



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

---

# **Application Notes for Xima Chronicall 4.2 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Xima Chronicall 4.2 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

In the compliance testing, Xima Chronicall used the System Management Services and Java Telephony Application Programming Interface from Avaya Aura® Application Enablement Services to provide real-time agent status monitoring and cradle to grave reporting.

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 Xima Chronicall 4.2 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

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, 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:

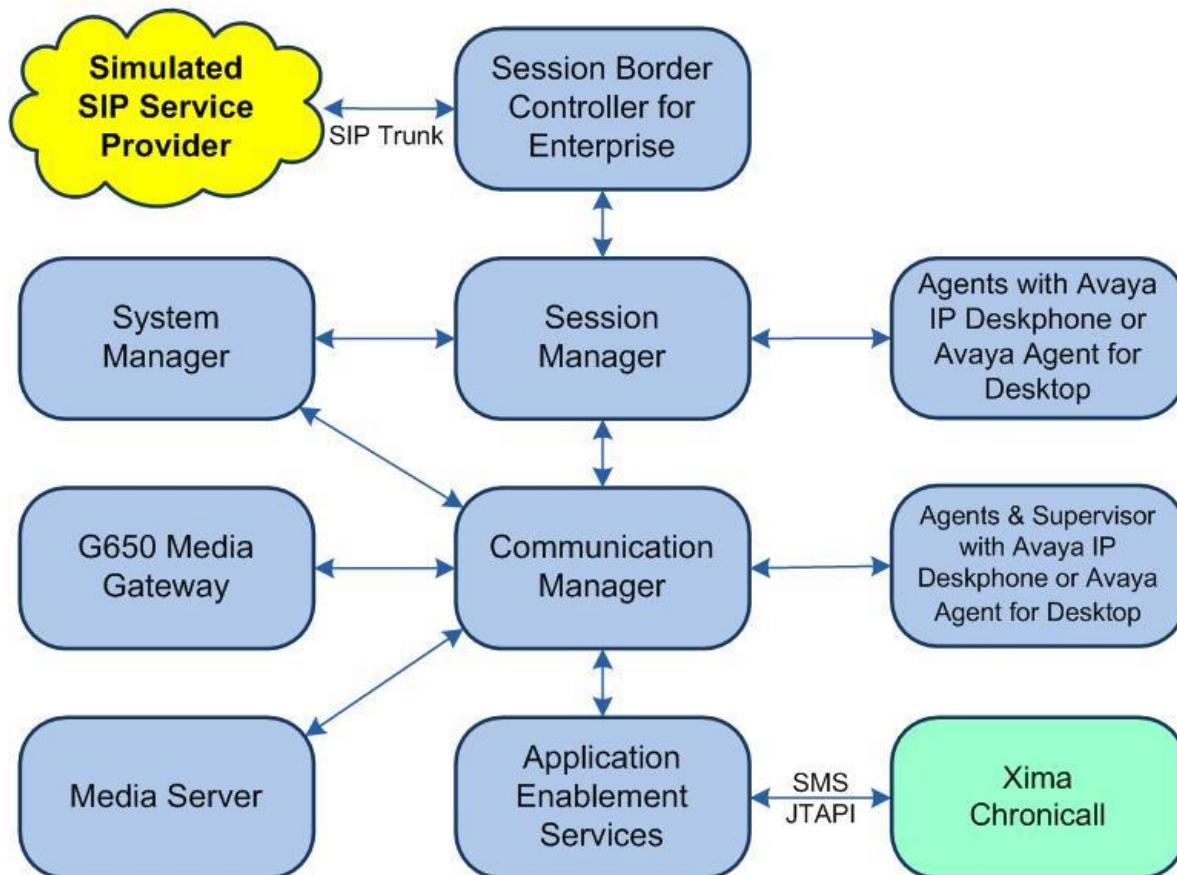
- **Phone:** (888) 944-XIMA
- **Email:** [support@ximasoftware.com](mailto:support@ximasoftware.com)
- **Web:** <http://ximacare.ximasoftware.com>

### 3. Reference Configuration

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

The configuration of Avaya Aura® Session Manager is performed via the web interface of Avaya Aura® 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



**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	8.1.2 (8.1.1.0.0.890.26095)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.127
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.2 (8.1.2.1.0.6-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.2 (8.1.2.1.812101)
Avaya Aura® System Manager in Virtual Environment	8.1.2 (8.1.2.0.0611517)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G IP Deskphone (H.323)	6.8304
Avaya J169 IP Deskphone (SIP)	4.0.2.1.3
Xima Chronicall on Windows Server 2016 <ul style="list-style-type: none"><li>Avaya JTAPI Windows Client (ecsjtapia.jar)</li></ul>	4.2 (7) Standard 6.3.3.26
Xima Chronicall Desktop on Windows 10 Pro	4.2 (7)

## 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
- 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	<b>Computer Telephony Adjunct Links? y</b>		
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	Digital Loss Plan Modification? y		
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y		
ATM WAN Spare Processor? n			

### 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			
<b>Extension: 60111</b>			
<b>Type: ADJ-IP</b>			
<b>Name: AES CTI Link</b>			
Unicode Name? n			
COR: 1			



### 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

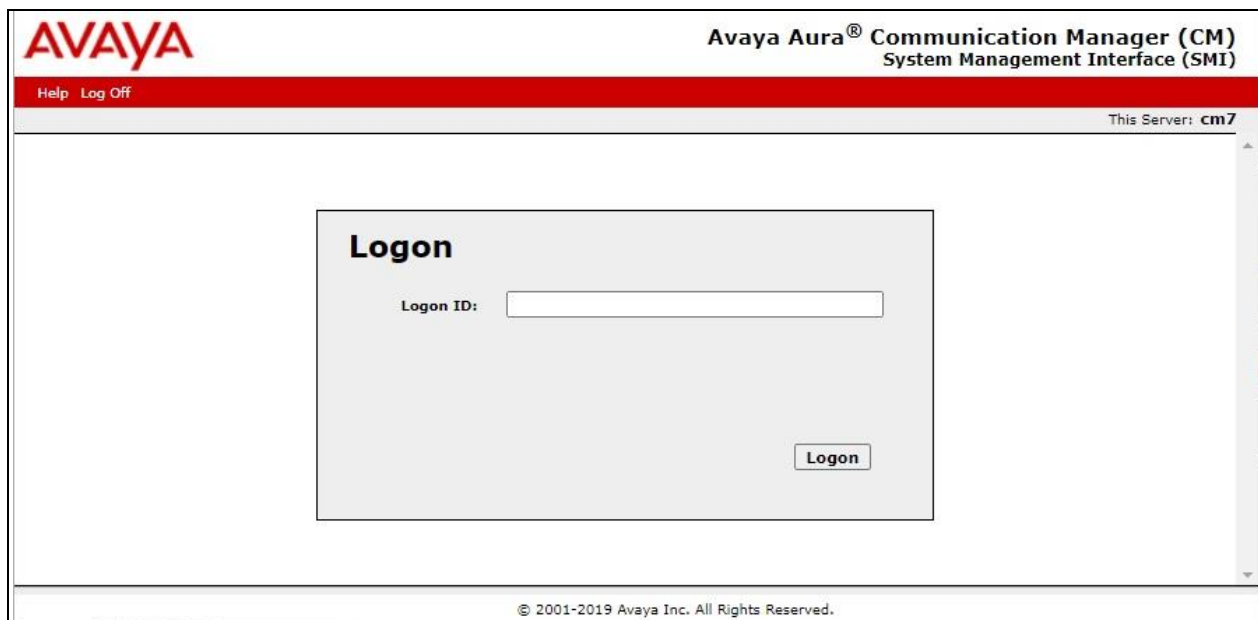
                                Aux Work/      Logout
                                Interruptible?

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

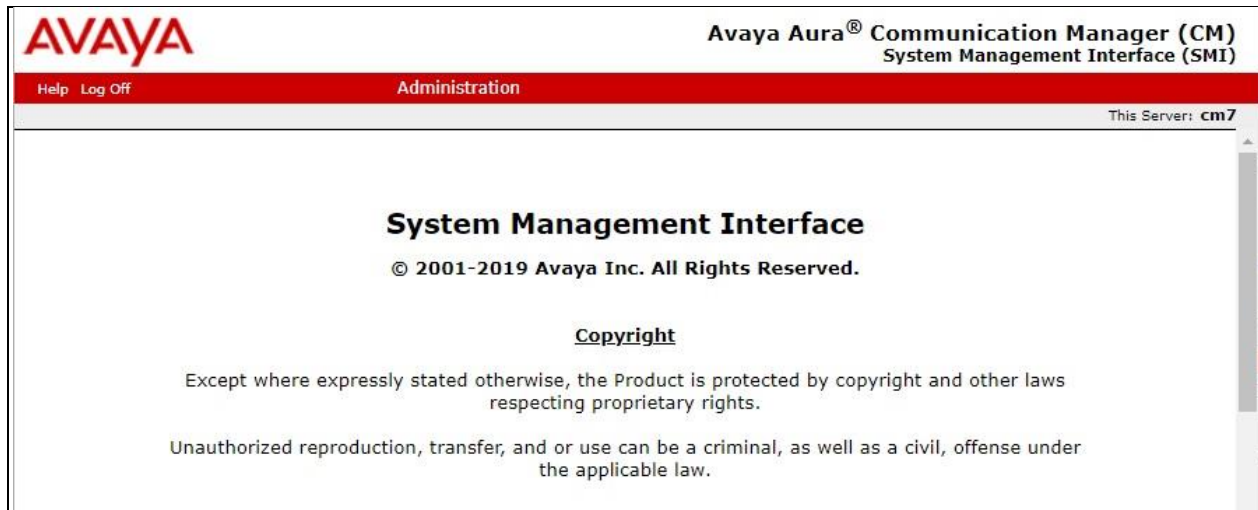
Default Reason Code:
```

### 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.



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



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



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

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administrator Accounts page. The page has a red header with the Avaya logo and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)". Below the header is a navigation bar with "Help" and "Log Off" links, and the "Administration" tab is selected. The main content area is titled "Administrator Accounts" and contains the text: "The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups." Below this text is a "Select Action:" section with several radio button options: "Add Login" (selected), "Privileged Administrator" (selected), "Unprivileged Administrator", "SAT Access Only", "Web Access Only", "CDR Access Only", "Business Partner Login (dadmin)", "Business Partner Craft Login", and "Custom Login". There are also three "Change Login", "Remove Login", and "Lock/Unlock Login" options, each with a "Select Login" dropdown menu. At the bottom of the "Select Action:" section are "Add Group" and "Remove Group" options, each with a "Select Group" dropdown menu. Below these options are "Submit" and "Help" buttons. On the left side of the page is a sidebar menu with categories: "Server Upgrades", "Data Backup/Restore", "Security", and "Miscellaneous". The "Security" category is expanded, showing sub-items like "Administrator Accounts", "Login Account Policy", "Change Password", "Login Reports", "Server Access", "Server Log Files", "Firewall", "Install Root Certificate", "Trusted Certificates", "Server/Application Certificates", "Certificate Alarms", "Certificate Signing Request", "SSH Keys", and "Web Access Mask". The "Administrator Accounts" sub-item is highlighted. At the bottom of the page is a copyright notice: "© 2001-2019 Avaya Inc. All Rights Reserved."

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.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for server cm7. The left sidebar contains a navigation menu with categories: Server Upgrades, Data Backup/Restore, Security, and Miscellaneous. The 'Administrator Accounts' link under the Security section is highlighted. The main content area is titled 'Administrator Accounts -- Add Login: Privileged Administrator'. It includes a descriptive text: '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.' Below this is a form with the following fields: Login name (xima), Primary group (susers), Additional groups (profile) (prof18), Linux shell (/bin/bash), Home directory (/var/home/xima), Lock this account (unchecked), SAT Limit (none), Date after which account is disabled-blank to ignore (YYYY-MM-DD) (empty), Enter password (masked with dots), Re-enter password (masked with dots), and Force password change on next login (radio buttons for No and Yes, with 'No' selected). At the bottom are 'Submit', 'Cancel', and 'Help' buttons. The footer contains the copyright notice: '© 2001-2019 Avaya Inc. All Rights Reserved.'

## 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.



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the OAM web interface, listing administrative domains and their functions. A welcome message and system status information are displayed in the top right corner.

**AVAYA Application Enablement Services Management Console**

Welcome: User  
Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.2.1.0.6-0  
Server Date and Time: Tue Dec 08 09:38:07 EST 2020  
HA Status: Not Configured

**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.

## 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).

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area is titled "Licensing" and provides instructions for setting up and maintaining the WebLM, including steps for WebLM Server Address, WebLM Server Access, and Reserved Licenses. The top header and navigation bar are consistent with the previous screenshot.

**AVAYA Application Enablement Services Management Console**

Welcome: User  
Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.2.1.0.6-0  
Server Date and Time: Tue Dec 08 09:38:07 EST 2020  
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  
Networking

**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 **Application Enablement (CTI)** screen in the right pane.

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

**AVAYA**  
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home User Management Licenses

L...

- WebLM Home
- Install license
- Licensed products
- APPL\_ENAB
- ▼ Application\_Enablement
  - View by feature
  - View by local WebLM
  - Enterprise configuration
  - ▶ Local WebLM Configuration
  - ▶ Usages
  - ▶ Allocations
  - Periodic status
- ASBCE
  - ▶ Session\_Border\_Controller\_E\_AE
- CCTR
  - ▶ ContactCenter
- COMMUNICATION\_MANAGER
  - ▶ Call\_Center
  - ▶ Communication\_Manager
- MESSAGING
  - ▶ Messaging
- MSR
  - ▶ Media\_Server
- SYSTEM\_MANAGER
  - ▶ System\_Manager
- SessionManager

**Application Enablement (CTI) - Release: 8 - SID: 10503000(Enterprise)**

You are here: Licensed Products > Application\_Enablement > View by Feature

License installed on: August 8, 2019 4:43:51 PM -05:00

<b>License File Host IDs:</b>	VE-83-02-2D-26-52-01
<b>Active License Mode</b>	Standard
<b>License State</b>	NA
<b>Pay Per Use License Available</b>	No
<b>Standard License Available</b>	Yes

Feature (License Keyword)	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
DLG (VALUE_AES_DLG)	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	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**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 8.1.2.1.0.6-0, Server Date and Time: Tue Dec 08 09:38:07 EST 2020, HA Status: Not Configured. The left navigation pane shows the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area is titled 'TSAPI Links' and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

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 “cm7” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Add TSAPI Links' form. The left navigation pane shows the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area is titled 'Add TSAPI Links' and contains the following fields: Link (dropdown menu with '1' selected), Switch Connection (dropdown menu with 'cm7' selected), Switch CTI Link Number (dropdown menu with '1' selected), ASAI Link Version (dropdown menu with '11' selected), and Security (dropdown menu with 'Unencrypted' selected). Below the fields are buttons for 'Apply Changes' and 'Cancel Changes'.



## 6.4. Administer Chronical 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title 'Application Enablement Services Management Console'. A welcome message and system status are shown in the top right corner. The left navigation pane lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User'. The main content area is titled 'Add User' and contains a form with the following fields:

- \* User Id: xima
- \* Common Name: xima
- \* Surname: xima
- \* User Password: [masked]
- \* Confirm Password: [masked]
- Admin Note: [empty]
- Avaya Role: None (dropdown)
- Business Category: [empty]
- Car License: [empty]
- CM Home: [empty]
- Css Home: [empty]
- CT User: Yes (dropdown)
- Department Number: [empty]
- Display Name: [empty]
- Employee Number: [empty]
- Employee Type: [empty]
- Enterprise Handle: [empty]
- Given Name: [empty]

Fields marked with \* can not be empty.

## 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.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Chronicall user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, including the last login time, number of failed login attempts, host name/IP, server offer type, SW version, server date and time, and HA status. Below the header is a red navigation bar with "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar contains a tree view of the console's sections: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and Control. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

## 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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information and system details. The left navigation pane shows a tree structure with "Maintenance" expanded and "Service Controller" selected. The main content area, titled "Service Controller", contains a table of services and their statuses. The "TSAPI Service" is checked, and the "Restart Service" button is highlighted in the action bar below the table.

Welcome: User  
Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.2.1.0.6-0  
Server Date and Time: Tue Dec 08 09:38:07 EST 2020  
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Date Time/NTP Server  
Security Database  
Service Controller  
Server Data  
Networking  
Security  
Status

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

## 6.7. 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#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, along with login details: "Welcome: User", "Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 8.1.2.1.0.6-0", "Server Date and Time: Tue Dec 08 09:38:07 EST 2020", and "HA Status: Not Configured".

The main navigation bar is red and contains the links "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks" (selected).

The main content area is titled "Tlinks" and shows a single Tlink entry with the name "AVAYA#CM7#CSTA#AES7". A "Delete Tlink" button is visible next to the entry.

## 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.

**AVAYA** Application Enablement Services  
Management Console

Welcome: User  
Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.2.1.0.6-0  
Server Date and Time: Tue Dec 08 09:38:07 EST 2020  
HA Status: Not Configured

Networking | Ports

Home | 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 Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

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 Min4101

Proxy Port Max4116

TLT; Reviewed:  
SPOC 1/28/2021

Solution & Interoperability Test Lab Application Notes  
©2021 Avaya Inc. All Rights Reserved.

21 of 44  
Xima-AES81

## 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "AE Services" expanded, and "SMS Properties" selected under the "SMS" category. The main content area displays the "SMS Properties" configuration form. The form contains several fields: "Default CM Host Address" (text input with value 10.64.125.236), "Default CM Admin Port" (text input with value 5022), "CM Connection Protocol" (dropdown menu with value SSH), "SMS Logging" (dropdown menu with value NORMAL), "SMS Log Destination" (dropdown menu with value apache), "CM Proxy Trace Logging" (dropdown menu with value NONE), "Max Sessions per CM" (text input with value 5), "Proxy Shutdown Timer" (text input with value 1800 and unit seconds), "SAT Login Keepalive" (text input with value 180 and unit seconds), "CM Terminal Type" (dropdown menu with value OSSIZ), and "Proxy Log Destination" (text input with value /var/log/avaya/aes/ossicm.log). At the bottom of the form are three buttons: "Apply Changes", "Restore Defaults", and "Cancel".

Welcome: User  
Last login: Tue Dec 8 09:12:46 2020 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.2.1.0.6-0  
Server Date and Time: Tue Dec 08 09:46:07 EST 2020  
HA Status: Not Configured

AE Services | SMS | SMS Properties Home | Help | Logout

▼ AE Services  
▶ CVLAN  
▶ DLG  
▶ DMCC  
▼ SMS  
▪ SMS Properties  
▶ TSAPI  
▶ TWS  
Communication Manager Interface  
High Availability  
▶ Licensing  
▶ Maintenance  
▶ Networking  
▶ Security  
▶ Status  
▶ User Management  
▶ Utilities  
▶ Help

**SMS Properties**

Default CM Host Address 10.64.125.236  
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  
Apply Changes Restore Defaults Cancel



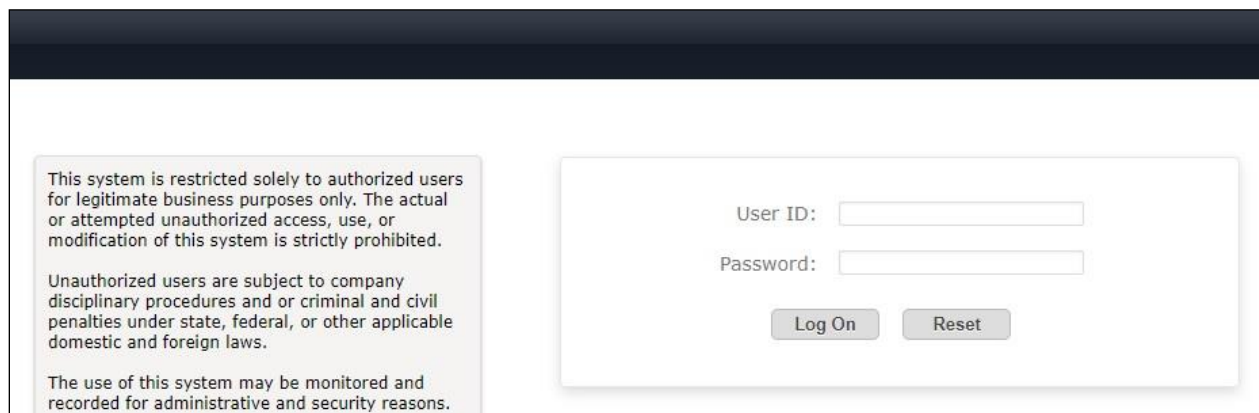
## 7. Configure Avaya Aura® Session Manager

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

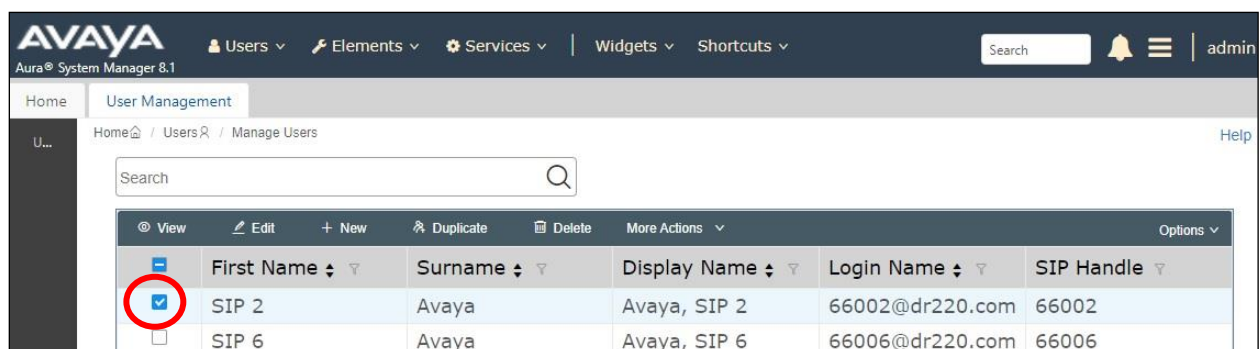
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



### 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 3**, in this case “66002”, and click **Edit**.



View	Edit	New	Duplicate	Delete	More Actions	Options
First Name	Surname	Display Name	Login Name	SIP Handle		
<input checked="" type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002	
<input type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006	

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.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon are also present. The main content area is titled 'User Profile | Edit | 66002@dr220.com' and includes buttons for 'Commit & Continue', 'Commit', and 'Cancel'. The 'Communication Profile' tab is selected, and the 'CM Endpoint Profile' is highlighted in the left sidebar. The 'Extension' field is set to '66002' and has a blue Editor icon highlighted with a red box. Other fields include 'System' (DR-CM), 'Profile Type' (Endpoint), 'Set Type' (J129), 'Port' (S000068), and 'Sip Trunk' (aar).

Field	Value
System	DR-CM
Profile Type	Endpoint
Extension	66002
Set Type	J129
Port	S000068
Sip Trunk	aar



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 3**. In the compliance testing, two SIP agent users 66002 and 66006 were configured.

The screenshot shows the 'Edit Endpoint' configuration page in the Avaya Aura System Manager 8.1 interface. The page is titled 'Edit Endpoint' and includes a 'Done' button and a '[Save As Template]' link. The configuration is organized into several sections:

- System Information:**
  - System: DR-CM
  - Extension: 66002
  - Template: Select (dropdown)
  - Set Type: J129
  - Port: S000068
  - Security Code: (empty)
  - Name: Avaya, SIP 2
- Configuration Tabs:**
  - General Options (G) \*
  - Feature Options (F)
  - Site Data (S)
  - Abbreviated Call Dialing (A)
  - Button Assignment (B)
  - Profile Settings (P)
  - Group Membership (M)
- General Options (G) \*:**
  - Class of Restriction (COR): 1
  - Emergency Location Ext: 66002
  - Tenant Number: 1
  - SIP Trunk: Qaar
  - Coverage Path 1: 1
  - Lock Message: ☐
  - Multibyte Language: Not Applicable (dropdown)
  - Class Of Service (COS): 1
  - Message Lamp Ext.: 66002
  - Type of 3PCC Enabled: Avaya (dropdown, highlighted with a red box)**
  - Coverage Path 2: (empty)
  - Localized Display Name: Avaya, SIP 2
  - Enable Reachability for Station Domain Control: system (dropdown)
- SIP URI:** (empty text field)

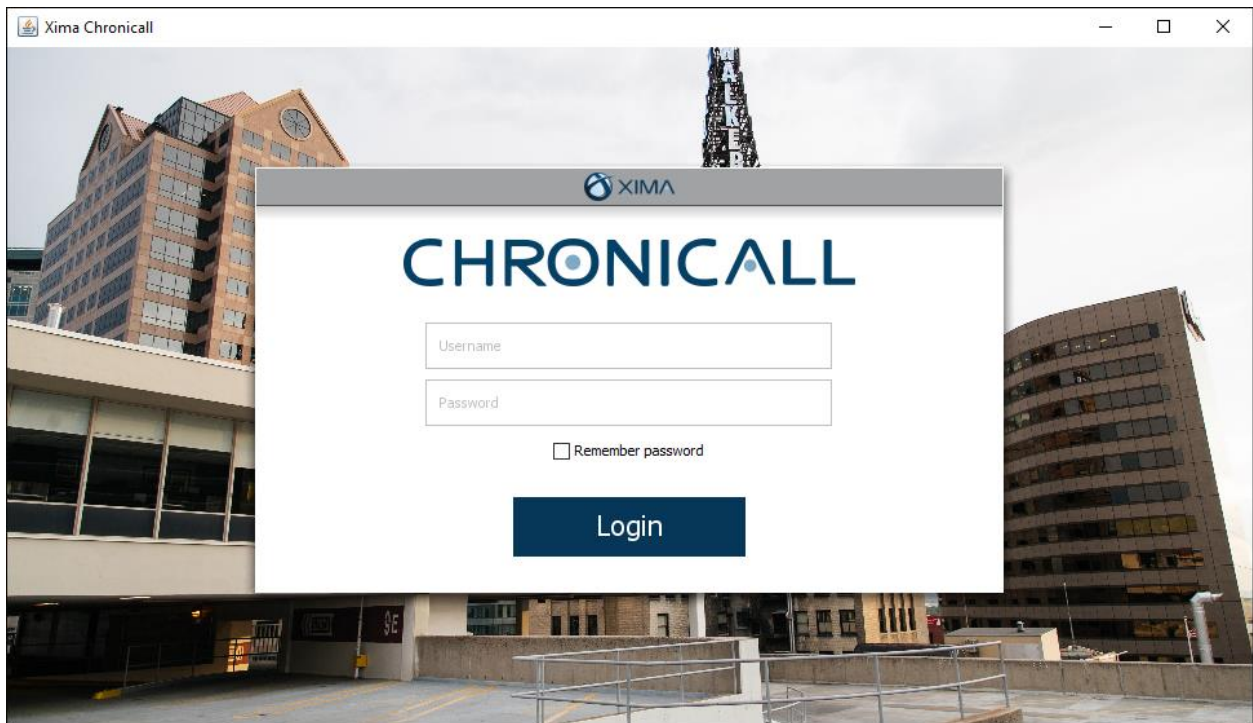
## 8. Configure Xima Chronicall

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**.



The screenshot shows a window titled "Xima Chronicall" with a standard Windows title bar. Inside the window is a configuration screen titled "Communication Manager (site 1) Configuration". The main section is "TSAPI Logging" and contains the following text: "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." Below this text are two radio button options: "Use TSAPI" (which is selected) and "Do not use TSAPI". At the bottom right of the configuration area are two buttons: "< Back" and "Next >". In the bottom left corner of the window is the XIMA logo, and in the bottom right corner is a "Skip" link.

## 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 5.4**.
- **CM Password:** The Communication Manager account password from **Section 5.4**.

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

Xima Chronicall

### 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

< Back   Next >

XIMA

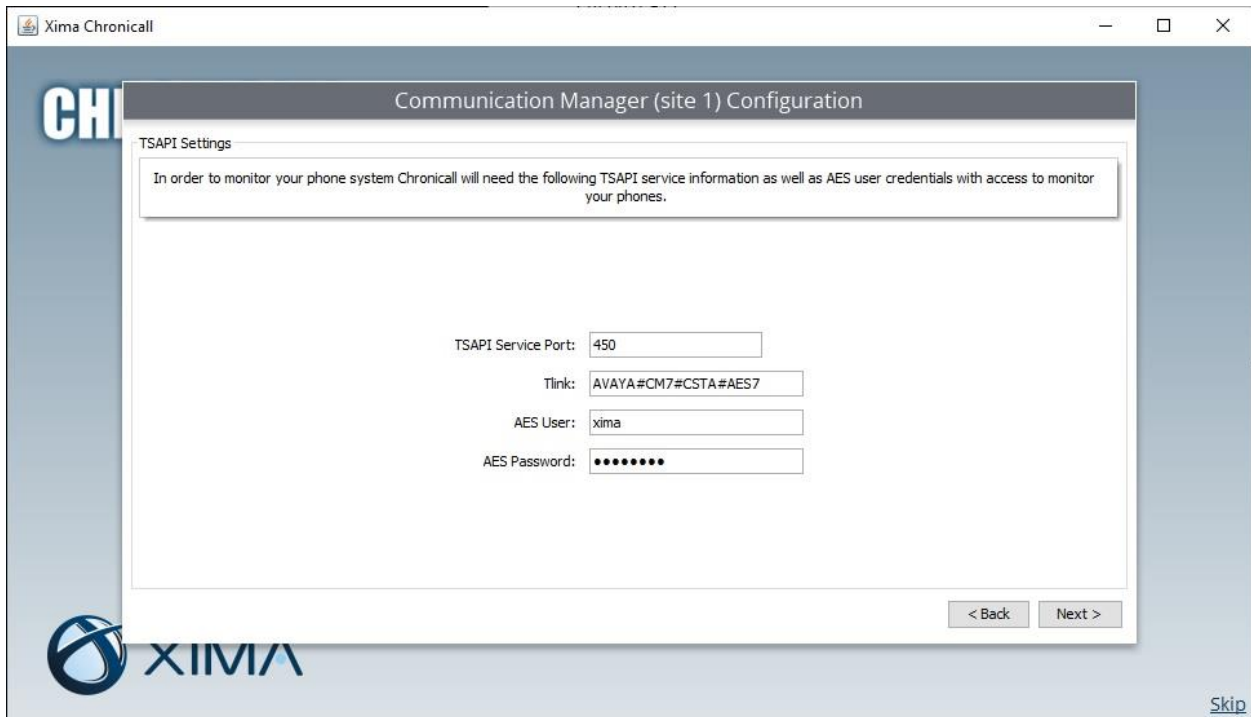
[Skip](#)

### 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.



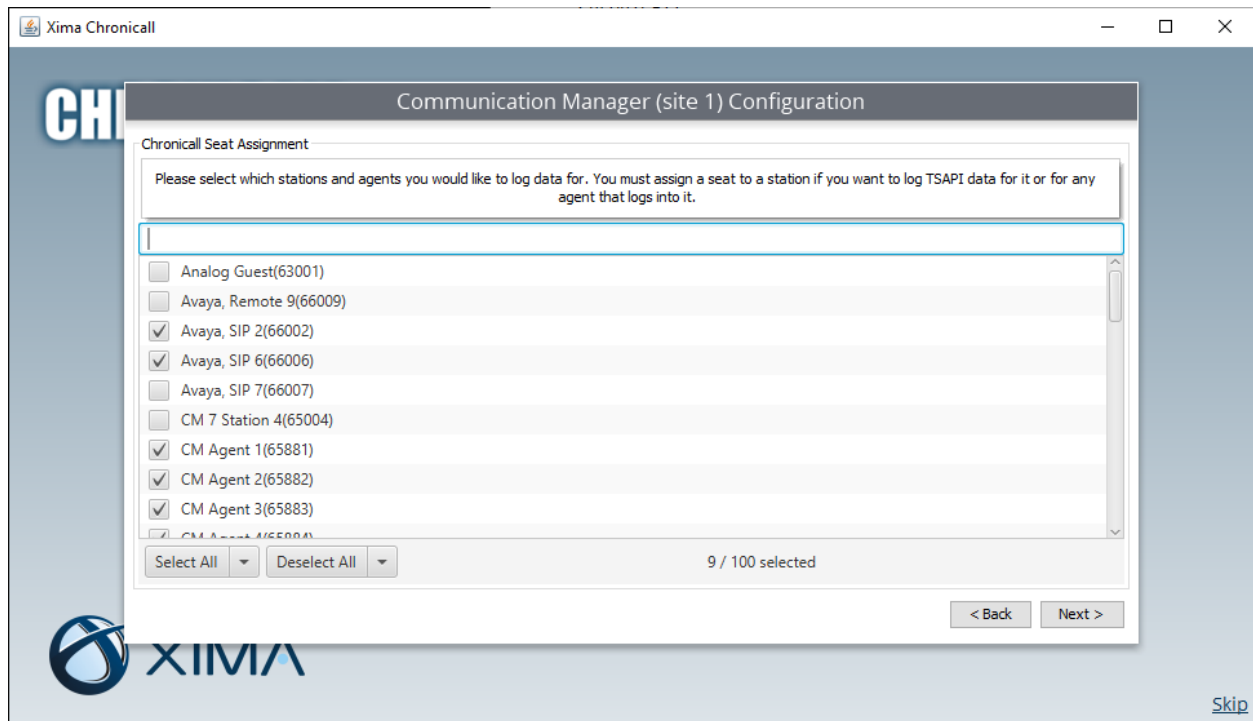
The screenshot shows a web-based configuration window titled "Xima Chronicall" with a sub-header "Communication Manager (site 1) Configuration". The main section is "TSAPI Settings". A message box states: "In order to monitor your phone system Chronicall will need the following TSAPI service information as well as AES user credentials with access to monitor your phones." Below this, there are four input fields: "TSAPI Service Port" with the value "450", "Tlink" with the value "AVAYA#CM7#CSTA#AES7", "AES User" with the value "xima", and "AES Password" with masked characters "••••••••". At the bottom right of the configuration area are "< Back" and "Next >" buttons. The Xima logo is visible in the bottom left corner, and a "Skip" link is in the bottom right corner.

## 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 3** were selected, as partially shown below.



## 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.

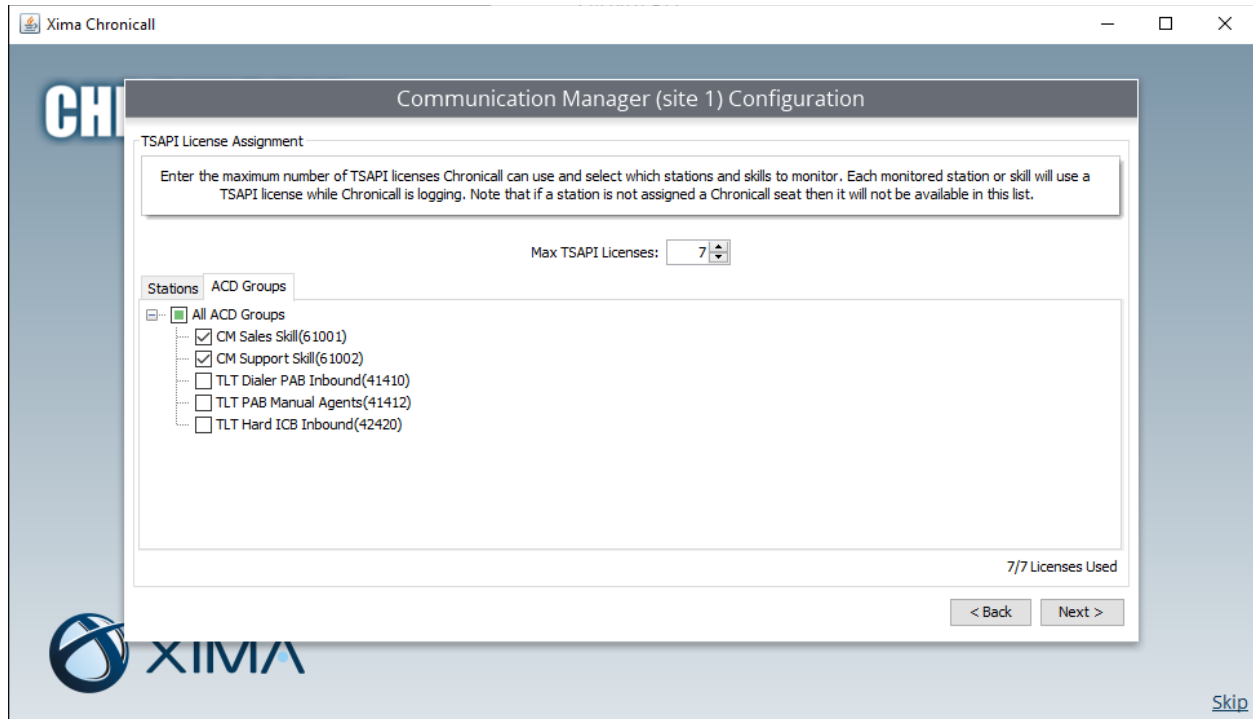
In the compliance testing, all five stations from **Section 3** were selected, as shown below.

The screenshot shows the 'Communication Manager (site 1) Configuration' window for 'Xima Chronicall'. The 'TSAPI License Assignment' section is active. It includes a text box with instructions: '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.' Below this, the 'Max TSAPI Licenses' is set to 7. The 'Stations' tab is selected, showing a list of five stations with checkboxes: 'Avaya, SIP 2(66002)', 'Avaya, SIP 6(66006)', 'CM Station 1(65001)', 'CM Station 2(65002)', and 'H323 Staff(65000)'. All five are checked. At the bottom, '5 selected' is shown, and '5/7 Licenses Used' is displayed. Navigation buttons '< Back' and 'Next >' are at the bottom right. A 'Skip' link is in the bottom right corner of the window.

Station	Selected
Avaya, SIP 2(66002)	<input checked="" type="checkbox"/>
Avaya, SIP 6(66006)	<input checked="" type="checkbox"/>
CM Station 1(65001)	<input checked="" type="checkbox"/>
CM Station 2(65002)	<input checked="" type="checkbox"/>
H323 Staff(65000)	<input checked="" type="checkbox"/>

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.

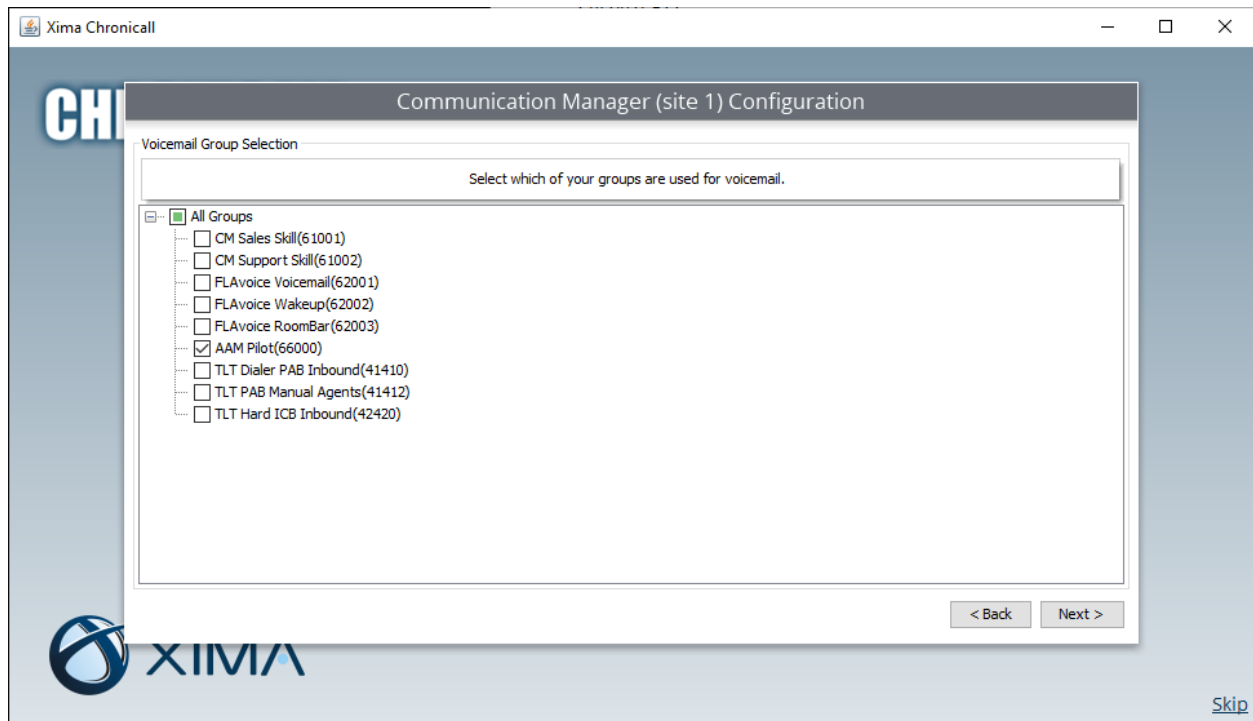
In the compliance testing, two skill groups from **Section 3** were selected, as shown below.





## 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.



## 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.

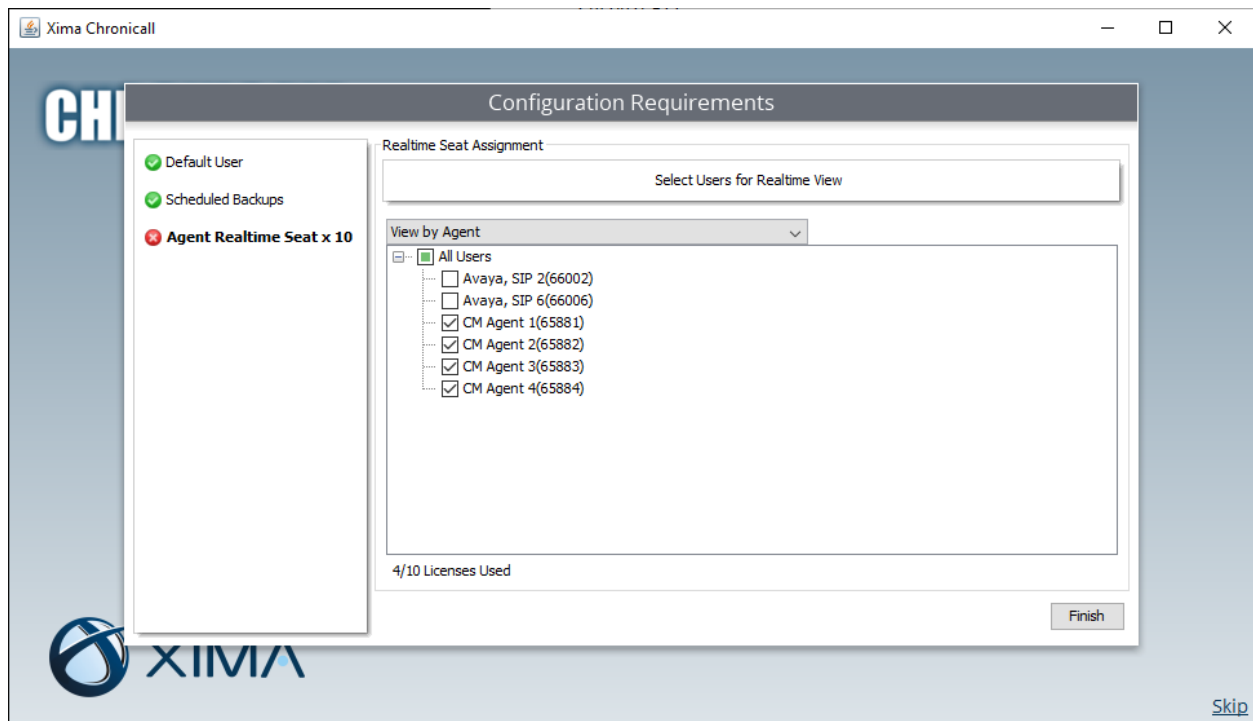
The screenshot shows a web application window titled "Xima Chronicall". The main content area is titled "Communication Manager (site 1) Configuration". Below this, there is a section titled "Aux Work Reason Codes". A message states: "If you use multiple Aux Work states then set the reason for each code so Chronicall can report reasons for each Aux event." Below this message is a table with two rows. The first row has a red 'X' icon, the number "1", and the text "Meeting". The second row has a red 'X' icon, the number "2", and the text "Lunch". At the bottom right of the table is an "Add" button. Below the table are two buttons: "< Back" and "Finish". In the bottom right corner of the window, there is a "Skip" link.

X	1	Meeting
X	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 Seat Assignment** screen and select all desired agent IDs to monitor.

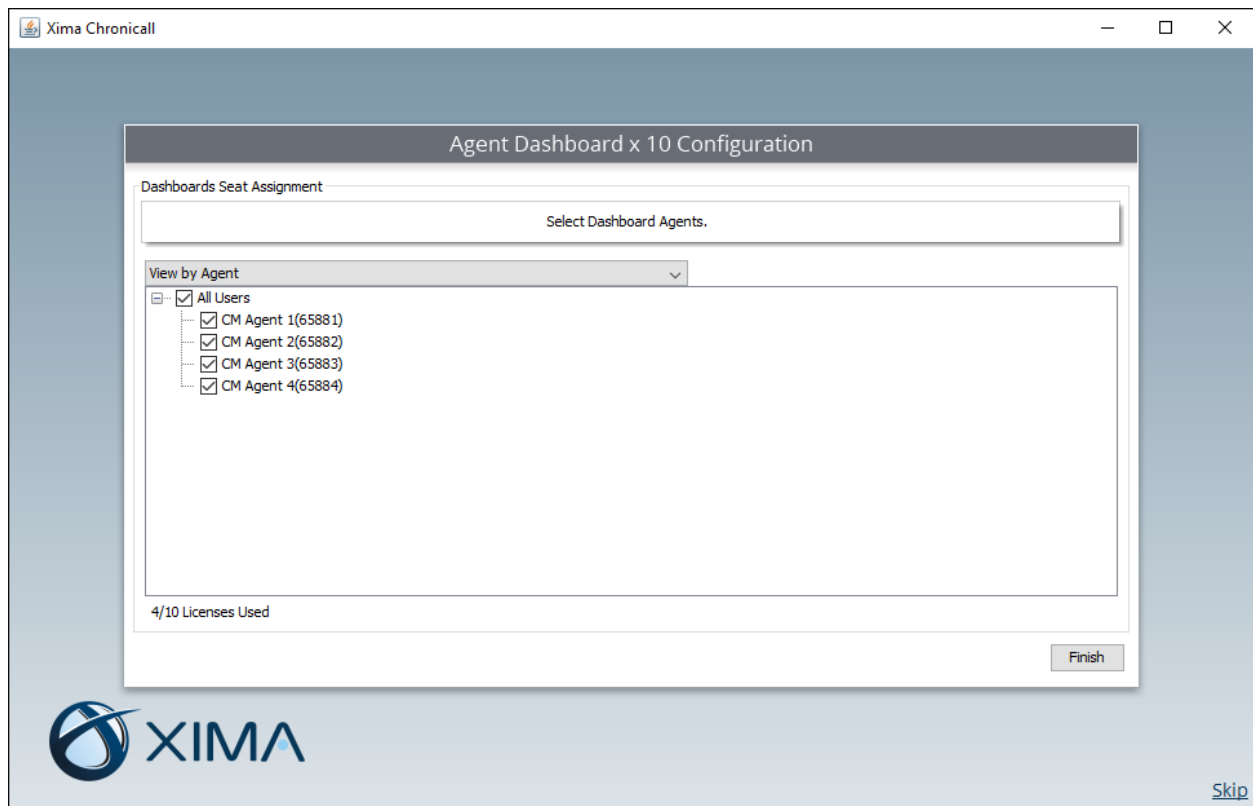
In the compliance testing, four agent IDs were selected, as shown below.



## 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 3** were selected, 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 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	11	no	aes7	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 “13”.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Dec 8 10:22:42 2020 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.2.1.0.6-0  
Server Date and Time: Tue Dec 08 10:47:14 EST 2020  
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

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	cm7	1	Talking	Fri Nov 27 10:52:28 2020	Online	18	13	302	288	30

OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

### 9.3. Verify Xima Chronicall

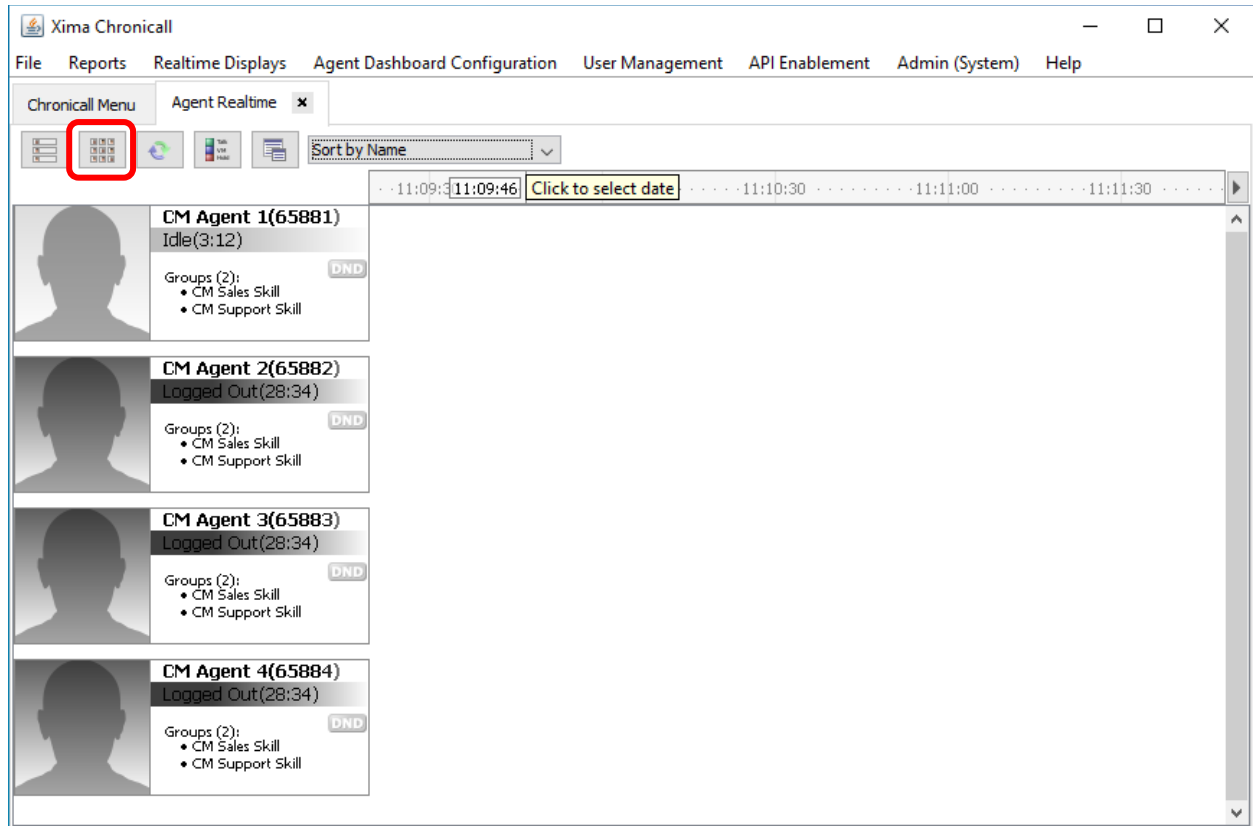
Follow the procedures in **Section 8.1** to launch the Chronicall Desktop client application, and log in using the appropriate credentials.

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

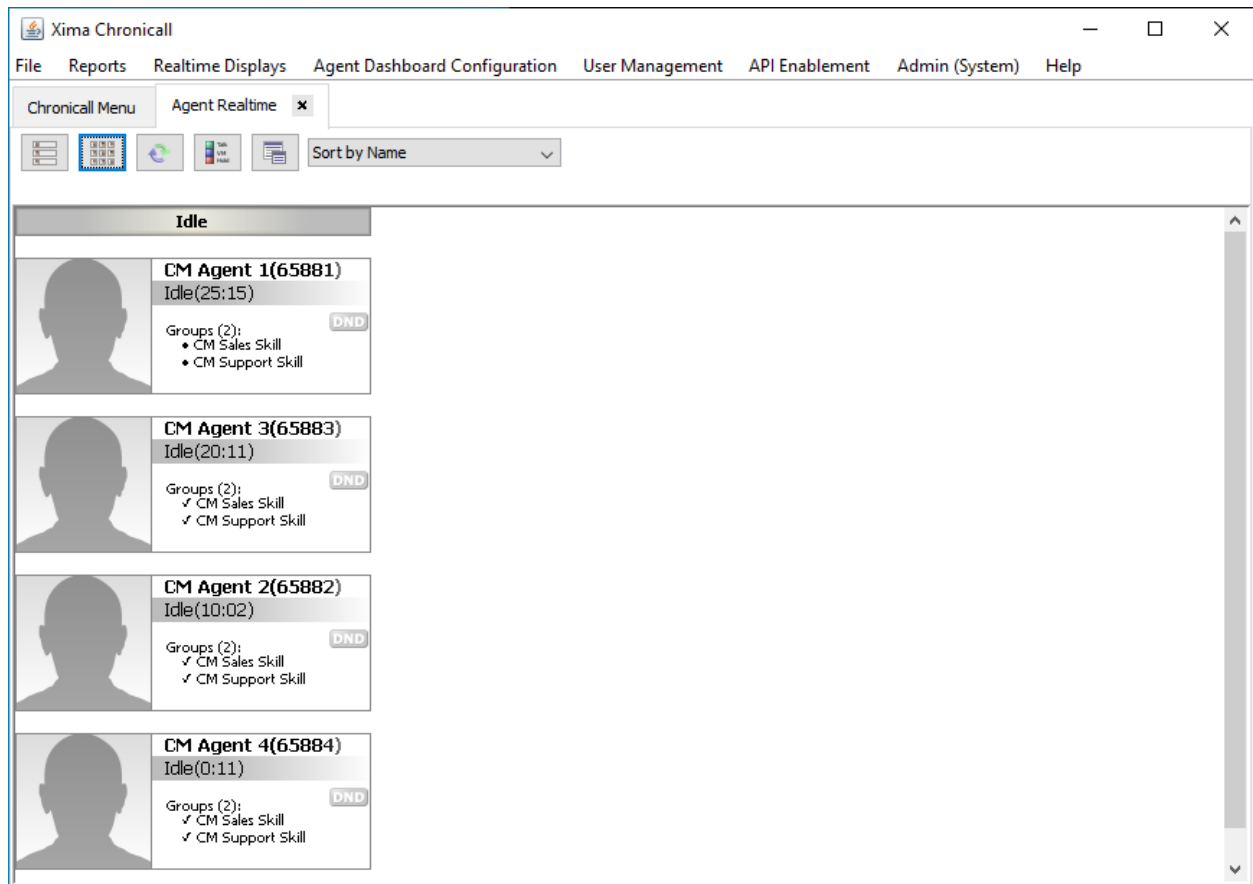


An **Agent Realtime** tab is created. Verify that all agent IDs selected for dashboard display from **Section 8.9** are shown below.

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.





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.

The screenshot shows the Xima Chronicall Agent Realtime dashboard. The interface includes a menu bar with options like File, Reports, Realtime Displays, Agent Dashboard Configuration, User Management, API Enablement, Admin (System), and Help. Below the menu, there's a 'Chronicall Menu' section with a 'Sort by Name' dropdown. The main area is divided into two columns: 'Idle' and 'Ringing'. The 'Idle' column lists three agents: CM Agent 1(65881) with an idle time of 26:55, CM Agent 3(65883) with 1:02, and CM Agent 2(65882) with 0:32. All three are associated with 'CM Sales Skill' and 'CM Support Skill' groups. The 'Ringing' column shows CM Agent 4(65884) with a ringing time of 0:22, also associated with the same skill groups. A 'DND' (Do Not Disturb) button is visible next to each agent's card.

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.

This screenshot shows the Xima Chronicall Agent Realtime dashboard after an agent has answered a call. The layout is identical to the previous one, but the 'Ringing' column has been replaced by a 'Talking' column. CM Agent 4(65884) is now in the 'Talking' state with a duration of 0:21. The 'Idle' column remains unchanged, showing the same three agents with their respective idle times and skill groups. The 'DND' button is still present for each agent.

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 screenshot shows the 'Cradle to Grave Criteria' window in the Xima Chronicall application. The window has a menu bar with 'File', 'Reports', 'Realtime Displays', 'Agent Dashboard Configuration', 'User Management', 'API Enablement', 'Admin (System)', and 'Help'. Below the menu bar, there are tabs for 'Chronicall Menu', 'Agent Realtime', and 'Cradle to Grave'. The 'Cradle to Grave' tab is active, displaying a calendar for December 2020. The date '8' is selected. Below the calendar, there is an 'Advanced...' button and an 'Optional Cradle to Grave Filters' section with an 'Add Filter' button. At the bottom, there are buttons for 'Save Filter(s)', 'Load Filter(s)', 'Execute' (highlighted with a red box), and 'Cancel'.

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.

The screenshot shows the 'Cradle to Grave' window in the Xima Chronicall application. The window has a menu bar with 'File', 'Reports', 'Realtime Displays', 'Agent Dashboard Configuration', 'User Management', 'API Enablement', 'Admin (System)', and 'Help'. Below the menu bar, there are tabs for 'Chronicall Menu', 'Agent Realtime', and 'Cradle to Grave'. The 'Cradle to Grave' tab is active, displaying a list of call details. The 'Call 15 - Inbound' entry is expanded, showing a detailed view of the call with columns for Call Info, Duration, Calling Party, Receiving Party, Location, Group, and Start Timestamp.

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 4.2 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 7, October 2020, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, November 2020, available at <http://support.avaya.com>.
4. *Chronicall Guide*, 4.2, available at <https://guide.ximasoftware.com/docs>.

---

**©2021 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).