



## **Application Notes for Unimax 2nd Nature 9.1 with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Unimax 2nd Nature 9.1 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. Unimax 2nd Nature is a centralized enterprise voice administration and provisioning solution.

In the compliance testing, Unimax 2nd Nature used the System Management Services from Avaya Aura® Application Enablement Services to provide an administration interface for provisioning of resources on Avaya Aura® Communication Manager.

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 Unimax 2nd Nature 9.1 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. Unimax 2nd Nature is a centralized enterprise voice administration and provisioning solution.

In the compliance testing, 2nd Nature used the System Management Services (SMS) from Application Enablement Services to provide an administration interface to 2nd Nature clients for provisioning of resources on Communication Manager.

SMS is a web service that provides programmatic access to a subset of administration objects available via Communication Manager System Access Terminal (SAT) screens. SMS enables clients with Simple Object Access Protocol (SOAP) based access to list, display, add, change, and remove specific managed objects on Communication Manager.

Testing was performed with the 2nd Nature client application, which supports the complete set of objects on the 2nd Nature server. The results should be extendable to other client applications LineOne, HelpOne, and Spotlight, with each supporting a subset of the objects on 2nd Nature.

## 2. General Test Approach and Test Results

All test cases were performed manually. Actions were taken on 2nd Nature and Communication Manager to alter data associated with supported objects, and to verify data stayed in sync between the two systems.

The objects were modified on 2nd Nature using the 2nd Nature client application, and modified on Communication Manager using SAT. For each supported object, a subset of parameters was chosen at random to modify and verify, therefore not all parameters were tested.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the 2nd Nature server.

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

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and 2nd Nature utilized the enabled capabilities of HTTPS.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on 2nd Nature:

- Use of SMS service to download, synchronize, and display specific managed objects.
- Use of SMS service to add, change, and remove specific managed objects.
- Proper handling of the following SMS objects:

AAR Analysis	Locations
Abbreviated Dialing Group	Node Names
Abbreviated Dialing System	Off PBX Telephone Feature Name Ext
Agent	Off PBX Telephone Station Mapping
Alias Station	Pickup Group
Amw	Public Unknown Numbering
Announcement	Remote Access
ARS Analysis	Route Pattern
Authorization Code	Service Hours Table
Configuration	Site Data
COR	Station
COS	System Parameters Customer Options
Coverage Answer Group	System Parameters Features
Coverage Path	System Parameters Special Applications
Coverage Remote	System Parameters Security
Data Module	Tenant
Dial Plan Analysis	Terminating Extension Group
Extension Station	Trunk Group
Feature Access Codes	Uniform Dial Plan
Holiday Tables	VDN
Hunt Group	Vector
Intercom Group	VRT
IP Stations	Vector Variables

The serviceability testing focused on verifying the ability of 2nd Nature to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the 2nd Nature server.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on 2nd Nature from the compliance testing.

- By design, 2nd Nature does not necessarily duplicate all parameter validations that are supported by Communication Manager.
- Attendant and remote access extensions did not get factored into the Extensions Available and Extension Used listings.
- Changes to the last entry in abbreviated dialing group lists and vector variables did not get sent properly to Communication Manager. This is being addressed by Unimax, and the fix will be made available in the next major and minor release.
- Cannot add vector numbers beyond 2000 for a large system despite capacity limit being 8000 on Communication Manager. This is being addressed by Unimax, and the fix will be made available in the next major and minor release.
- Creation of ring-stat station button was allowed by 2nd Nature despite the associated SA8428 Station User Button Ring Control special application being disabled. This creation request was subsequently rejected by Communication Manager.

## 2.3. Support

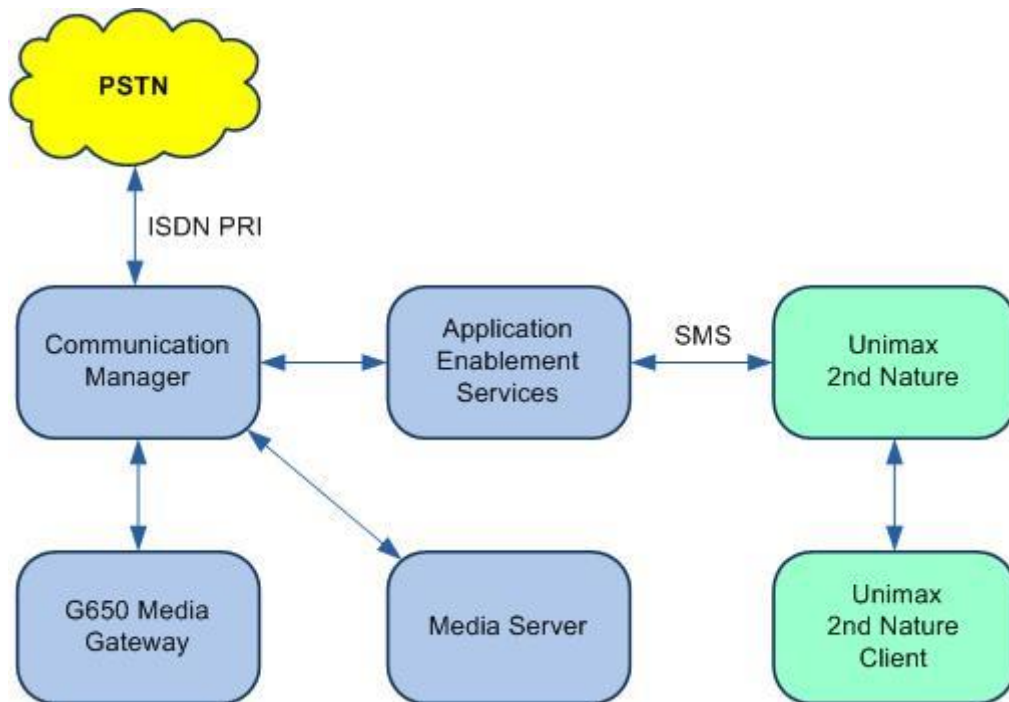
Technical support on 2nd Nature can be obtained through the following:

- **Phone:** (612) 204-3661
- **Email:** <http://www.unimax.com/support>

### 3. Reference Configuration

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

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of objects on Communication Manager are not the focus of these Application Notes and will not be described.



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.0.1 (8.0.1.0.0.822.25031)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.0.150
Avaya Aura® Application Enablement Services in Virtual Environment	8.0 (8.0.0.0.0.6-0)
Unimax 2nd Nature on Windows Server 2012 R2 Standard <ul style="list-style-type: none"><li>• Microsoft SQL Server 2014 Express</li></ul>	9.1 G4 12.0.2000.8
Unimax 2nd Nature on Windows 10 Pro	9.1 G4

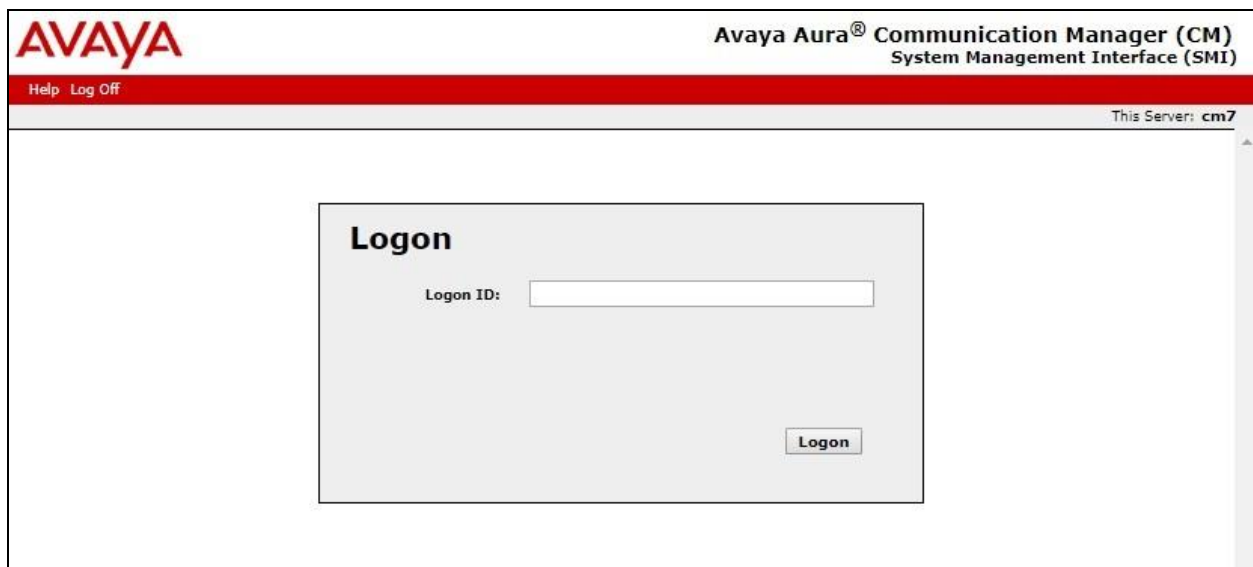
## 5. Configure Avaya Aura® Communication Manager

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

- Administer accounts

### 5.1. Administer Accounts

Access the 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 login page of the Avaya Aura® Communication Manager (CM) System Management Interface (SMI). The header includes the AVAYA logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and links for "Help" and "Log Off". A status bar indicates "This Server: cm7". The main content area features a "Logon" box with a "Logon ID:" label, a text input field, and a "Logon" button.

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



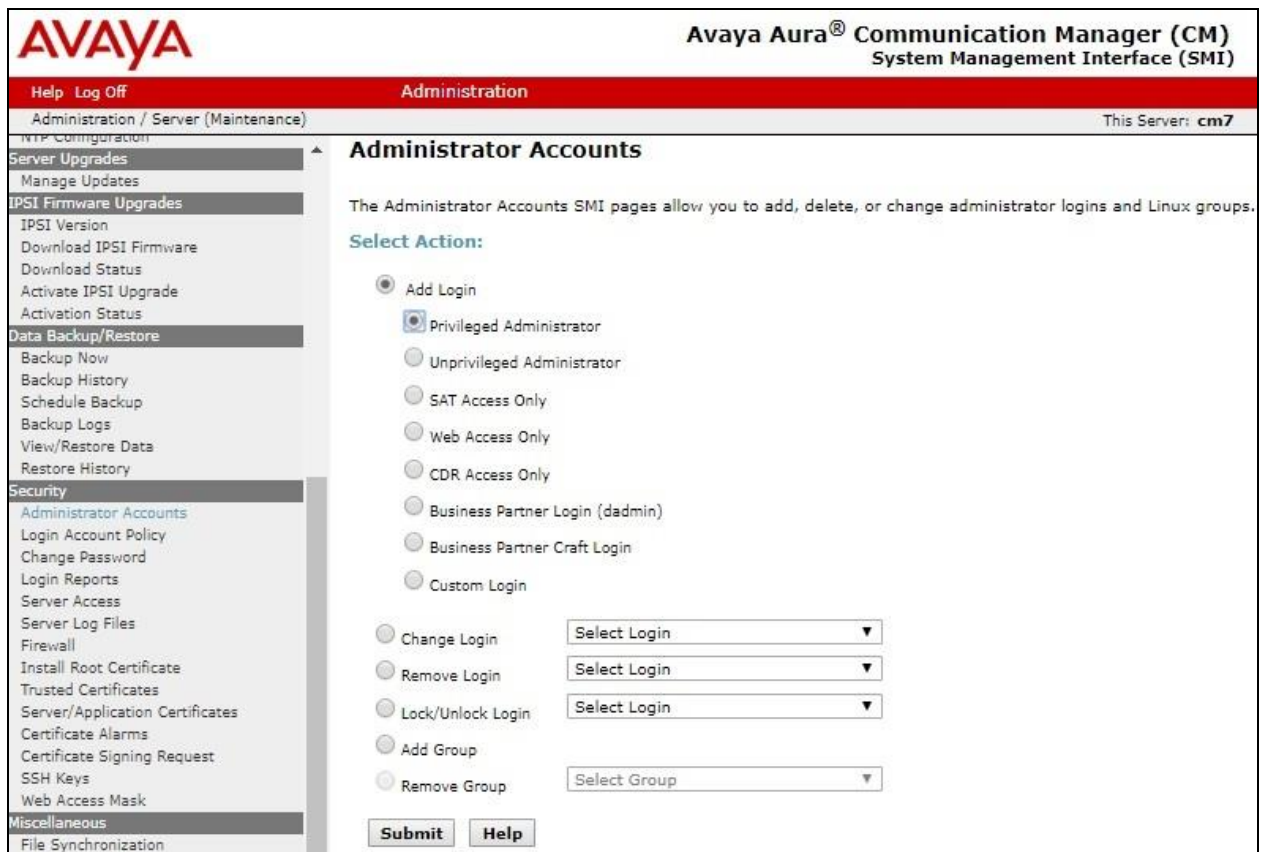
The screenshot shows the "Administration" screen of the Avaya Aura® Communication Manager (CM) System Management Interface (SMI). The header includes the AVAYA logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and links for "Help" and "Log Off". A status bar indicates "This Server: cm7". The main content area displays "System Management Interface" and "© 2001-2018 Avaya Inc. All Rights Reserved." Below this is a "Copyright" section with the following text: "Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law."



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

Make a note of the account credentials, which will be used later to configure 2nd Nature.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration page. The page title is "Administrator Accounts -- Add Login: Privileged Administrator". The left sidebar contains a navigation menu with categories: NTP Configuration, Server Upgrades, IPSI Firmware Upgrades, Data Backup/Restore, Security, and Miscellaneous. The "Security" category is expanded, showing "Administrator Accounts" as the selected option. The main content area contains a form for adding a new login. The form fields are: Login name (Unimax2N), Primary group (susers), Additional groups (profile) (prof18), Linux shell (/bin/bash), Home directory (/var/home/Unimax2N), Lock this account (unchecked), SAT Limit (none), Date after which account is disabled-blank to ignore (YYYY-MM-DD) (empty), Enter password (masked with dots), Re-enter password (masked with dots), and Force password change on next login (radio buttons for No and Yes, with No selected). The form is submitted via a "Submit" button, with "Cancel" and "Help" buttons also present.

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

Help Log Off Administration This Server: cm7

Administration / Server (Maintenance)

NTP Configuration  
Server Upgrades  
Manage Updates  
IPSI Firmware Upgrades  
IPSI Version  
Download IPSI Firmware  
Download Status  
Activate IPSI Upgrade  
Activation Status  
Data Backup/Restore  
Backup Now  
Backup History  
Schedule Backup  
Backup Logs  
View/Restore Data  
Restore History  
Security  
Administrator Accounts  
Login Account Policy  
Change Password  
Login Reports  
Server Access  
Server Log Files  
Firewall  
Install Root Certificate  
Trusted Certificates  
Server/Application Certificates  
Certificate Alarms  
Certificate Signing Request  
SSH Keys  
Web Access Mask  
Miscellaneous  
File Synchronization

**Administrator Accounts -- Add Login: Privileged Administrator**

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

Login name: Unimax2N

Primary group: susers

Additional groups (profile): prof18

Linux shell: /bin/bash

Home directory: /var/home/Unimax2N

Lock this account: ☐

SAT Limit: none

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

Enter password: .....

Re-enter password: .....

Force password change on next login: ☒ No ☐ Yes

Submit Cancel 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
- 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 separates the header from the main content area. In the center of the page is a login box with a light gray background. Inside this box, the text "Please login here:" is followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

 **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Feb 12 08:48:41 2019 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.0.0.6-0  
Server Date and Time: Tue Feb 12 10:39:11 EST 2019  
HA Status: Not Configured

Home

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. 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 configure **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 Feb 12 08:48:41 2019 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.0.0.6-0  
Server Date and Time: Tue Feb 12 10:39:11 EST 2019  
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

Server Media

RTP Local UDP Port Min\*30000

RTP Local UDP Port Max\*49999

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

SMS Proxy Ports

Proxy Port Min4101

Proxy Port Max4116

TLT; Reviewed:  
SPOC 4/17/2019

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

13 of 24  
Unimax-2N-AES8

### 6.3. Administer SMS Properties

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

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Tue Feb 12 08:48:41 2019 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 8.0.0.0.0.6-0", "Server Date and Time: Tue Feb 12 10:39:11 EST 2019", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "AE Services | SMS | SMS Properties" and "Home | Help | Logout". The left sidebar is dark gray and lists the following options: "AE Services" (expanded), "CVLAN", "DLG", "DMCC", "SMS" (expanded), "SMS Properties" (selected), "TSAPI", "TWS", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", and "Security".

The right pane displays the "SMS Properties" configuration form. The fields and their values are as follows:

Field	Value
Default CM Host Address	10.64.125.236
Default CM Admin Port	5022
CM Connection Protocol	SSH
SMS Logging	NORMAL
SMS Log Destination	apache
CM Proxy Trace Logging	NONE
Max Sessions per CM	5
Proxy Shutdown Timer	1800 seconds
SAT Login Keepalive	180 seconds
CM Terminal Type	OSSIZ
Proxy Log Destination	/var/log/avaya/aes/ossicm.log

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



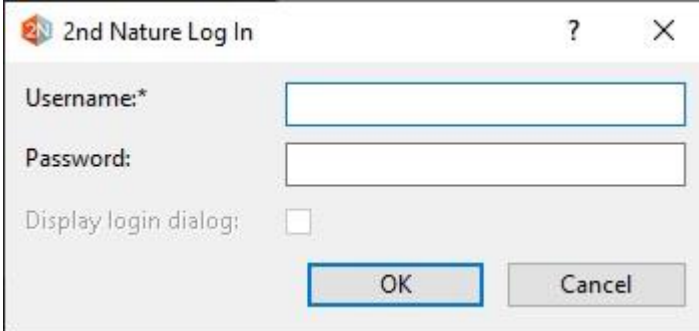
## 7. Configure Unimax 2nd Nature

This section provides the procedures for configuring 2nd Nature. The procedures include the following areas:

- Launch 2nd Nature
- Administer system
- Administer system connection
- Administer system releases
- Start communication service
- Download data

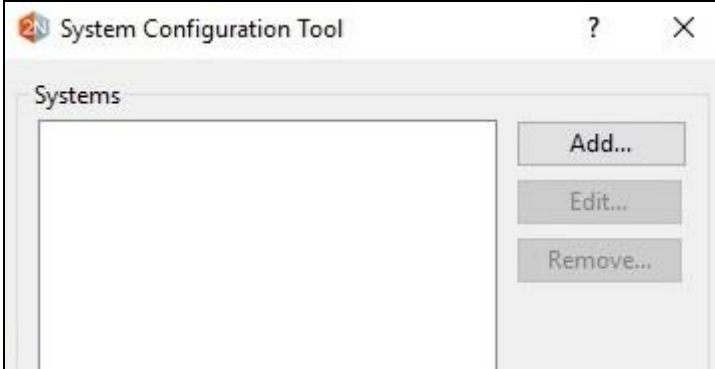
### 7.1. Launch 2nd Nature

From the 2nd Nature server, select **Start → 2nd Nature → 2nd Nature** to launch the application. The **2nd Nature Log In** screen below is displayed. Log in using the appropriate credentials.

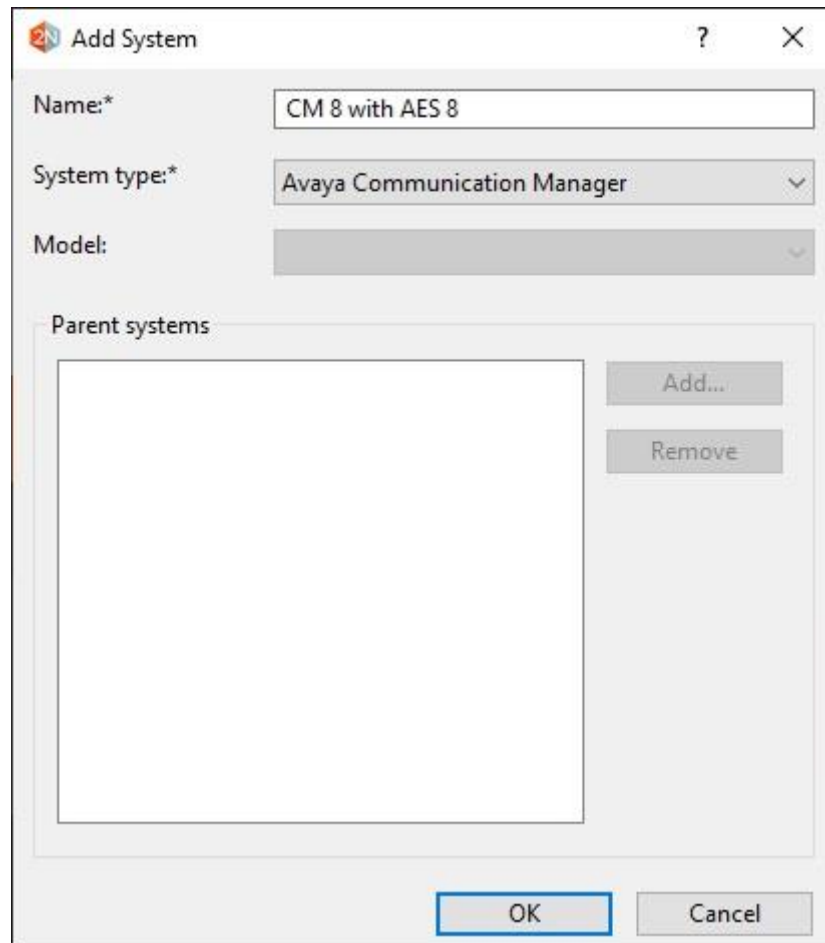
A screenshot of the '2nd Nature Log In' dialog box. The title bar shows the 2N logo, the text '2nd Nature Log In', and standard window controls (minimize, maximize, close). The dialog contains three input fields: 'Username:\*' with a text box, 'Password:' with a text box, and 'Display login dialog:' with an unchecked checkbox. At the bottom are 'OK' and 'Cancel' buttons.

### 7.2. Administer System

Upon initial log in, the **System Configuration Tool** screen is displayed next. Select **Add** to add a new system.

A screenshot of the 'System Configuration Tool' window. The title bar shows the 2N logo, the text 'System Configuration Tool', and standard window controls. The main area is titled 'Systems' and contains a large empty list box. To the right of the list box are three buttons: 'Add...', 'Edit...', and 'Remove...'.

The **Add System** screen is displayed. Enter a descriptive **Name**, and select “Avaya Communication Manager” from the **System type** drop-down list, as shown below.



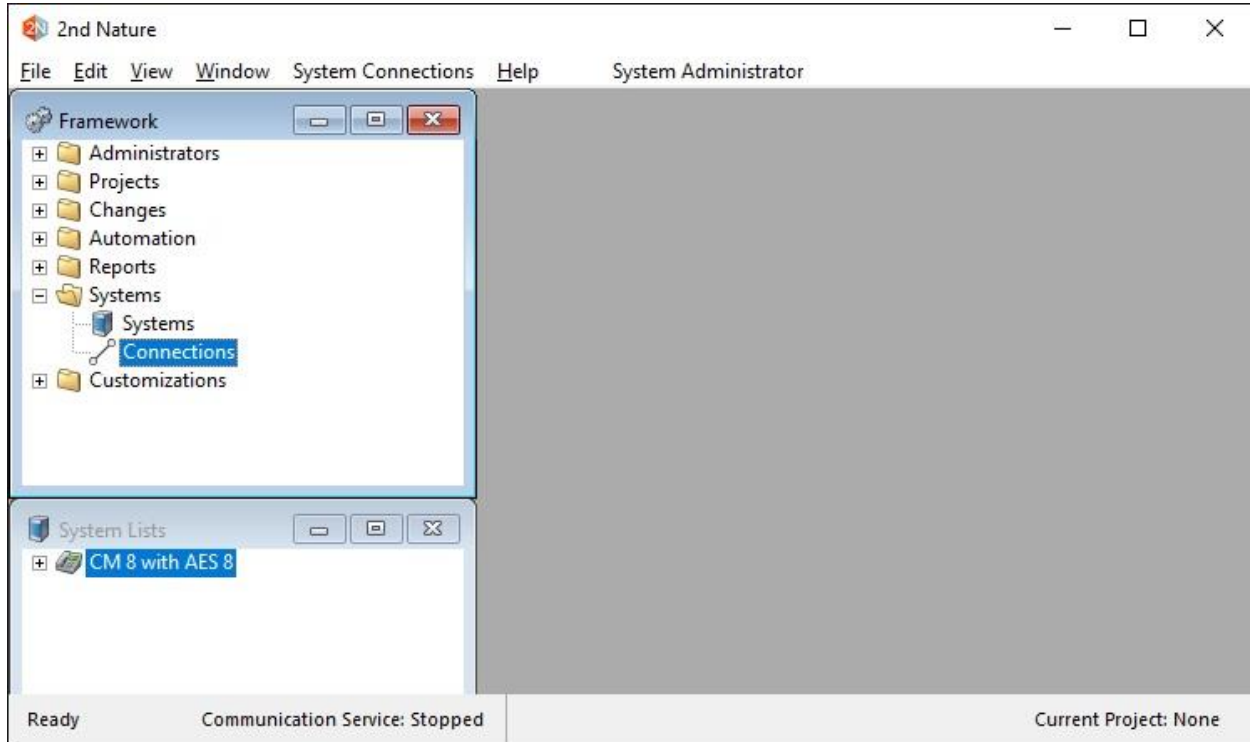
The screenshot shows a Windows-style dialog box titled "Add System". It has a standard title bar with a question mark icon and a close button (X). The dialog contains the following fields and controls:

- Name:** A text input field containing the text "CM 8 with AES 8".
- System type:** A dropdown menu with "Avaya Communication Manager" selected.
- Model:** A dropdown menu that is currently empty.
- Parent systems:** A section containing a large empty rectangular box on the left and two buttons, "Add..." and "Remove", on the right.
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.



### 7.3. Administer System Connection

The **2nd Nature** screen below is displayed. From the **Framework** pane, expand and right click on **Systems** → **Connections**, and select **Create** to create a new connection.



The **Field Selections** screen is displayed next. Click **Browse** and select the system name from **Section 7.2**.

The Field Selections dialog box contains the following information:

Please make your selection(s) and continue

Field	Value
System name*	CM 8 with AES 8 <input data-bbox="1047 1507 1218 1549" type="button" value="Browse..."/>
Type*	SOAP <input data-bbox="1193 1564 1218 1596" type="button" value="v"/>

The **Multiple Record Editor** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

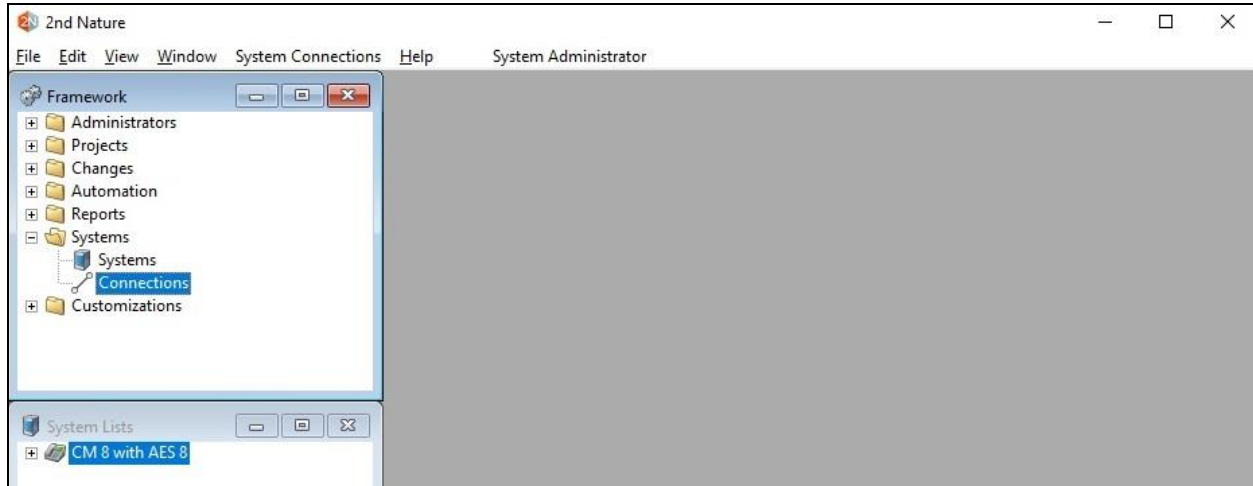
- **Communicator server:** Host name of the 2nd Nature server.
- **Host name:** Host name or IP address of Application Enablement Services.
- **Use encryption:** Check this field.
- **Port number:** “443”
- **Username:** Account name from **Section 5.1**, concatenated with IP address.
- **Password:** Account password from **Section 5.1**.

For **Username**, use the format “x@y”, where “x” is the account name from **Section 5.1** and “y” is the IP address of Communication Manager.

Field	Value
System name*	CM 8 with AES 8
Type*	SOAP
Name*	SOAP
Description	
Communication server*	WIN-LD0N0TK8GKE
Active	<input checked="" type="checkbox"/>
Priority	High
Host name*	10.64.101.239
Use encryption	<input checked="" type="checkbox"/>
Port number*	443
Username*	Unimax2N@10.64.101.236
Password	*****
Avaya CM terminal emulator enabled	<input type="checkbox"/>
Avaya CM terminal emulator executable path	
Avaya CM terminal emulator server name	
Avaya CM terminal emulator username	
Avaya CM terminal emulator password	

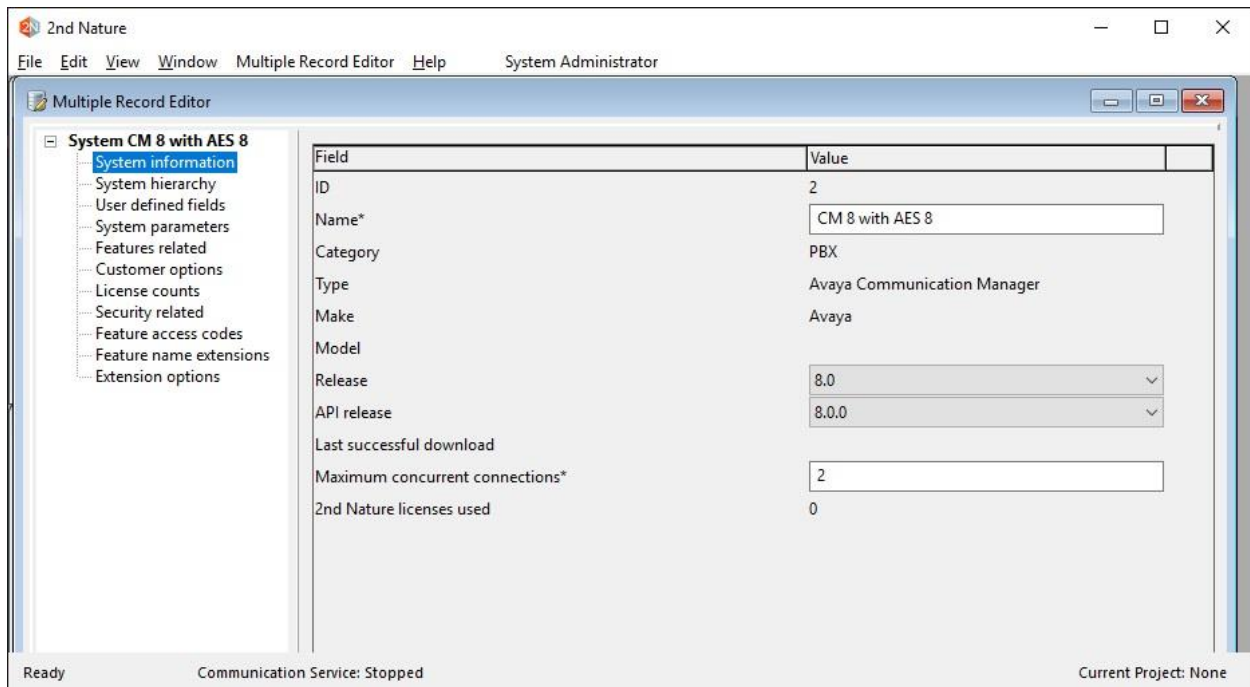
## 7.4. Administer System Releases

The **2nd Nature** screen below is displayed again. In the **System Lists** pane, right click on the entry associated with the system name from **Section 7.2** and select **Modify**.



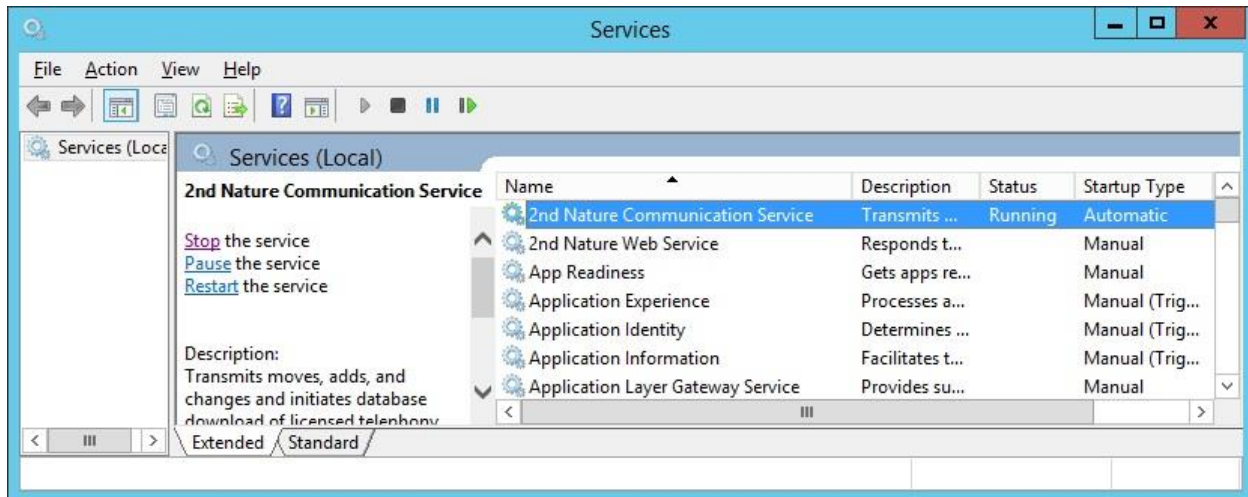
The **Multiple Record Editor** screen below is displayed. Select the following values for the specified fields, and retain the default values for the remaining fields.

- **Release:** Release of Communication Manager, in this case “8.0”.
- **API release:** Release of Application Enablement Services SMS, in this case “8.0.0”.



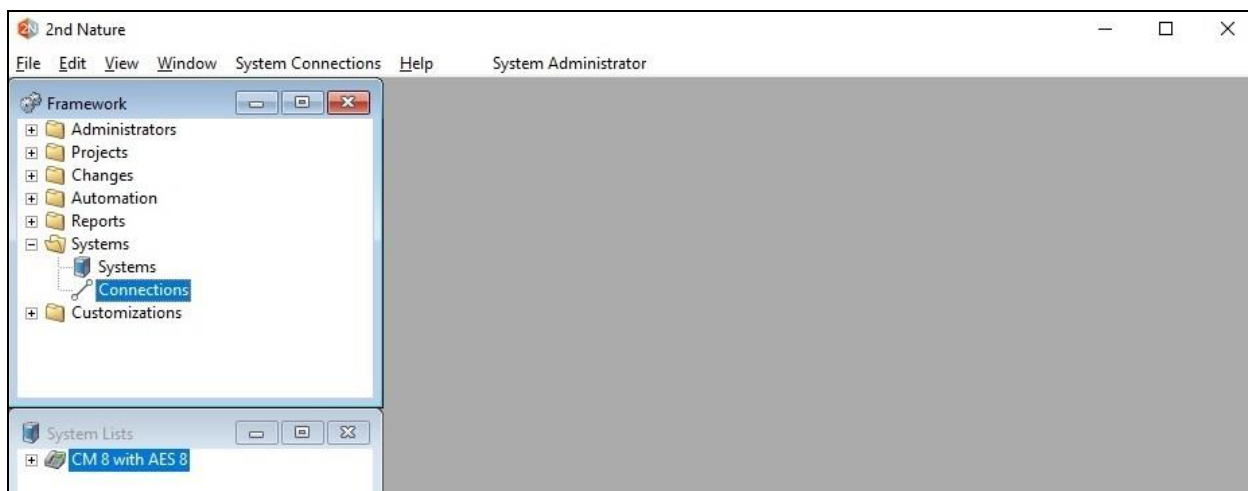
## 7.5. Start Communication Service

From the 2nd Nature server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Start the **2nd Nature Communication Service** shown below.



## 7.6. Download Data

The **2nd Nature** screen below is displayed again. In the **System Lists** pane, right click on the entry associated with the system name from **Section 7.2** and select **Download** to obtain data and to populate the 2nd Nature database.



The **Multiple Record Editor** screen below is displayed. Retain all default values to start the download. Note that downloads can also be scheduled to be performed on a regular basis.

The screenshot shows the 'Multiple Record Editor' window in the '2nd Nature' application. The window title bar includes '2nd Nature' and standard window controls. The menu bar contains 'File', 'Edit', 'View', 'Window', 'Multiple Record Editor', 'Help', and 'System Administrator'. The main area is titled 'Multiple Record Editor' and contains a tree view on the left with 'Project Schedule Download C' expanded, showing 'Schedule' and 'Options' sub-items. The main pane displays scheduling options:

- ☒ Send now
- ☐ Run at a specific date and time: 2/12/2019 10:55:07 AM
- ☐ Postpone
- ☐ Expired
- ☐ Recurring:
  - Recurring day:**
    - ☐ Every day
    - ☐ Every: S M T W T F S (all unchecked)
  - Recurring time:**
    - ☐ Run at: 10:55:07 AM
    - ☐ Repeat every: [ ] hrs [ ] mins
    - ☐ from: 10:55:07 AM to: 10:55:07 AM

At the bottom right are 'OK' and 'Cancel' buttons. The status bar at the very bottom shows 'Ready', 'Communication Service: Running', and 'Current Project: None'.

## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and 2nd Nature.

For Communication Manager, log into SAT and issue command for a supported SMS object from **Section 2.1**, in this case “list authorization-code”.

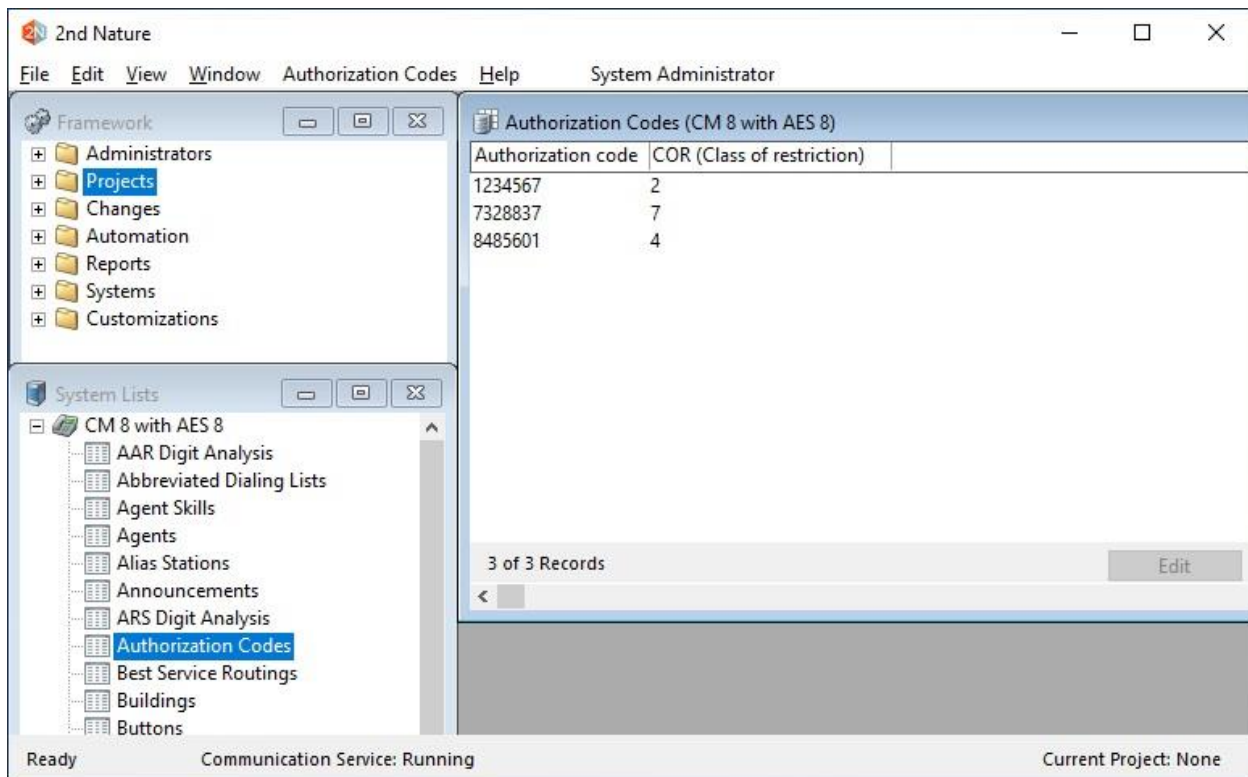
```
list authorization-code
```

LIST AUTHORIZATION CODES REPORT

Authorization Code	Class of Restriction(COR)
1234567	2
7328837	7
8485601	4

On the **2nd Nature** screen, expand the entry in the **System Lists** pane, and double click on **Authorization Codes**.

Verify that the **Authorization Codes** pane is created, showing a list of authorization codes retrieved from Communication Manager, as shown below. Also verify that the entries match the results from Communication Manager SAT screen above.



## 9. Conclusion

These Application Notes describe the configuration steps required for Unimax 2nd Nature 9.1 to successfully interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 2.1, November 2018, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.0, Issue 1, July 2018, available at <http://support.avaya.com>.
3. *2nd Nature Administrator Guide*, Version 9.1, September 2018, available as part of 2nd Nature installation.
4. *2nd Nature Avaya Communication Manager User Guide*, Version 9.1, September 2018, available as part of 2nd Nature installation.

---

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

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

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