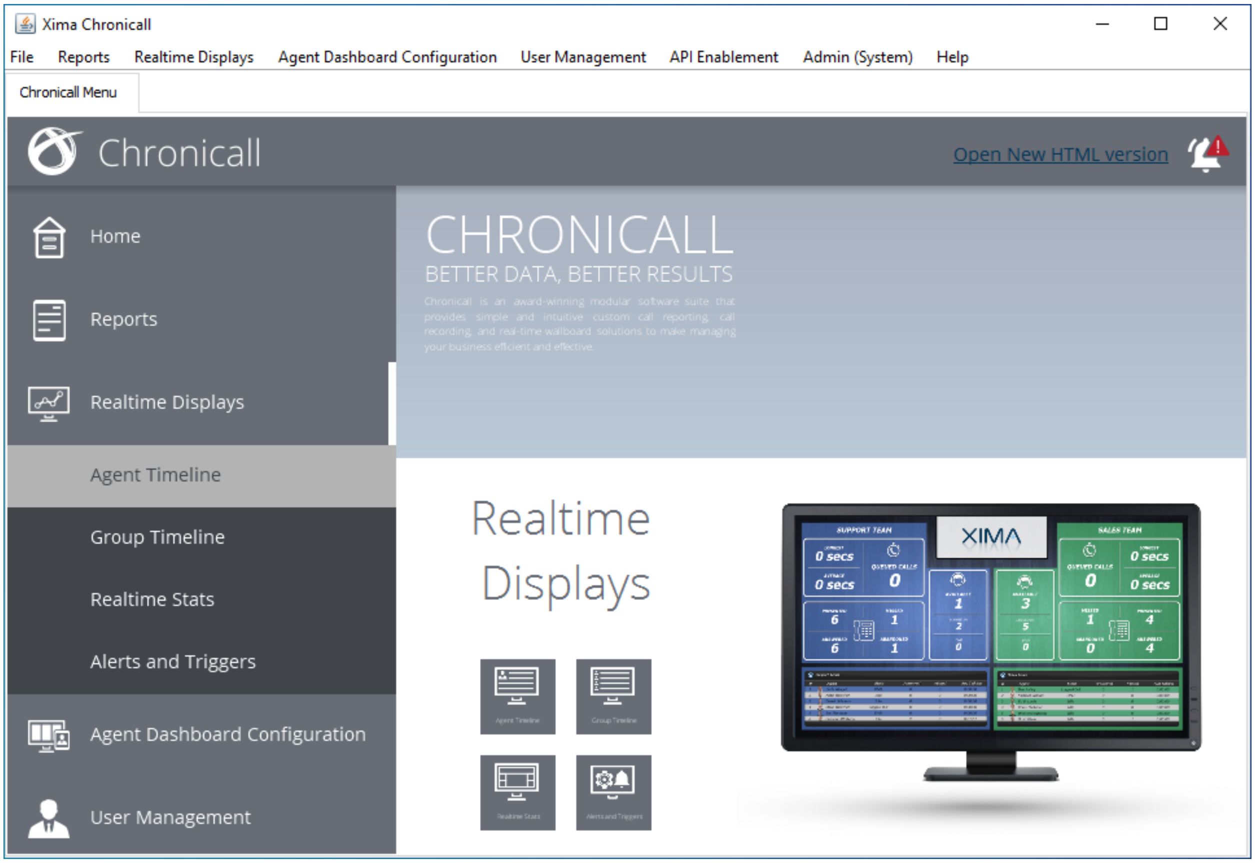
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm	1	Talking	Fri Jan 5 13:55:15 2024	Online	20	7	53	55	30

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

9.3. Verify Xima Chronicall

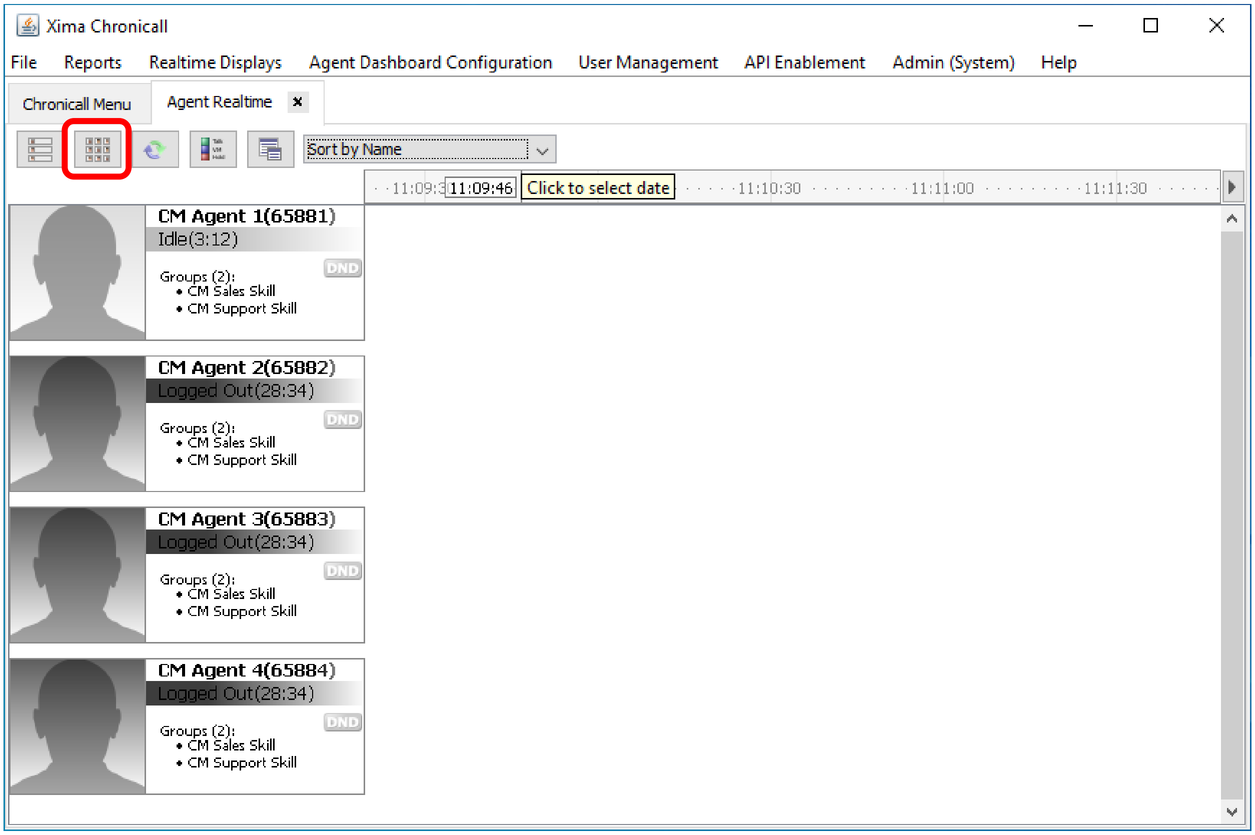
Follow the procedures in **Section 8.1** to launch the Chronicall Desktop client application, and log in using the appropriate credentials.

The **Chronicall Menu** tab is automatically created, as shown below. Select **Realtime Displays → Agent Timeline**.

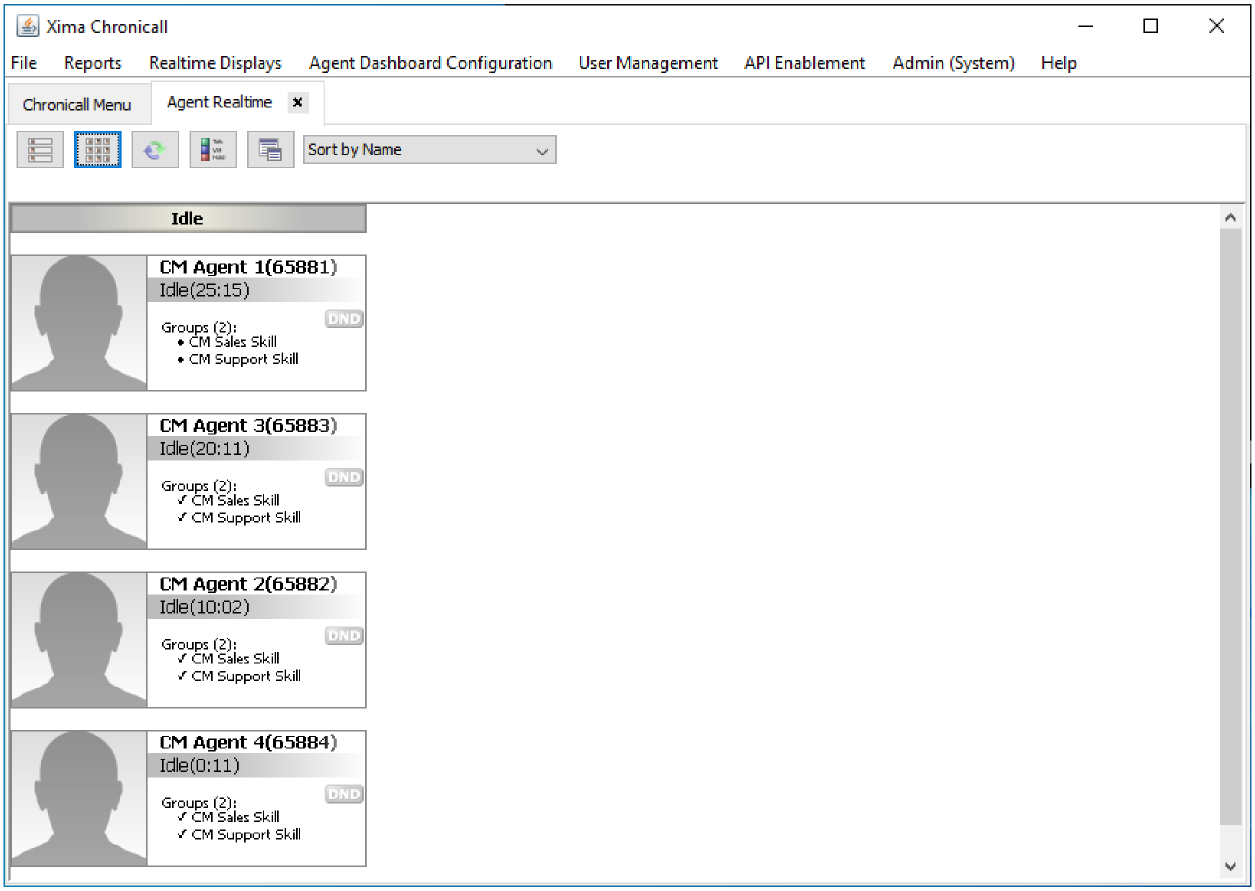


An **Agent Realtime** tab is created. Verify that all agent IDs selected for dashboard display from **Section 8.9** are shown below.

Select the **Show Live Columns** icon shown below.



Log agents into the skill groups on Communication Manager and place into the available mode. Verify that the screen is updated to reflect logged in and available agents as "Idle", along with proper skill group information, as shown below.



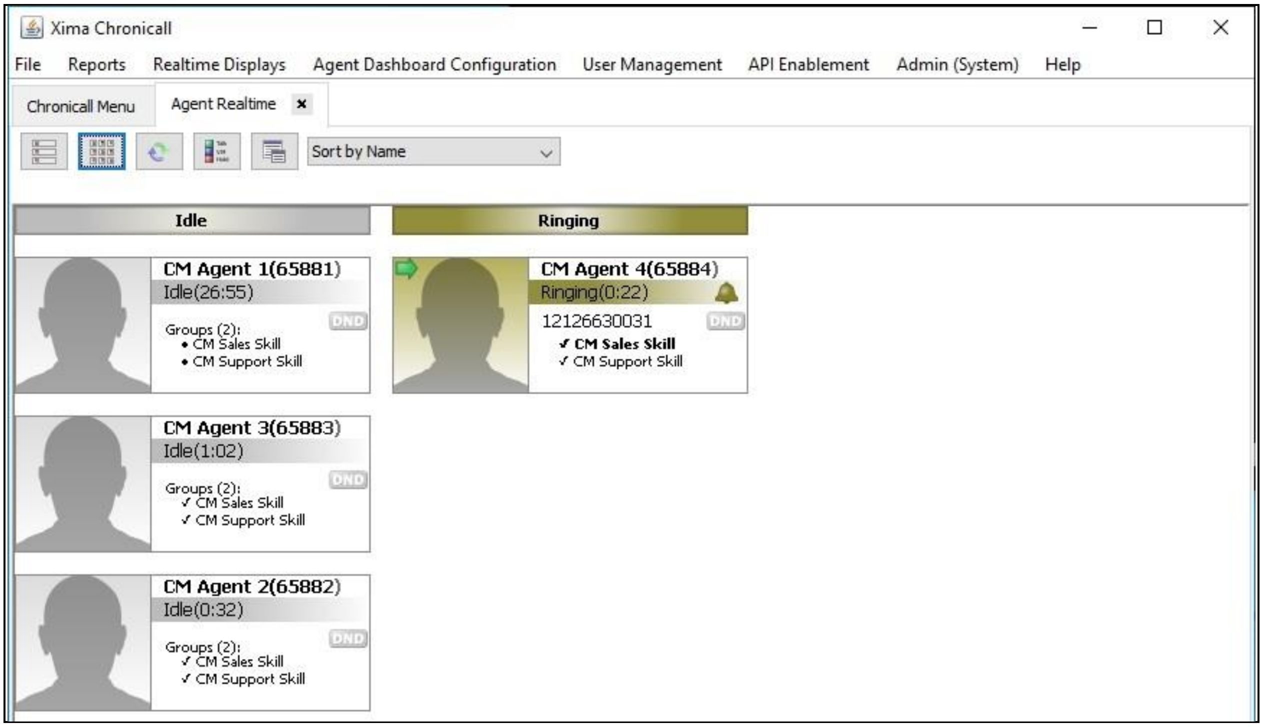
CM Agent 1(65881)
Idle(25:15)
Groups (2):
- CM Sales Skill
- CM Support Skill

CM Agent 3(65883)
Idle(20:11)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

CM Agent 2(65882)
Idle(10:02)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

CM Agent 4(65884)
Idle(0:11)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

Make an incoming ACD call from the PSTN. Verify that the call is ringing at an available agent and reflected properly in the **Ringing** column below.



Idle

CM Agent 1(65881)
Idle(26:55)
Groups (2):
- CM Sales Skill
- CM Support Skill

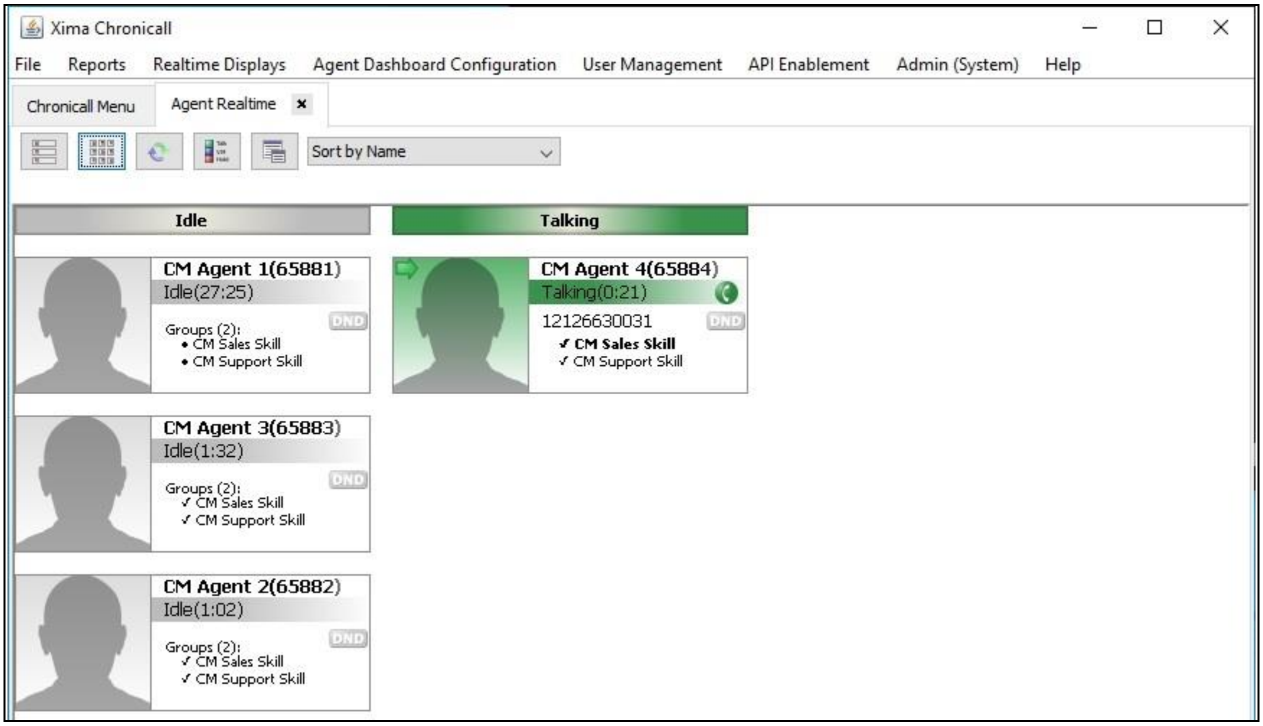
CM Agent 3(65883)
Idle(1:02)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

CM Agent 2(65882)
Idle(0:32)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

Ringing

CM Agent 4(65884)
Ringing(0:22)
12126630031
✓ **CM Sales Skill**
✓ CM Support Skill

Answer the ACD call at the agent telephone. Verify that the call is connected to the agent and properly reflected in the **Talking** column shown below.



CM Agent 1(65881)
Idle(27:25)
Groups (2):
- CM Sales Skill
- CM Support Skill

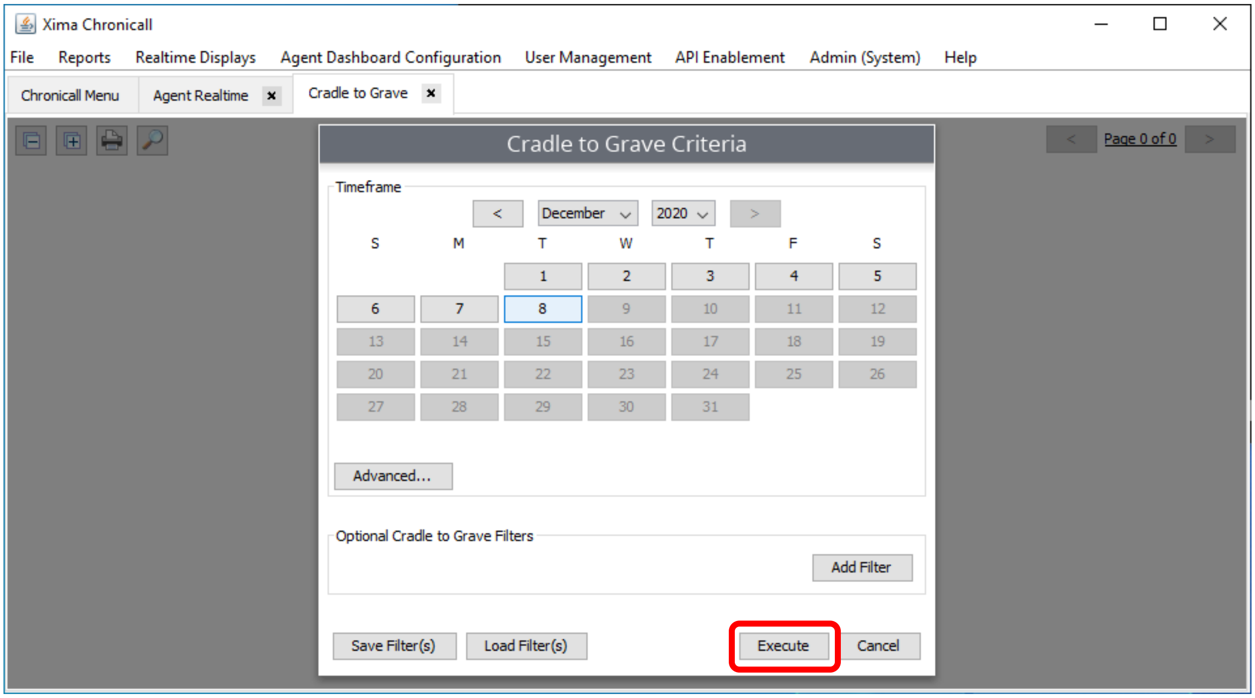
CM Agent 3(65883)
Idle(1:32)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

CM Agent 2(65882)
Idle(1:02)
Groups (2):
✓ CM Sales Skill
✓ CM Support Skill

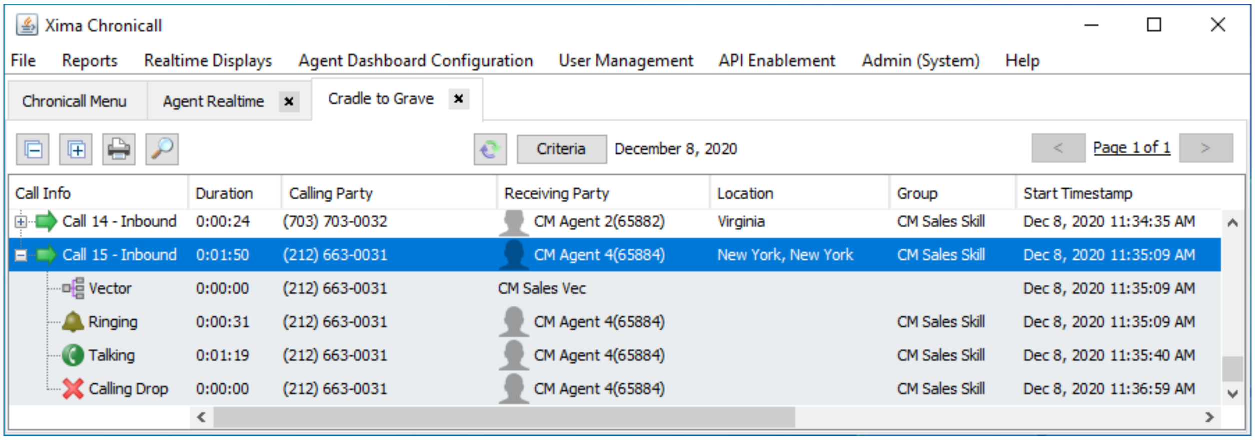
CM Agent 4(65884)
Talking(0:21)
12126630031
✓ **CM Sales Skill**
✓ CM Support Skill

Complete the active ACD call. Select **Reports → Cradle to Grave** from the top menu.

The **Cradle to Grave** tab is created and displays the **Cradle to Grave Criteria** screen below. Select the desired date range and click **Execute**.



The **Cradle to Grave** tab is updated as shown below. Verify that there is an entry reflecting the last call, in this case “Call 15”. Expand the entry and verify that the reported details reflect the last call with proper values in the respective columns, as shown below.



December 8, 2020

Call Info	Duration	Calling Party	Receiving Party	Location	Group	Start Timestamp
Call 14 - Inbound	0:00:24	(703) 703-0032	CM Agent 2(65882)	Virginia	CM Sales Skill	Dec 8, 2020 11:34:35 AM
Call 15 - Inbound	0:01:50	(212) 663-0031	CM Agent 4(65884)	New York, New York	CM Sales Skill	Dec 8, 2020 11:35:09 AM
Vector	0:00:00	(212) 663-0031	CM Sales Vec			Dec 8, 2020 11:35:09 AM
Ringing	0:00:31	(212) 663-0031	CM Agent 4(65884)		CM Sales Skill	Dec 8, 2020 11:35:09 AM
Talking	0:01:19	(212) 663-0031	CM Agent 4(65884)		CM Sales Skill	Dec 8, 2020 11:35:40 AM
Calling Drop	0:00:00	(212) 663-0031	CM Agent 4(65884)		CM Sales Skill	Dec 8, 2020 11:36:59 AM

10. Conclusion

These Application Notes describe the configuration steps required for Xima Chronicall 4.4 to successfully interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. All feature and serviceability test cases were completed with observations noted in **Section** Error! Reference source not found..

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 7, May 2023, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

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