



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

---

# **Application Notes for Xima Chronicall 3.10 with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Xima Chronicall 3.10 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0.

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 user 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 3.10 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0.

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 user 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 user 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, and 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 user actions such as hold/reconnect were performed from the user 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 Chronical:

- Chronical does not support TSAPI user credentials with the special character semicolon.
- By design, all VDNs obtained from the SMS connection are monitored by Chronical.
- For outbound calls to PSTN, internal calls, and abandoned incoming calls from PSTN, the cradle to grave report will reflect “Receiving Drop” regardless of which party initiated the drop.
- By design, do not disturb is only reflected in agent timeline against the agent stations and not agent IDs.
- This release of Chronical does not provide full agent timeline reflection and cradle to grave report support for call forwarding and service observing scenarios.
- For the blind conference scenarios, one of the three cradle to grave entries reported the conference-to agent as both the calling and the receiving party.
- For an outbound call scenario to the PSTN that was subsequently transferred to an agent, the agent realtime and cradle to grave report did not reflect the call as answered by the transferred-to agent. The attended transfer actions can be used as workaround.
- By design, when a user has two calls at the telephone, the agent timeline reflects the status of the call that the user is active on.
- When the Chronical server’s Ethernet connection was disrupted, the Chronical Desktop ceased reflecting activity updates, and remained so post Chronical server recovery. The workaround is to restart the Chronical Desktop for proper status and subsequent activities to be reflected.

## 2.3. Support

Technical support on Chronical can be obtained through the following:

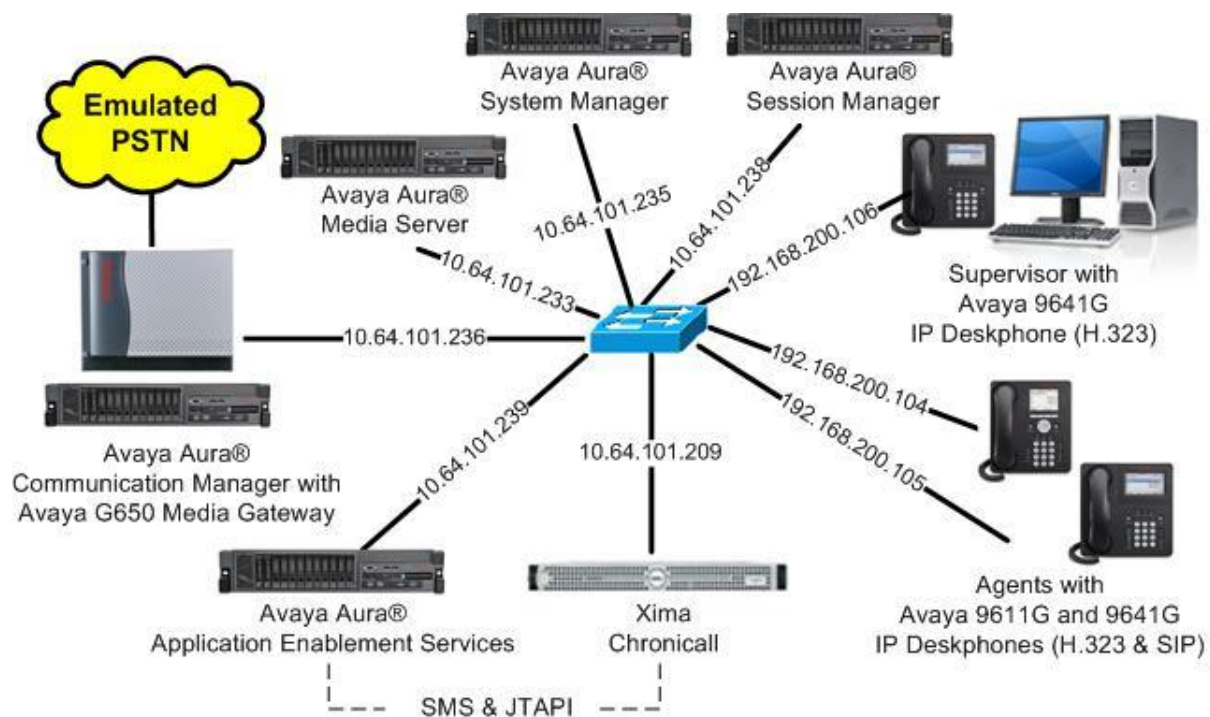
- **Phone:** (888) 944-XIMA
- **Email:** [support@ximasoftware.com](mailto:support@ximasoftware.com)
- **Web:** <http://www.ximasoftware.com/support>

### 3. Reference Configuration

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

The configuration of 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, 60002
Skill Group	61001, 61002
Supervisor Station	65000 (H.323)
Agent ID	65881, 65882
Agent Station	65001 (H.323), 66006 (SIP)



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.0.1 (8.0.1.0.0.822.25031)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.0.150
Avaya Aura® Application Enablement Services in Virtual Environment	8.0 (8.0.0.0.0.6-0)
Avaya Aura® Session Manager in Virtual Environment	8.0 (8.0.0.0.80035)
Avaya Aura® System Manager in Virtual Environment	8.0 (8.0.0.0.098174)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6604
Avaya 9641G IP Deskphone (SIP)	7.1.3.0.11
Xima Chronicall on Windows Server 2012 R2 Standard <ul style="list-style-type: none"><li>• Avaya JTAPI Windows Client (ecsjtapia.jar)</li></ul>	3.10 (6) 6.3.3.26
Xima Chronicall Desktop on Windows 10 Pro	3.10 (6)

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



### 5.3. Obtain Reason Codes

For call centers that use reason codes for aux work, 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

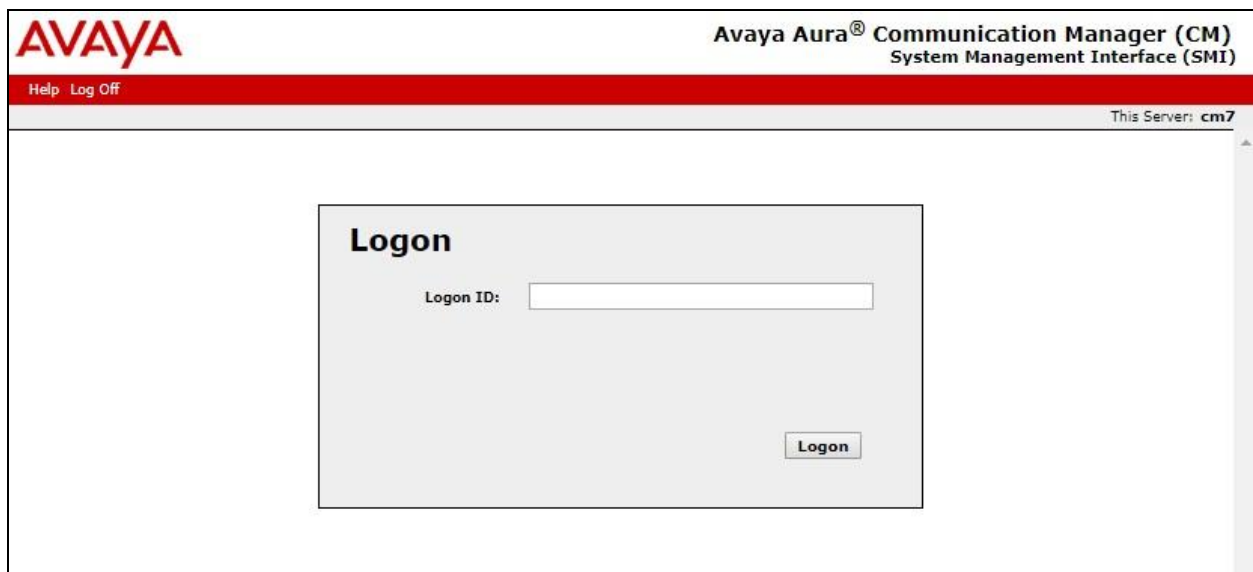
                                Aux Work/                    Logout
                                Interruptible?

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

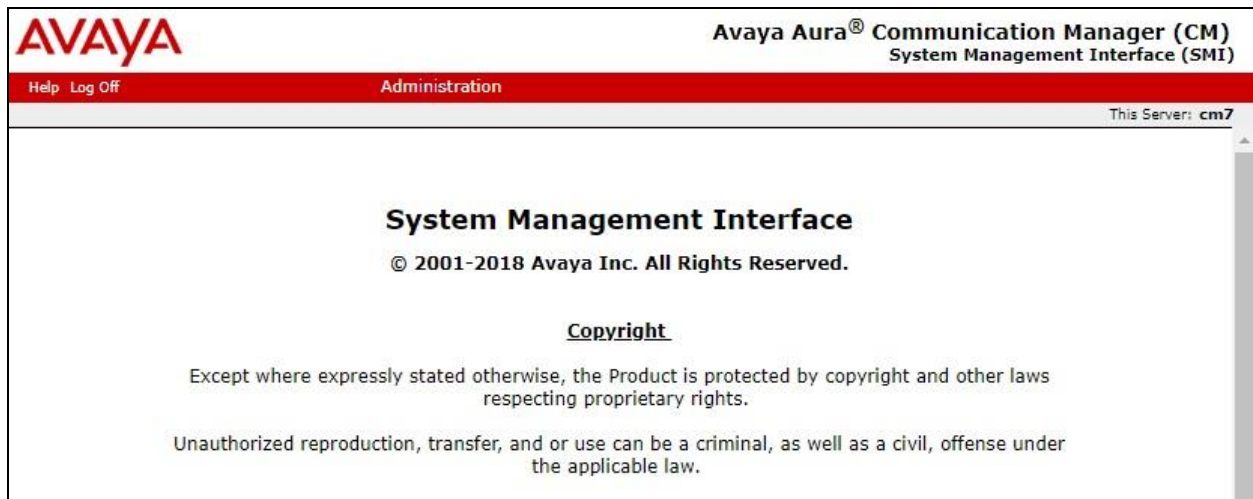
Default Reason Code:
```

### 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.

**AVAYA** Avaya Aura® Communication Manager (CM)  
System Management Interface (SMI)

Help Log Off Administration

Administration / Server (Maintenance) This Server: **cm7**

### 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
- ☐ Remove Login
- ☐ Lock/Unlock Login
- ☐ Add Group
- ☐ Remove Group

**Submit Help**

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 displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', and 'Administration'. Below this, a red banner shows 'Administration / Server (Maintenance)' and 'This Server: cm7'. The left sidebar contains a tree view with categories: 'Server Upgrades', 'Data Backup/Restore', 'Security', and 'Miscellaneous'. The 'Security' category is expanded, showing 'Administrator Accounts' as the selected option. The main content area is titled 'Administrator Accounts -- Add Login: Privileged Administrator'. It contains 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 text are several form fields: 'Login name' (text box with 'xima'), 'Primary group' (text box with 'susers'), 'Additional groups (profile)' (dropdown menu with 'prof18'), 'Linux shell' (text box with '/bin/bash'), 'Home directory' (text box with '/var/home/xima'), 'Lock this account' (checkbox), 'SAT Limit' (dropdown menu with 'none'), 'Date after which account is disabled-blank to ignore (YYYY-MM-DD)' (text box), 'Enter password' (password box with masked characters), 'Re-enter password' (password box with masked characters), and 'Force password change on next login' (radio buttons with 'No' selected). At the bottom of the form are three buttons: 'Submit', 'Cancel', and 'Help'.

## 6. Configure Avaya Aura® Application Enablement Services

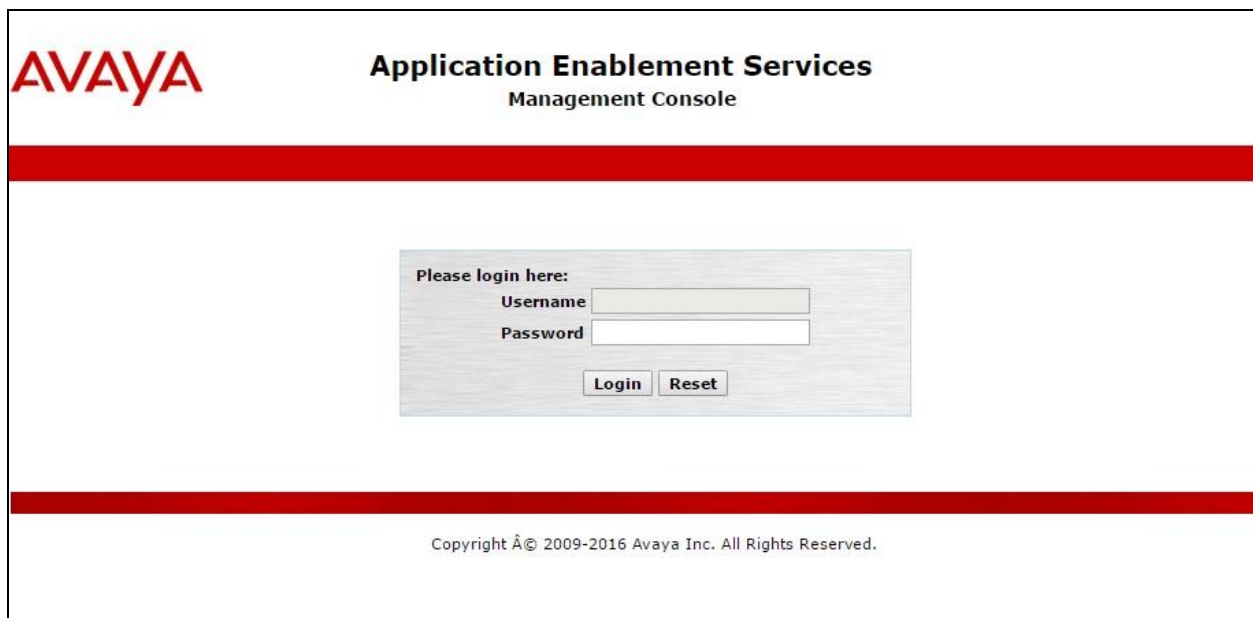
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. 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 thick red horizontal bar spans the width of the page. Below this bar, centered, is a light gray rectangular box containing the login form. The form has the heading "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located at the bottom of the page, above the footer text.

AVAYA

**Application Enablement Services**  
Management Console

Please login here:

Username

Password

Login Reset

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

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". On the right, a welcome message for the user is shown, including login details and system information. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area, titled "Welcome to OAM", provides an overview of the console's purpose and lists the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. Each domain is accompanied by a brief description of its function.

Welcome: User  
Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0  
Server Date and Time: Tue Jan 29 12:01:40 EST 2019  
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, titled "Licensing", provides instructions on how to set up and maintain the WebLM, including the use of the WebLM Server Address, WebLM Server Access, and Reserved Licenses. The left sidebar also shows the "WebLM Server Access" option under the "Licensing" section.

Welcome: User  
Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0  
Server Date and Time: Tue Jan 29 12:01:40 EST 2019  
HA Status: Not Configured

Licensing | Home | Help | Logout

**AE Services**  
**Communication Manager Interface**  
**High Availability**  
**Licensing**  
WebLM Server Address  
WebLM Server Access  
Reserved Licenses  
**Maintenance**  
**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 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰

Home 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
      - COMMUNICATION\_MANAGER
        - Call\_Center
        - Communication\_Manager
      - MESSAGING
        - Messaging
      - MSR

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

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

License installed on: October 13, 2018 3:09:09 AM +00:00

License File Host IDs: V4-42-5D-06-BF-08-01

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16

### 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 header includes the AVAYA logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and system status. The left navigation pane shows a tree structure with "AE Services" expanded, and "TSAPI Links" selected. The main content area displays the "TSAPI Links" screen, which includes 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" screen displayed. The left navigation pane shows "AE Services" expanded, and "TSAPI Links" selected. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The Link field is set to 1, Switch Connection is set to cm7, Switch CTI Link Number is set to 1, ASAI Link Version is set to 9, and Security is set to Unencrypted. 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 information are shown in the top right corner. The main navigation pane on the left lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The 'Add User' form on the right contains several fields: 'User Id' (xima), 'Common Name' (xima), 'Surname' (xima), 'User Password' (masked with dots), 'Confirm Password' (masked with dots), 'Admin Note' (empty), 'Avaya Role' (None), 'Business Category' (empty), 'Car License' (empty), 'CM Home' (empty), 'Css Home' (empty), 'CT User' (Yes), 'Department Number' (empty), 'Display Name' (empty), 'Employee Number' (empty), 'Employee Type' (empty), 'Enterprise Handle' (empty), and 'Given Name' (empty). Fields marked with an asterisk are required.

Welcome: User  
Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0  
Server Date and Time: Tue Jan 29 12:01:40 EST 2019  
HA Status: Not Configured

User Management | User Admin | Add User Home | Help | Logout

AE Services  
Communication Manager Interface  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Service Admin  
User Admin  
Add User  
Change User Password  
List All Users  
Modify Default Users  
Search Users  
Utilities  
Help

Add User

Fields marked with \* can not be empty.

\* User Id xima  
\* Common Name xima  
\* Surname xima  
\* 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

## 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 that 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". A user information box in the top right corner shows: "Welcome: User", "Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0", "Server Date and Time: Tue Jan 29 12:01:40 EST 2019", and "HA Status: Not Configured".

The main navigation bar is red and contains "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar menu is expanded to "Security", which is highlighted in dark grey. Under "Security", the following options are listed: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), and Control (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

## 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**.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0  
Server Date and Time: Tue Jan 29 12:01:40 EST 2019  
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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart 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-S#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 side of the header, there is a welcome message for the user, including the last login time (Tue Jan 29 11:43:48 2019), the number of failed login attempts (0), the host name/IP (aes7/10.64.101.239), the server offer type (VIRTUAL\_APPLIANCE\_ON\_VMWARE), the SW version (8.0.0.0.0.6-0), the server date and time (Tue Jan 29 12:01:40 EST 2019), and the 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" (highlighted).

The main content area is titled "Tlinks" and shows a single Tlink entry with the name "AVAYA#CM7#CSTA-S#AES7". There is a "Delete Tlink" button 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 Jan 29 11:43:48 2019 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: 8.0.0.0.6-0  
Server Date and Time: Tue Jan 29 12:01:40 EST 2019  
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 2/19/2019

Solution & Interoperability Test Lab Application Notes  
©2019 Avaya Inc. All Rights Reserved.

21 of 43  
Xima-Chron-AES8

## 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 and the title "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0", "Server Date and Time: Tue Jan 29 12:01:40 EST 2019", and "HA Status: Not Configured".

The main navigation bar shows "AE Services | SMS | SMS Properties" and includes links for "Home | Help | Logout". The left sidebar contains a tree view with the following items: "AE Services" (expanded), "CVLAN", "DLG", "DMCC", "SMS" (expanded), "SMS Properties" (selected), "TSAPI", "TWS", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help".

The "SMS Properties" configuration panel on the right contains the following fields and values:

- 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

At the bottom of the panel are three buttons: "Apply Changes", "Restore Defaults", and "Cancel".



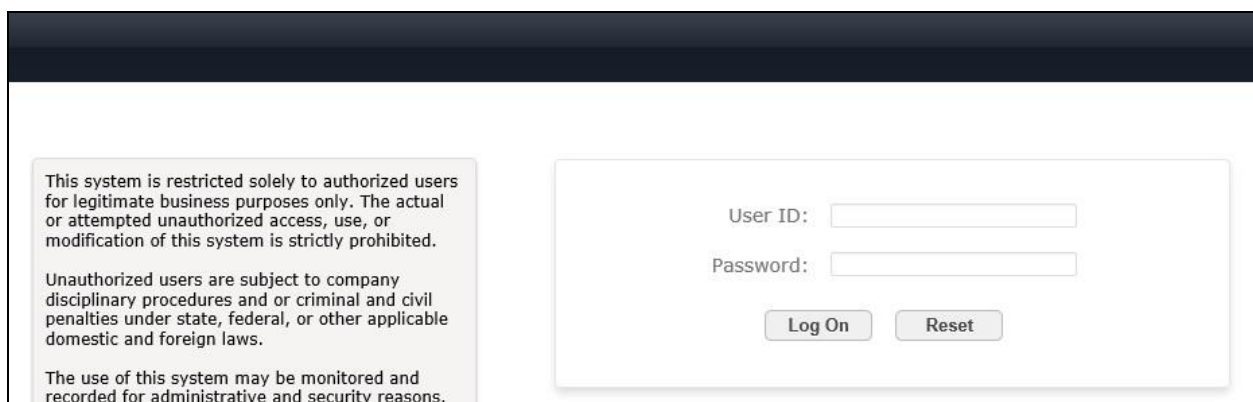
## 7. Configure Avaya Aura® Session Manager

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

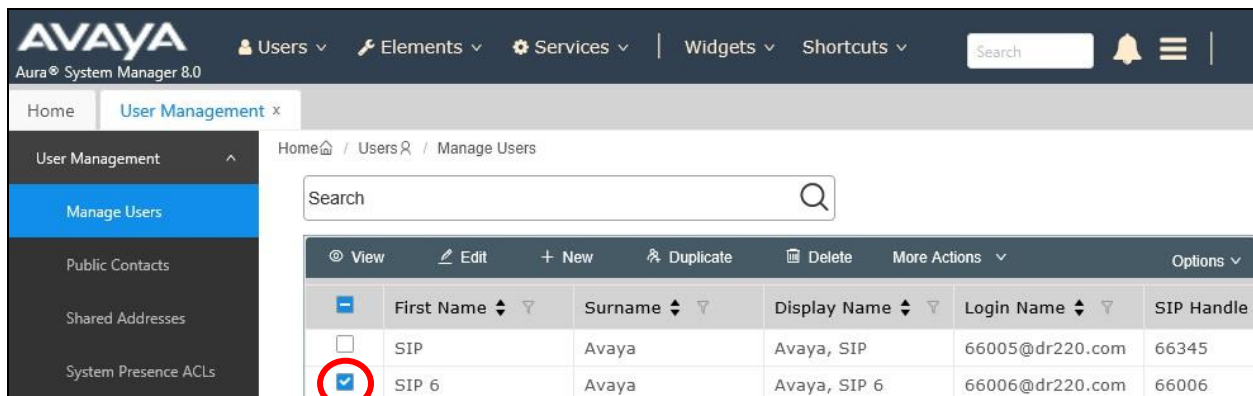
### 7.1. Launch System Manager

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**. Select **User Management → Manage Users** 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 “66006”, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	Avaya	Avaya, SIP	66005@dr220.com	66345
<input checked="" 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 8.0 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.0", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The left sidebar shows the "User Management" menu with options like "Manage Users", "Public Contacts", "Shared Addresses", "System Presence ACLs", and "Communication Profile...". The main content area is titled "User Profile | Edit | 66006@dr220.com" and has tabs for Identity, Communication Profile, Membership, and Contacts. The "Communication Profile" tab is active, showing fields for "System" (DR-CM), "Profile Type" (Endpoint), "Extension" (66006), "Set Type" (9641SIPCC), "Port" (S00018), "Preferred Handle" (Select), and "Sip Trunk" (aar). The "CM Endpoint Profile" is highlighted in the left sidebar. The "Extension" field has an Editor icon circled in red.



In the pop-up screen, locate the **Type of 3PCC Enabled** parameter, and select “Avaya” from the drop-down list as shown below. Retain the existing values in the remaining fields.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains navigation links: Home, User Management (selected), Manage Users, Public Contacts, Shared Addresses, System Presence ACLs, and Communication Profile... The main content area is titled 'User Profile | Edit | 66006@dr220.com'. It features tabs for Identity, Communication Profile (selected), Membership, and Contacts. Below the tabs are several sections: General Options (G) with fields for Class of Restriction (COR), Emergency Location Ext, Tenant Number, SIP Trunk, Coverage Path 1, Lock Message, and Multibyte Language; Feature Options (F) with fields for Class Of Service (COS), Message Lamp Ext, Type of 3PCC Enabled (highlighted with a red box and set to 'Avaya'), Coverage Path 2, Localized Display Name, and Enable Reachability for Station Domain Control; Site Data (S); Abbreviated Call Dialing (A); Enhanced Call Fwd (E); Button Assignment (B); Profile Settings (P); and Group Membership (M). At the bottom, there are sections for Primary Session Manager (IPv4: 10.64.101.238, IPv6: ) and Secondary Session Manager.

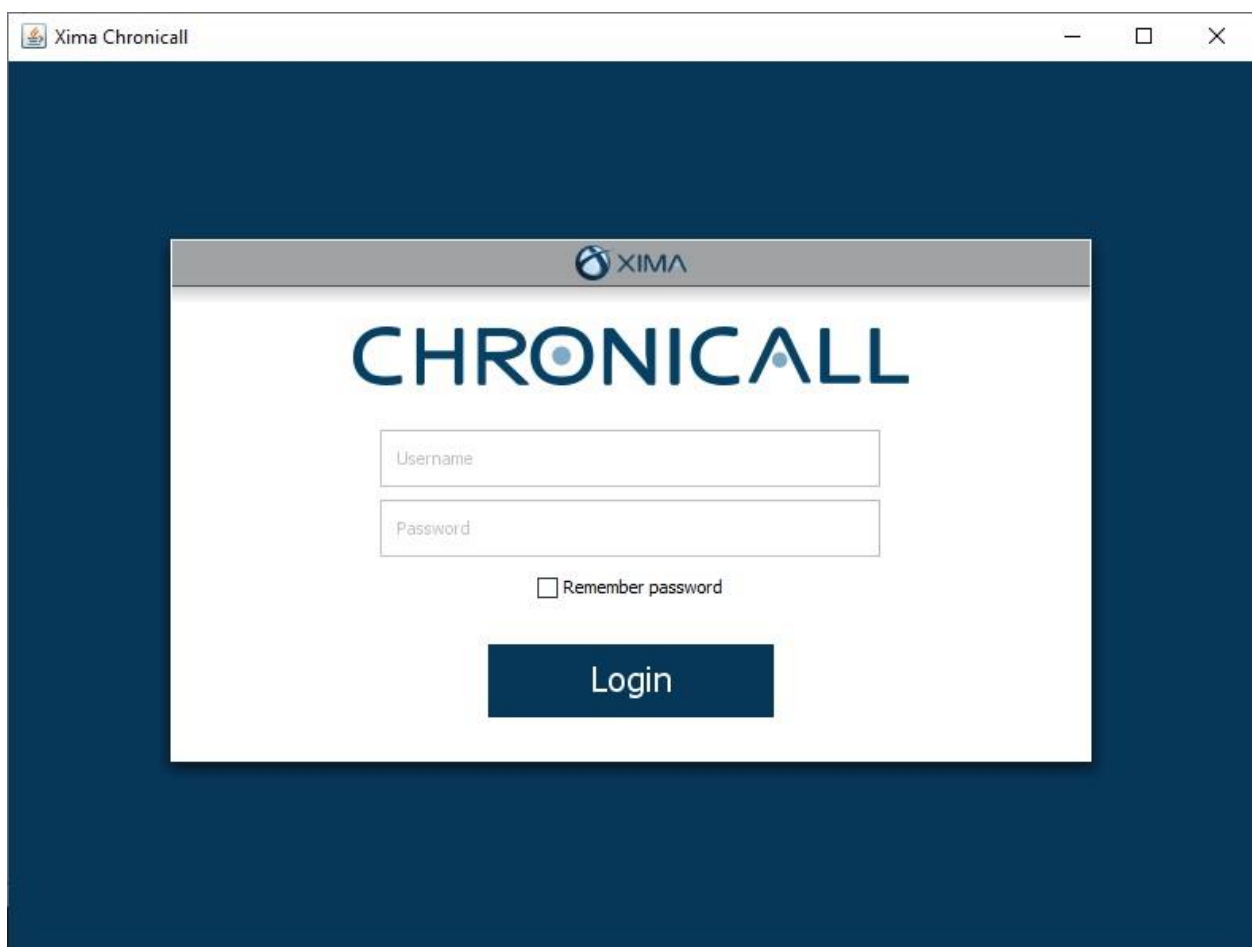
## 8. Configure Xima Chronicall

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

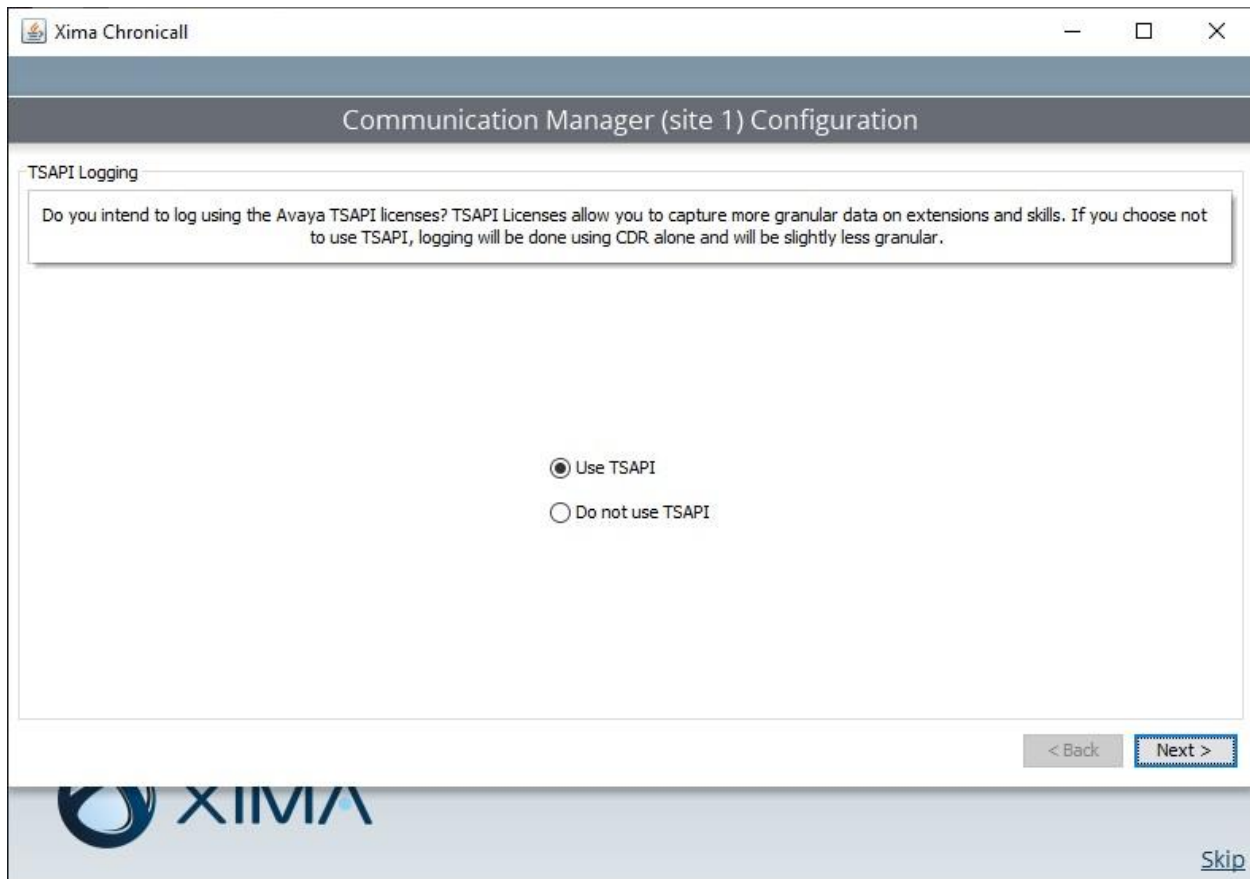
- Launch Chronicall Desktop
- Administer SMS settings
- Administer TSAPI settings
- Administer seat assignment
- Administer license assignments
- Administer voicemail group
- Administer reason codes
- Administer realtime seat assignment
- Administer dashboards seat assignment

### 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 standard window controls. The main heading is "Communication Manager (site 1) Configuration". Below this, the "TSAPI Logging" section contains a text box with 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 the text box are two radio button options: "Use TSAPI" (which is selected) and "Do not use TSAPI". At the bottom right of the configuration area are "< Back" and "Next >" buttons. The footer of the window features the XIMA logo on the left and a "Skip" link on the right.

## 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 account login name from **Section 5.4**.
- **CM Password:** The 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

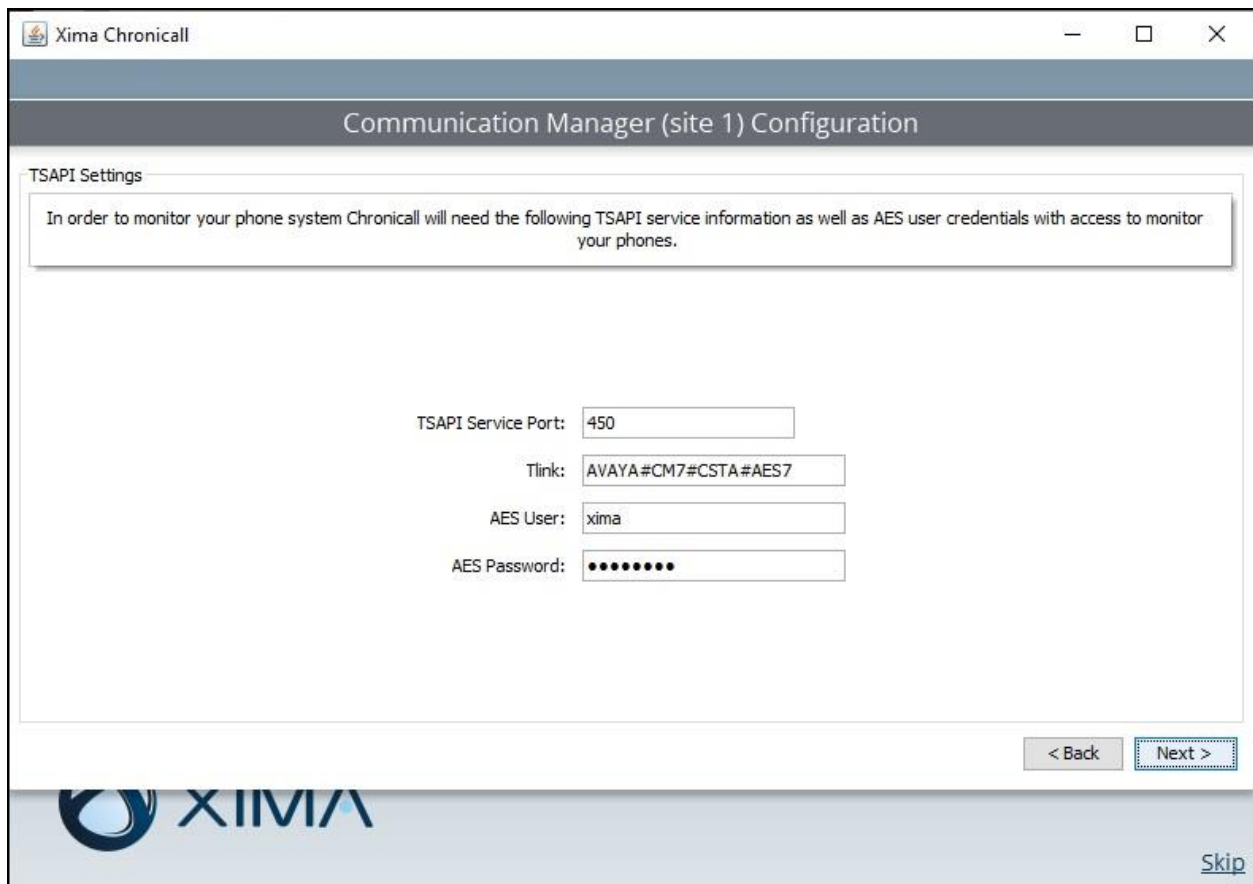
[Skip](#)

### 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 standard window controls. The main heading is "Communication Manager (site 1) Configuration". Below this, a section titled "TSAPI Settings" contains an informational message: "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 the message 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 form area are two buttons: "< Back" and "Next >". The footer of the window displays the XIMA logo on the left and a "Skip" link on the right.

## 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 shown below.

The screenshot shows the 'Xima Chronicall' application window. The title bar reads 'Xima Chronicall'. The main header is 'Communication Manager (site 1) Configuration'. Below this is the 'Chronicall Seat Assignment' section. A message box states: '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.' Below the message is a search bar with the placeholder text 'Search: (i.e. "200-299, 400-499" or "Agent Name(204)")'. A list of items follows, each with a checkbox and a label: 'Avaya, SIP 4(66004)', 'Avaya, SIP 6(66006)', 'CM 7 Station 4(65004)', 'CM Agent 1(65881)', 'CM Agent 2(65882)', 'CM Agent 3(65883)', 'CM Station 1(65001)', 'CM Station 3(65003)', and 'CM Supervisor(65000)'. The checkboxes for 'Avaya, SIP 6(66006)', 'CM Agent 1(65881)', 'CM Agent 2(65882)', 'CM Station 1(65001)', and 'CM Supervisor(65000)' are checked. Below the list are 'Select All' and 'Deselect All' buttons. To the right of these buttons, it says '5 / 500 selected'. At the bottom right are '< Back' and 'Next >' buttons. The 'Next >' button is highlighted. The XIMA logo is at the bottom left, and a 'Skip' link is at the bottom right.

## 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 Chronical, in this case “5”.

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.

The screenshot shows the 'Xima Chronical' application window with the title bar. The main content area is titled 'Communication Manager (site 1) Configuration'. Below this, there is a section for 'TSAPI License Assignment'. A text box contains instructions: 'Enter the maximum number of TSAPI licenses Chronical can use and select which stations and skills to monitor. Each monitored station or skill will use a TSAPI license while Chronical is logging. Note that if a station is not assigned a Chronical seat then it will not be available in this list.' Below the text box, there is a 'Max TSAPI Licenses:' label followed by a spinner control set to '5'. There are two tabs: 'Stations' (selected) and 'ACD Groups'. Below the tabs is a search bar with the placeholder text 'Search: (i.e. "200-299, 400-499" or "Agent Name(204)")'. Below the search bar is a list of three items, each with a checked checkbox: 'Avaya, SIP 6(66006)', 'CM Station 1(65001)', and 'CM Supervisor(65000)'. Below the list are two buttons: 'Select All' and 'Deselect All', both with dropdown arrows. To the right of these buttons, it says '3 selected'. At the bottom right of the list area, it says '5/5 Licenses Used'. At the very bottom of the window, there is a footer with the XIMA logo on the left and a 'Skip' link on the right. Navigation buttons '< Back' and 'Next >' are located at the bottom right of the main content area.

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

The screenshot shows the 'Xima Chronicall' application window titled 'Communication Manager (site 1) Configuration'. The 'TSAPI License Assignment' section is active, displaying 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.'

The 'Max TSAPI Licenses' is set to 5. Below this, the 'ACD Groups' tab is selected, showing a tree view with 'All ACD Groups' expanded. The following skill groups are listed with checkboxes:

- ☒ CM Sales Skill(61001)
- ☒ CM Support Skill(61002)
- ☐ TLT Dialer PAB Inbound(41410)
- ☐ TLT PAB Manual Agents(41412)
- ☐ TLT Hard ICB Inbound(42420)

The status '5/5 Licenses Used' is shown at the bottom right of the list. Navigation buttons '< Back' and 'Next >' are at the bottom right. The XIMA logo is in the bottom left, and a 'Skip' link is in the bottom right corner.



## 8.6. Administer Voicemail Group

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

The screenshot shows a web application window titled "Xima Chronicall". The main heading is "Communication Manager (site 1) Configuration". Below this is a section titled "Voicemail Group Selection" with a subtitle "Select which of your groups are used for voicemail." A tree view on the left shows "All Groups" expanded, listing several hunt groups with checkboxes: "CM Sales Skill(61001)", "CM Support Skill(61002)", "AAM Pilot(66000)" (which is checked), "TLT Dialer PAB Inbound(41410)", "TLT PAB Manual Agents(41412)", and "TLT Hard ICB Inbound(42420)". At the bottom right of the configuration area are "< Back" and "Next >" buttons. The footer of the application displays the XIMA logo and a "Skip" link.

## 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.

Xima Chronicall

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.

<input type="checkbox"/>	1	Meeting
<input type="checkbox"/>	2	Lunch

Add

< Back Finish

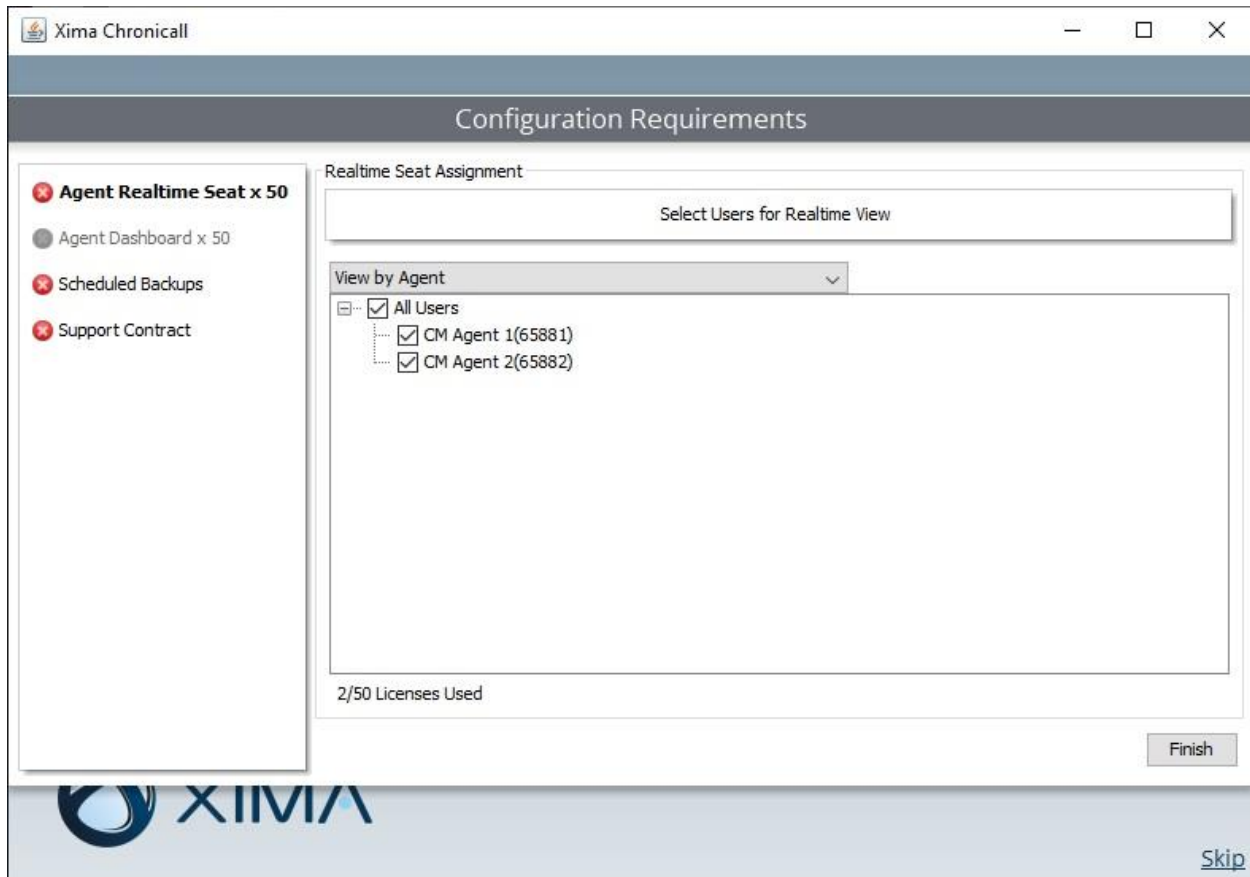
XIMA

[Skip](#)

## 8.8. Administer Realtime Seat Assignment

For deployments with Chronicall Realtime licenses, the **Realtime Seat Assignment** screen is displayed next, listing the selected agent IDs from **Section 8.4**. Select the desired agent IDs to monitor.

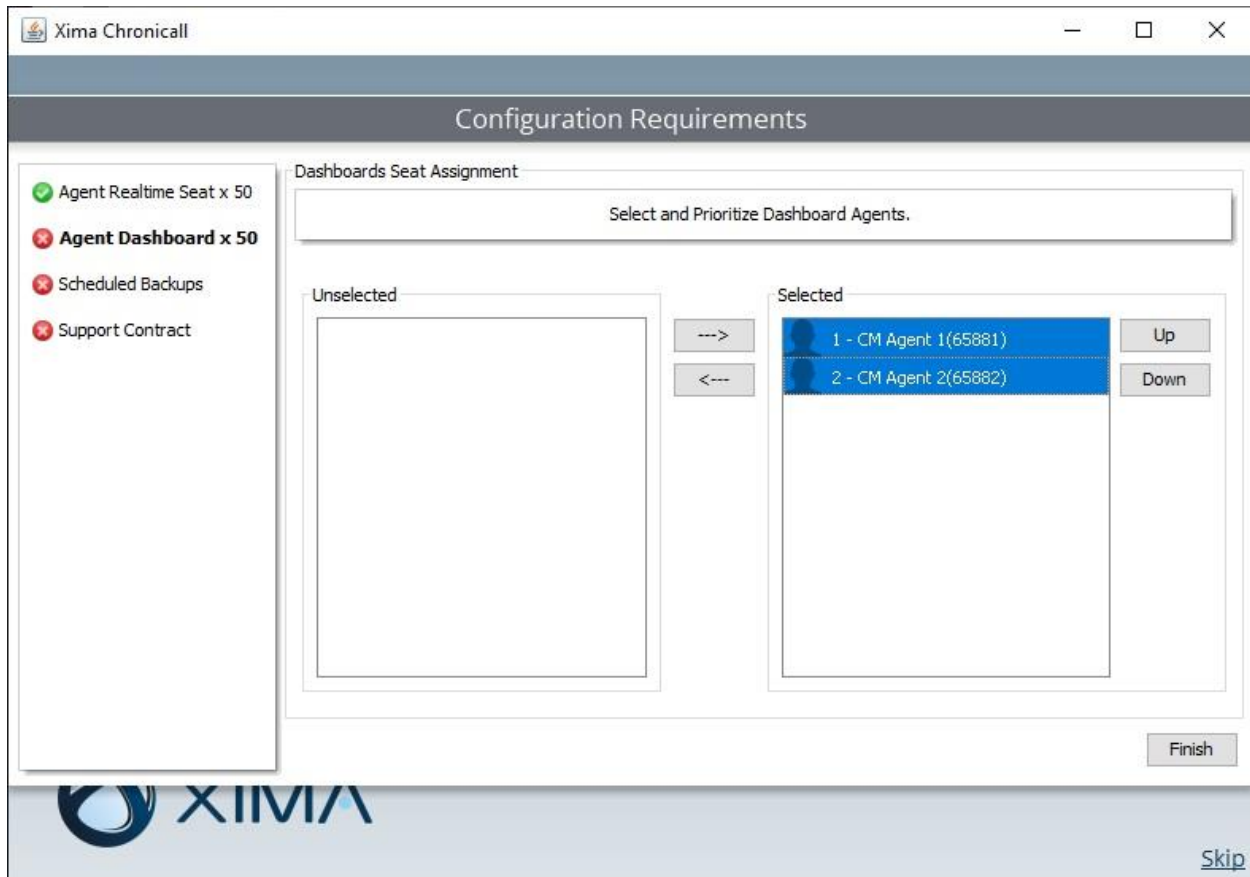
In the compliance testing, two agents IDs were selected, as shown below.



## 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**. Move the desired agent IDs from the **Unselected** to the **Selected** column for monitoring via dashboard.

In the compliance testing, both agent IDs 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	9	no	aes7	established	152	157

### 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 below). 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 “11”.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Jan 29 11:43:48 2019 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: 8.0.0.0.6-0  
Server Date and Time: Tue Jan 29 12:01:40 EST 2019  
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

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	Wed Jan 16 17:03:01 2019	Online	18	11	157	152	30

Online Offline

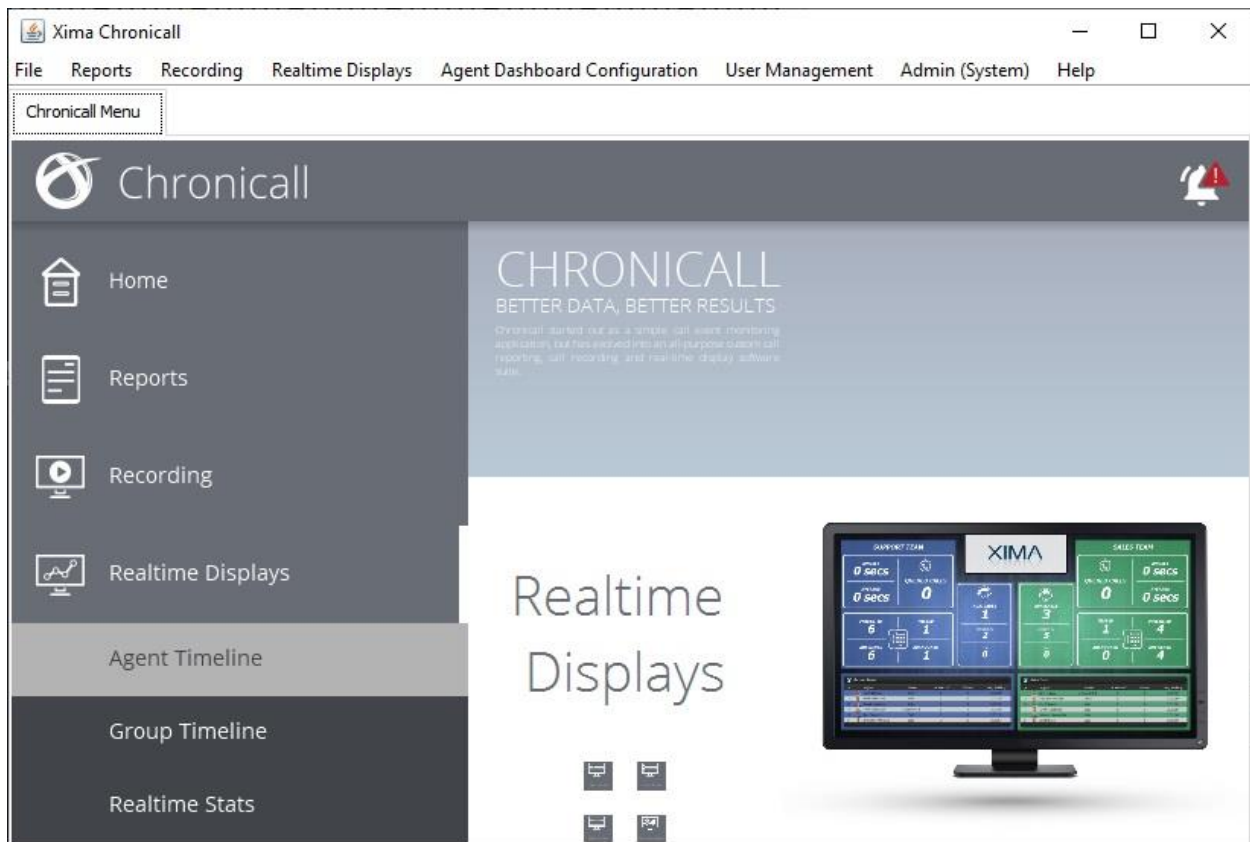
For service-wide information, choose one of the following:

TSAPI Service Status TLink Status User Status

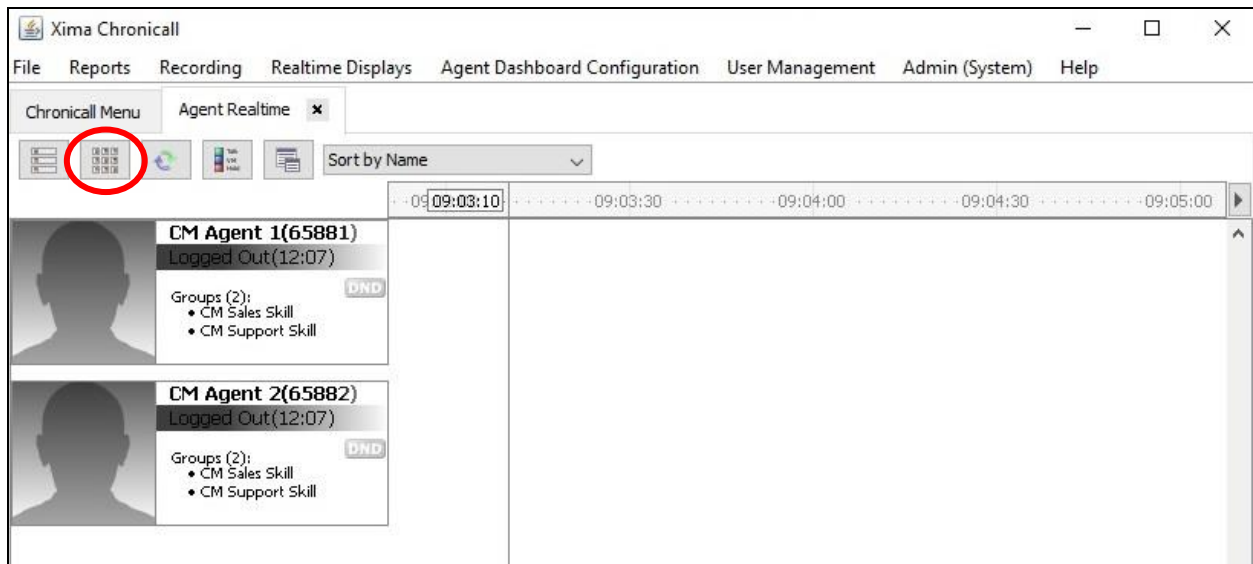
### 9.3. Verify Xima Chronicall

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

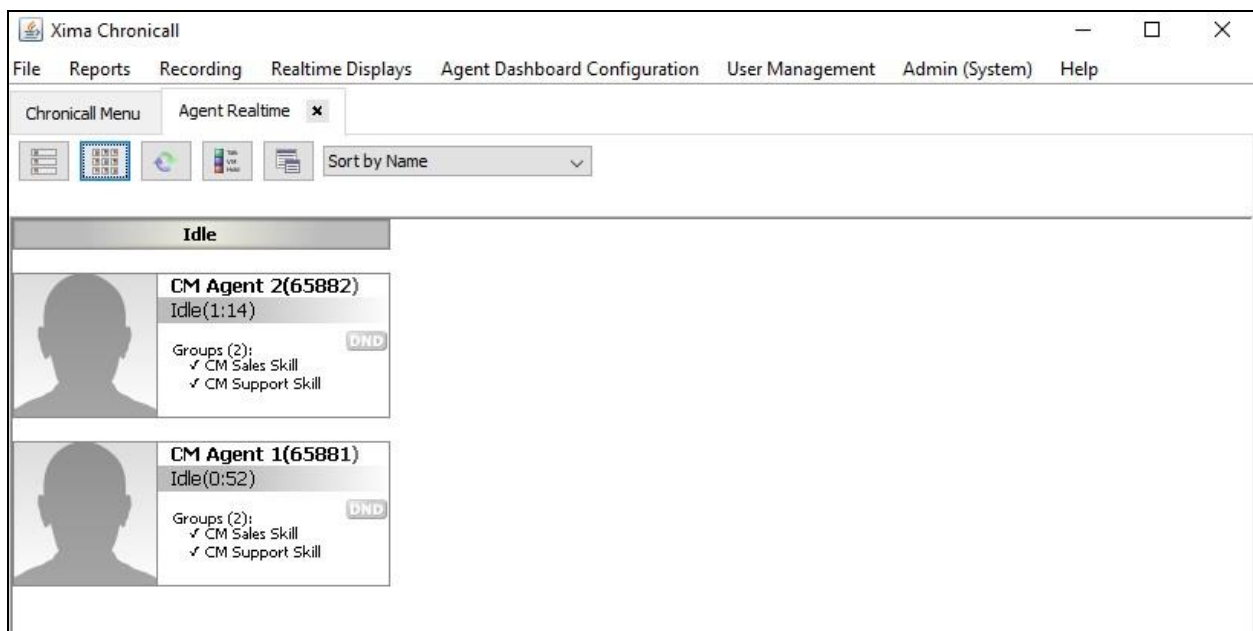
The **Chronicall Menu** tab is automatically created, as shown below. Select **Realtime Displays** → **Agent Timeline**.



An **Agent Realtime** tab is created. Click the **Show Live Columns** icon, and verify that the selected agents for monitoring from **Section 8.8** are shown below.



Log the 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 top menu includes File, Reports, Recording, Realtime Displays, Agent Dashboard Configuration, User Management, Admin (System), and Help. The main area is divided into two columns: Idle and Ringing. Under the Idle column, CM Agent 1(65881) is shown with an Idle(1:21) timer and a DND button. Under the Ringing column, CM Agent 2(65882) is shown with a Ringing(0:02) timer and a DND button. Both agents are associated with the phone number 9089532103 and have skills in CM Sales Skill and CM Support Skill.

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

The screenshot shows the Xima Chronicall Agent Realtime dashboard. The top menu includes File, Reports, Recording, Realtime Displays, Agent Dashboard Configuration, User Management, Admin (System), and Help. The main area is divided into two columns: Idle and Talking. Under the Idle column, CM Agent 1(65881) is shown with an Idle(1:36) timer and a DND button. Under the Talking column, CM Agent 2(65882) is shown with a Talking(0:10) timer and a DND button. Both agents are associated with the phone number 9089532103 and have skills in CM Sales Skill and 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 screenshot shows the 'Cradle to Grave Criteria' window in the Xima Chronicall application. The window has a menu bar with 'File', 'Reports', 'Recording', 'Realtime Displays', 'Agent Dashboard Configuration', 'User Management', '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, showing a calendar for January 2019. The 29th is selected. Below the calendar, there is an 'Advanced...' button and a section for 'Optional Cradle to Grave Filters'. At the bottom, there are buttons for 'Save Filter(s)', 'Load Filter(s)', 'Execute' (circled in red), 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 6”. Expand the entry, and verify that the reported details reflected the last call with proper values in the respective columns.

The screenshot shows the 'Cradle to Grave' window in the Xima Chronicall application. The window has a menu bar with 'File', 'Reports', 'Recording', 'Realtime Displays', 'Agent Dashboard Configuration', 'User Management', '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, showing a list of calls. The 'Call 6 - Inbound' entry is expanded, showing details for the call, including duration, calling party, receiving party, group, location, and start timestamp.

Call Info	Duration	Calling Party	Receiving Party	Group	Location	Start Timestamp
<b>Calls (5 total)</b>						
Call 1 - Internal	0:00:08	Avaya, SIP 6(66006)				Jan 29, 2019 9:05:41 AM
Call 2 - Internal	0:00:04	CM Agent 2(65882)				Jan 29, 2019 9:05:50 AM
Call 3 - Internal	0:00:09	CM Agent 2(65882)	CM Supervisor(65000)			Jan 29, 2019 9:07:52 AM
Call 4 - Internal	0:00:06	CM Station 1(65001)				Jan 29, 2019 9:08:13 AM
Call 6 - Inbound	0:00:36	(908) 953-2103	CM Agent 2(65882)	CM Sales Skill	Bernardsville, New Jersey	Jan 29, 2019 9:09:42 AM
Vector	0:00:00	(908) 953-2103	CM Sales Vec			Jan 29, 2019 9:09:42 AM
Ringing	0:00:06	(908) 953-2103	CM Agent 2(65882)	CM Sales Skill		Jan 29, 2019 9:09:42 AM
Talking	0:00:29	(908) 953-2103	CM Agent 2(65882)	CM Sales Skill		Jan 29, 2019 9:09:49 AM
Receiving Dro	0:00:00	(908) 953-2103	CM Agent 2(65882)	CM Sales Skill		Jan 29, 2019 9:10:18 AM

## 10. Conclusion

These Application Notes describe the configuration steps required for Xima Chronicall 3.10 to successfully interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. 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 8.0, Issue 2.1, November 2018, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.0, Issue 1, July 2018, available at <http://support.avaya.com>.
3. *Avaya CM – Server Installation*, v3.10.6, available at <https://guide.ximasoftware.com/docs/avaya-cm-server-installation>.

---

**©2019 Avaya Inc. All Rights Reserved.**

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

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