



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

Abstract

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

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

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

The SMS interface is used by Xima Chronicall to obtain configured contact center resources on Avaya Aura® Communication Manager via Avaya Aura® Application Enablement Services to facilitate configuration of Xima Chronicall.

The JTAPI interface is used by Xima Chronicall to monitor VDNs, skills, and agent 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 Avaya Aura® 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 sends SMS requests to obtain configured agents, skill groups, stations, uniform dial plan, VDNs, and vectors, and sends JTAPI/TSAPI requests to monitor VDNs, skills, and agent 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.

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 service 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, blind/attended transfer, blind/attended conference, voicemail coverage, voicemail retrieval, queuing, park/unpark, service observing, EC500, 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 Chronical:

- Chronical does not support TSAPI user credentials with the special character semi colon.
- 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.
- Upon launching Chronical Desktop, the agent timeline will place users that have not had any activities in the past 15 minutes under the “Miscellaneous” column.
- By design, do not disturb and call forwarding are 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 the following features: park/unpark, call pickup, call forwarding, bridging, and service observing. For example, when a call for user-1 is picked up by user-2, the Agent Timeline reflects user-1 in “Talking” state instead of user-2, and the subsequently cradle to grave report only reflects call with user-2.
- 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.
- The agent timeline reflected users that are active on conferences under the “Miscellaneous” column until all parties from the conference have dropped.
- 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.

2.3. Support

Technical support on Chronical can be obtained through the following:

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

3. Reference Configuration

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

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

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent ID	65881, 65882
Agent Station	65001, 66002

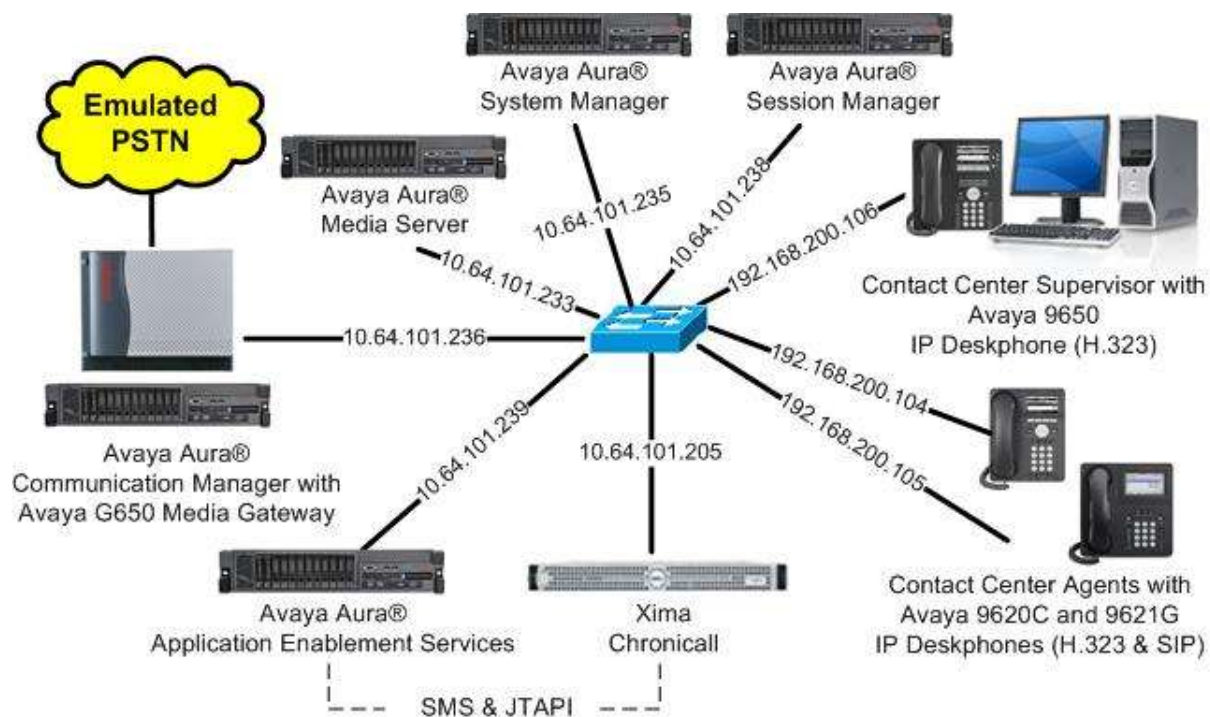


Figure 1: Compliance Testing Configuration

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	7.0.1 (7.0.1.0.0.441.23012)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.1.15)
Avaya Aura® Session Manager in Virtual Environment	7.0.1 (7.0.1.0.701007)
Avaya Aura® System Manager in Virtual Environment	7.0.1 (7.0.1.0.064859)
Avaya 9620C & 9650 IP Deskphones (H.323)	3.260A
Avaya 9621G IP Deskphone (SIP)	7.0.0.39
Xima Chronicall on Windows Server 2012 R2 Standard <ul style="list-style-type: none">Avaya JTAPI Windows Client (ecsjtapia.jar)	3.7 (55) NA 6.3.9600
Xima Chronicall Desktop on Windows 7 Professional	3.7 (55) SP 1

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

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

5.2. Administer CTI Link

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

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 60111		
Type: ADJ-IP		
		COR: 1
Name: AES CTI Link		

5.3. Obtain Reason Codes

For contact 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/ Interruptible?	Logout
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
Reason Code 8:		/n
Reason Code 9:		/n

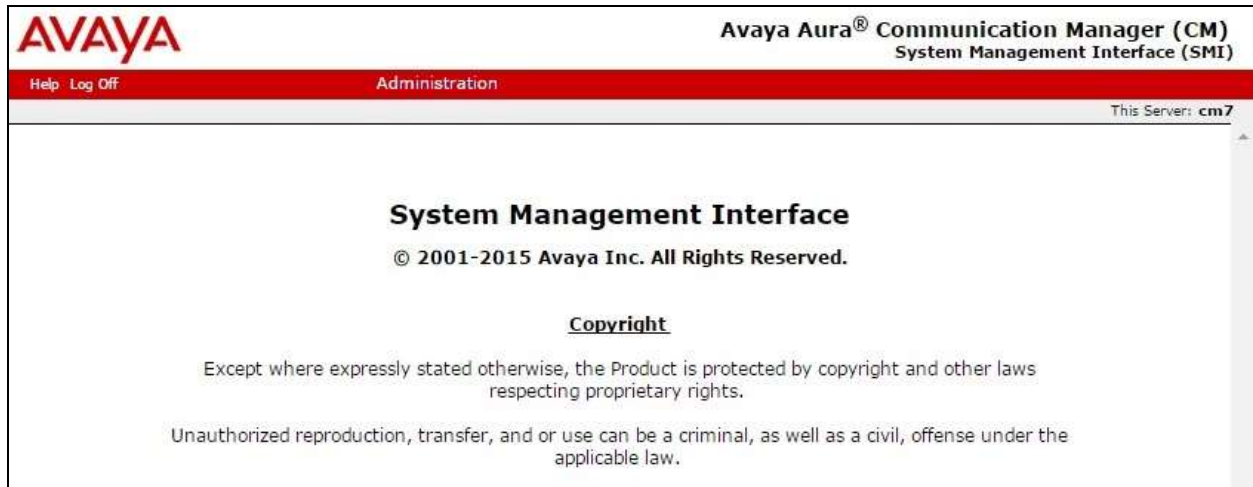
Default Reason Code:

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 screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) login page. The header includes the Avaya logo, the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and links for "Help" and "Log Off". The main content area features a "Logon" box with fields for "Logon ID:" and "Password:", and a "Logon" button. The text "This Server: cm7" is visible in the top right corner.

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) for server cm7. The left sidebar contains a navigation menu with categories like Static Routes, Server Upgrades, IPSI Firmware Upgrades, Data Backup/Restore, and Security. The main content area is titled "Administrator Accounts" and includes a description: "The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups." Below this, a "Select Action:" section offers several options: "Add Login" (selected), "Privileged Administrator", "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 fields for "Change Login", "Remove Login", "Lock/Unlock Login", "Add Group", and "Remove Group", each with a dropdown menu labeled "Select Login" or "Select Group". At the bottom are "Submit" and "Help" buttons.

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 or key**, and **Re-enter password or key**. 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 the Avaya logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and links for "Help" and "Log Off". Below this, a red banner indicates the current section is "Administration".

The left sidebar contains a tree view of system management functions, including Alarms, SNMP, Diagnostics, Server, Server Configuration, Server Upgrades, IPSI Firmware Upgrades, and Data Backup/Restore. The "Administration / Server (Maintenance)" path is selected.

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."

The form contains the following fields and options:

- Login name:** xima
- Primary group:** susers
- Additional groups (profile):** prof18
- Linux shell:** /bin/bash
- Home directory:** /var/home/xima
- Lock this account:** ☐
- SAT Limit:** none
- Date after which account is disabled-blank to ignore (YYYY-MM-DD):** (empty field)
- Select type of authentication:**
 - ☐ ASG: Auto-generate key
 - ☐ ASG: enter key
 - ☒ Password
- Enter password or key:** (masked with dots)
- Re-enter password or key:** (masked with dots)
- Force password/key change on next login:**
 - ☒ No
 - ☐ Yes

At the bottom of the form are three buttons: "Submit", "Cancel", and "Help".

6. Configure Avaya Aura® Application Enablement Services

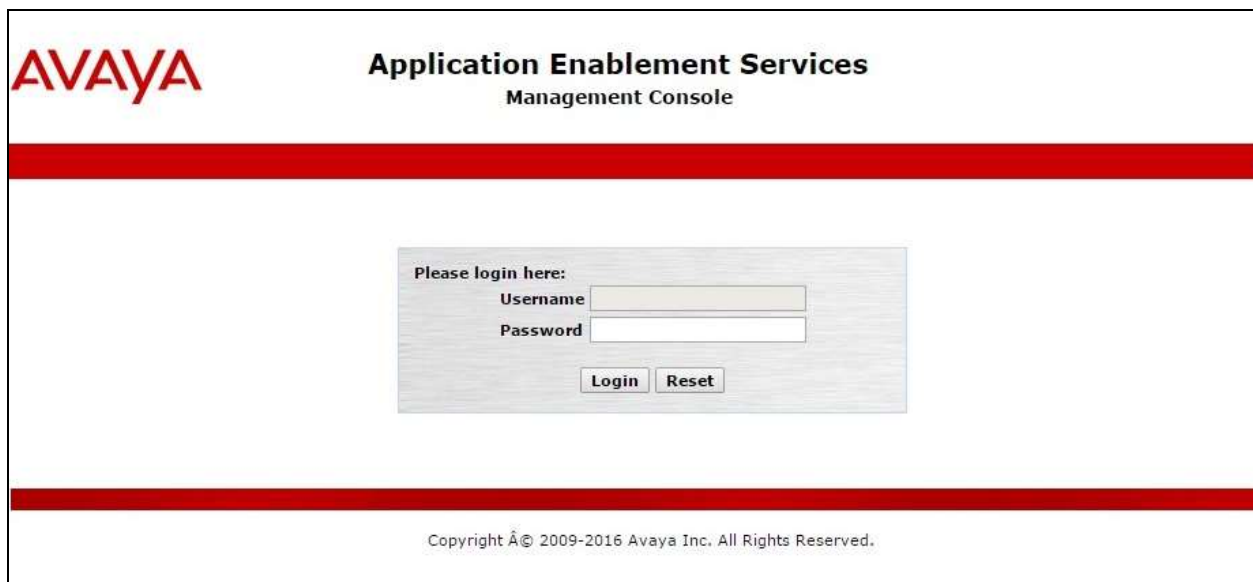
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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 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". At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2016 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". On the right, a welcome message for the user is shown, including login details and system status. 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 Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 09:46:36 EDT 2016
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 need to use the following: 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 Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 09:46:36 EDT 2016
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 7.0

Last Logged on at: June 14, 2016 9:09 AM
Log off

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
Application Enablement
View license capacity
View peak usage
COMMUNICATION_MANAGER
Communication Manager
Call Center
Configure Centralized Licensing
MSR
Media Server
SessionManager
SessionManager
Uninstall license
Server properties
Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 7 - SID: 10503000 **Standard**

You are here: Licensed Products > Application Enablement > View License Capacity

License installed on: October 12, 2015 3:21:49 PM +04:00

License File Host IDs: V1-19-37-80-8F-8F

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASA VALUE_AES_CVLAN_ASA	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;d380g3;d385g1;d385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; IXP_001, BasicUnrestricted; DMCUnrestricted; IXM_001, BasicUnrestricted; DMCUnrestricted; PC_001, BasicUnrestricted; DMCUnrestricted; CIE_001, BasicUnrestricted; DMCUnrestricted; OSPC_001, BasicUnrestricted; DMCUnrestricted; YP_001, BasicUnrestricted; DMCUnrestricted; SAMETIME_001, VALUE_AES CCE_001, BasicUnrestricted, AdvancedUnresb CSI_T1_001, BasicUnrestricted, AdvancedUnn CSI_T2_001, BasicUnrestricted, AdvancedUnn AVAYAVERINT_001, BasicUnrestricted, Advan DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Ager BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Ager BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

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, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. 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".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
------	-------------------	-------------------	-------------------	----------

[Add Link](#) [Edit Link](#) [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 "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. 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 7, and "Security" is set to Unencrypted. There are buttons for "Apply Changes" and "Cancel Changes".

Add TSAPI Links

Link: 1
Switch Connection: cm7
Switch CTI Link Number: 1
ASAI Link Version: 7
Security: Unencrypted

[Apply Changes](#) [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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 09:46:36 EDT 2016
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 Idchronicall

* Common Namechronicall

* Surnamechronicall

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked, as shown below.

In the event that the security database is used by the customer with parameter already enabled, then follow reference [2] to configure access privileges for the Chronical 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 welcome message in the top right corner states: "Welcome: User", "Last login: Tue Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0", "Server Date and Time: Tue Jun 14 09:46:36 EDT 2016", and "HA Status: Not Configured".

The main navigation pane on the left lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and Control. The Security Database section is selected, and the Control sub-item is active.

The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. It contains two checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Both checkboxes are unchecked. 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**.

AVAYA Application Enablement Services
Management Console

Welcome: User
Last login: Tue Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 09:46:36 EDT 2016
HA Status: Not Configured

Maintenance | Service ControllerHome | 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#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, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows the "Tlinks" page with a single Tlink named "AVAYA#CM7#CSTA#AES7" and a "Delete Tlink" button.

Welcome: User
Last login: Tue Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 09:46:36 EDT 2016
HA Status: Not Configured

Security | Security Database | Tlinks

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

Tlinks

Tlink Name
AVAYA#CM7#CSTA#AES7
Delete Tlink

6.8. Administer Ports

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

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 09:46:36 EDT 2016
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 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

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 user status area on the right showing "Welcome: User", "Last login: Tue Jun 14 09:25:20 2016 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: 7.0.1.0.1.15-0", "Server Date and Time: Tue Jun 14 09:46:36 EDT 2016", and "HA Status: Not Configured".

The main navigation pane on the left shows a tree structure under "AE Services":

- CVLAN
- DLG
- DMCC
- SMS** (selected)
 - SMS Properties** (selected)
 - TSAPI
 - TWS
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

The right pane displays the "SMS Properties" configuration form with the following fields and values:

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

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

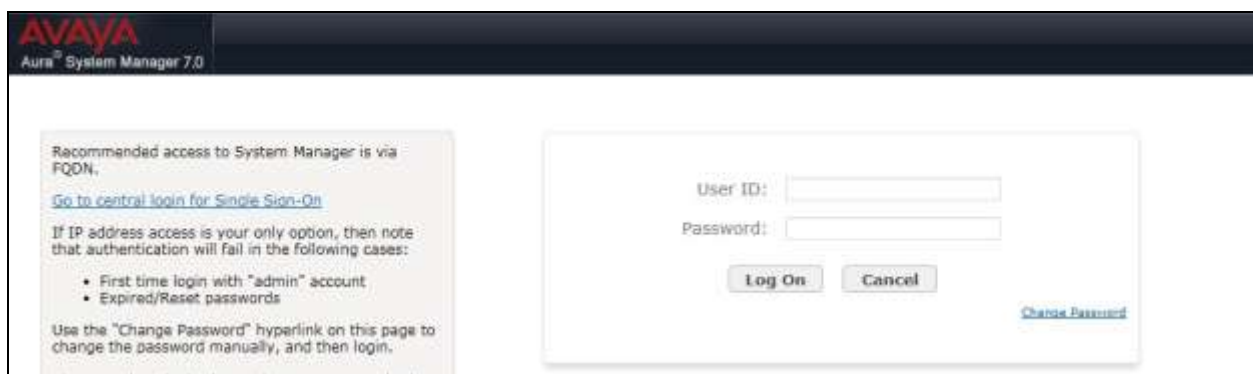
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

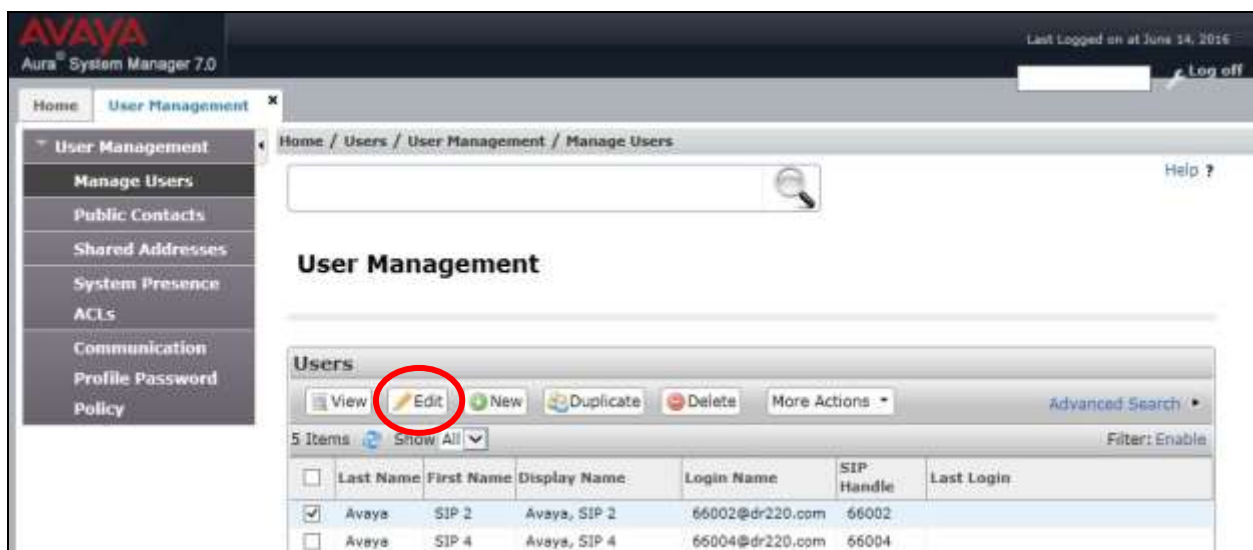
7.1. Launch System Manager

Access the System Manager web-based 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 **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3** that will be monitored by Chronicall, in this case “66002”, and click **Edit**.



The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA
Aura System Manager 7.0

Last Logged on at: June 14, 2016 9:32 AM
Log off

Home / User Management / Manage Users

User Profile Edit: 66002@dr220.com

Commit & Continue Commit Cancel

Identity **Communication Profile** Membership Contacts

Communication Profile

Communication Profile Password: ***** Edit

New Delete Done Cancel

Name

Primary

Select: None

Name: Primary

Default: ☒

Communication Address

New Delete Done Cancel

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

Select: All, None

☒ Session Manager Profile

☒ CM Endpoint Profile

System: DR220-CM7-ES

Profile Type: Endpoint

Use Existing Endpoints: ☐

Extension: 66002

Endpoint Editor

Template: Select/Reset

Set Type: 9621SIPCC

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent stations to be monitored by Chronicall.

AVAYA
Aura System Manager 7.0

Last Logged in at June 14, 2016 9:32 AM
Log off

Home User Management

User Management

Home / Users / User Management / Manage Users

Help ?

Done Cancel

[Save As Template]

System DR220-CM7-ES Extension 66002

Template Select Set Type 96215IPCC

Port 500004 Security Code

Name Avaya, SIP 2

General Options (G) Feature Options (F) Site Data (S) Abbreviated Call Dialing (A)

Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR) 1 * Class Of Service (COS) 1

* Emergency Location Ext 66002 * Message Lamp Ext. 66002

* Tenant Number 1

* SIP Trunk Q ear Type of 3PCC Enabled Avaya

Coverage Path 1 1 Coverage Path 2

Lock Message ☐ Localized Display Name Avaya, SIP 2

Multibyte Language Not Applicable Enable Reachability for Station Domain Control System

* Required

Done Cancel

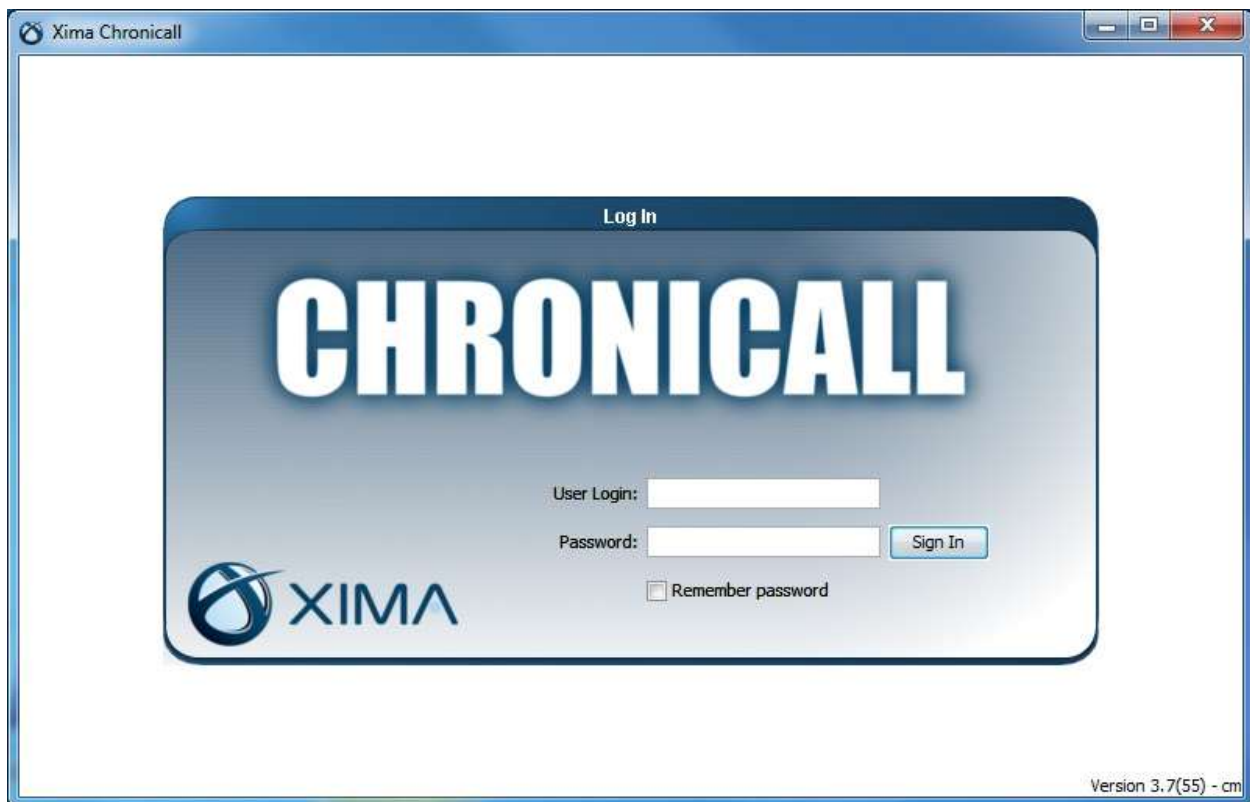
8. Configure Xima Chronicall

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

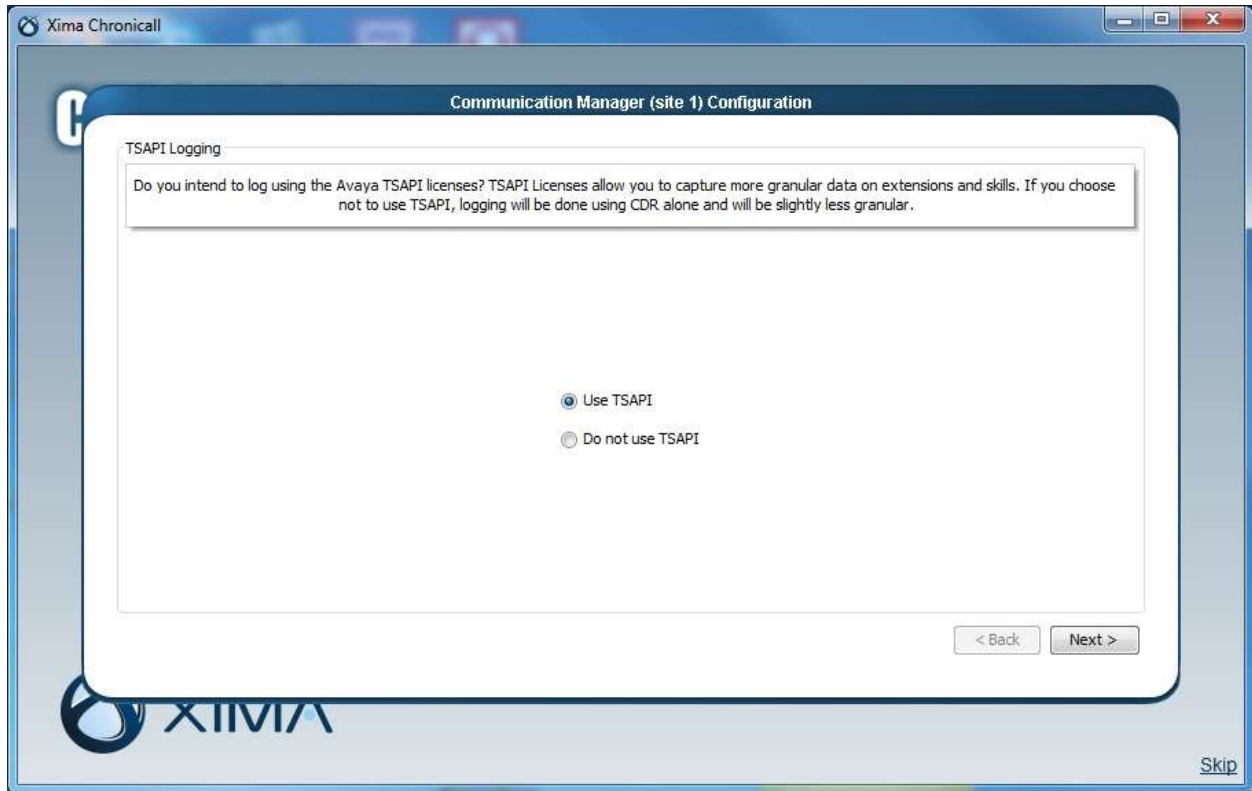
- Launch Chronicall Desktop
- Administer SMS settings
- Administer TSAPI settings
- Administer seat assignment
- Administer license assignments
- Administer voicemail group
- Administer reason codes
- Administer realtime seat assignment
- Administer dashboard seat assignment

8.1. Launch Chronicall Desktop

From a PC where Chronicall Desktop is installed, select **All Programs → Xima Software → Chronicall (browserless)** 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**.



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

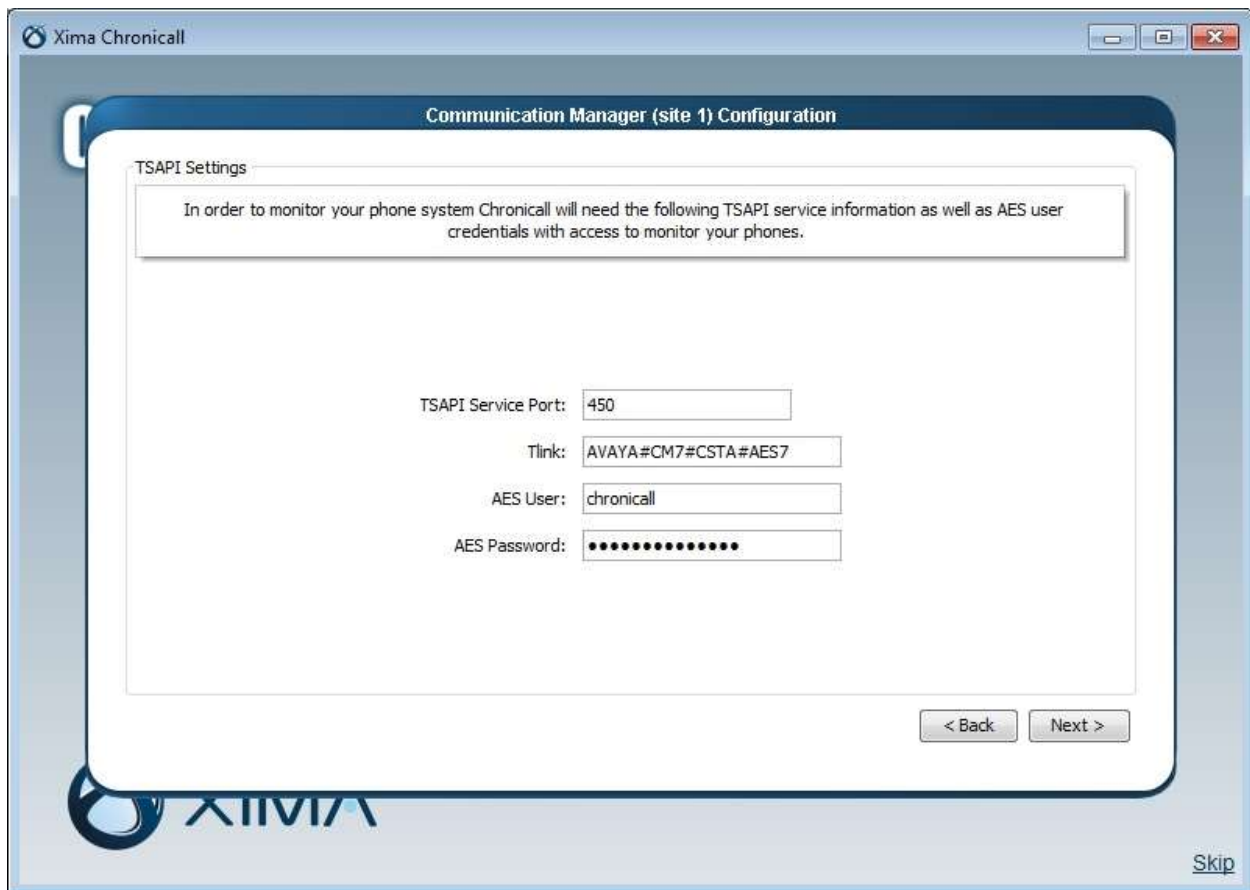
[Skip](#)

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 window titled "Xima Chronicall" with a sub-header "Communication Manager (site 1) Configuration". Inside, the "TSAPI Settings" section contains a 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 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 "chronicall", and "AES Password" with a masked password "••••••••••". At the bottom right of the configuration area are two buttons: "< Back" and "Next >". 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 agents obtained via the SMS connection to Application Enablement Services.

Scroll the screen as necessary, and select all desired stations and agents for Chronicall to log data for. In the compliance testing, all stations and agent IDs from **Section 3** were selected, as shown below.

Communication Manager (site 1) Configuration

Chronicall Seat Assignment

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

Search: (i.e. "200-299, 400-499" or "Agent Name(204)")

<input checked="" type="checkbox"/>	Avaya, SIP 2(66002)
<input type="checkbox"/>	Avaya, SIP 4(66004)
<input checked="" type="checkbox"/>	CM7 Agent 1(65881)
<input checked="" type="checkbox"/>	CM7 Agent 2(65882)
<input checked="" type="checkbox"/>	CM7 Station 1(65001)
<input type="checkbox"/>	CM7 Station 2(65002)
<input type="checkbox"/>	CM7 Station 3(65003)
<input type="checkbox"/>	CM7 Station 5(65006)
<input checked="" type="checkbox"/>	CM7 Supervisor(65000)

Select All ▼ Deselect All ▼ 5 / 100 selected

< Back Next >

[Skip](#)

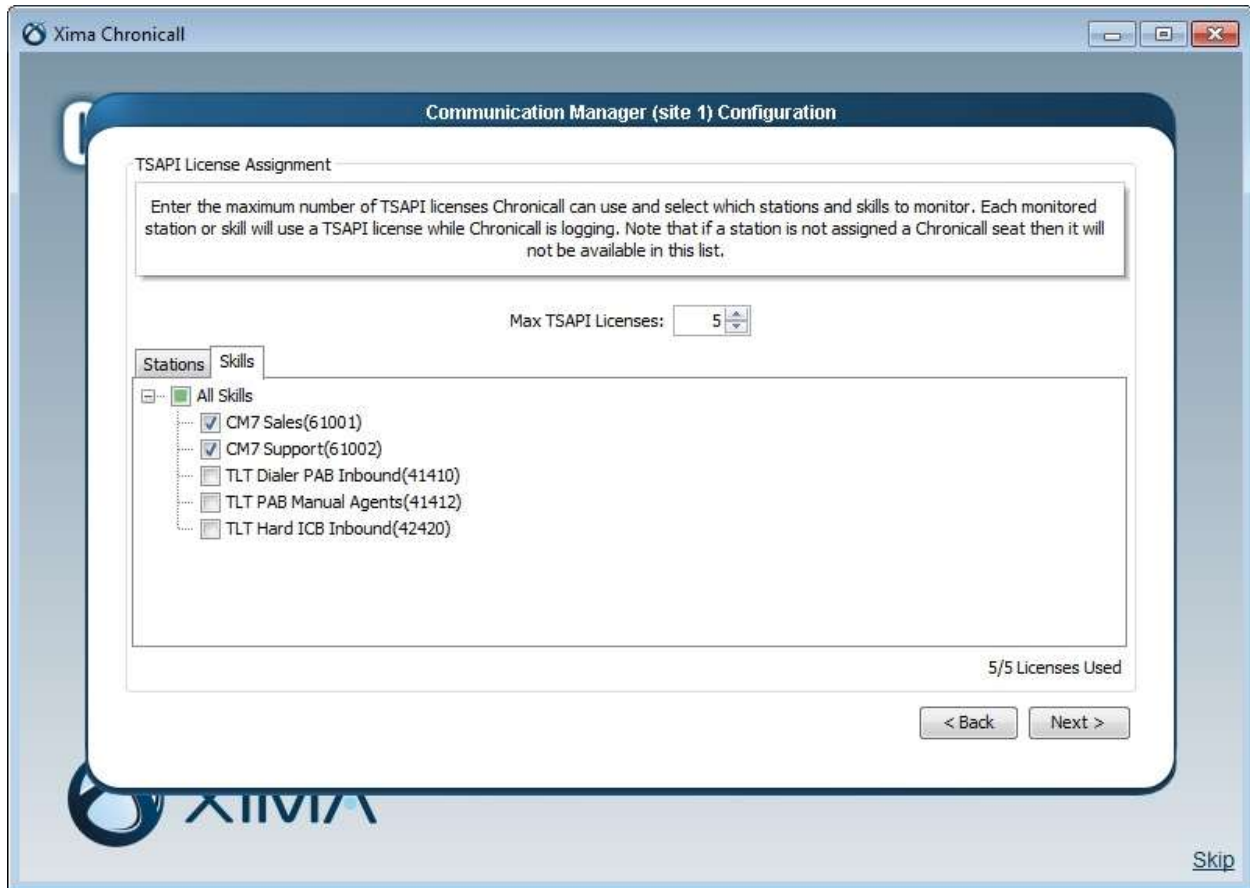
8.5. Administer License Assignment

The **TSAPI License Assignment** screen is displayed next. For **Max TSAPI Licenses**, select the maximum number of stations and skills to be monitored by 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.

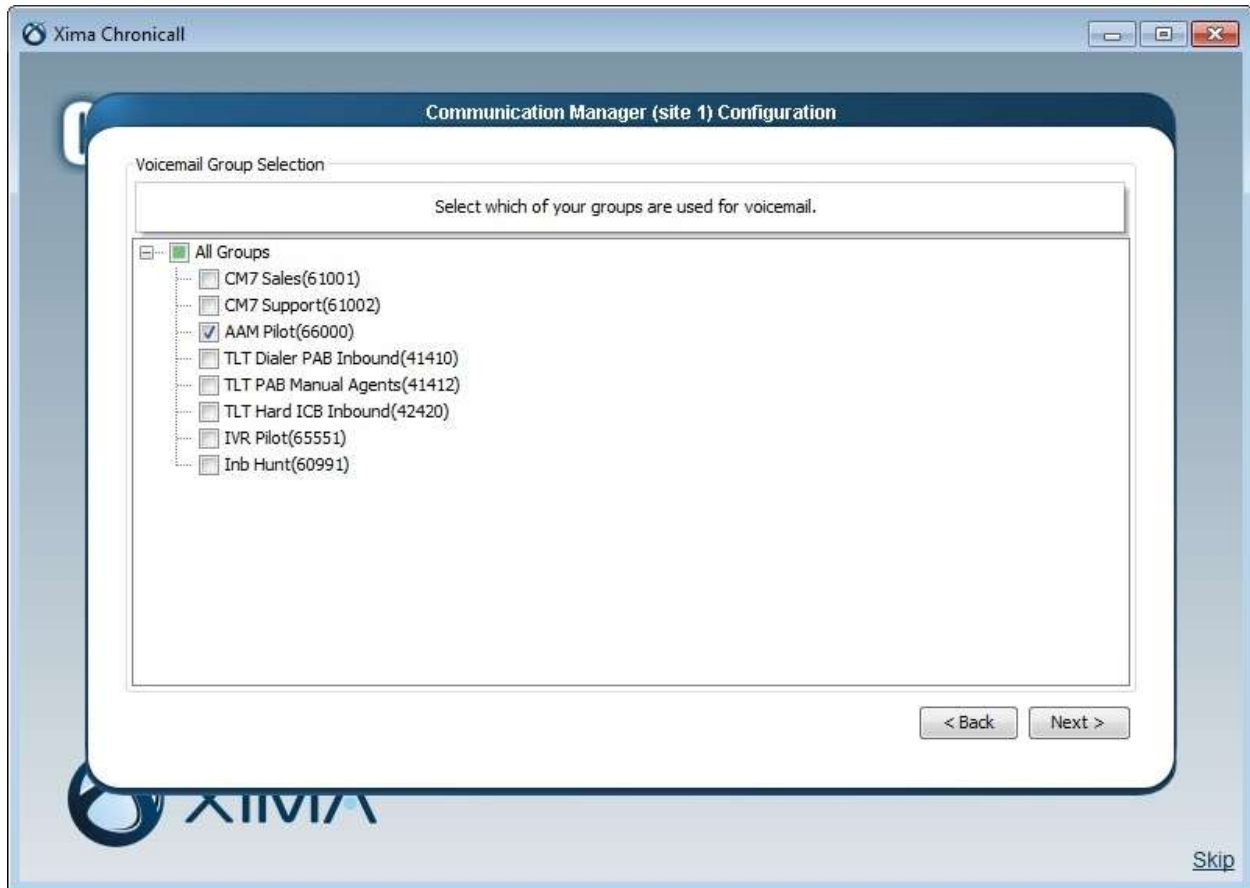
The screenshot shows the 'Xima Chronical' application window. The title bar reads 'Xima Chronical'. The main content area is titled 'Communication Manager (site 1) Configuration'. Inside this, there is a sub-section 'TSAPI License Assignment'. A text box contains instructions: 'Enter the maximum number 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 this, there is a 'Max TSAPI Licenses:' label followed by a spinner box set to '5'. There are two tabs: 'Stations' (selected) and 'Skills'. The 'Stations' tab displays a list of three items, each with a checked checkbox: 'Avaya, SIP 2(66002)', 'CM7 Station 1(65001)', and 'CM7 Supervisor(65000)'. At the bottom of the list are 'Select All' and 'Deselect All' buttons. To the right of these buttons, it says '3 selected'. Below the list, it says '3/5 Licenses Used'. 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.

Select the **Skills** tab to display a list of skills that were obtained from Application Enablement Services via the SMS connection. Select the desired skills to monitor.



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.



8.7. Administer Reason Codes

The **Aux Work Reason Codes** screen is displayed next. For contact 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 the 'Xima Chronicall' application window. The title bar reads 'Xima Chronicall'. The main window has a header 'Communication Manager (site 1) Configuration'. Below this is a section titled 'Aux Work Reason Codes'. Inside this section, there is a text box that says: 'If you use multiple Aux Work states then set the reason for each code so Chronicall can report reasons for each Aux event.' Below the text box is a table with two rows:

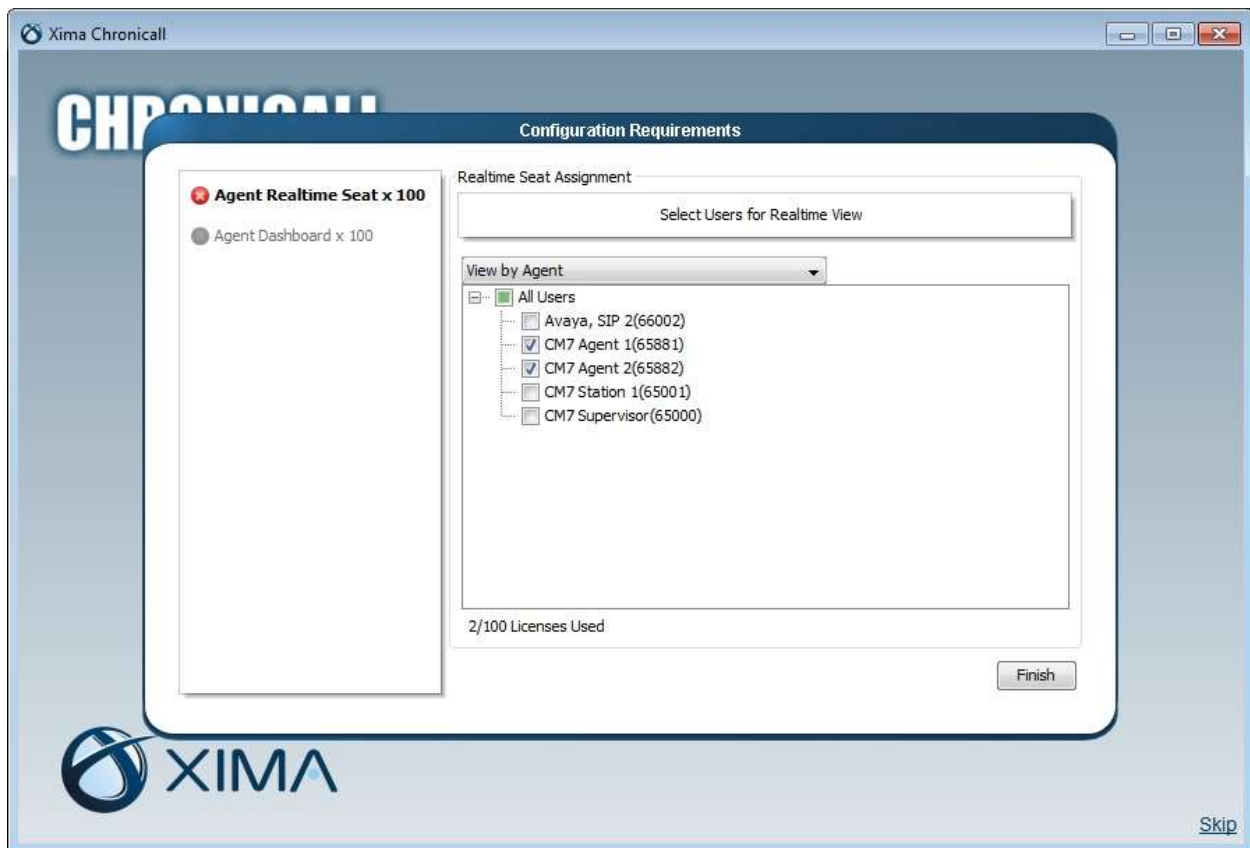
<input type="checkbox"/>	1	Meeting
<input type="checkbox"/>	2	Lunch

Below the table is an 'Add' button. At the bottom of the configuration window are two buttons: '< Back' and 'Finish'. In the bottom right corner of the main window, there is a 'Skip' link.

8.8. Administer Realtime Seat Assignment

For deployments with Chronicall Realtime licenses, the **Realtime Seat Assignment** screen is displayed next, listing all selected stations and agents from **Section 8.4**. Select the desired users to monitor with real time.

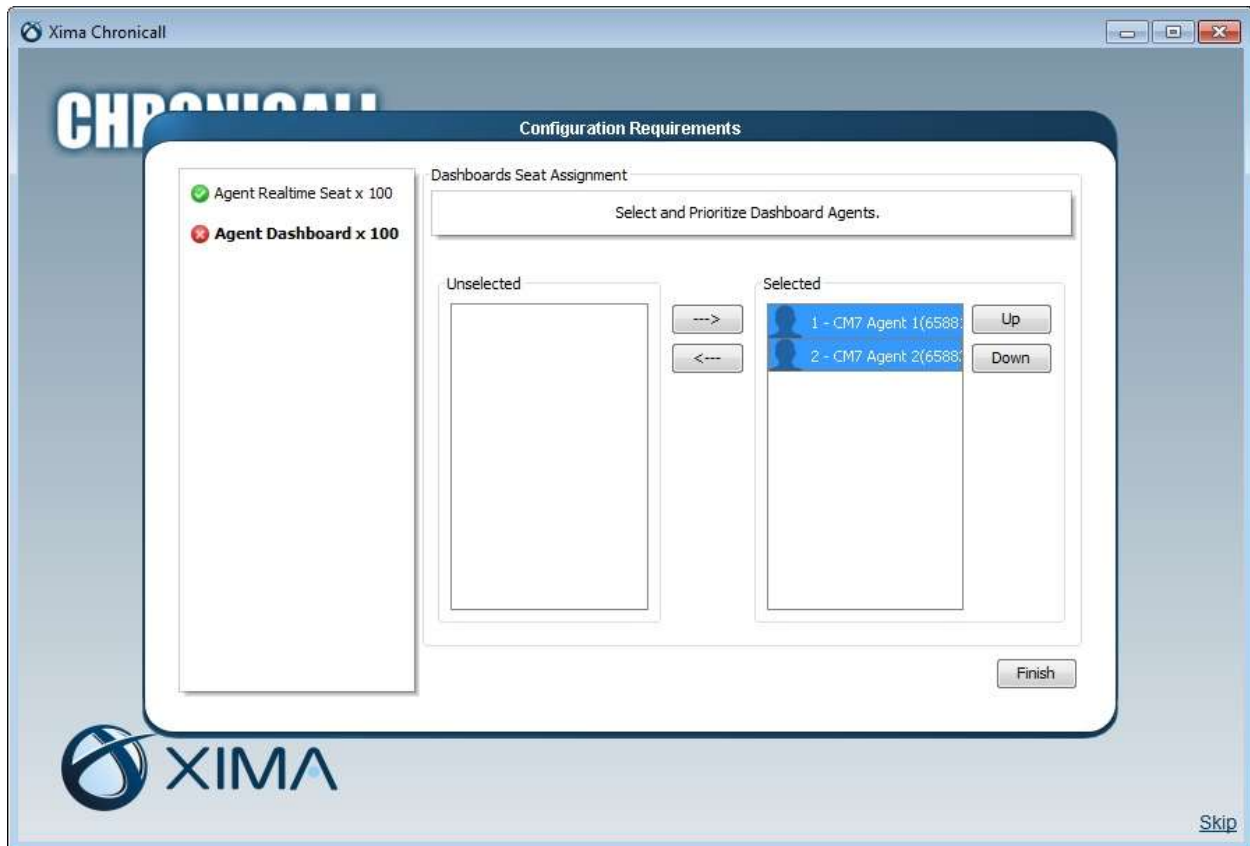
In the compliance testing, two agents IDs were selected, as shown below.



8.9. Administer Dashboard Seat Assignment

For deployments with Chronicall Realtime licenses, the **Dashboard Seat Assignment** screen is displayed next, listing all selected users from **Section 8.8**. Move the desired users from the **Unselected** to the **Selected** column for monitor with dashboard.

In the compliance testing, both agents 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	7	no	aes7	established	621	604

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, and agents, in this case “19”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jun 14 09:49:01 2016 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: 7.0.1.0.1.15-0
Server Date and Time: Tue Jun 14 11:07:15 EDT 2016
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

▶ Log Manager

▶ Logs

▼ Status and Control

TSAPI Link Details

☐ Enable page refresh every 60 seconds

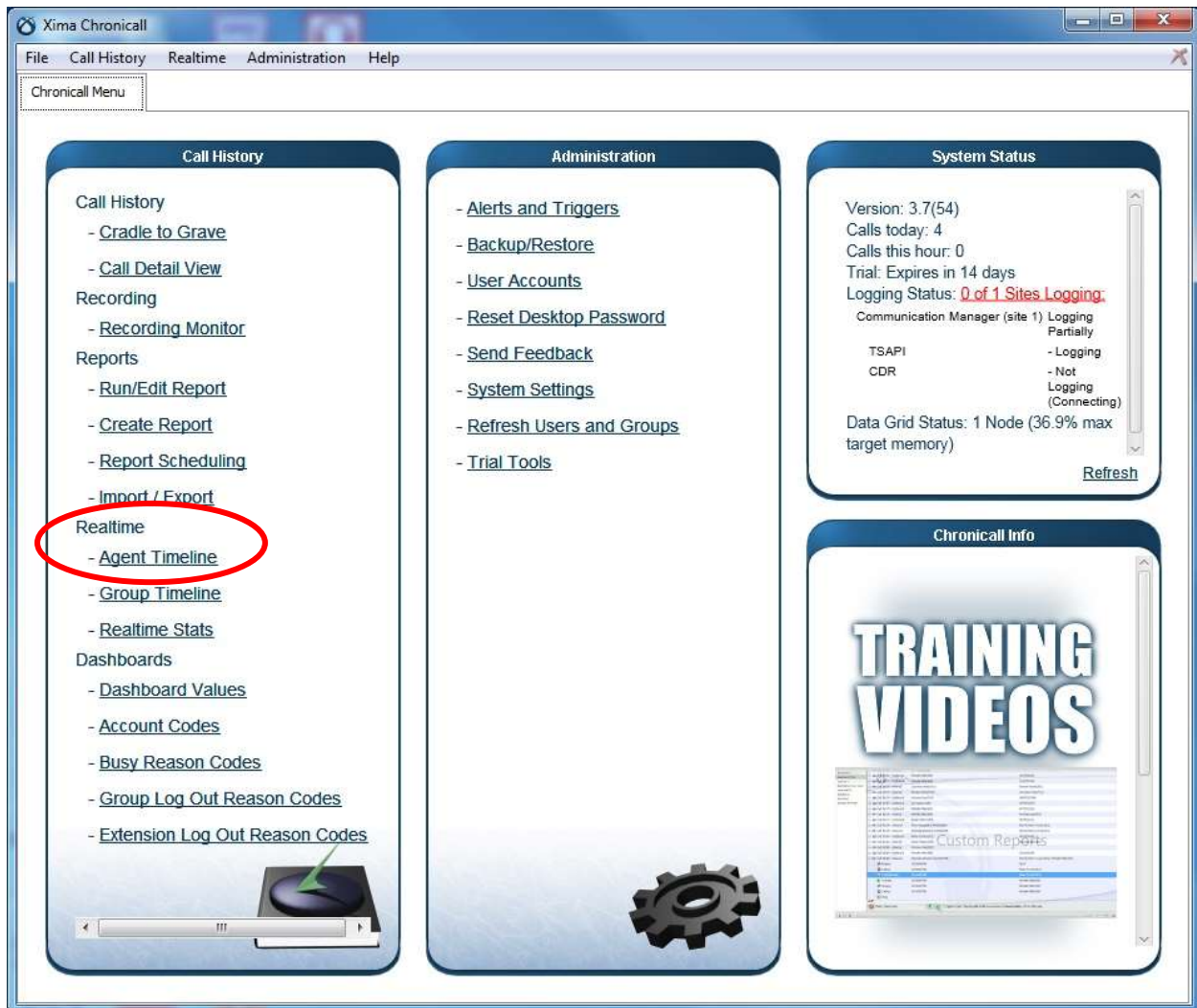
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Jun 8 10:52:37 2016	Online	17	19	604	621	30

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

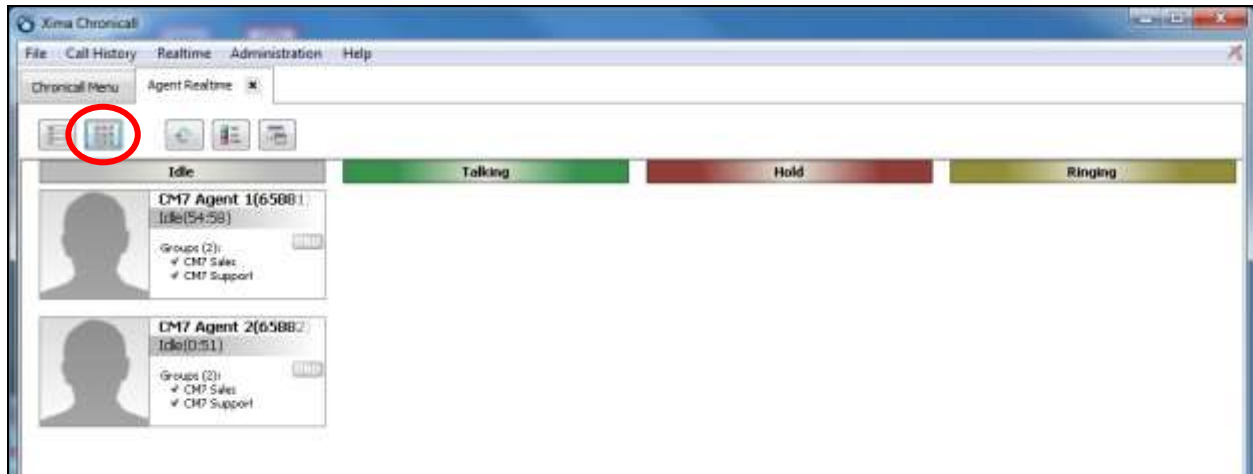
9.3. Verify Xima Chronicall

Log some agents into Communication Manager. From the supervisor PC, select **All Programs** → **Xima Software** → **Chronicall (browserless)** to launch the client application, and log in using the appropriate credentials.

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



An **Agent Realtime** tab is automatically created, as shown below. Click the **Show Live Columns** icon, and verify that the selected users for realtime monitoring from **Section 8.8** are reflected in the appropriate columns based on current activities. In the compliance testing, both agents were logged into skills “CM7 Sales” and “CM7 Support” and ready for calls “Idle”.



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



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



Complete the active ACD call. From the **Chronicall Menu** tab shown in the beginning of this section, select **Call History** → **Cradle to Grave**.

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

The screenshot shows the 'Xima Chronicall' application window with the 'Cradle to Grave Criteria' tab active. The window has a menu bar with 'File', 'Call History', 'Realtime', 'Administration', and 'Help'. Below the menu bar are tabs for 'Chronicall Menu', 'Agent Realtime', and 'Cradle to Grave'. The main content area displays the 'Cradle to Grave Criteria' dialog. At the top of the dialog is a 'Timeframe' section with a calendar for June 2016. The 14th is selected. Below the calendar is an 'Advanced...' button. Underneath is a section for 'Optional Cradle to Grave Filters' which contains a table with columns for filter type and value. The table has a header 'Call Filter' and a 'delete' button. The filter types listed are: Agent, Agent Does Not Equal, Calling Agent, Event Type, Event Type Does Not Equal, Group, Group Does Not Equal, Receiving Agent, Role, and Tag. Each filter type has a corresponding input field and a '...' button. At the bottom of the dialog are buttons for 'Save Filter(s)', 'Load Filter(s)', 'Execute' (circled in red), and 'Cancel'.

Event Level	Call Filter	delete
Agent		...
Agent Does Not Equal		...
Calling Agent		...
Event Type		...
Event Type Does Not Equal		...
Group		...
Group Does Not Equal		...
Receiving Agent		...
Role		...
Tag		...

The **Cradle to Grave** tab is updated as shown below. Verify that there is an entry reflecting the last call, in this case “Call 10”. Expand the entry, and verify that the reported details reflect the call with proper values in the respective columns.

The screenshot shows the Xima Chronicall application window. The 'Cradle to Grave' tab is active, displaying a list of calls. Call 10 is selected and expanded, showing its detailed lifecycle stages.

Call Info	Duration	Calling Party	Receiving Party	Caller Name	Location	Group	Start Timestamp
Calls (7 total)							
Call 2 - Inbound	0:00:39	(908) 848-5601	CM7 Agent 1(65881)		Bernardsville, New Jersey	CM7 Sales	Jun 14, 2016 7:13:40 AM
Call 3 - Internal	0:01:44	UNLICENSED(000)	CM7 Agent 1(65881)				Jun 14, 2016 7:20:17 AM
Call 4 - Internal	0:00:04	CM7 Agent 1(65881)					Jun 14, 2016 7:28:09 AM
Call 6 - Internal	0:00:07	Avaya, SIP 2(66002)					Jun 14, 2016 7:49:16 AM
Call 8 - Inbound	0:00:50	(908) 848-5601	CM7 Agent 1(65881)		Bernardsville, New Jersey	CM7 Sales	Jun 14, 2016 8:08:52 AM
Call 9 - Inbound	0:00:07	(908) 848-5601	CM7 Agent 2(65882)		Bernardsville, New Jersey	CM7 Sales	Jun 14, 2016 9:03:42 AM
Call 10 - Inbound	0:01:25	(908) 848-5601	CM7 Agent 1(65881)		Bernardsville, New Jersey	CM7 Sales	Jun 14, 2016 9:53:14 AM
Vector	0:00:02	(908) 848-5601	Sales Vec				Jun 14, 2016 9:53:14 AM
Ringing	0:00:11	(908) 848-5601	CM7 Agent 1(65881)			CM7 Sales	Jun 14, 2016 9:53:15 AM
Talking	0:01:12	(908) 848-5601	CM7 Agent 1(65881)			CM7 Sales	Jun 14, 2016 9:53:26 AM
Calling Drop	0:00:00	(908) 848-5601	CM7 Agent 1(65881)			CM7 Sales	Jun 14, 2016 9:54:38 AM

10. Conclusion

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

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2, May 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, May 2016, available at <http://support.avaya.com>.
3. *Avaya Communication Manager Configuration Guide*, February 2016, available at <https://www.ximasoftware.com/resources>.

©2016 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.