



Avaya Solution & Interoperability Test Lab

Application Notes for Unimax 2nd Nature 8.4 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Unimax 2nd Nature 8.4 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. Unimax 2nd Nature is a centralized enterprise voice administration and provisioning solution.

In the compliance testing, Unimax 2nd Nature used System Management Services from Avaya Aura® Application Enablement Services to provide an administration interface for provisioning 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 8.4 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. Unimax 2nd Nature is a centralized enterprise voice administration and provisioning solution.

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

SMS is a web service that provides programmatic access to a subset of administration objects available via the Communication Manager System Access Terminal (SAT) screens. SMS enables clients using 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 were 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.

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: Agent, Alias Station, Announcement, Authorization Code, Configuration, COR, COS, Coverage Answer Group, Coverage Path, Coverage Remote, Dial Plan Analysis, Hunt Group, Locations, Off PBX Station Mapping, Pickup Group, Site Data, Station, Uniform Dial Plan, VDN, Vector, and VRT.

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.

- When the Multiple Locations customer option is disabled on Communication Manager, the 2nd Nature system download project can fail. The workaround is to manually remove List Location All from the project and resume download.
- When the Multiple Level Precedence & Preemption customer option is disabled on Communication Manager, 2nd Nature will show the Precedence call waiting parameter as enabled on every station.
- Attendant extensions did not get factored into the Extensions Available and Extension Usage Report.
- The application requires a vector to be in existence before being configured as part of a VDN.
- The current version of the application only supports up to 100 tenants.
- By design, 2nd Nature does not necessarily duplicate all parameter validations that are supported by Communication Manager for each object.
- The current release does not fully support the Modify nor Delete actions for Uniform Dial Plans entries.
- In the testing, the removal of an off-pbx station-mapping entry from 2nd Nature indicated success, although still in existence on Communication Manager. The workaround is to manually remove the entry from 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.

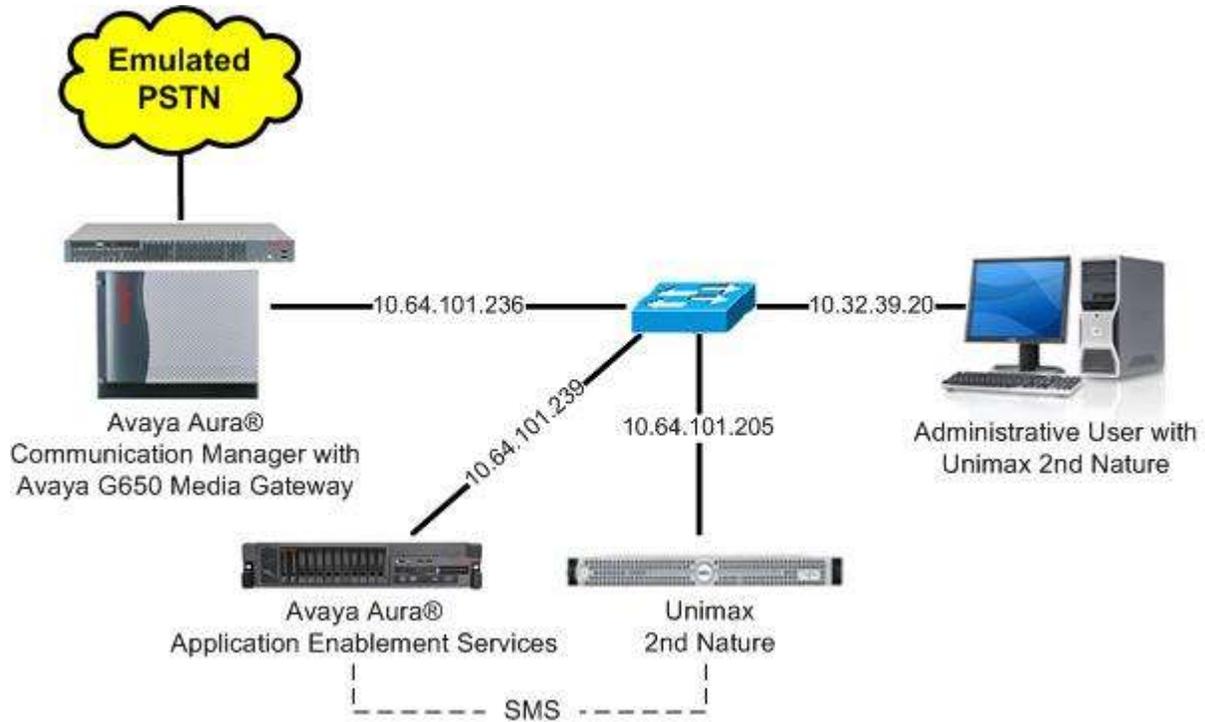


Figure 1: Compliance Testing Configuration

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	7.0 SP1 (7.0.0.1.0.441.22477)
Avaya G650 Media Gateway	NA
Avaya Aura® Application Enablement Services in Virtual Environment	7.0 Patch 1 (7.0.0.0.1.13)
Unimax 2nd Nature on Windows Server 2008 R2 Enterprise <ul style="list-style-type: none">• Microsoft SQL Server 2014 Express	8.4 B0 (FL.44645.20151020) SP1 12.0.2000.8
Unimax 2nd Nature on Windows 7 Professional	8.4 B0 (FL.44645.20151020) SP1

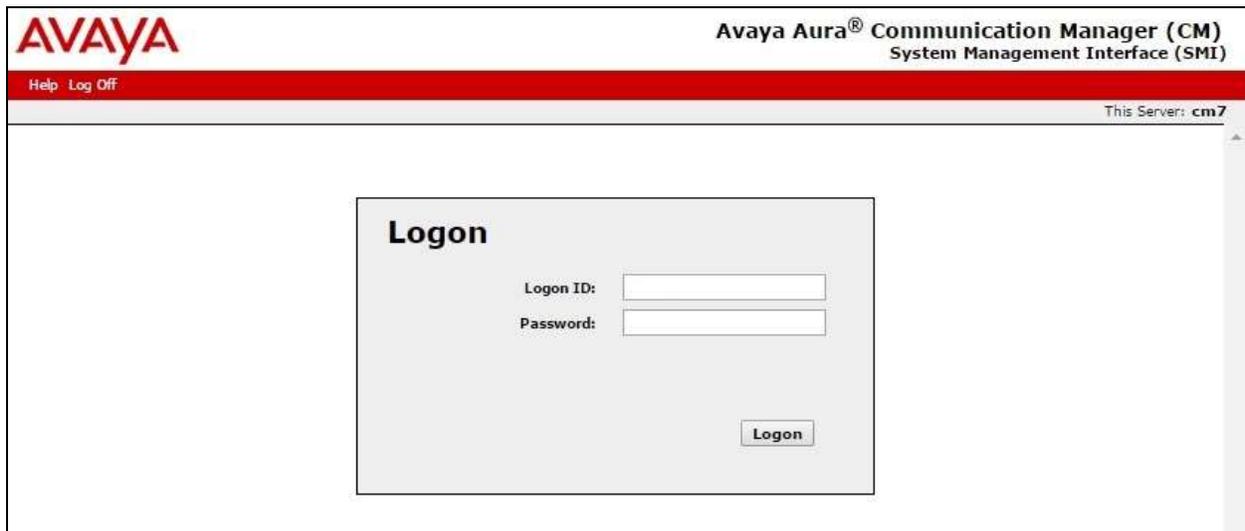
5. Configure Avaya Aura® Communication Manager

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

- Administer accounts

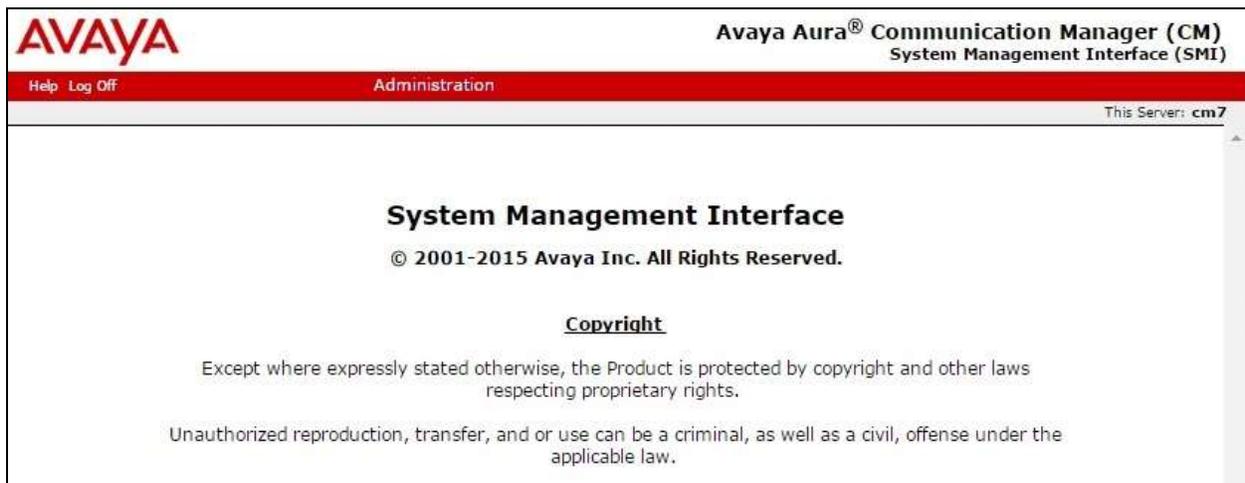
5.1. Administer Accounts

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 header includes the AVAYA logo on the left, the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right, and "Help Log Off" on the far left. Below the header, it says "This Server: cm7". The main content area is a light gray box titled "Logon" containing two input fields: "Logon ID:" and "Password:". A "Logon" button is positioned below the password field.

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

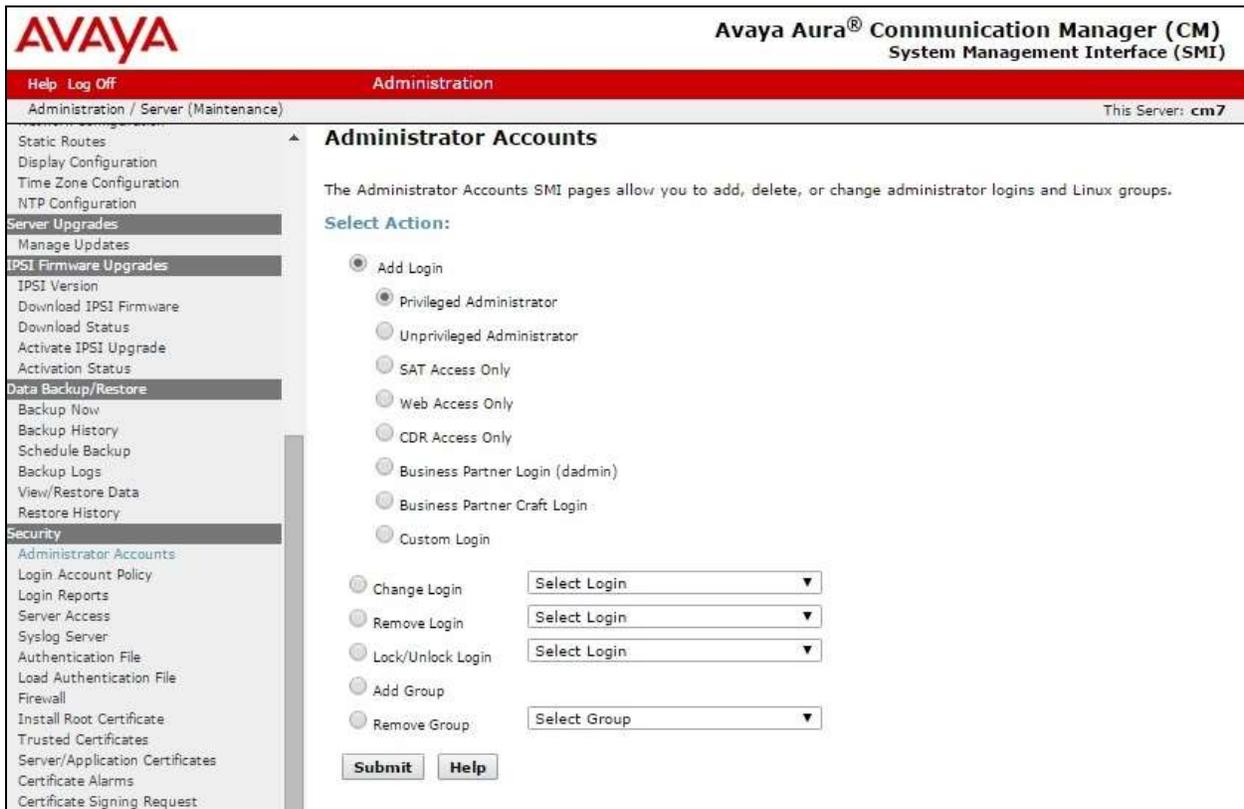


The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration screen. The header includes the AVAYA logo on the left, the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" on the right, and "Help Log Off" on the far left. Below the header, it says "Administration" and "This Server: cm7". The main content area displays "System Management Interface" and "© 2001-2015 Avaya Inc. All Rights Reserved." Below this, there is a section titled "Copyright" 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 or key**, and **Re-enter password or key**. Retain the default values in the remaining fields.

Make a note of the account credentials, which will be used later to configure 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 like "Static Routes", "Server Upgrades", "Data Backup/Restore", "Security", and "Miscellaneous". The main content area includes a description: "This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root." Below this, there are several form 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]
- Select type of authentication:** ASG: Auto-generate key, ASG: enter key, Password
- Enter password or key:** [masked with dots]
- Re-enter password or key:** [masked with dots]
- Force password/key change on next login:** No, Yes

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

6. Configure Avaya Aura® Application Enablement Services

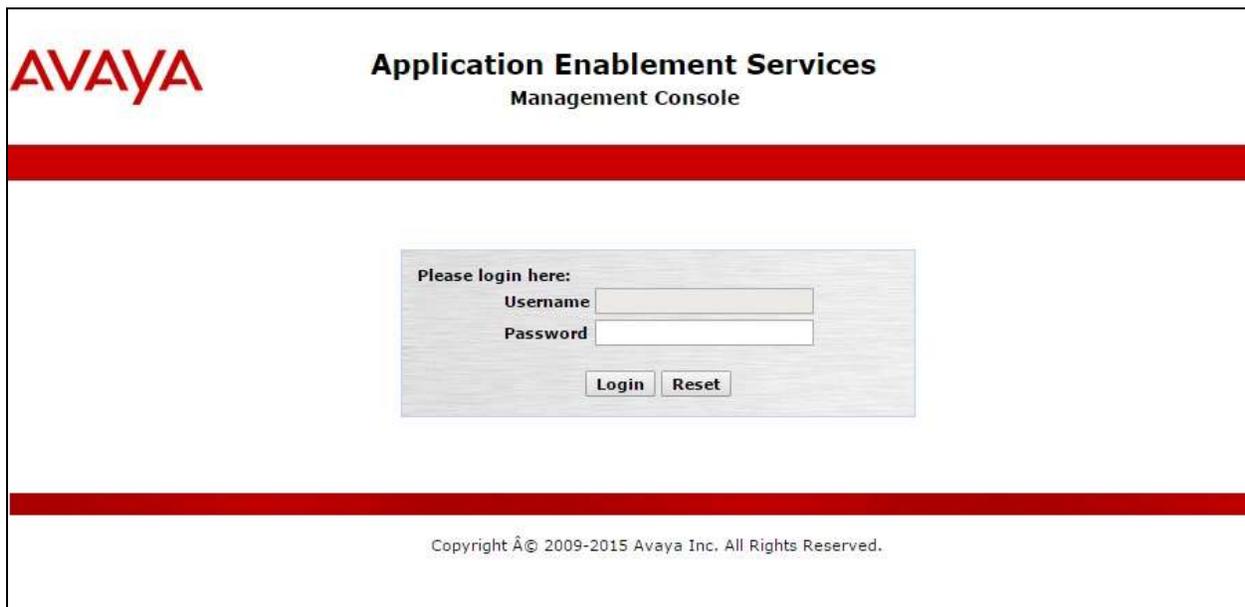
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- 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 © 2009-2015 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. To its right is the title 'Application Enablement Services Management Console'. In the top right corner, there is a 'Welcome' message with system details: 'Welcome: User', 'Last login: Tue Oct 20 08:59:28 2015 from 10.32.39.25', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.0.0.1.13', 'Server Date and Time: Tue Oct 20 08:59:46 EDT 2015', and 'HA Status: Not Configured'. Below the title bar is a red navigation bar with 'Home' on the left and 'Home | Help | Logout' on the right. On the left side of the main content area is a vertical menu with items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area is titled 'Welcome to OAM' and contains a paragraph: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. This is followed by a bulleted list of domains and their functions: '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 infomations.', '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.', and 'Help - Use Help to obtain a few tips for using the OAM Help system'. At the bottom of the main content area, a note states: '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 Oct 20 08:59:28 2015 from 10.32.39.25
 Number of prior failed login attempts: 0
 HostName/IP: aes7/10.64.101.239
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.0.0.1.13
 Server Date and Time: Tue Oct 20 09:01:00 EDT 2015
 HA Status: Not Configured

Networking | Ports
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▼ Networking
- AE Service IP (Local IP)
- Network Configure
- Ports
- TCP Settings
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Ports

CVLAN Ports Enabled Disabled

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

DLG Port Enabled Disabled

TCP Port	5678		<input checked="" type="radio"/>	<input type="radio"/>
----------	------	--	----------------------------------	-----------------------

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 type="radio"/>	<input checked="" type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" 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"/>			

Apply Changes
Restore Defaults

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". On the right side of the header, there is a welcome message: "Welcome: User", "Last login: Tue Oct 20 08:59:28 2015 from 10.32.39.25", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.0.0.1.13", "Server Date and Time: Tue Oct 20 09:02:13 EDT 2015", and "HA Status: Not Configured".

The main navigation bar is red and contains "AE Services | SMS | SMS Properties" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services" (expanded), "CVLAN", "DLG", "DMCC", "SMS" (expanded), "SMS Properties" (selected), "TSAPI", "TWS", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help".

The main content area is titled "SMS Properties" and contains the following configuration fields:

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

At the bottom of the 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

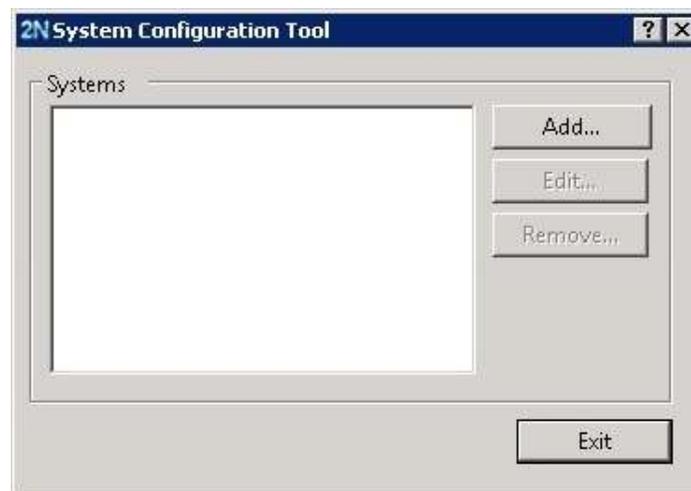
7.1. Launch 2nd Nature

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



7.2. Administer System

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



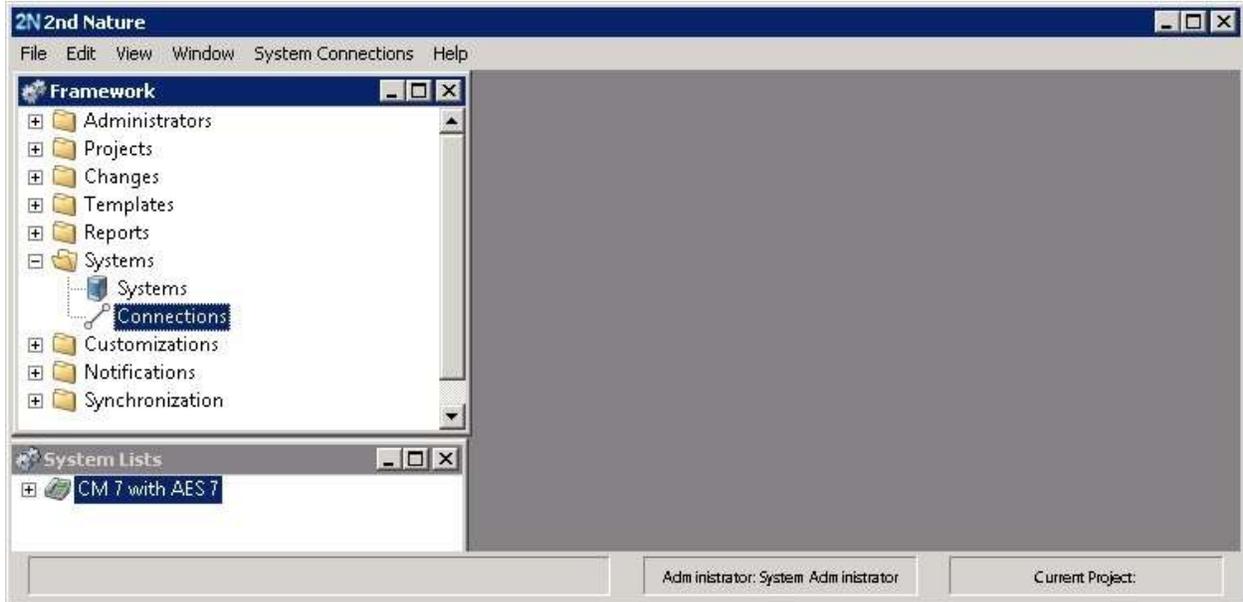
The **Add System** screen is displayed. Enter a descriptive **Name**, and select “Avaya Communication Manager” from the **System type** drop-down list, as shown below.

The screenshot shows a dialog box titled "2N Add System". It contains the following fields and controls:

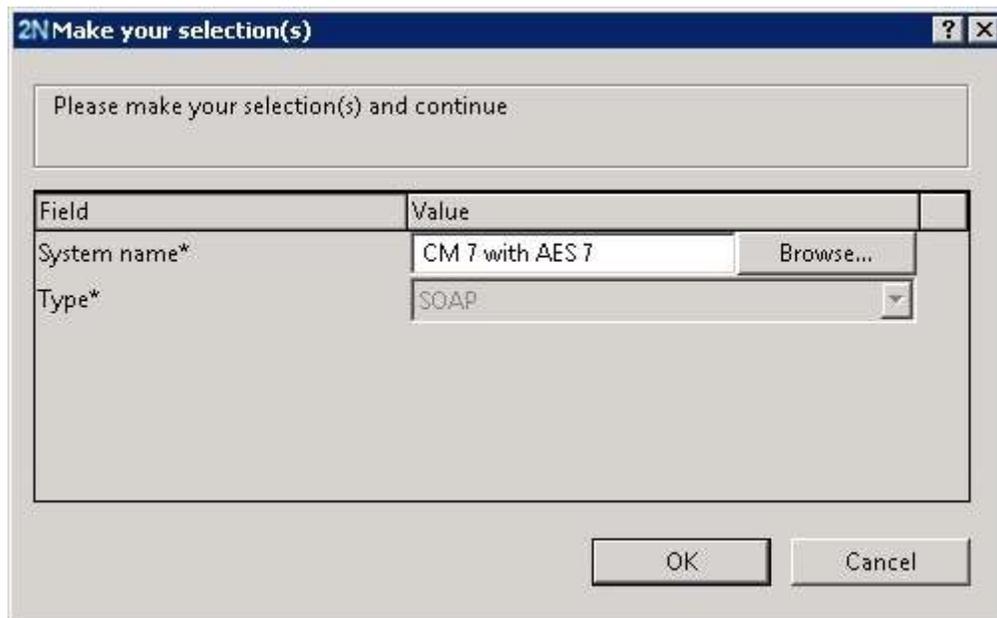
- Name:** A text input field containing "CM 7 with AES 7".
- System type:** A dropdown menu with "Avaya Communication Manager" selected.
- Model:** An empty dropdown menu.
- Parent systems:** A section containing an empty list box and two buttons: "Add..." and "Remove".
- Buttons:** "OK" and "Cancel" buttons at the bottom 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.



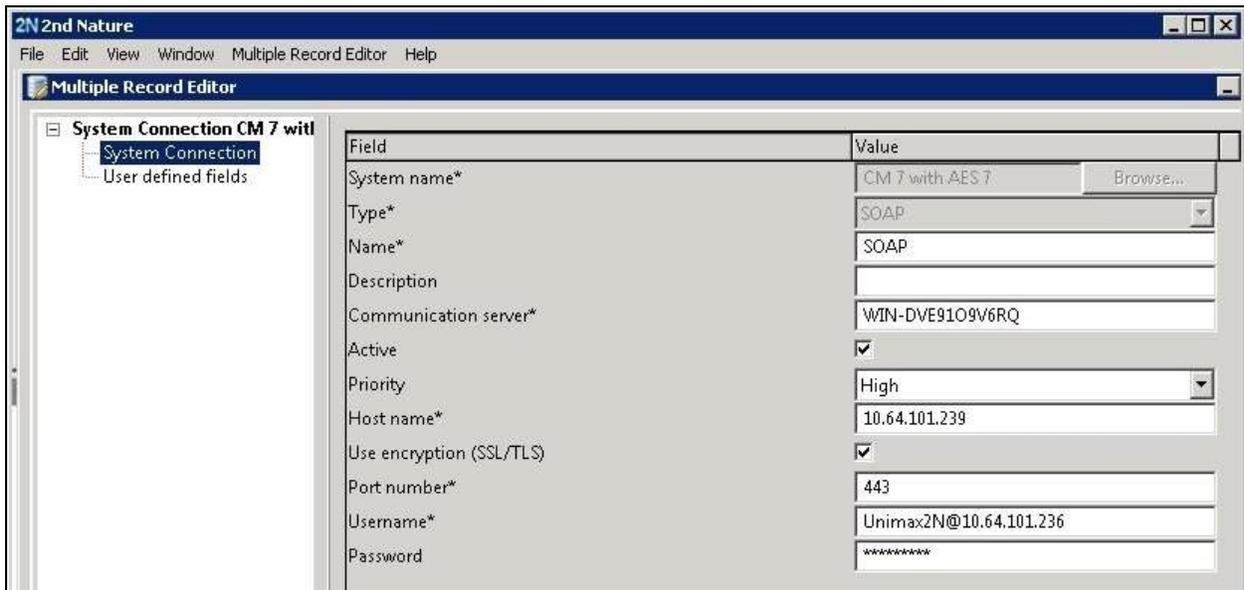
The **Make your selection(s)** screen is displayed next. Click **Browse** and select the system name from **Section 7.2**.



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

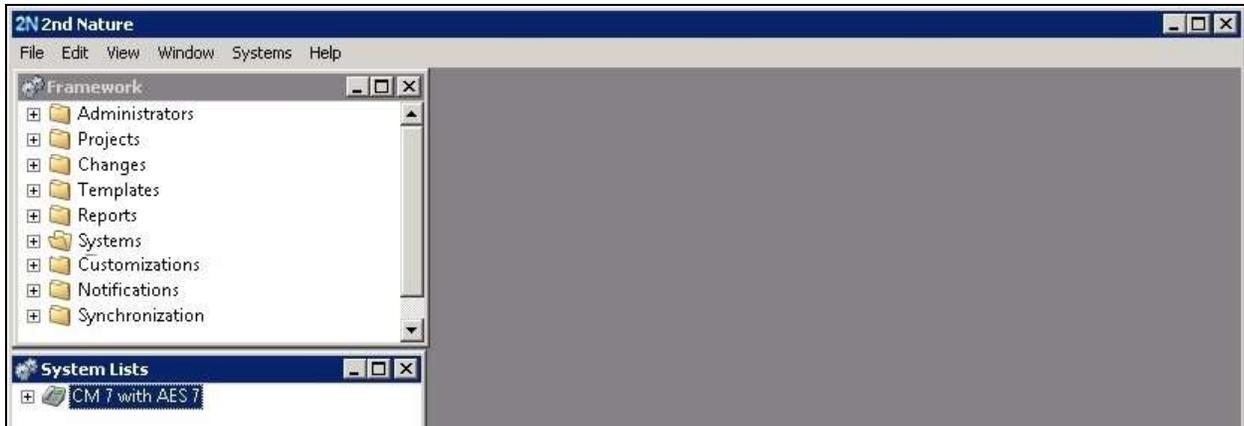
- **Host name:** The host name or IP address of Application Enablement Services.
- **Use encryption:** Check this field.
- **Port number:** “443”
- **Username:** The account name from **Section 5**, concatenated with an IP address.
- **Password:** The account password from **Section 5**.

For **Username**, use the format “x@y”, where “x” is the account name from **Section 5** and “y” is the IP address of Communication Manager.



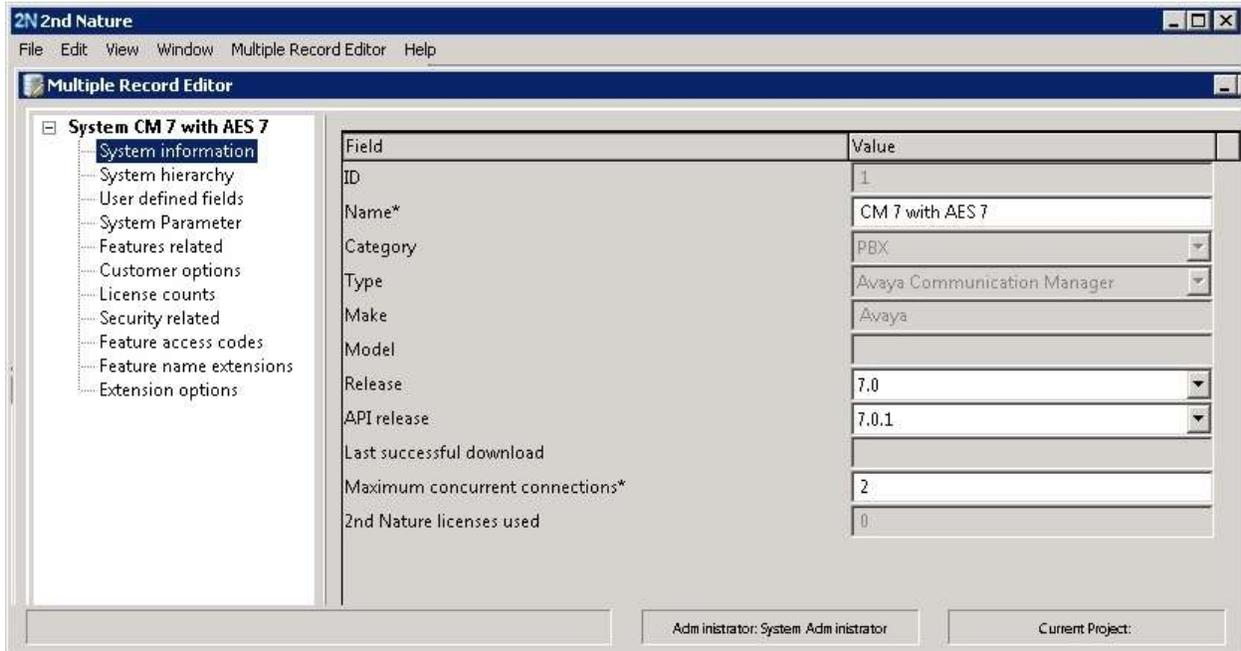
7.4. Administer System Releases

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**.



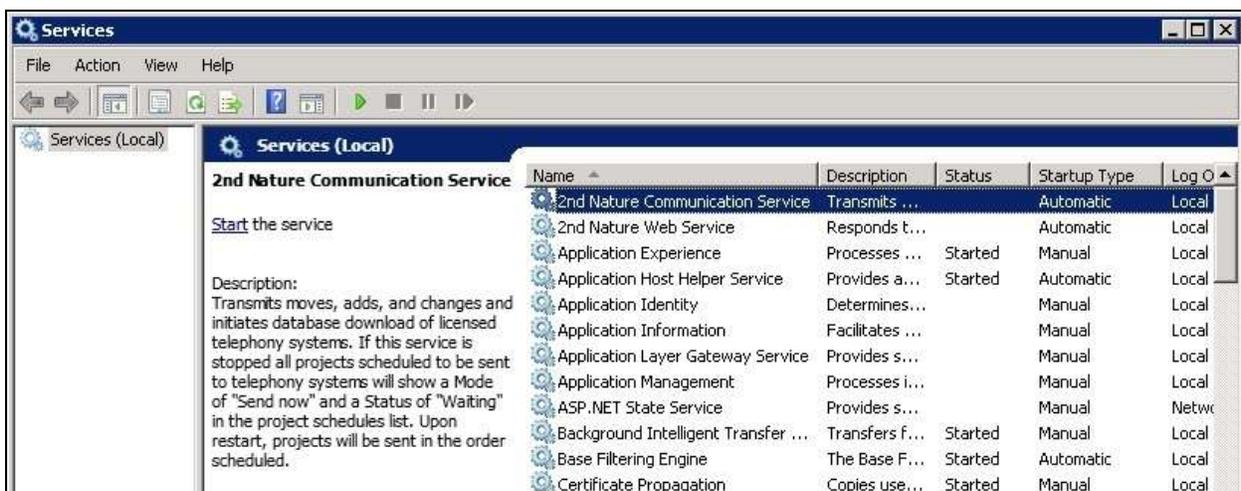
The **Multiple Record Editor** screen below is displayed. Select the following values for the specified fields, and retain the default values for the remaining fields.

- **Release:** Release of Communication Manager, in this case “7.0”.
- **API release:** Release of Application Enablement Services, in this case “7.0.1”.



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.

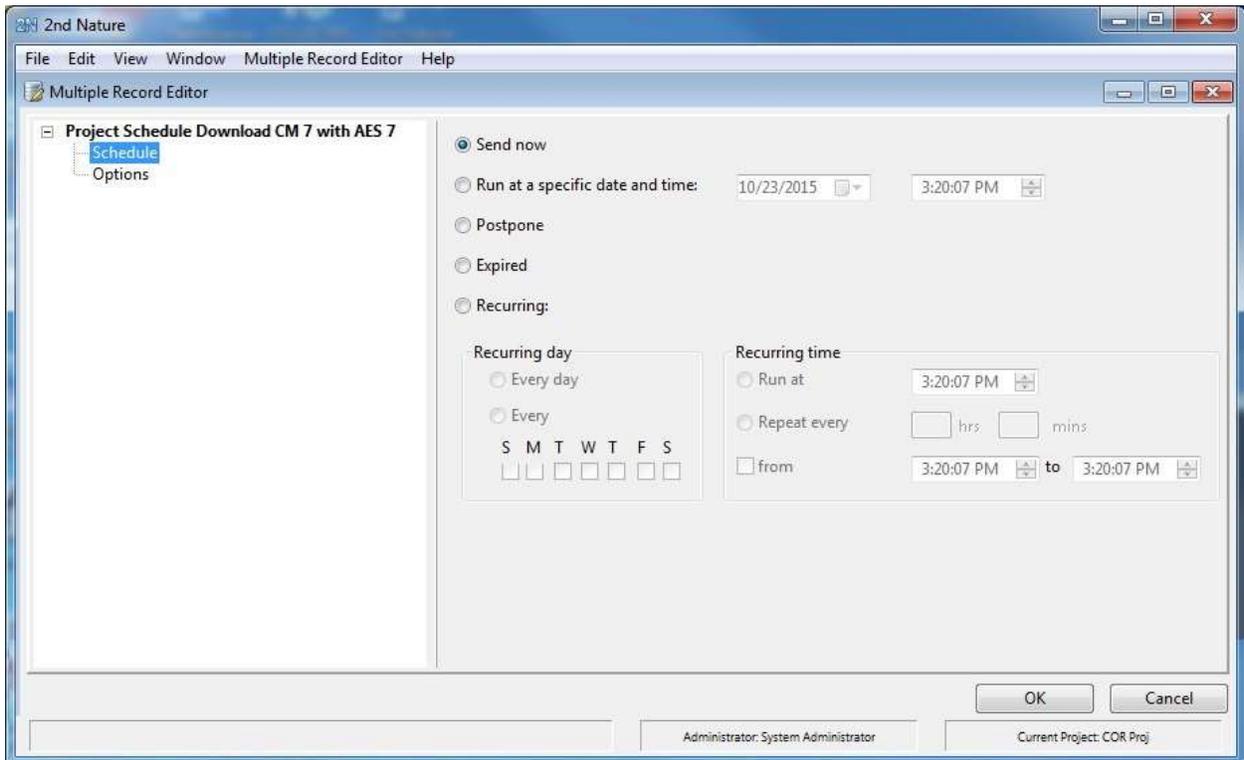


7.6. Download Data

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, to sync data between 2nd Nature and Communication Manager.



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 in to the SAT screen and issue a command for a supported SMS object from **Section 2.1**, in this case “list authorization-code”.

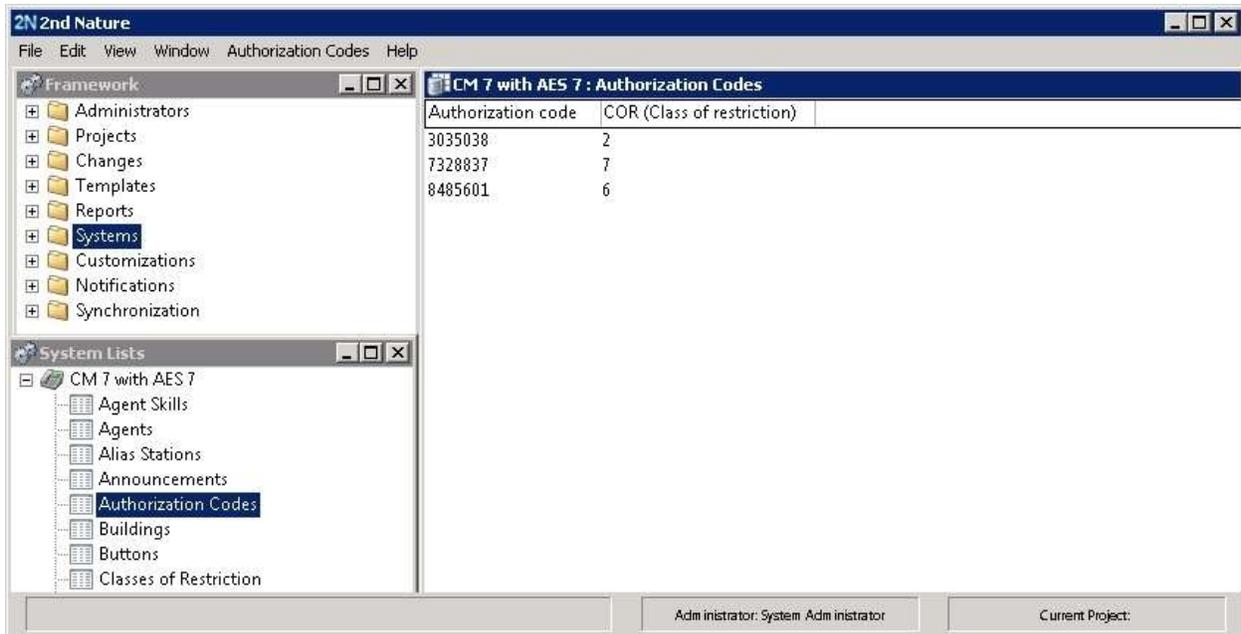
```
list authorization-code

LIST AUTHORIZATION CODES REPORT

Authorization Code   Class of Restriction(COR)
3035038              2
7328837              7
8485601              6
```

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

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



9. Conclusion

These Application Notes describe the configuration steps required for Unimax 2nd Nature 8.4 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. 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 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
3. *2nd Nature Administrator Guide*, for use with 2nd Nature Release 8.4, available as part of 2nd Nature installation.
4. *2nd Nature Avaya Communication Manager User Guide*, for use with 2nd Nature Release 8.4, available as part of 2nd Nature installation.

©2015 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.