

A photograph of a modern office interior. In the foreground, a man in a blue shirt and jeans stands on the left, gesturing towards a man in a grey blazer and glasses who is seated at a table. The man in the blazer is looking at a laptop. To his right, a woman with curly hair in a black and white striped shirt is also seated at the table, looking towards the man in the blazer. On the far right, a woman in a white t-shirt and glasses stands, leaning over the table and looking at a laptop. The table is blue with yellow legs and has several laptops, a coffee cup, and a pen holder on it. The background shows other office desks, a whiteboard with a world map, and large windows. The ceiling has exposed pipes and several pendant lights.

XIMA

# AVAYA COMMUNICATION MANAGER CONFIGURATION GUIDE

Updated February 29, 2016

# Table Of Contents

---

## Section 1 – CM Configuration

1.1 – Accessing Communication Manager.....	1
1.2 – Adding a user profile .....	5
1.3 – Configure CM to send CDR data .....	13
1.4 – Exporting CM users and groups for CDR reporting .....	17
1.5 – Configuring TSAPI CTI LINK (only require for installs with an AES server) .....	19
1.6 – Configuring AES server (only require for installs with an AES server).....	23

## Section 2 – Install Chronicall

2.1 - Installation Setup.....	29
-------------------------------	----

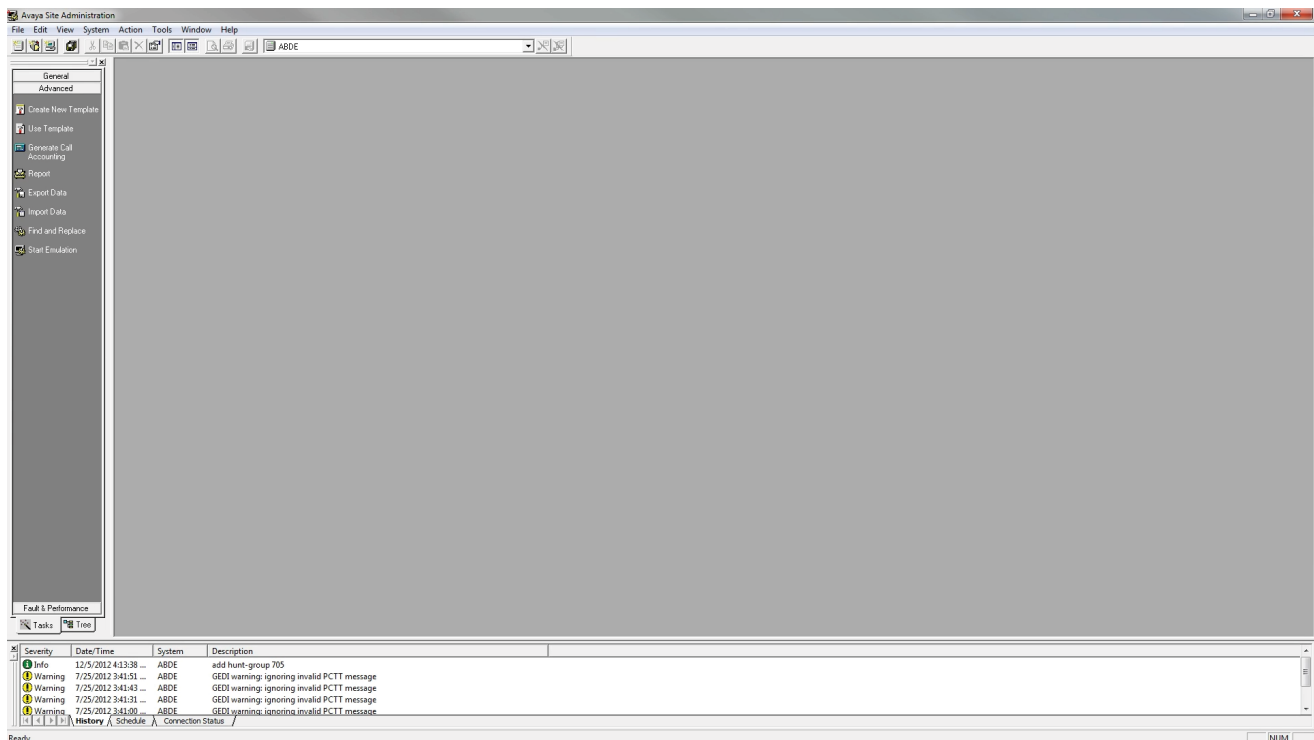
Installing Chronicall for Avaya Communication Manager requires a few simple configuration changes.

1. First, create login information for Chronicall to use on your CM server
2. Next, configure CDR services (if applicable) to enable Chronicall to connect and log call events
3. Next, configure your AES server (if applicable) to enable Chronicall to connect and log call events
4. Finally, install Chronicall

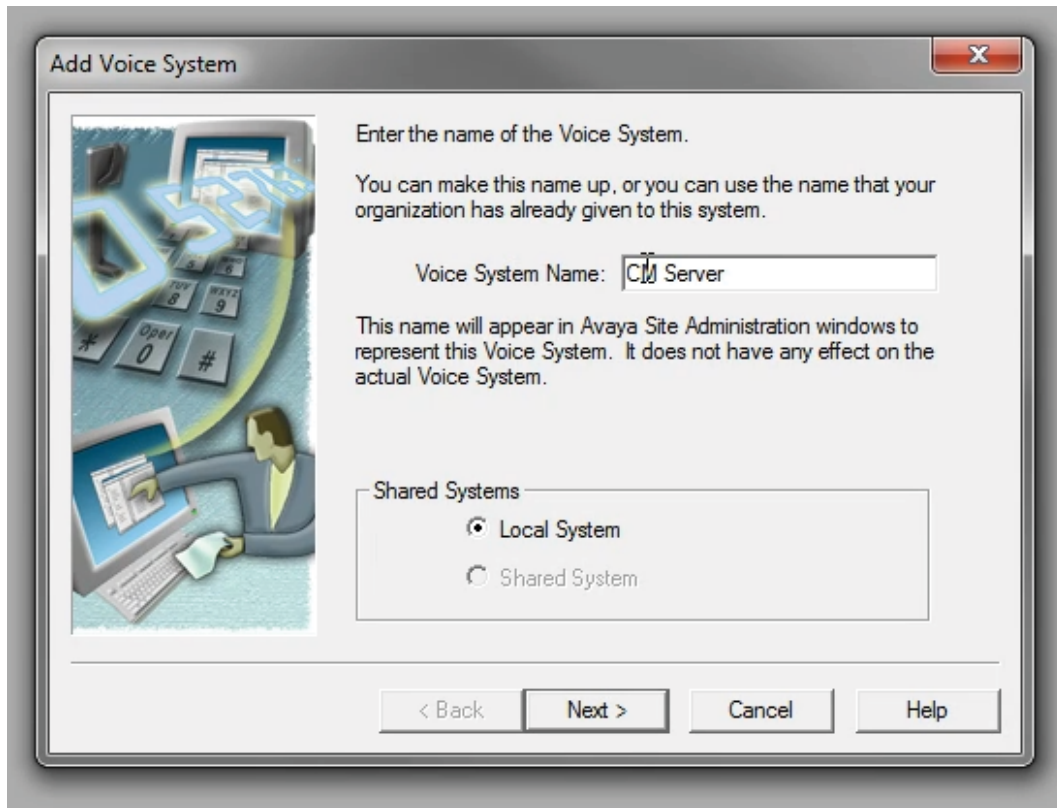
## Section 1.1 – CM Configuration

---

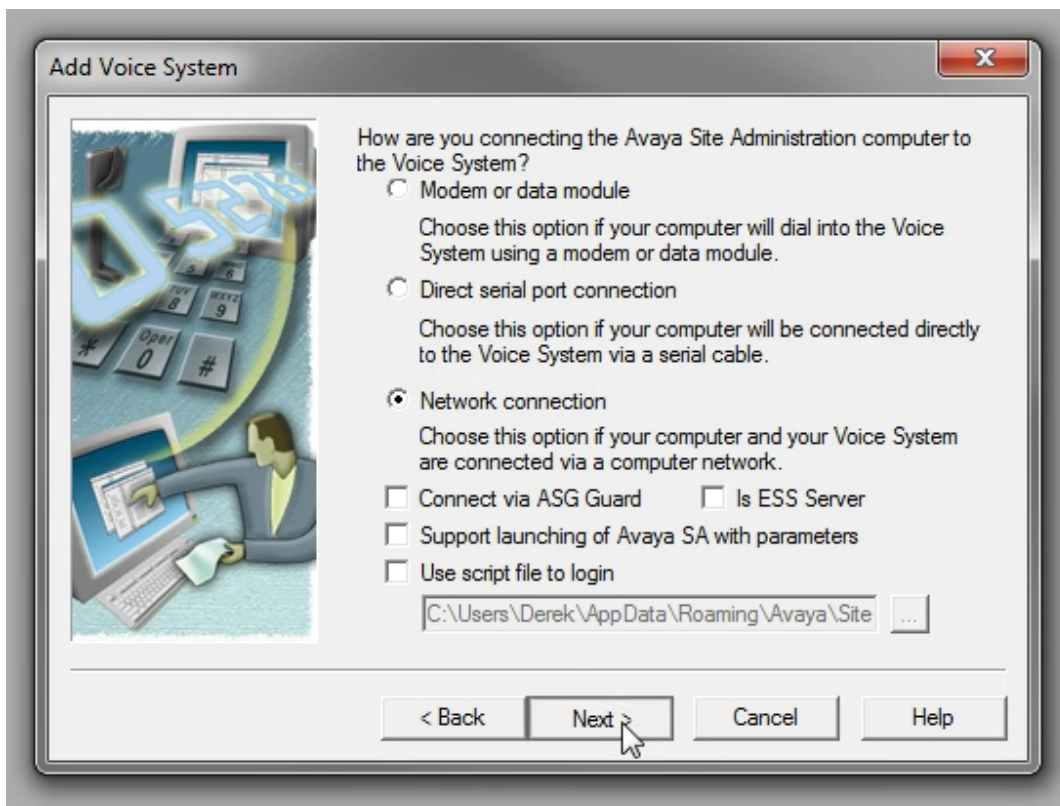
Access the CM server and open the Avaya site administration (ASA) application.



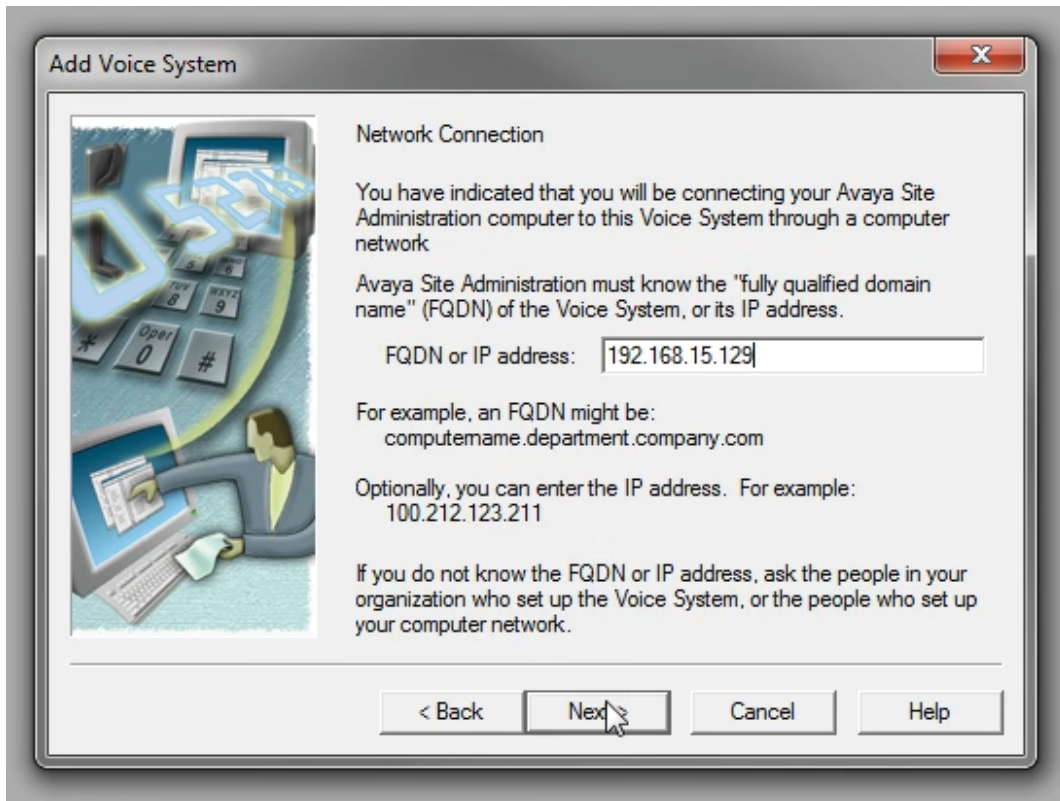
Add a new Voice System by opening File > New > Voice System. Name this new system and press Next.



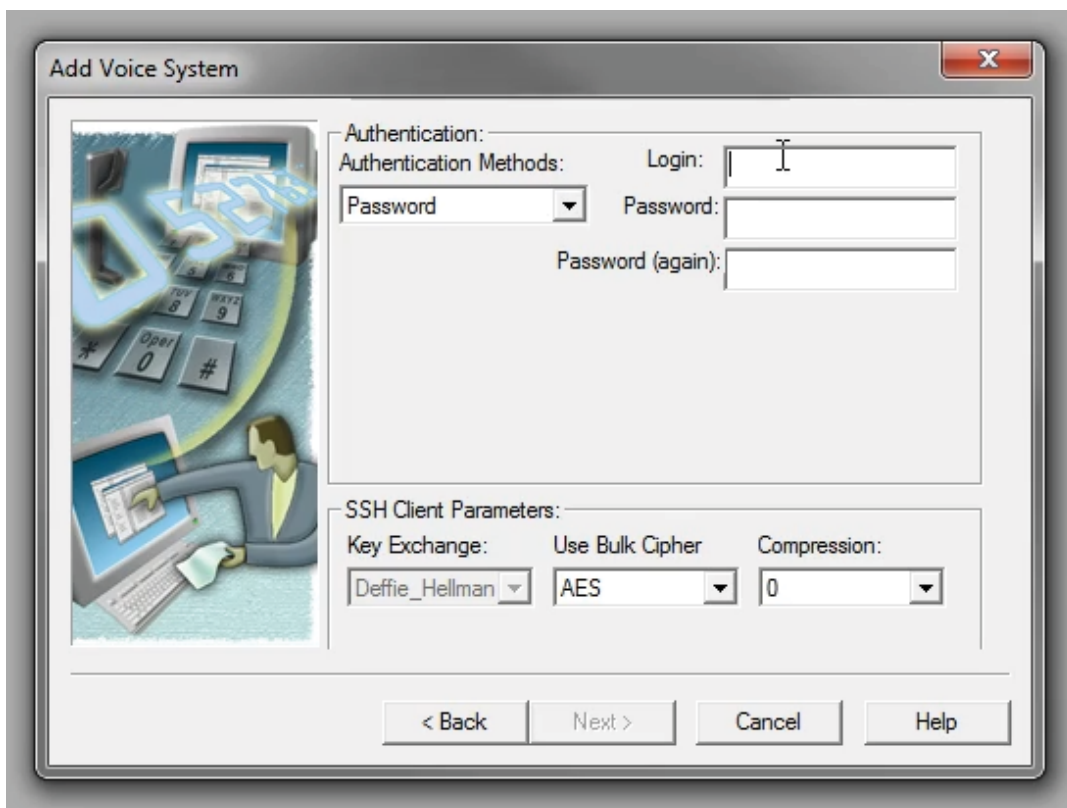
Make sure that Network Connection is selected, then press Next.



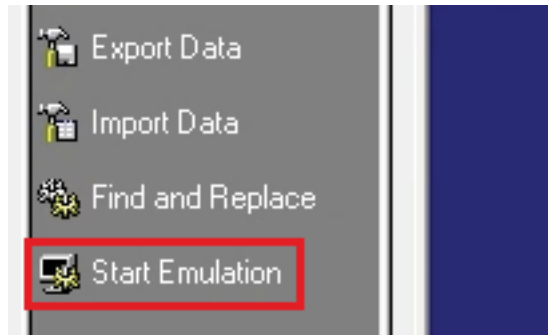
Make sure that Network Connection is selected, then press Next.



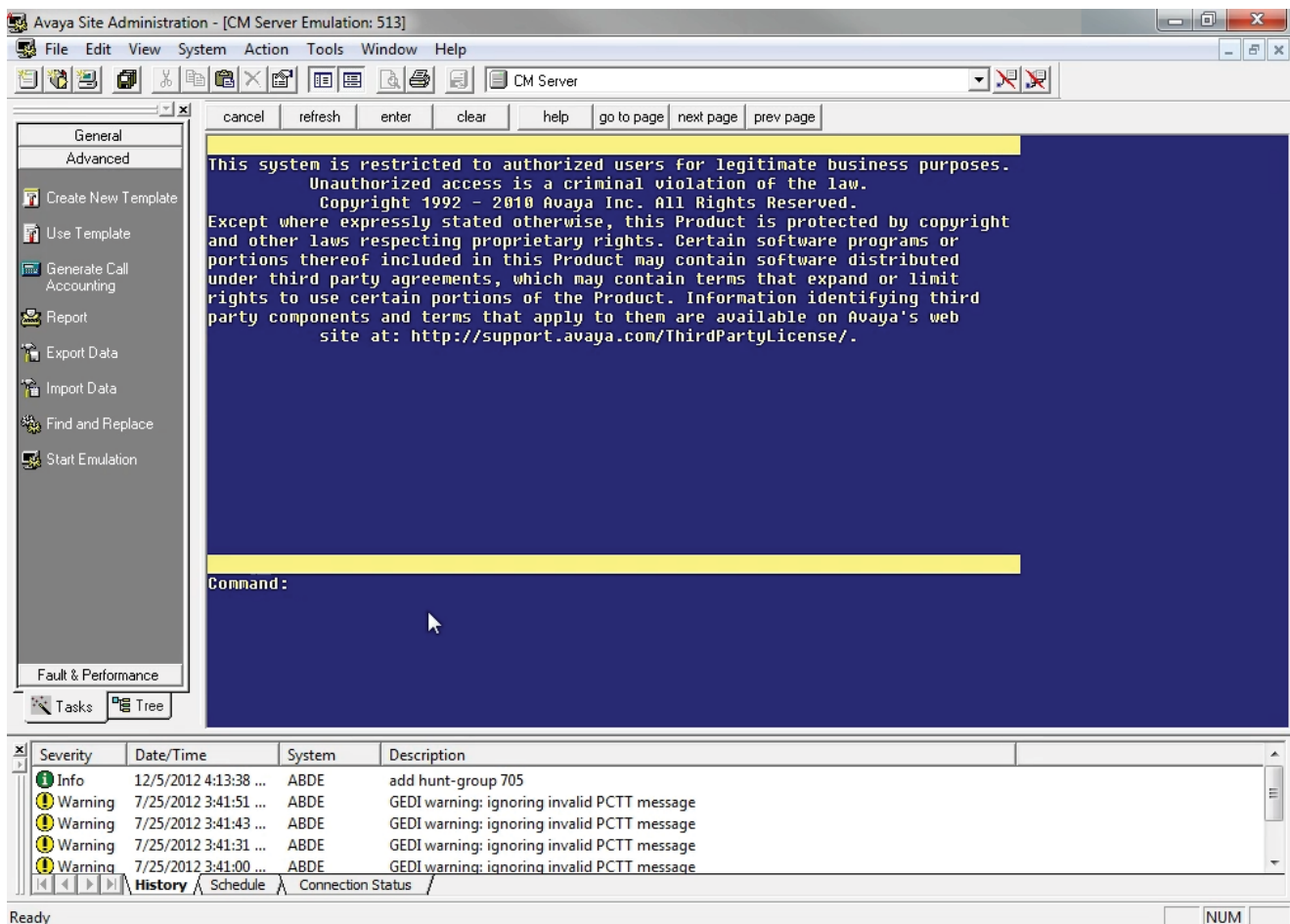
Accept the default options on the next few screens until you are asked for a login name and password. Enter the information of a privileged administrator account. Continue moving through the next few screens until the process is complete.



Once this is finished, click Start Emulation in the advanced section of the sidebar to the left.

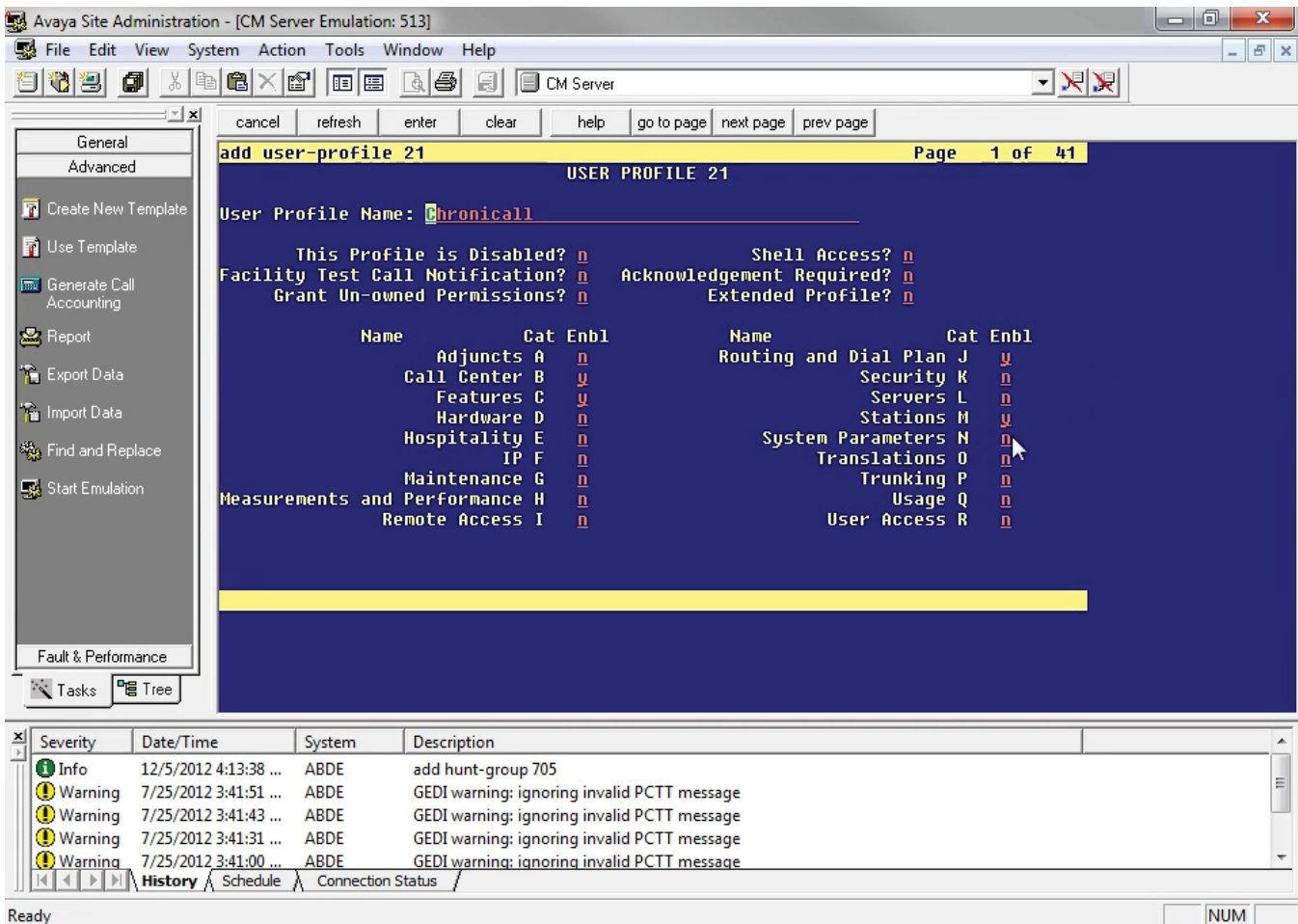


This will bring up a blue command line screen. First, you will need to create a user profile. This profile will outline Chronical's access privileges. Later, when you create a user, you will apply this user profile to it.

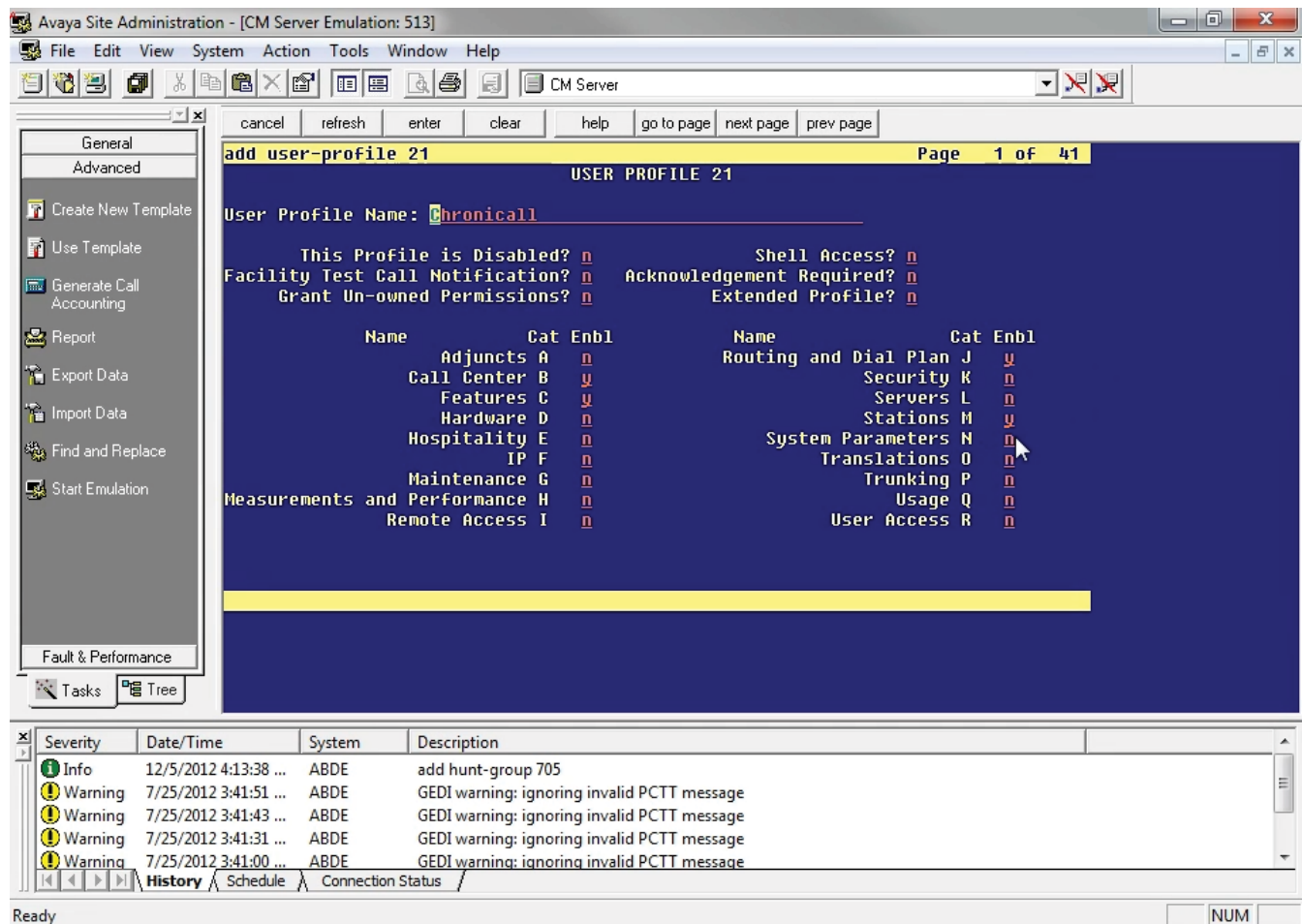


# Section 1.2 - Adding a User Profile

**Step 1** - Enter list user-profiles into the command line. This will show you a list of user profiles that currently exist on the system. User profiles 0 through 19 are reserved by the system, so any user profile number you choose will need to be 20 or higher. Once you've chosen a number, enter add user-profile followed by the profile number. For example, add user-profile 20. This will bring up a new user profile screen.

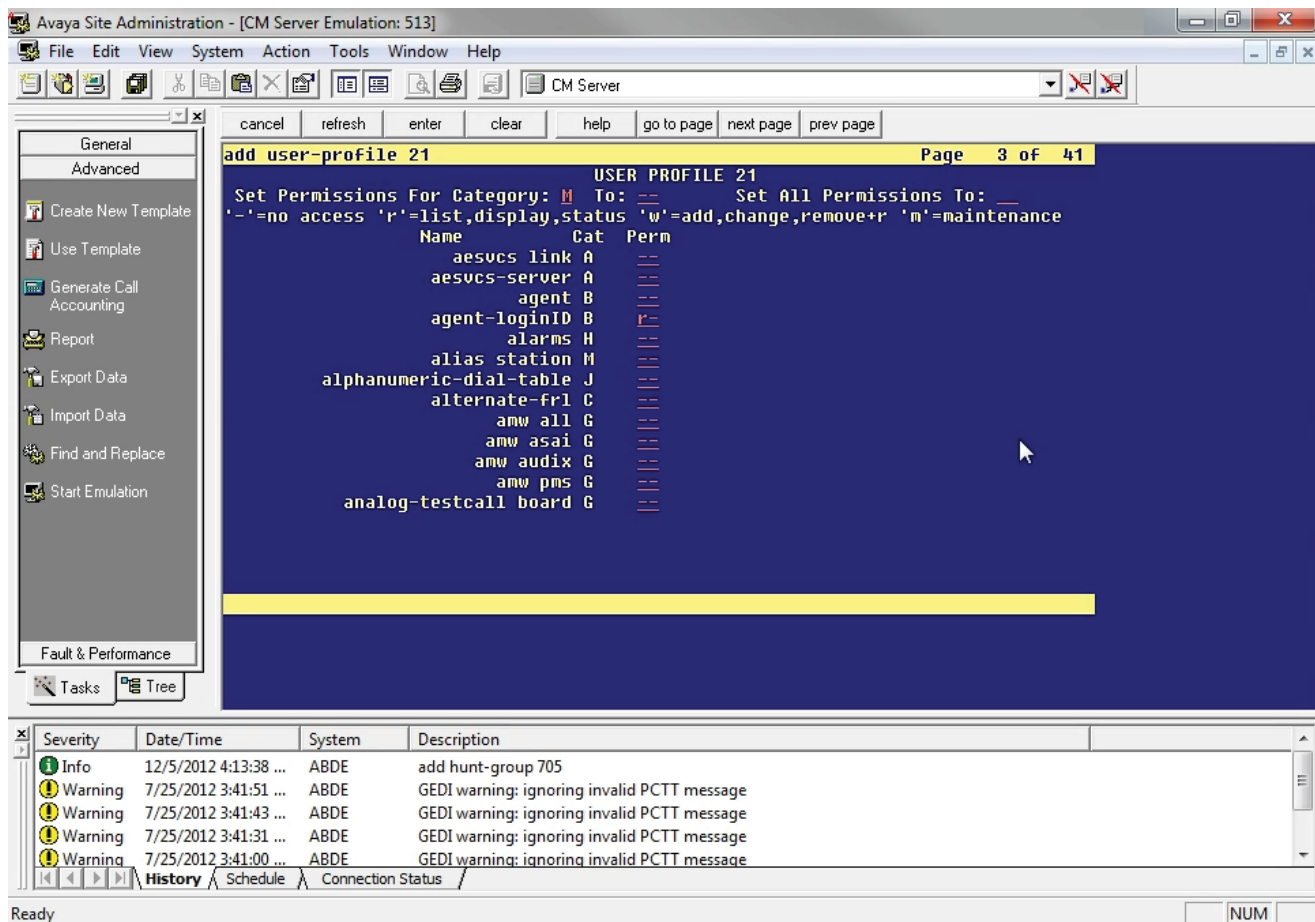


**Step 2** - In the User Profile Name field, enter Chronicall. Next, you need to enable specific permissions for this user profile. Arrow down to the Enbl column and change n to y for Call Center (B), Features (C), Routing and Dial Plan (J), and Stations (M).





**Step 3** - Move to the next page using Page Down. This section shows specific read and write functions in each of the categories listed before. Change the permissions for the categories listed above to --, meaning no access.

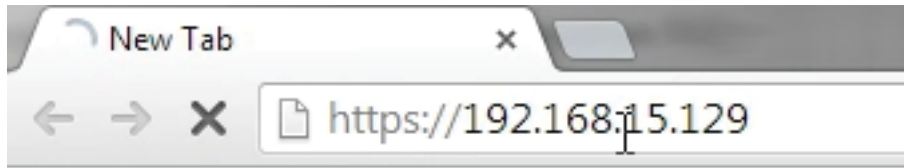


**Step 4** - Next, give read (r-) access to the following functions:

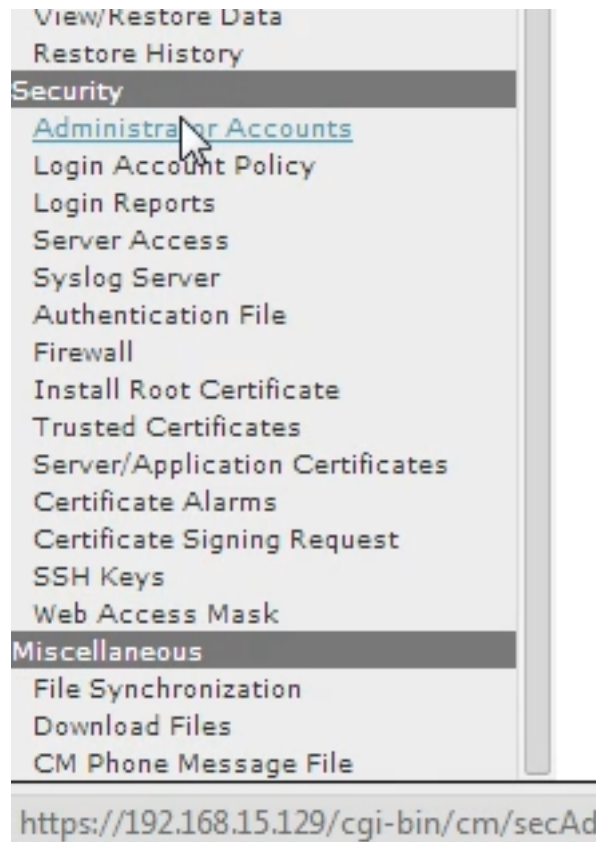
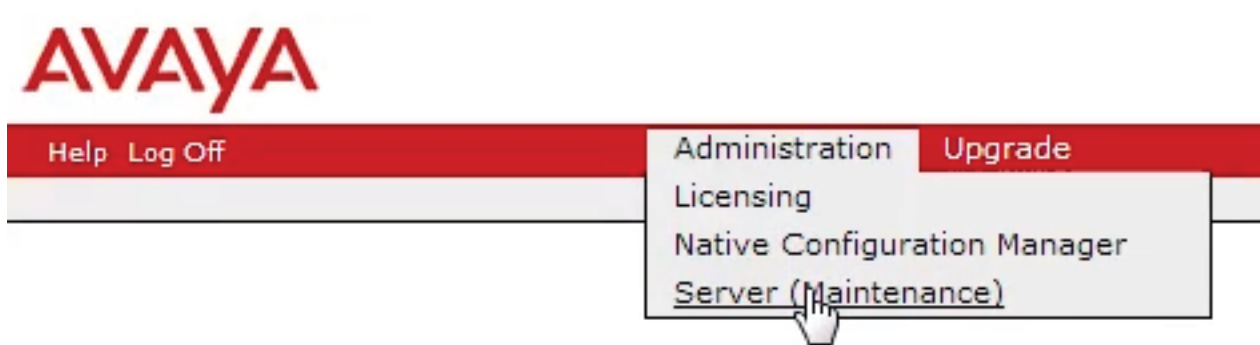
- page 3                    agent-loginID
- Page 14                 hunt-group
- Page 31                 station
- Page 37                 uniform-dialplan
- Page 39                 vdn
- Page 39                 vector

Once this is finished, click the Enter button at the top of the screen.

**Step 5** - Open your web browser and navigate to [https://\[CM server IP address\]](https://[CM server IP address]). This will open the Avaya System Management Interface, or SMI.



**Step 6** - Log in, open the Administration drop-down menu at the top of the page, and click Server (Maintenance). Under the Security tab on the left, click Administrator Accounts.



## Step 7 - Choose Add Group and Submit.



Help Log Off Administration Upgrade

Administration / Server (Maintenance)

### Administrator Accounts

The Administrator Accounts web 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
  - Modem Access Only
  - CDR Access Only
  - CM Messaging Access Only
  - Business Partner Login (dadmin)
  - Business Partner Craft Login
  - Custom Login
- Change Login
- Remove Login
- Lock/Unlock Login
- Add Group
- Remove Group

**Navigation Menu:**

- Current Alarms
- Agent Status
- SNMP Agents
- SNMP Traps
- Filters
- SNMP Test
- Diagnostics**
  - Restarts
  - System Logs
  - Temperature/Voltage
  - Ping
  - Traceroute
  - Netstat
  - Network Time Sync
- Server**
  - Status Summary
  - Process Status
  - Shutdown Server
  - Server Date/Time
  - Software Version
- Server Configuration**
  - Server Role
  - Network Configuration
  - Static Routes
  - Display Configuration
  - Eject CD/DVD
- Server Upgrades**
  - Make Upgrade Permanent
  - Boot Partition
  - Manage Updates
  - BIOS Upgrade
- IPSI Firmware Upgrades**
  - IPSI Version
  - Download IPSI Firmware
  - Download Status
  - Activate IPSI Upgrade
  - Activation Status

**Step 8** - In the Add a new access-profile group list, choose the profile number that matches the user profile you created earlier, then click Submit.



Help Log Off Administration Upgrade

Administration / Server (Maintenance)

### Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile group.

**Select Action:**

- Add a new access-profile group:
- Add a new non-access-profile group:

Group Name:

Group Number:

**Access Profile List:**

- prof21
- prof22
- prof23
- prof24
- prof25
- prof26
- prof27
- prof28
- prof29
- prof30
- prof31
- prof32
- prof33
- prof34
- prof35
- prof36
- prof37
- prof38
- prof39

**Navigation Menu:**

- Current Alarms
- Agent Status
- SNMP Agents
- SNMP Traps
- Filters
- SNMP Test
- Diagnostics**
- Restarts
- System Logs
- Temperature/Voltage
- Ping
- Traceroute
- Netstat
- Network Time Sync
- Server**
- Status Summary
- Process Status
- Shutdown Server
- Server Date/Time
- Software Version
- Server Configuration**
- Server Role
- Network Configuration
- Static Routes
- Display Configuration
- Eject CD/DVD

**Step 9** - When you return to the Administrator Accounts page, select SAT Access Only in the Add Login list.



Help Log Off Administration Upgrade

Administration / Server (Maintenance)

- Current Alarms
- Agent Status
- SNMP Agents
- SNMP Traps
- Filters
- SNMP Test
- Diagnostics**
- Restarts
- System Logs
- Temperature/Voltage
- Ping
- Traceroute
- Netstat
- Network Time Sync
- Server**
- Status Summary
- Process Status
- Shutdown Server
- Server Date/Time
- Software Version
- Server Configuration**
- Server Role
- Network Configuration
- Static Routes
- Display Configuration
- Eject CD/DVD
- Server Upgrades**
- Make Upgrade Permanent
- Boot Partition
- Manage Updates
- BIOS Upgrade
- IPSI Firmware Upgrades**
- IPSI Version
- Download IPSI Firmware
- Download Status
- Activate IPSI Upgrade
- Activation Status

### Administrator Accounts

The Administrator Accounts web pages allow you to add, delete, or change administrator accounts.

**Select Action:**

- Add Login
  - Privileged Administrator
  - Unprivileged Administrator
  - SAT Access Only
  - Web Access Only
  - Modem Access Only
  - CDR Access Only
  - CM Messaging Access Only
  - Business Partner Login (dadmin)
  - Business Partner Craft Login
  - Custom Login
- Change Login
- Remove Login
- Lock/Unlock Login
- Add Group
- Remove Group

**Step 10** - On the next page, enter a login name, select users from the Primary group list, and choose the profile you created earlier from the Additional groups list. Create a password, then press Submit.

**AVAYA**

Help Log Off Administration Upgrade

Administration / Server (Maintenance)

### Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Manage

Login name:

Primary group:  susers  users

Additional groups (profile):

Linux shell:

Home directory:

Lock this account:

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Select type of authentication:  Password  ASG: enter key  ASG: Auto-generate key

Enter password or key:

Re-enter password or key:

Force password/key change on next login:  Yes  No

**Submit** **Cancel** **Help**

**Warnings:**

- You must assign a profile that has no web access if you want a login with SAT access only.
- This shell setting does NOT disable the "go shell" SAT command for this user.

Your user is now created and has been assigned all of the necessary permissions to run Chronicall.

# Section 1.3 - Configure CM to send CDR data

**\*\*Special note - if you are not using CDR data you can skip section 1.3**

## Step 1 - Add Chronical CDR server to Node Names IP

Add the IP Address of the Chronical server into the IP NODE NAMES. Type change node-names ip to access the node names and add the server Name and IP Address as shown below (example uses xxx.xxx.xxx.xxx - you will need to use an actual IP Address):

```
change node-names ip Page 1 of 2
      IP NODE NAMES
      Name          IP Address
  CLAN-AES         10.0.1.20
  Chronical        xxx.xxx.xxx.xxx
  default          0.0.0.0
  procr            10.0.1.20
  procr6           ::
```

## Step 2 - Setup CDR Service

Type change ip-services to setup a CDR link to the Chronical Server using the following information. Note the following information may be needed when setting up the Chronical CDR service on the Chronical server.

- Local Node is procr
- Remote Node: This is the Chronical node you added in step 1.
- Service Type is CDR1
- Remote Port: This is the only information you will need when installing Chronical. number in this example is 9089 but can be any free port number (please make note of the port number that you use)

See example below:

```
change ip-services Page 3 of 4
      SESSION LAYER TIMERS
      Service Type  Reliable Protocol  Packet Resp Timer  Session Connect Message Cntr  SPDU Cntr  Connectivity Timer
  CDR1             n             30                3                3                60
```

### Step 3 - Configure CDR Parameters

Type change system-parameters cdr. Ensure all the fields are as shown below on Page 1 of system-parameters cdr.

1. Note the Primary Output Endpoint is that of the service type added on Step 2.
2. Please change the CDR Date Format to: month/day Chronicall expects this date format to match this, and then you can change how it is presented to you on the reports within Chronicall.
3. Please ensure that all Data Item Length entries are the same as outlined below on Page 2 of system-parameters cdr. Items 35 – seq-num, and item 37 ucid are recommended but optional. In order to enable these features they need to be enabled by Avaya. Please open a ticket with Avaya and ask them to enable special application SA8702.

```
change system-parameters cdr Page 1 of 2
                                CDR SYSTEM PARAMETERS
Node Number (Local PBX ID):          CDR Date Format: month/day
Primary Output Format: customized    Primary Output Endpoint: CDR1
Secondary Output Format: _____
Use ISDN Layouts? n                  Enable CDR Storage on Disk? n
Use Enhanced Formats? n              Condition Code 'T' For Redirected Calls? y
Use Legacy CDR Formats? n            Remove # From Called Number? n
Modified Circuit ID Display? n        Intra-switch CDR? y
Record Outgoing Calls Only? n         Outg Trk Call Splitting? y
Suppress CDR for Ineffective Call Attempts? n Outg Attd Call Record? y
Disconnect Information in Place of FRL? n Interworking Feat-flag? n
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n        Record Agent ID on Outgoing? y
Inc Trk Call Splitting? y
Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
Record Call-Assoc TSC? n              Digits to Record for Outgoing Calls: dialed
Privacy - Digits to Hide: 0           CDR Account Code Length: 15
Remove '+' from SIP Numbers? y
```



```

change system-parameters cdr                                     Page 2 of 2
                                CDR SYSTEM PARAMETERS

Data Item - Length      Data Item - Length      Data Item - Length
1: date - 6             17: in-trk-code - 4     33: node-num - 2
2: space - 1            18: space - 1           34: space - 1
3: time - 4             19: in-crt-id - 3      35: seq-num - 10
4: space - 1            20: space - 1           36: space - 1
5: sec-dur - 5          21: out-crt-id - 3     37: ucid - 20
6: space - 1            22: space - 1           38: return - 1
7: cond-code - 1        23: ppm - 5            39: line-feed - 1
8: space - 1            24: space - 1           40: _____
9: code-used - 4        25: isdn-cc - 11       41: _____
10: space - 1           26: space - 1           42: _____
11: code-dial - 4       27: attd-console - 2   43: _____
12: space - 1           28: space - 1           44: _____
13: dialed-num - 18     29: vdn - 5            45: _____
14: space - 1           30: space - 1           46: _____
15: clg-num/in-tac - 10 31: acct-code - 15     47: _____
16: space - 1           32: space - 1           48: _____

                                Record length = 152

```

#### Step 4 - Enable Missed and Internal Calls

To allow missed calls to appear on the Chronical CDR reports, set CDR Reports to r in the trunk group used for outgoing/incoming calls.

1. Type change trunk-group x where x is the number of the incoming/outgoing trunk group.

\*\* Please ensure that CDR Reports is set to r

See example below:

```

change trunk-group 1                                         Page 1 of 21
                                TRUNK GROUP

Group Number: 1                Group Type: isdn          CDR Reports: r
Group Name: Main              COR: 1                 TN: 1                 TAC: 8001
Direction: two-way          Outgoing Display? n     Carrier Medium: PRI/BRI
Dial Access? n              Busy Threshold: 255    Night Service: _____
Queue Length: 0
Service Type: tie           Auth Code? n           TestCall ITC: rest
Far End Test Line No:    
TestCall BCC: 4

```

Step 5 - To enable intra-switch calls to be reported, type change intra-switch-cdr and add the Extension numbers of the sets that are to be reported for internal calls.

See example below:

```
change intra-switch-cdr                                     Page 1 of 3
INTRA-SWITCH CDR
Assigned Members: 8 of 1000 administered
Extension          Extension          Extension          Extension
1000
4000
4012
4013
4014
4015
4016
4017
Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other members
```

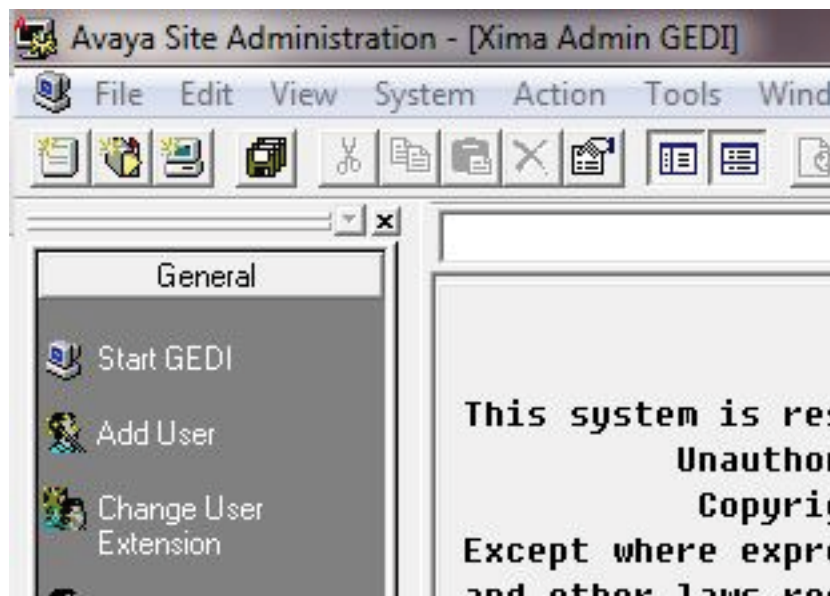
END

# Section 1.4 - Exporting CM Users and Groups for CDR Reporting

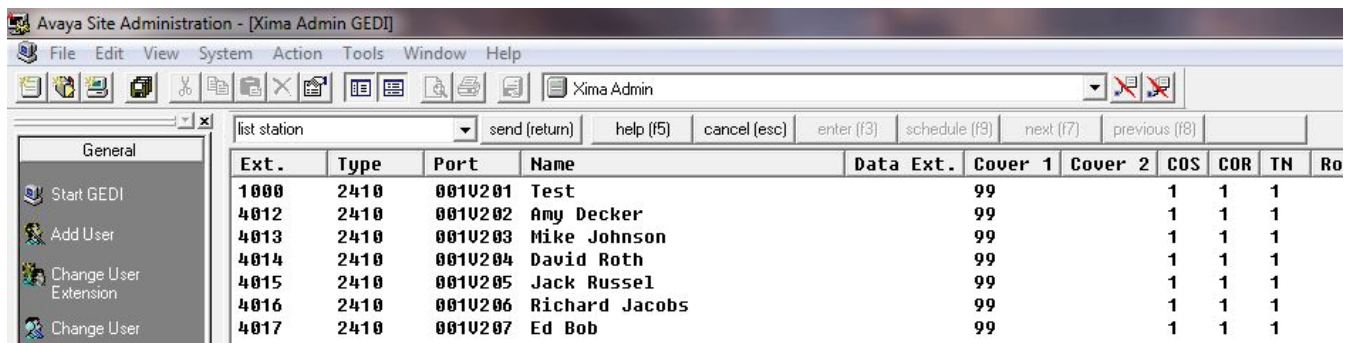
\*\*Special note - if you are not using CDR for reporting, or if you have an AES Server you can skip section 1.4. The AES server can send Chronical all the usernames and groups.

This section will show you how to export your stations, agents, groups, VDNs and vectors.

Step 1 - Please open a GEDI connection to your Communication Manager



Step 2 - Run a list command to query the data you want.

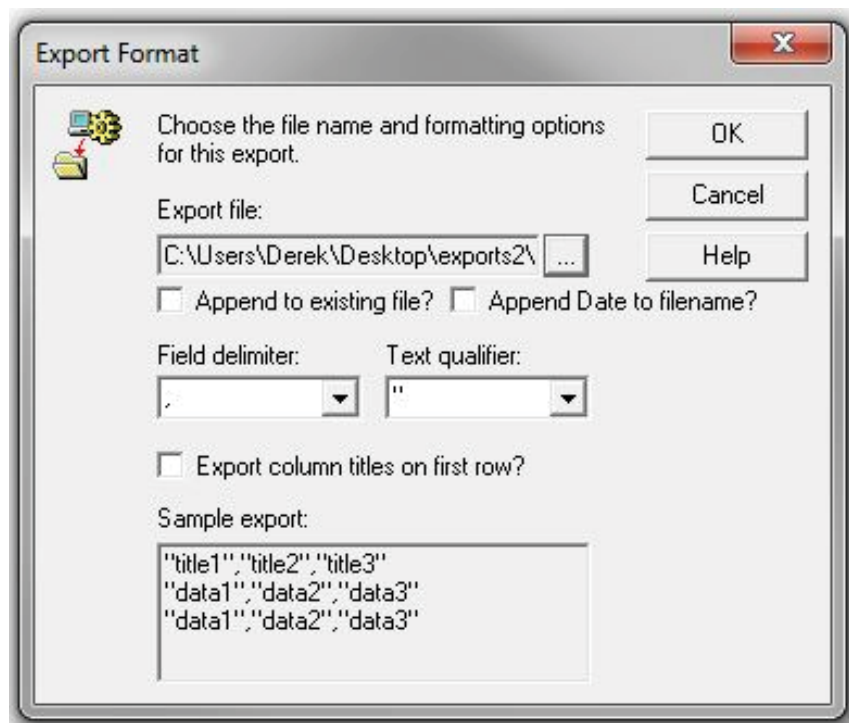


### Step 3 - Go to File → Export



### Step 4 - Choose a location for the export file and hit OK

You'll want to put all of the exports in a directory together and name them smartly to make it easy to find them when Chronical asks for them.



**Step 5 - You'll need to repeat these steps for each of the following commands resulting in the 5 files:**

list vdn  
list vector  
list hunt-group  
list station  
list agent-loginID

**Step 6: During the Chronicall installation you will be asked to import these files. Again you don't need these files if you are using an AES Server.**

End

## Section 1.5 - Configure TSAPI CTI LINK

---

**\*\*Special Note – If you are not using an AES Server you may skip this section**

### Step 1 - Add CTI Link

Type add cti-link x command, where x is a number between 1 and 64. Enter a valid extension number under the provisioned dial plan. Set the Typ Field to ADJ-IP and assign a descriptive Name to the CTI LINK. Default values may be used in the remaining fields.

Example Below:

```
add cti-link 2                                     Page 1 of 3
                                         CTI LINK
CTI Link: 2
Extension: 4098
Type: ADJ-IP
Name: Chronicall
COR: 1
```

## Step 2 - Enter Node Name

Type change node-names ip In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, Avaya IP Agents, and Avaya AES DMCC stations). The CLAN-AES IP address was used for connectivity to the Avaya AES server. Please note if you are configuring the AES to connect to an S8300 the IP Address needs to be the same IP as your processor.

See example below:

```
change node-names ip Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
CLAN-AES	10.0.1.20
default	0.0.0.0
procr	10.0.1.20
procr6	::

## Step 3 - Change IP Services

Type change ip-services On Page 1, configure the Service Type field to AESVCS and the Enabled field to y. The Local Node field should be pointed to the CLANAES board that was configured previously in the node-name ip form. During the compliance test, the default port was utilized for the Local Port field.

See example below:

```
change ip-services Page 1 of 3
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

#### Step 4 - Change IP Services

Type change ip-services On Page 3, configure the Service Type field to AESVCS and the Enabled field to y. The Local Node field should be pointed to the CLANAES board that was configured previously in the node-name ip form. During the compliance test, the default port was utilized for the Local Port field.

See example below:

change ip-services		Page 3 of 3		
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	<u>aesxima</u>	<u>*</u>	<u>y</u>	in use
2:	<u>                    </u>	<u>                    </u>	<u>-</u>	
3:	<u>                    </u>	<u>                    </u>	<u>-</u>	
4:	<u>                    </u>	<u>                    </u>	<u>-</u>	

#### Step 5 - Log into the AES web Interface

See example below:

**Please login here:**

**Username**

## Step 6 - Add New Connection

Select Communication Manager Interface and add new connection. The next page will prompt you to enter a password. If your processor is already configured please proceed to next step.

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
s8300	No	30	1

You will need to enter the switch password that you configured in step 4

Communication Manager Interface | Switch Connections Home | Help | Logout

Connection Details - s8300

Switch Password

Confirm Switch Password

Msg Period  Minutes (1 - 72)

Provide AE Services certificate to switch

Secure H323 Connection

Processor Ethernet



## Step 7 - Add CLAN to AES

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on Edit CLAN IPs. Enter the IP address of the CLAN used for Avaya AES connectivity from Section 3.6, and click on Add Name or IP.

See example below:



Name or IP Address	Status
<input checked="" type="radio"/> 10.0.1.20	In Use

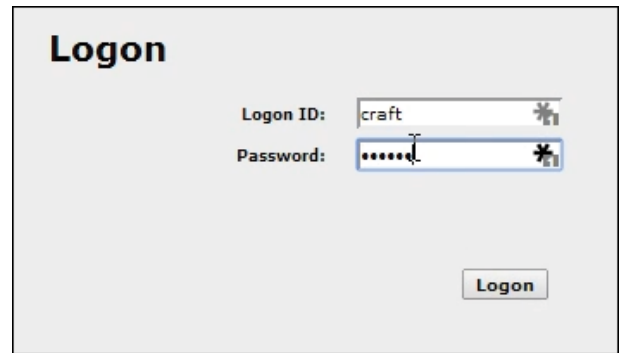
From here your Communication Manager should be able to communicate with your AES Server.

END

## Section 1.6 - Configure AES Server

You will also need to set up an AES user. You can do this by accessing the Management Console on the AES server.

**Step 1** - In a web browser, navigate to [http://\[AES server IP address\]](http://[AES server IP address]) and log in.

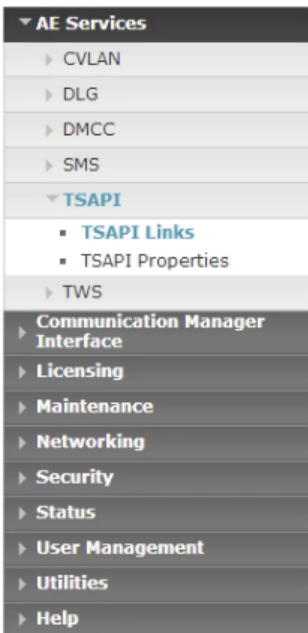


Log in and expand the AE Services section at the top of the sidebar to the left, followed by TSAPI, then TSAPI Links. Make sure the TSAPI link is selected and select Edit. Change the ASAI Link Version to 5 and apply the changes.



## Application Enablement Services Management Console

AE Services | TSAPI | TSAPI Links



### Edit TSAPI Links

Link	1
Switch Connection	cmsim
Switch CTI Link Number	1
ASAI Link Version	5
Security	Both
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/> <input type="button" value="Advanced Settings"/>	

**Step 2** - Under User Management, open User Admin and select Add User. Give the new user a name and a password. Change the CT User option to Yes, then scroll down and press Apply.

\*\* Special Note – for the password alphanumeric is accepted and the following special characters . , @ \$



Ap

User Management | User Admin | Add User

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ 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	<input type="text" value="chronicall"/>
* Common Name	<input type="text" value="chronicall"/>
* Surname	<input type="text" value="chronicall"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>

**Step 3** - You may also need to enable SDB for TSAPI Service, JTAPI and Telephony Web Services under Security, Security Database, Control.



**Security | Security Database | Control**

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ **Security**
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ **Security Database**
    - **Control**
    - ⊕ CTI Users
    - Devices
    - Device Groups
    - Tlinks
    - Tlink Groups
    - Worktops
  - Standard Reserved Ports
  - Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

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

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

Apply Changes

**Step 4** - Expand the CTI Users section next to the Control Link and select List All Users. Select the Chronical user and select Edit. Instead of giving this user specific access privileges, select the Unrestricted Access box. Chronical itself will handle the appropriate access permissions.



## Application Enablement Services Management Console

Security | Security Database | CTI Users | List All Users

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control
    - ▣ CTI Users
      - List All Users
      - Search Users
    - Devices
    - Device Groups
    - Tlinks
    - Tlink Groups
    - Worktops
  - Standard Reserved Ports
  - Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Edit CTI User

User Profile:	User ID: chronicall Common Name: chronicall Worktop Name: NONE ▼ Unrestricted Access: <input checked="" type="checkbox"/>	
Call and Device Control:	Call Origination/Termination and Device Status	None ▼
Call and Device Monitoring:	Device Monitoring	None ▼
	Calls On A Device Monitoring	None ▼
	Call Monitoring	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▼

For future reference, you will want to copy the first Tlink under Security, Security Database, Tlinks, and paste it somewhere it will be easy to access later.



Security | Security Database | Tlinks

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security**
  - Account Management
  - Audit
  - Certificate Management
  - Enterprise Directory
  - Host AA
  - PAM
  - Security Database**
    - Control
    - CTI Users
    - Devices
    - Device Groups
    - Tlinks**
    - Tlink Groups
    - Worktops
  - Standard Reserved Ports
  - Tripwire Properties
- Status
- User Management
- Utilities
- Help

**Tlinks**

Tink Name

- AVAYA#CMSIM#CSTA#AESSIM
- AVAYA#CMSIM#CSTA-S#AESSIM

Delete Tink

Under Maintenance, open the Service Controller. Here, you will need to select TSAPI Service and click Restart Service.



## Application Enablement Services Management Console

Maintenance | Service Controller

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance**
  - Date Time/NTP Server
  - Security Database
  - Service Controller**
  - Server Data
- Networking
- Security
- Status
- User Management
- Utilities
- Help

**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop **Restart Service** Restart AE Server Restart Linux Restart Web Server

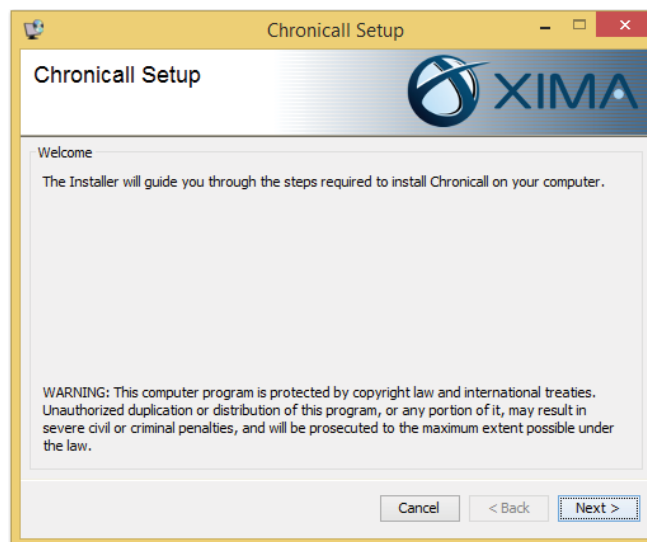
END

# Install Chronicall

The final step is to download and install Chronicall. Visit our downloads page at [www.ximasoftware.com/chronicall/downloads](http://www.ximasoftware.com/chronicall/downloads) and enter your serial key to access file downloads. If you do not have a serial key, visit [www.ximasoftware.com/chronicall/trial](http://www.ximasoftware.com/chronicall/trial) or talk to your Xima re-seller

Once you have downloaded the Chronicall installer, run it and follow the installation instructions as given.

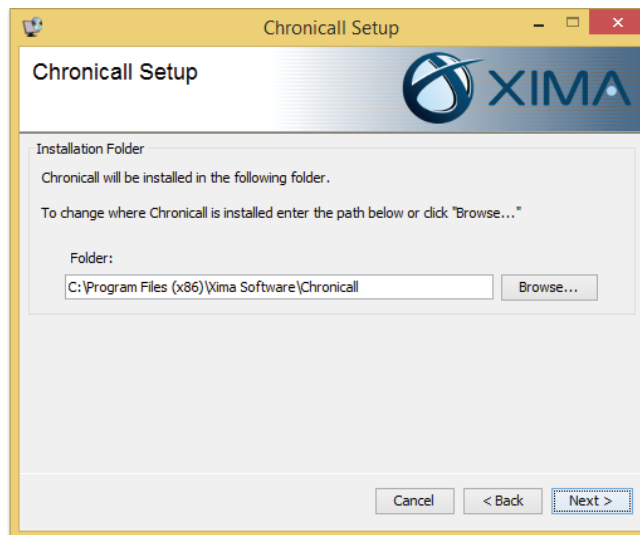
\*The most current version of Oracle's JVM is required for installation of Chronicall.



Read the License Agreement. You must accept the terms of this agreement before continuing with the installation.

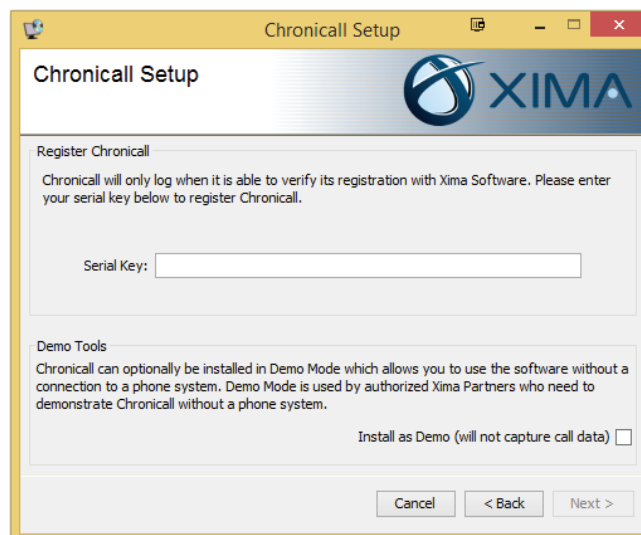


Chronicall will be installed in the folder shown. To change where Chronicall is installed, enter the file path or click Browse.



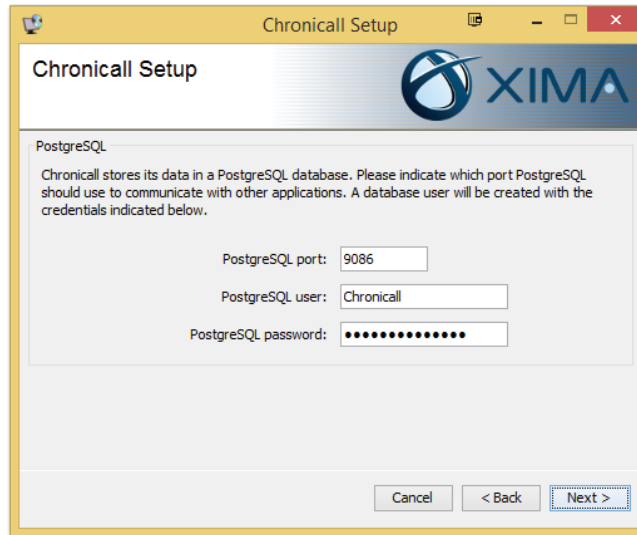
Chronicall will only log when it is able to verify its registration with Xima Software. Please enter your serial key below to register Chronicall.

Chronicall can optionally be installed in Demo Mode, which allows you to use the software without a connection to a phone system. Demo Mode is used by authorized Xima Partners who need to demonstrate Chronicall without a phone system.

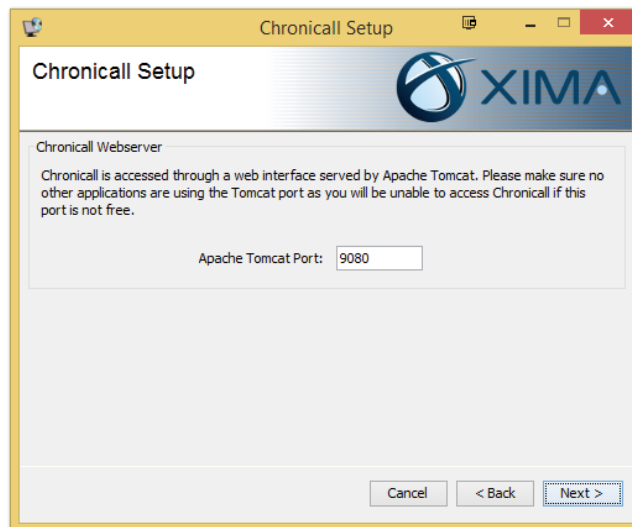




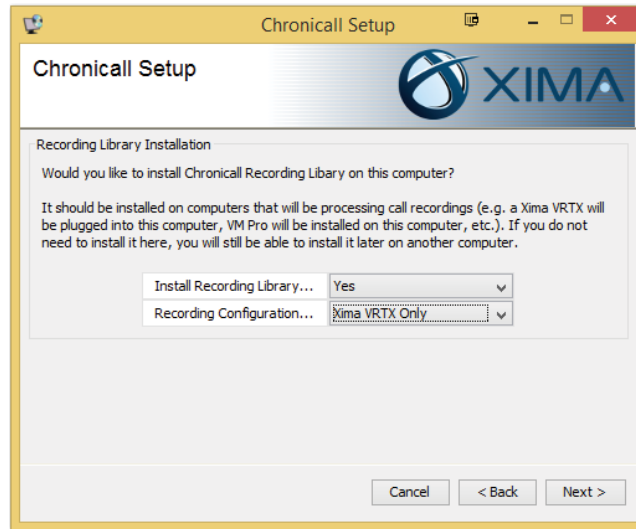
Chronicall stores its data in a PostgreSQL database. Indicate which port PostgreSQL should use to communication with other applications. A database user will be created with the credentials listed.



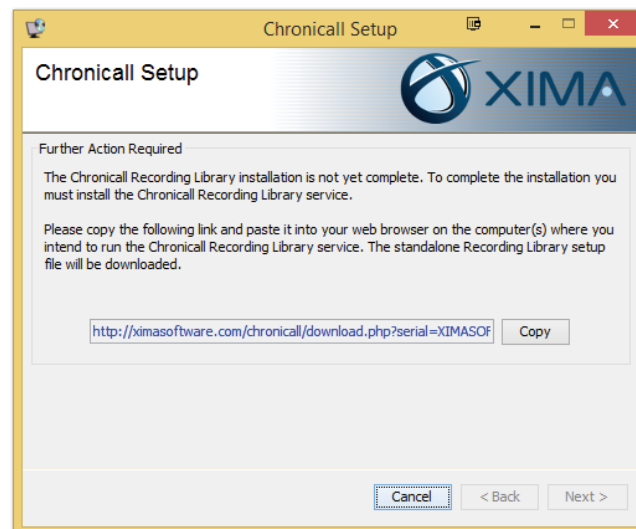
Chronicall is accessed through a web interface served by Apache Tomcat. Please make sure no other applications are using the Tomcat port as you will be unable to access Chronicall if this port is not free.



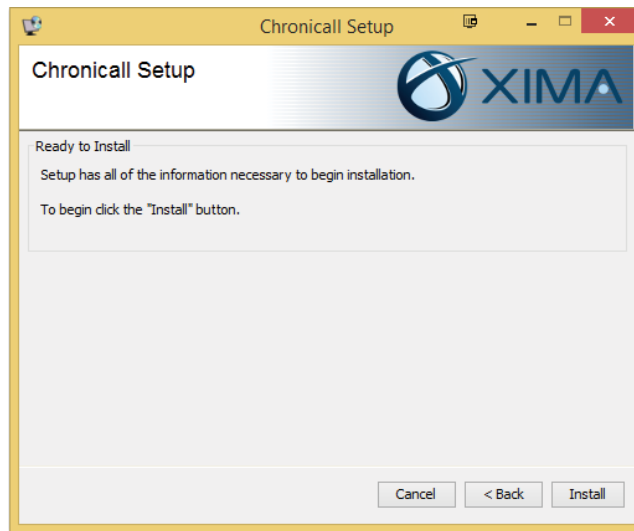
If your customer purchased Recording Library it will ask if you would like to Install the Recording Library Service. If this is the PC where the recordings will be stored please select "yes".



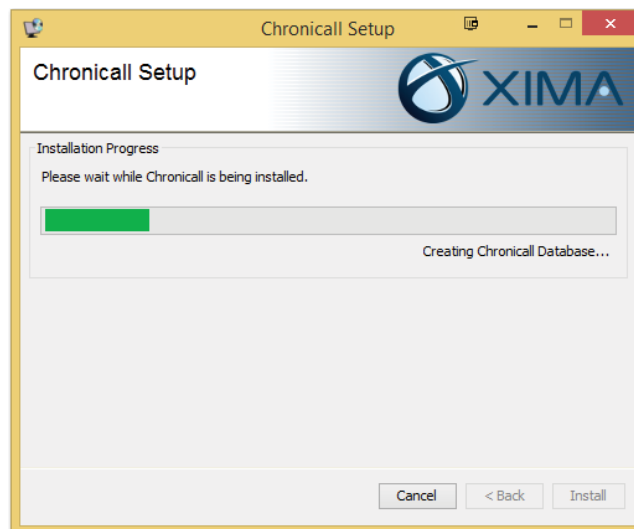
If this is not the PC where the recordings will be stored it will ask you to copy a URL that you can use to install the Recording Library software on the storage PC.



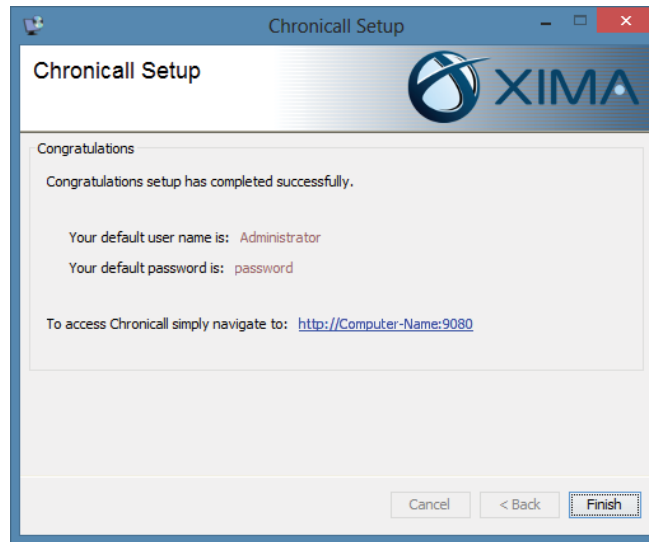
Once you reach this screen, the installer has all of the information necessary to begin installation. To begin, click the Install button.



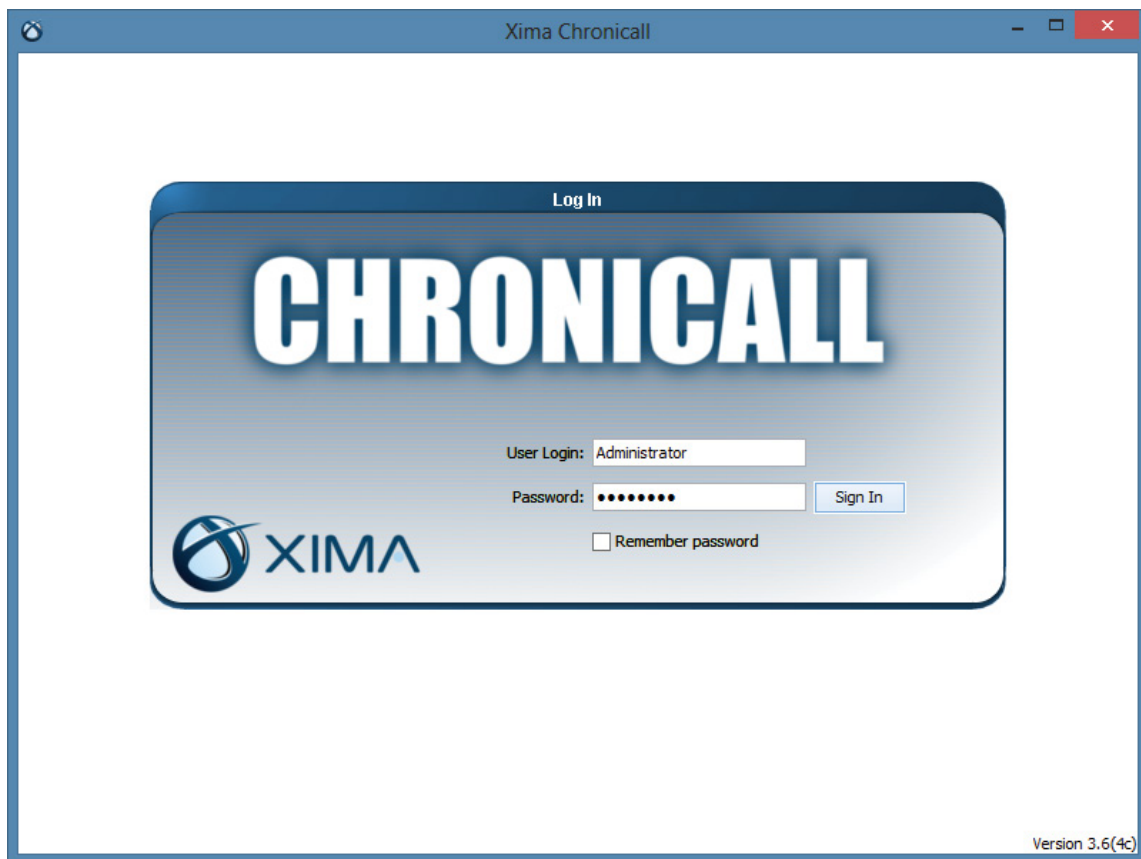
A progress bar will be displayed while Chronical is installed.



When the installation is finished, copy or bookmark the web address given to you. This is how you will access Chronicall.



Open Chronicall. The default user login is **Administrator**, and the password is **password**. These can be changed later.



The first time you open the Chronicall web client, you will be presented with a short setup wizard that will help you connect your phone system and choose agents for Realtime and Agent Dashboards functions. You can skip this setup process by clicking Skip in the bottom right corner of the Chronicall window, but it will reappear the next time you use Chronicall.

Are you going to use TSAPI licenses to log additional details? If yes, select Use TSAPI. If no, select Do Not use TSAPI

Communication Manager (site 1) Configuration

TSAPI Logging

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

Use TSAPI

Do not use TSAPI

< Back    Next >

If you Select yes, please follow the next step. If you selected no, please proceed to CDR only installation.

The first time you open the Chronicall web client, you will be presented with a short setup wizard that will help you connect your phone system and choose agents for Realtime and Agent Dashboards functions. You can skip this setup process by clicking Skip in the bottom right corner of the Chronicall window, but it will reappear the next time you use Chronicall.

Enter your AES and CM server information. Hitting next will verify that your CM user is created and has necessary access. After your CM user is verified it will download information including your users and groups which may take a couple of minutes.

The screenshot shows a configuration window titled "Communication Manager (site 1) Configuration". The main heading is "Load Users and Groups". Below this, a text box explains: "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." Below the text are four input fields: "AES IP Address:" with a placeholder "xxx.xxx.xxx.xxx", "CM IP Address:" with a placeholder "xxx.xxx.xxx.xxx", "CM User:" with a placeholder "Username", and "CM Password:" with a placeholder of ten dots. At the bottom right, there are two buttons: "< Back" and "Next >".

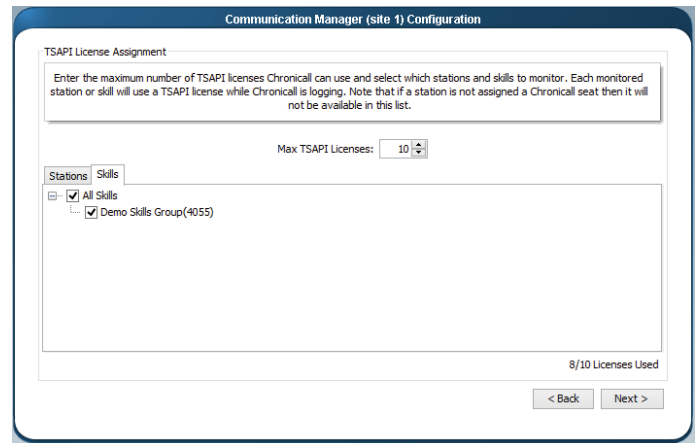
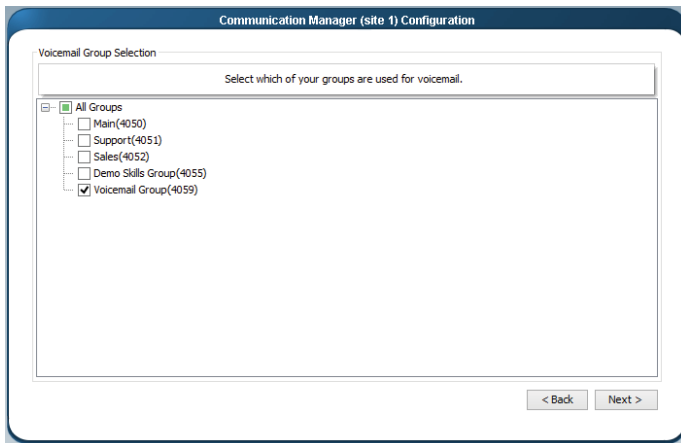
Enter the requested TSAPI and AES information. Hitting next will verify that your AES user is created and has necessary access.

The screenshot shows a configuration window titled "Communication Manager (site 1) Configuration". Inside, there is a section for "TSAPI Settings" with 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 message are four input fields: "TSAPI Service Port" (containing "450"), "Tlink", "AES User", and "AES Password". At the bottom right, there are two buttons: "< Back" and "Next >".

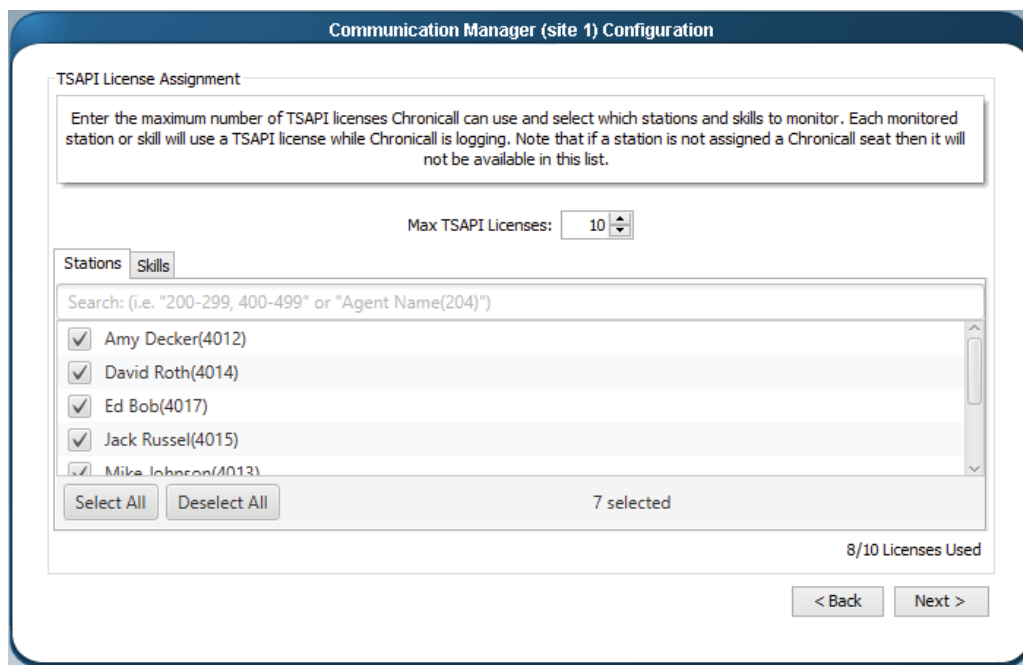
Enter which stations, and agents you would like to log data for within Chronicall.

The screenshot shows a configuration window titled "Communication Manager (site 1) Configuration". Inside, there is a section for "Chronicall Seat Assignment" with a message: "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 this message is a search bar with the text "Search: (i.e. '200-299, 400-499' or 'Agent Name(204)')". Below the search bar is a list of agents with checkboxes: Amy Decker(4012), David Roth(4014), Ed Bob(4017), Jack Russel(4015), Mike Johnson(4013), Richard Jacobs(4016), Test(1000), and Xima Skills Agent(64014). At the bottom left, there are two buttons: "Select All" and "Deselect All". At the bottom right, there is a status indicator "8 / 100 selected" and two buttons: "< Back" and "Next >".

Set a number of max TSAPI licenses and check the boxes for the stations and skills you would like to monitor. Please note, that if you don't assign a TSAPI license to a station or agent, they will default to CDR logging. Logging both TSAPI and CDR is possible.

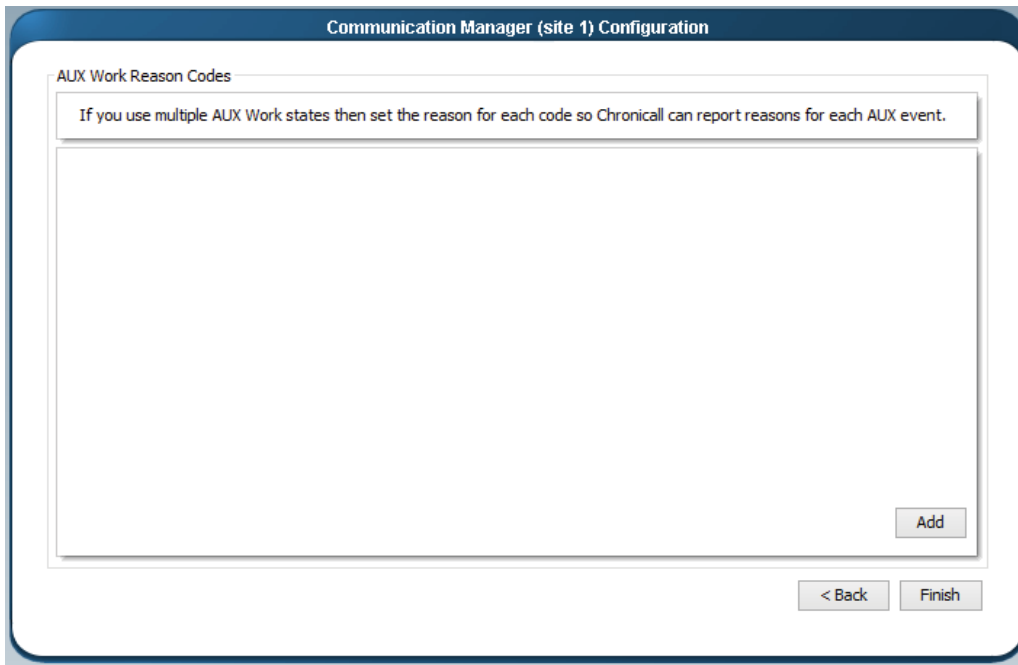


Select the hunt group you use for voicemail.

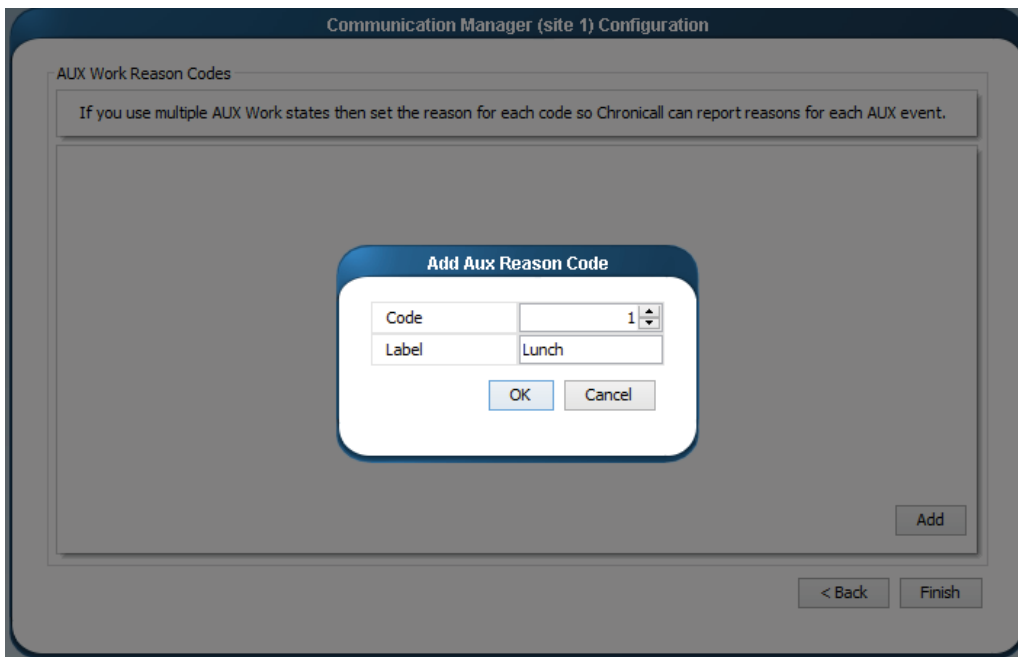




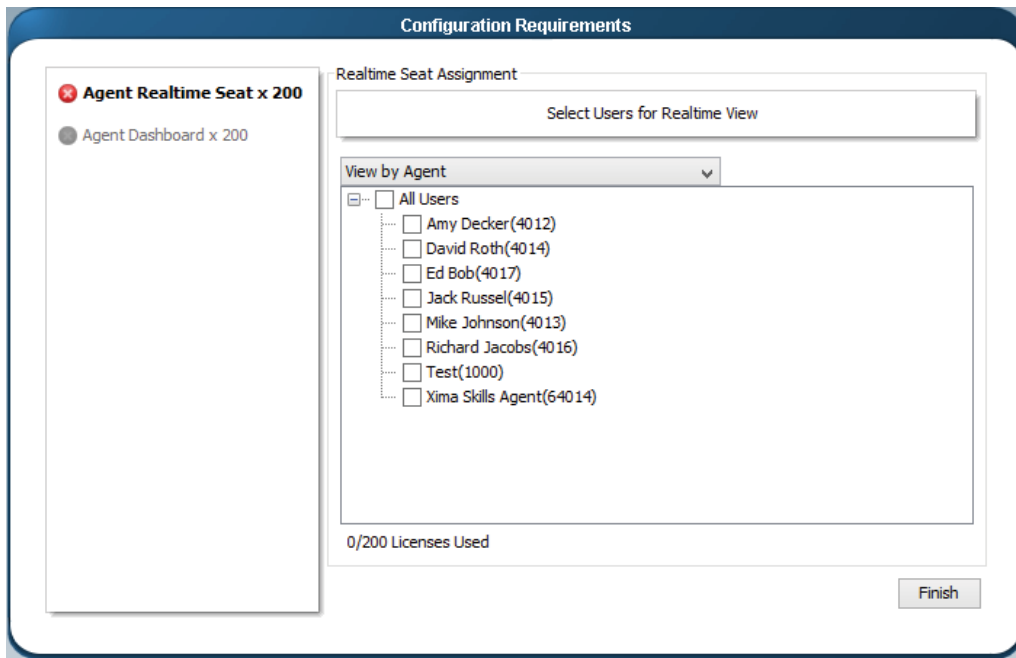
On this screen, you can enter information about your AUX Work states and reason codes. Select Add to add a new reason code.



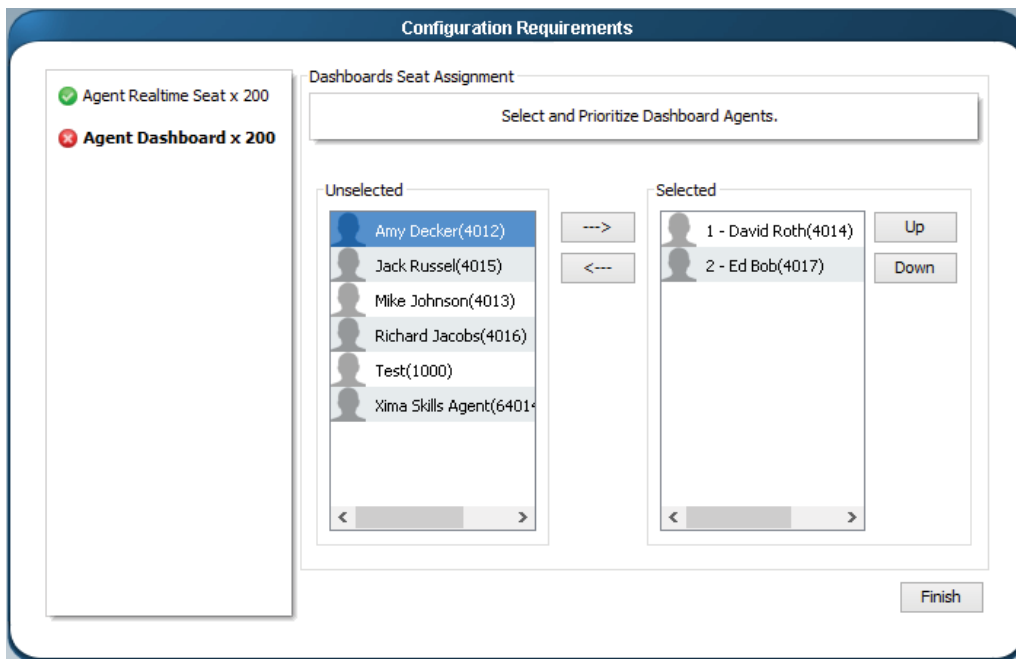
Choose a code number and name for each reason code, then press OK.



On this screen, choose the users you would like to monitor with Realtime.



On this screen, choose the users you would like to monitor with Dashboards.



## CDR Installation instructions

If you are logging data with an AES server please select Do not use TSAPI.

The screenshot shows a configuration window titled "Communication Manager (site 1) Configuration". The section is "TSAPI Logging". A text box contains the following text: "Do you intend to log using the Avaya TSAPI licenses? TSAPI Licenses allow you to capture more granular data on extensions and skills. If you choose not to use TSAPI, logging will be done using CDR alone and will be slightly less granular." Below this text are two radio button options: "Use TSAPI" (unselected) and "Do not use TSAPI" (selected). At the bottom right, there are two buttons: "< Back" and "Next >".

Enter your AES and CM server information. Hitting next will verify that your CM user is created and has necessary access. After your CM user is verified it will download information including your users and groups which may take a couple of minutes. If you do not have an AES server, please click Import Configuration Manually to import your users and groups.

The screenshot shows a configuration window titled "Communication Manager (site 1) Configuration". The section is "Load Users and Groups". A text box contains the following text: "In order to automatically load your users and groups Chronical 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." Below this text are four input fields with labels: "AES IP Address:", "CM IP Address:", "CM User:", and "CM Password:". At the bottom right, there is a green link labeled "Import Configuration Manually" and two buttons: "< Back" and "Next >".

You will need to import each of the files listed below in order to categorize the database with the CDR records

Communication Manager (site 1) Configuration

Manual Configuration Import

Please use Avaya Site Administrator to export your vdns, vectors, groups, stations, and agents. Then select the export files to be imported into Chronical. Chronical uses this information to associate extensions in CDR records to the actual device on your system.

CM IP Address:

VDN Export  
 Browse...

Vector Export  
 Browse...

Group Export  
 Browse...

Station Export  
 Browse...

Agent Export  
 Browse...

< Back    Next >

Each file should be imported as a .txt file

Communication Manager (site 1) Configuration

Manual Configuration Import

Please use Avaya Site Administrator to export your vdns, vectors, groups, stations, and agents. Then select the export files to be imported into Chronical. Chronical uses this information to associate extensions in CDR records to the actual device on your system.

CM IP Address:

VDN Export  
 Browse...

Vector Export  
 Browse...

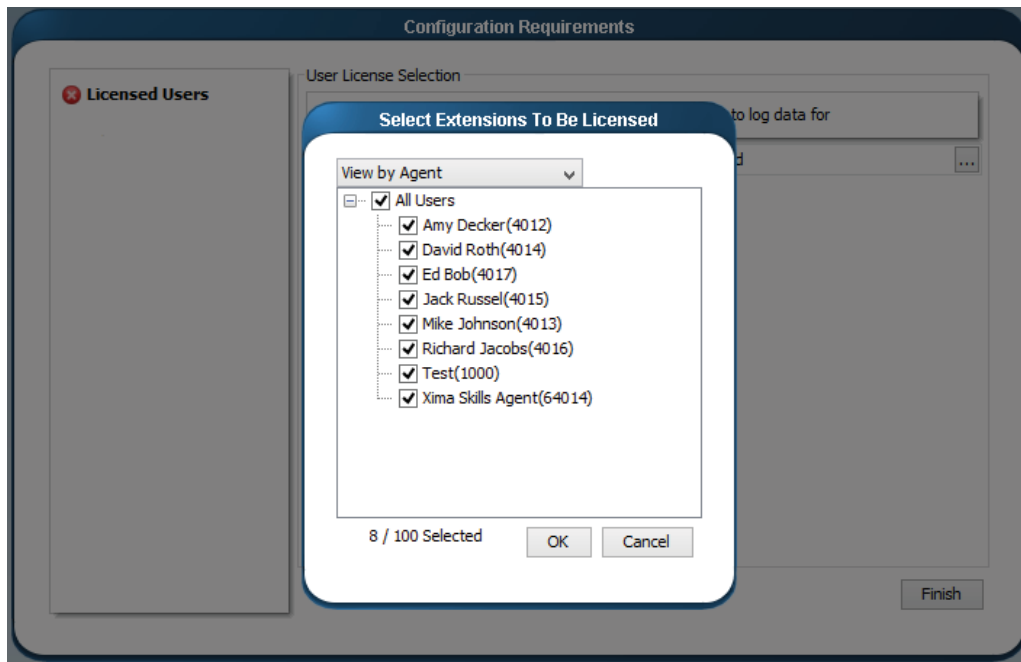
Group Export  
 Browse...

Station Export  
 Browse...

Agent Export  
 Browse...

< Back    Next >

Please select which users receive a Chronicall logging license



You have finished installing Chronicall.

Press Finish and you will be taken to the main Chronicall interface. Visit our support site at [www.ximasoftware.com/support](http://www.ximasoftware.com/support) for additional information.