



Avaya Solution & Interoperability Test Lab

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.

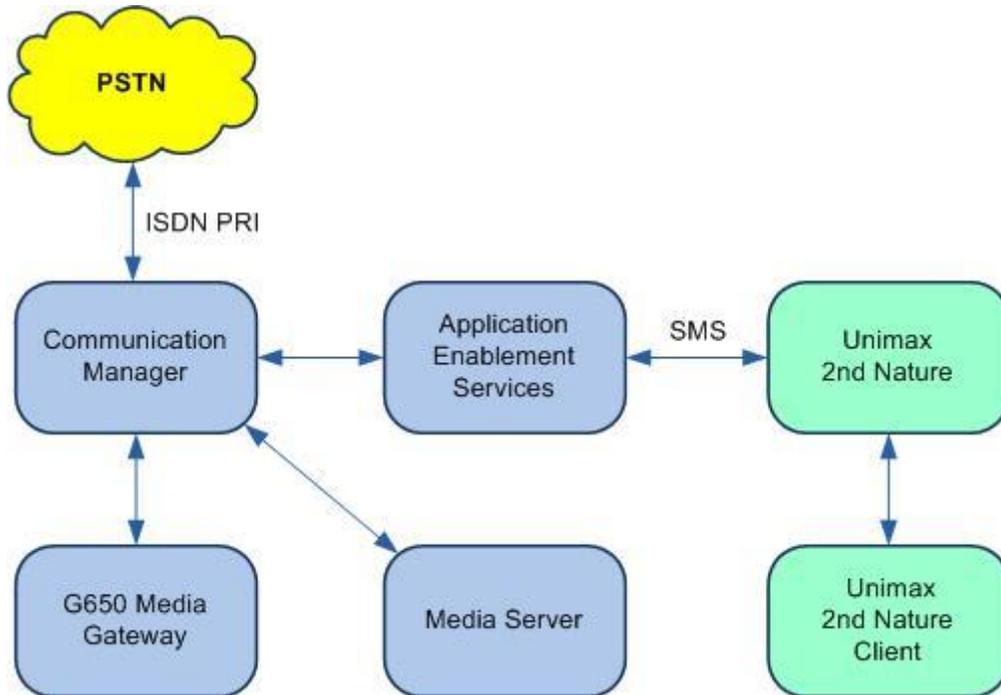


Figure 1: Compliance Testing Configuration

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">• Microsoft SQL Server 2014 Express	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 Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Logon screen. The page features the Avaya logo in the top left corner and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" in the top right. A red navigation bar contains "Help" and "Log Off" links. The main content area is titled "Logon" and contains a "Logon ID:" label next to a text input field. A "Logon" button is positioned below the input field. The server name "This Server: cm7" is displayed in the top right corner of the main content area.

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

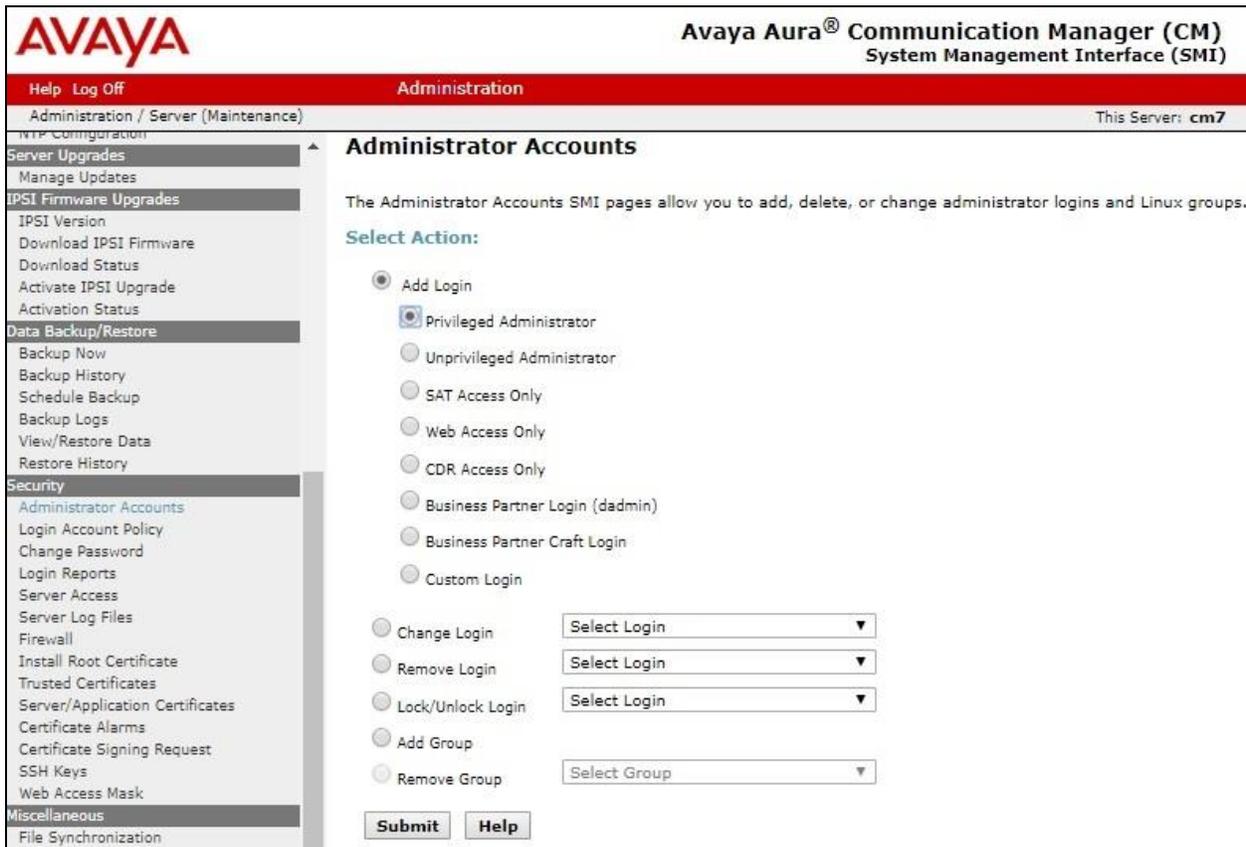


The screenshot shows the Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Administration screen. The page features the Avaya logo in the top left corner and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" in the top right. A red navigation bar contains "Help" and "Log Off" links, and the "Administration" menu item is highlighted. The main content area is titled "System Management Interface" and contains the copyright notice "© 2001-2018 Avaya Inc. All Rights Reserved." and a "Copyright" section. The server name "This Server: cm7" is displayed in the top right corner of the main content area.

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, Manage Updates, IPSI Firmware Upgrades, Data Backup/Restore, Security, and Miscellaneous. The "Administrator Accounts" option is selected under the Security category. The main content area contains the following fields and options:

- 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):** [Empty field]
- Enter password:** [Masked with dots]
- Re-enter password:** [Masked with dots]
- Force password change on next login:** No, Yes

At the bottom of the form are three buttons: **Submit**, **Cancel**, and **Help**. The top navigation bar includes "Help Log Off" and "Administration". The server name "cm7" is displayed in the top right corner.

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 reads "Application Enablement Services" and "Management Console". Below this is a red horizontal bar. The main content area contains a login form with the heading "Please login here:". The form includes two input fields: "Username" and "Password". Below the fields are two buttons: "Login" and "Reset". At the bottom of the page, there is a red horizontal bar and a copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the text "Application Enablement Services Management Console". At the top right, there is a welcome message for the user, including login details, host information, and server status. Below this is a red navigation bar with "Home", "Help", and "Logout" links. On the left side, there is a vertical menu with various service categories. The main content area displays a "Welcome to OAM" message, followed by a paragraph explaining the OAM web's purpose and a bulleted list of administrative domains and their functions. At the bottom of the main content area, there is a note about administrative domains.

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 | 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.

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 Enabled Disabled

Unencrypted TCP Port	9999	<input checked="" type="radio"/> <input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>	<input type="radio"/> <input type="radio"/>

DLG Port Enabled Disabled

TCP Port	5678	
----------	------	--

TSAPI Ports Enabled Disabled

TSAPI Service Port	450	<input checked="" type="radio"/> <input type="radio"/>
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	
Unencrypted TLINK Ports		
TCP Port Min	<input type="text" value="1050"/>	
TCP Port Max	<input type="text" value="1065"/>	
Encrypted TLINK Ports		
TCP Port Min	<input type="text" value="1066"/>	
TCP Port Max	<input type="text" value="1081"/>	

DMCC Server Ports Enabled Disabled

Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/> <input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>	<input type="radio"/> <input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>	<input type="radio"/> <input checked="" type="radio"/>

H.323 Ports Enabled Disabled

TCP Port Min	<input type="text" value="20000"/>	
TCP Port Max	<input type="text" value="29999"/>	
Local UDP Port Min	<input type="text" value="20000"/>	
Local UDP Port Max	<input type="text" value="29999"/>	
Server Media		
RTP Local UDP Port Min*	<input type="text" value="30000"/>	<input checked="" type="radio"/> <input type="radio"/>
RTP Local UDP Port Max*	<input type="text" value="49999"/>	

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

SMS Proxy Ports

Proxy Port Min	<input type="text" value="4101"/>	
Proxy Port Max	<input type="text" value="4116"/>	

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 right corner shows system information: "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", and "HA Status: Not Configured". A red navigation bar contains "AE Services | SMS | SMS Properties" and "Home | Help | Logout". The left sidebar lists navigation 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 main content area is titled "SMS Properties" and contains the following configuration fields: 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), and Proxy Log Destination (/var/log/avaya/aes/ossicm.log). At the bottom of the configuration area are three buttons: "Apply Changes", "Restore Defaults", and "Cancel".

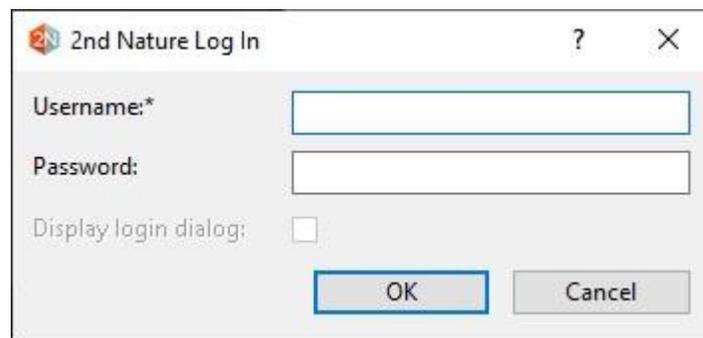
7. Configure Unimax 2nd Nature

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

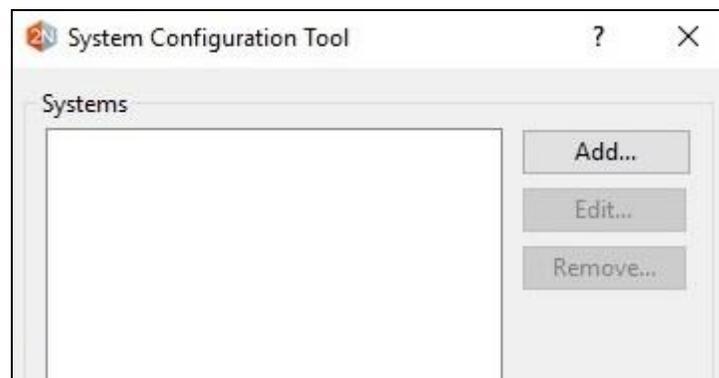
From the 2nd Nature server, select **Start** → **2nd Nature** → **2nd Nature** to launch the application. The **2nd Nature Log In** screen below is displayed. Log in using the appropriate credentials.



The screenshot shows a dialog box titled "2nd Nature Log In". It contains three input fields: "Username:*" with an asterisk indicating it is required, "Password:", and "Display login dialog:" with an unchecked checkbox. Below the input fields are two buttons: "OK" and "Cancel".

7.2. Administer System

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



The screenshot shows a dialog box titled "System Configuration Tool". It features a list box labeled "Systems" which is currently empty. To the right of the list box are three buttons: "Add...", "Edit...", and "Remove...".

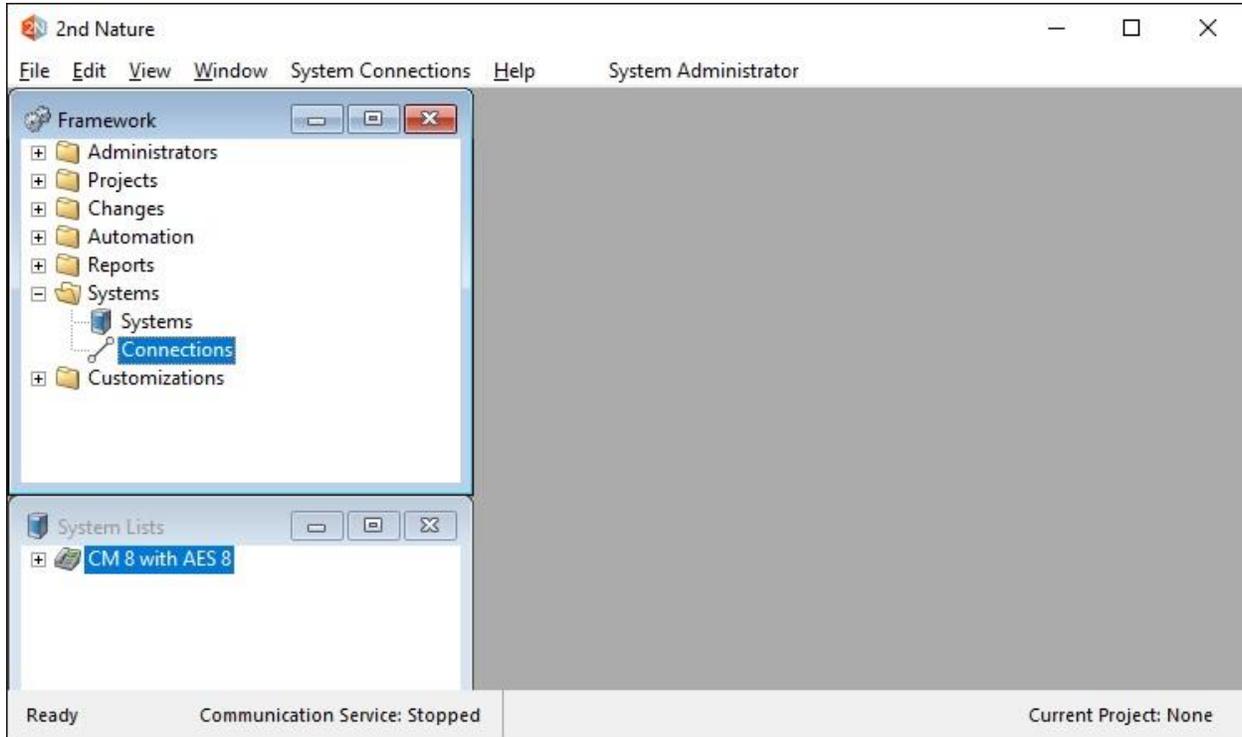
The **Add System** screen is displayed. Enter a descriptive **Name**, and select “Avaya Communication Manager” from the **System type** drop-down list, as shown below.

The screenshot shows a dialog box titled "Add System" with a question mark icon and a close button (X). The dialog contains the following fields and controls:

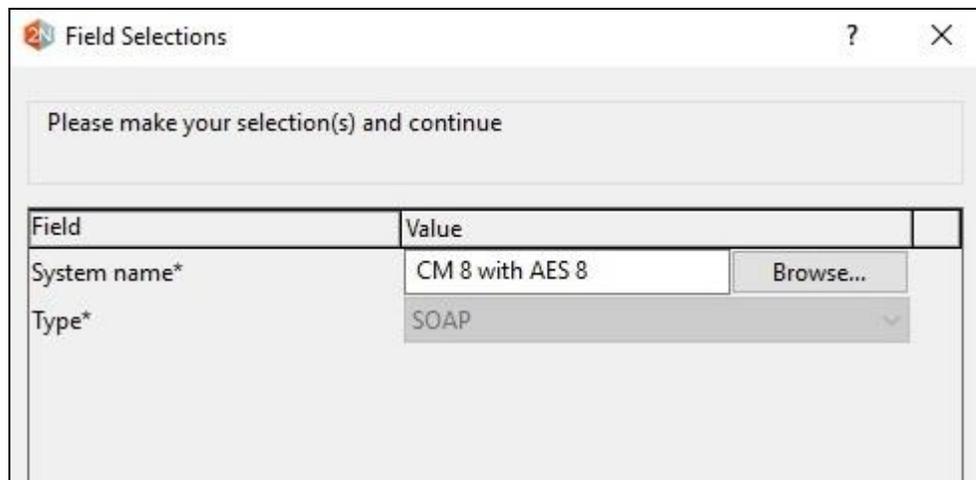
- Name:** A text input field containing "CM 8 with AES 8".
- System type:** A dropdown menu with "Avaya Communication Manager" selected.
- Model:** A dropdown menu that is currently empty.
- Parent systems:** A section containing an empty list box and two buttons: "Add..." and "Remove".
- Buttons:** "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 **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	

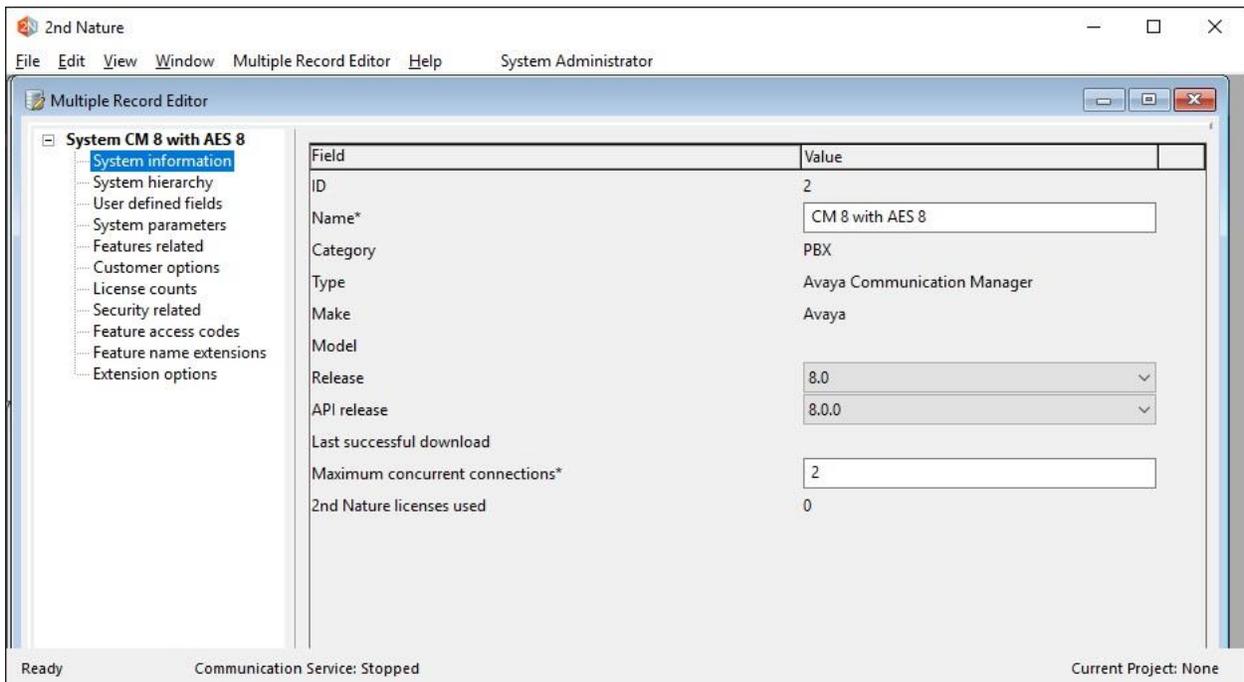
7.4. Administer System Releases

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**.



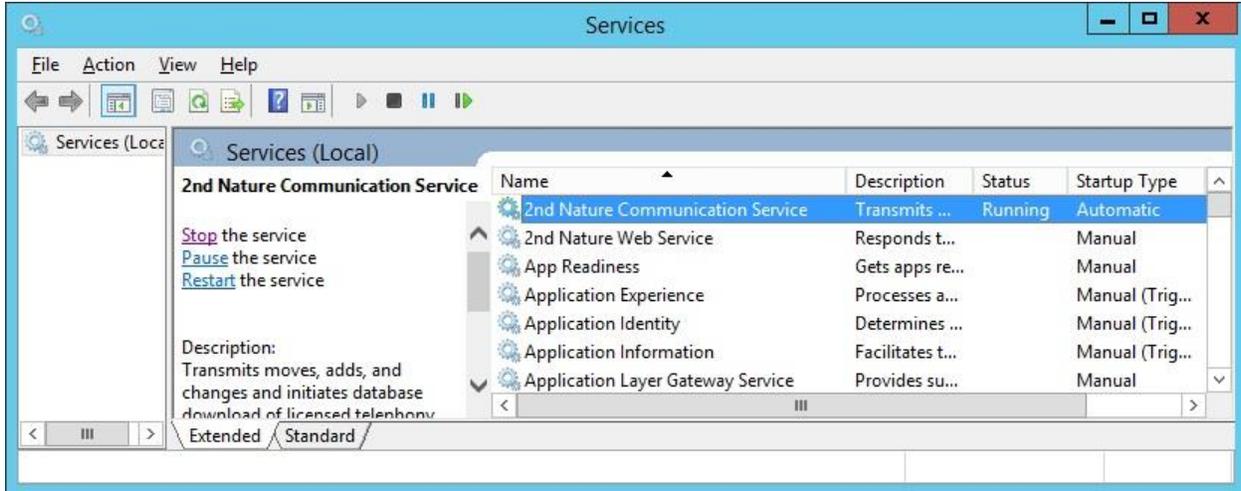
The **Multiple Record Editor** screen below is displayed. Select the following values for the specified fields, and retain the default values for the remaining fields.

- **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.

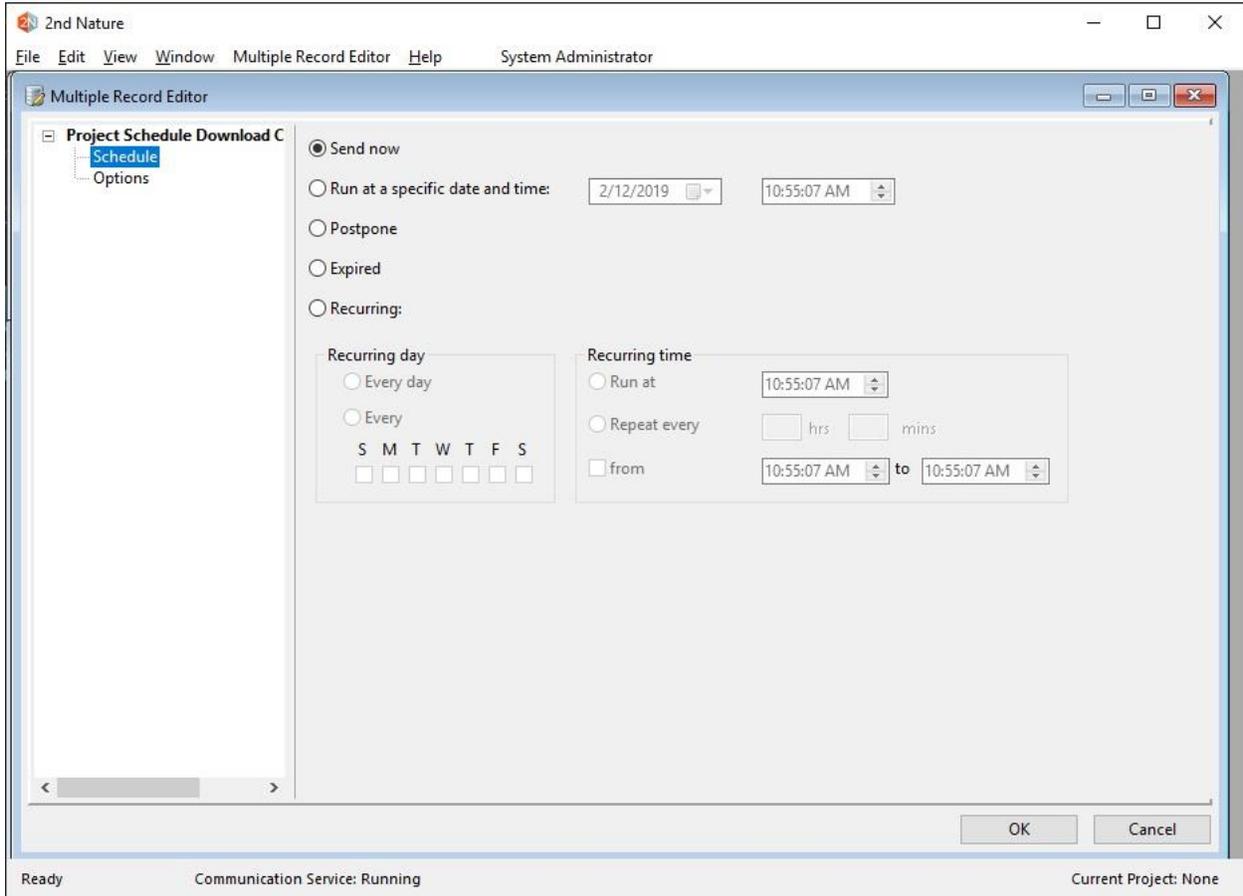


7.6. Download Data

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.



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”.

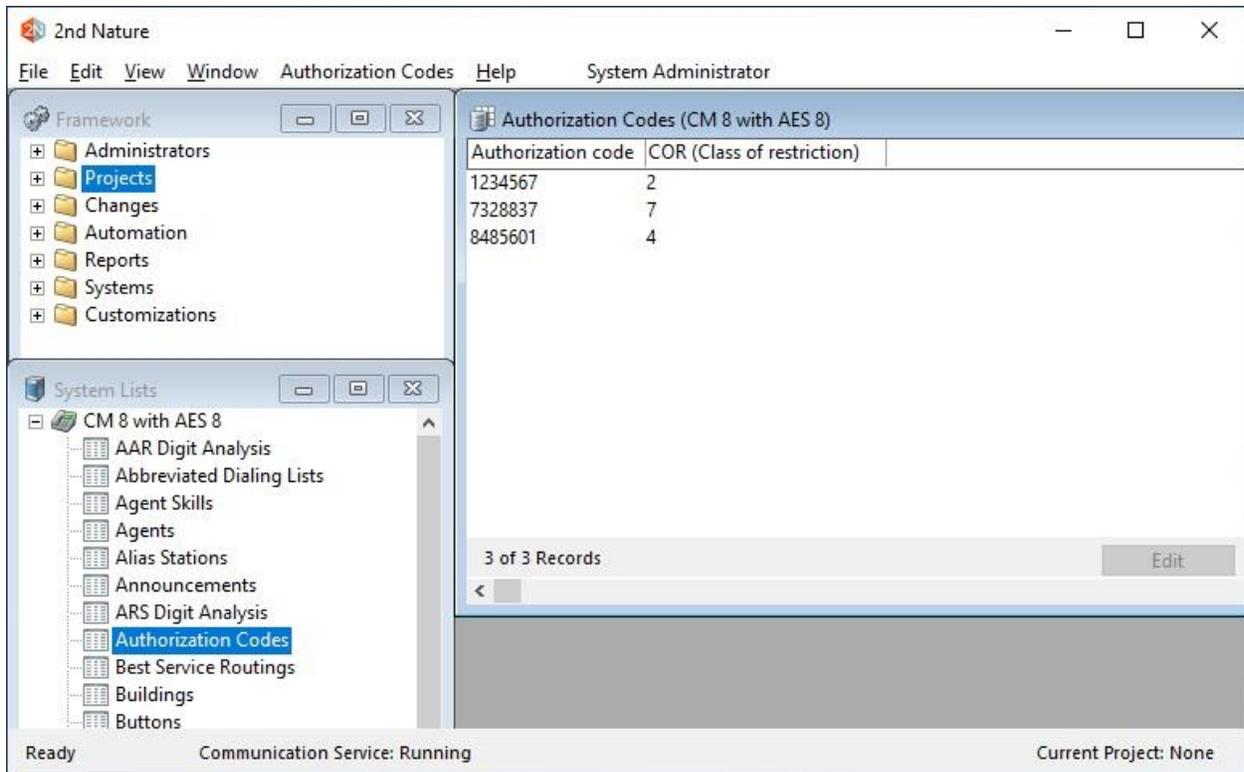
```
list authorization-code

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 Avaya 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.