



DevConnect Program

Application Notes for Unimax 2nd Nature 9.6 with Avaya Aura® System Manager 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Unimax 2nd Nature 9.6 to interoperate with Avaya Aura® System Manager 10.1 using User Management Web Services and Routing Web Service. Unimax 2nd Nature is a centralized enterprise voice administration and provisioning solution.

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.

1. Introduction

These Application Notes describe the configuration steps required for Unimax 2nd Nature 9.6 to interoperate with Avaya Aura® System Manager 10.1 using User Management Web Services (UMWS) and Routing Web Service (RWS).

2nd Nature is a centralized enterprise voice administration and provisioning solution. The UMWS interface is used by 2nd Nature to manage users and their communication profiles associated with various Avaya products. The communication profiles below were included in the compliance testing.

- Session Manager Profile
- CM Endpoint Profile
- CM Agent Profile

The RWS interface is used by 2nd Nature to provision routing administration data on System Manager. The routing resources below were included in the compliance testing.

- Adaptations
- Dial Patterns
- Domains
- Locations
- Routing Policies

Testing was performed with the 2nd Nature client application, which supports the full set of scope listed above. The results should be extendable to other client applications including LineOne, HelpOne, and Spotlight, with each supporting a subset of scope.

2. General Test Approach and Test Results

All test cases were performed manually. Actions were taken on 2nd Nature and System Manager to alter data associated with supported users, their communication profiles, and of routing resources.

The data were modified on 2nd Nature using the 2nd Nature client application. A subset of user parameters including communication profiles and of routing resource parameters were chosen at random for modification and verification, therefore not all parameters were necessarily 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 System Manager 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 UMWS to download, change, and delete user data including subset of parameters associated with Session Manager Profile, CM Endpoint Profile, and CM Agent Profile.
- Use of UMWS to add user data including Session Manager Profile.
- Use of RWS to download, add, change, and delete adaptations and dial patterns.
- Use of RWS to download locations, domains, and routing policies.

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 support all parameter nor duplication of all parameter validations that are supported by System Manager.
- By design, 2nd Nature also requires System Management Services integration with Avaya Aura® Application Enablement Services for creation and update of all parameters in the CM Endpoint Profile and CM Agent Profile. As such, the compliance testing only included update of supported parameters via UMWS.
- 2nd Nature only supports display of downloaded domains, and display of downloaded locations and routing policies name. In addition, only parameters associated with the digit conversion module in dial patterns are supported.
- 2nd Nature does not perform certificate validation for the UMWS and RWS connections.

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 System Manager, Session Manager, and Communication Manager are not the focus of these Application Notes and will not be described.

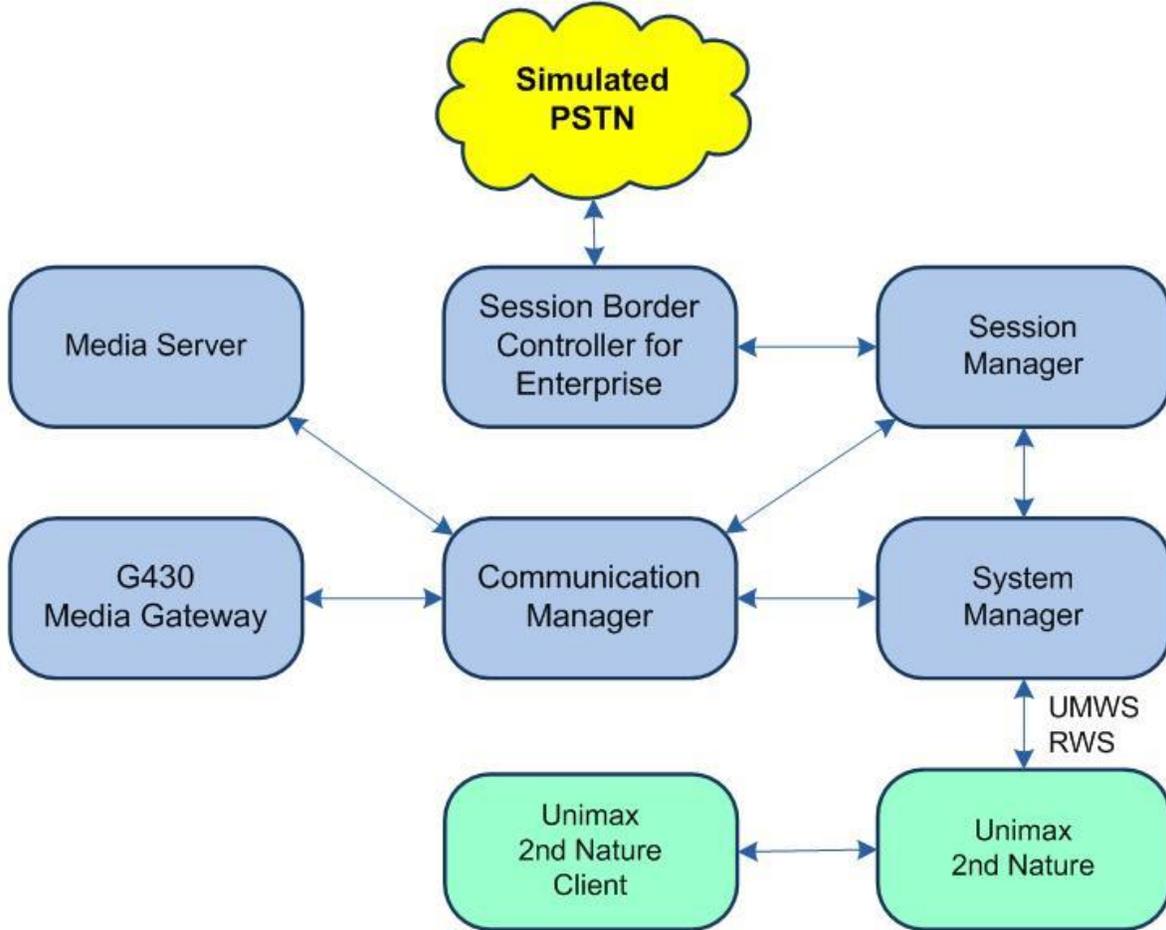


Figure 1: Compliance Testing Configuration

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	10.1.2 (10.1.2.0.0.974.27783)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1.0.125
Avaya Aura® Session Manager in Virtual Environment	10.1.2 (10.1.2.0.101.2016)
Avaya Aura® System Manager in Virtual Environment	10.1.2 (10.1.2.0.0715476)
Avaya Session Border Controller for Enterprise in Virtual Environment	10.1 (10.1.0.0-32-21432)
Unimax 2nd Nature on Windows Server 2019 <ul style="list-style-type: none">• Microsoft SQL Server 2019 Express	9.6 G2 Standard
Unimax 2nd Nature on Windows 10 Pro	9.6 G2

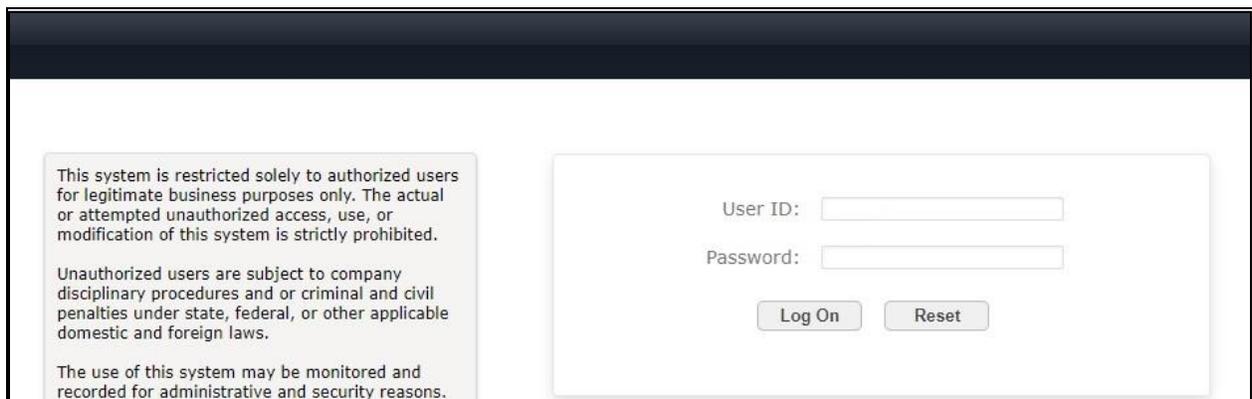
5. Configure Avaya Aura® System Manager

This section provides the procedures for configuring an administrative user on System Manager for UMWS and RWS integration. The procedures include the following areas:

- Launch System Manager
- Administer administrative users

5.1. Launch System Manager

Access the System Manager web interface by using the URL **https://ip-address** in an Internet browser window, where **ip-address** is the IP address of System Manager. Log in using the appropriate credentials.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

User ID:

Password:

Log On Reset

5.2. Administer Administrative Users

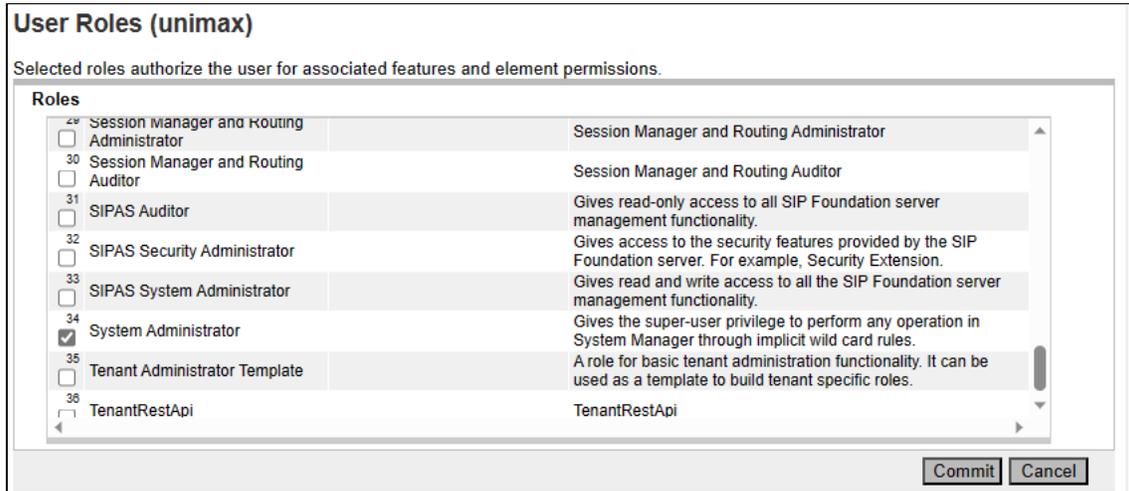
Select **Users** → **Administrators** → **Administrative Users** from the top menu to display a list of existing administrative users (not shown). Select **Add** (not shown) from the right pane to add a new administrative user for 2nd Nature to be used for UMWS and RWS integration.

The **Add New Administrative User** screen is displayed. Enter desired **User ID**, **Full Name**, **Temporary password**, and **Re-enter password** as shown below. For **Authentication Type**, retain **Local**.

The screenshot displays the Avaya System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, along with a search bar and a user profile for 'admin'. The left sidebar shows a tree view with 'Administrative Users' selected. The main content area is titled 'Add New Administrative User' and contains the following fields and options:

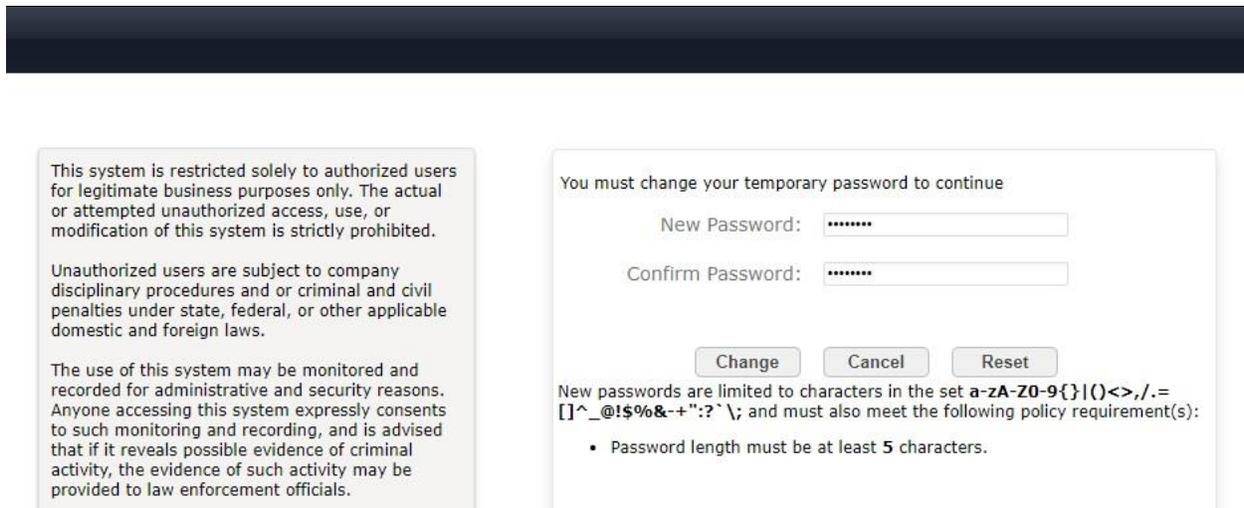
- Host Name: smgr7.dr220.com | User Name: admin
- Step 1: Identify the new user. Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.
- * User ID: unimax (1-31) (Allowed characters are a-z, A-Z, 0-9, ., - and _)
- Authentication Type: Local, External
- * Full Name: unimax
- E-Mail: [Empty field]
- The user will receive notifications on this E-Mail address.
- * Temporary password: [Masked field]
- * Re-enter password: [Masked field]
- The user will be required to change this password when logging in.
- Allowed characters in the password are: a-zA-Z0-9[]()<>./=!@#\$%&+*~?'\. The length of your password must be at least 5 characters.
- Generate Password button

The screen below is displayed next for assigning role(s) to the new administrative user. Scroll the right pane as necessary to locate and check **32 System Administrator** as shown below.



Note that the new administrative user is required to change the temporary password upon initial log in, therefore log off from the web interface and log back into System Manager using the new administrative user credentials created in this section.

The screen below is displayed upon succesful log in. Enter desired password for **New Password** and **Confirm Password**. Click **Change** to update the password.



6. Configure Unimax 2nd Nature

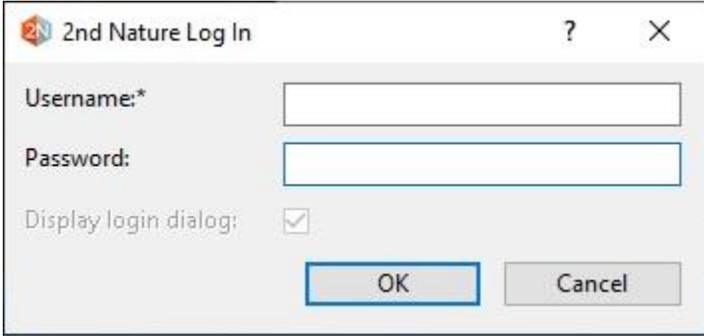
This section provides the procedures for configuring 2nd Nature. The procedures include the following areas:

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

The configuration of 2nd Nature is performed by the Unimax Customer Service team. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch 2nd Nature

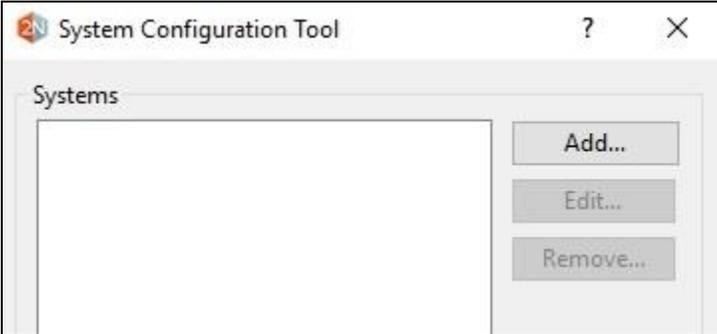
From the 2nd Nature server, select **Windows** → **2nd Nature** → **2nd Nature** to launch the application. The **2nd Nature Log In** screen below is displayed. Log in using the appropriate credentials.



The screenshot shows a dialog box titled "2nd Nature Log In". It contains three input fields: "Username:*", "Password:", and "Display login dialog:". The "Display login dialog:" field has a checked checkbox. At the bottom, there are "OK" and "Cancel" buttons.

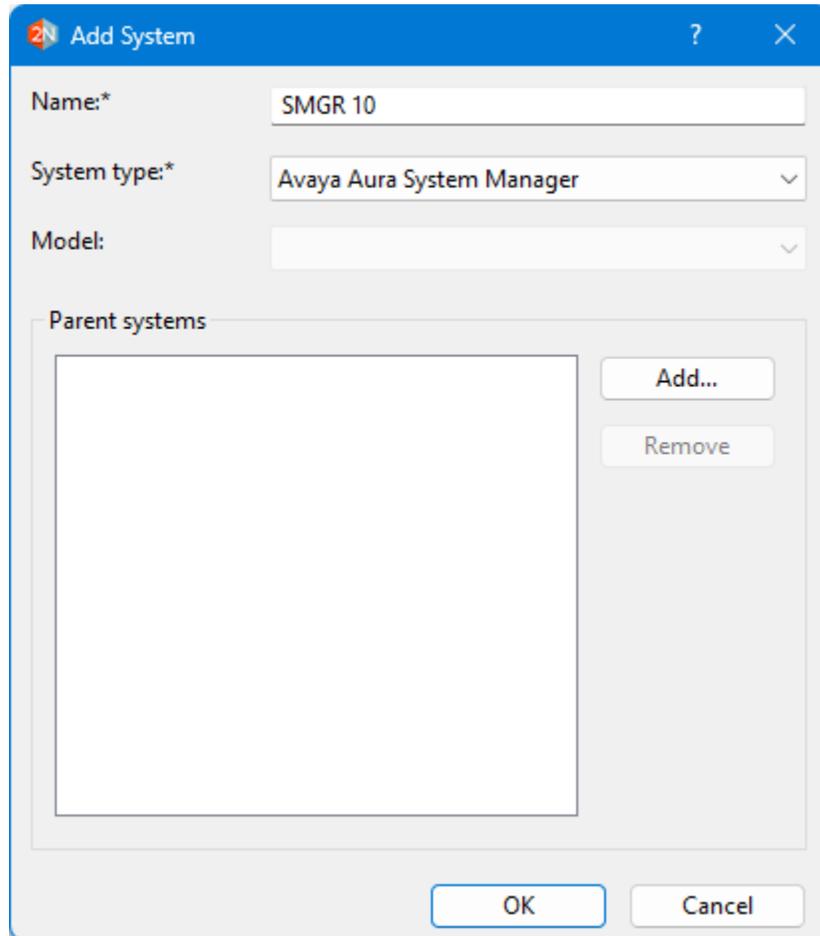
6.2. Administer System

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



The screenshot shows a dialog box titled "System Configuration Tool". It features a "Systems" section with a large empty rectangular area. To the right of this area are three buttons: "Add...", "Edit...", and "Remove...".

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

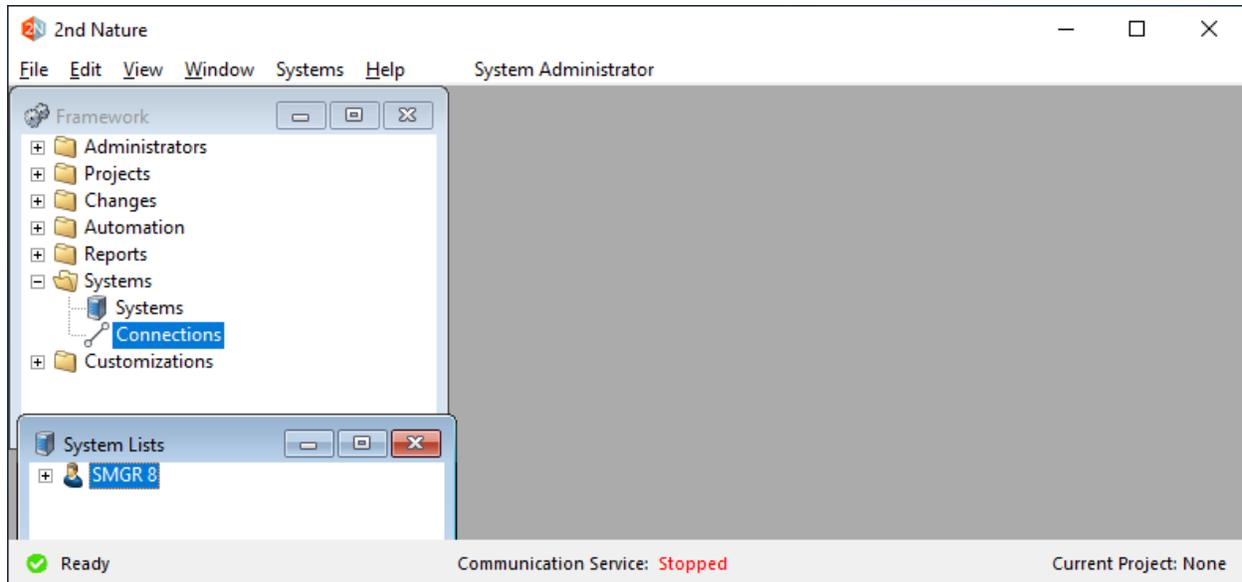


The screenshot shows a dialog box titled "Add System" with a blue header bar containing a question mark and a close button. The dialog has the following fields and controls:

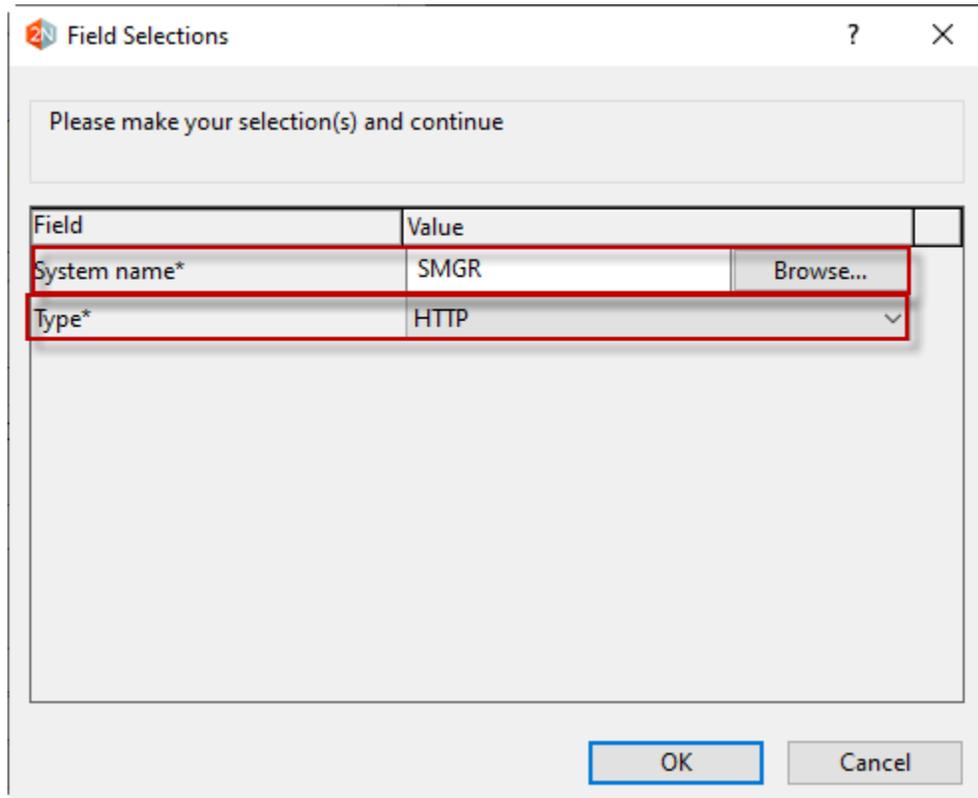
- Name*:** A text input field containing "SMGR 10".
- System type*:** A dropdown menu with "Avaya Aura System Manager" selected.
- Model:** An empty dropdown menu.
- Parent systems:** A large empty rectangular area for listing parent systems, with "Add..." and "Remove" buttons to its right.
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.

6.3. Administer System Connection

The **2nd Nature** screen below is displayed. From the **Framework** pane, expand and right click on **Systems** → **Connections**, and select **Create** (not shown) to create a new connection.



The **Field Selections** screen is displayed next. Click **Browse** and select the system name from **Section 6.2**.



The image shows a dialog box titled "Field Selections" with a question mark and a close button in the top right corner. Below the title bar is a text box containing the instruction "Please make your selection(s) and continue". Below this is a table with two columns: "Field" and "Value". The first row has "System name*" in the "Field" column, "SMGR" in the "Value" column, and a "Browse..." button to the right. The second row has "Type*" in the "Field" column and "HTTP" in the "Value" column, with a dropdown arrow on the right. At the bottom of the dialog are "OK" and "Cancel" buttons.

Field	Value	
System name*	SMGR	Browse...
Type*	HTTP	▼

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:** Host name or IP address of System Manager.
- **Use encryption:** Checked
- **Username:** The updated System Manager user credential from **Section 5.2**.
- **Password:** The updated System Manager user credential from **Section 5.2**.

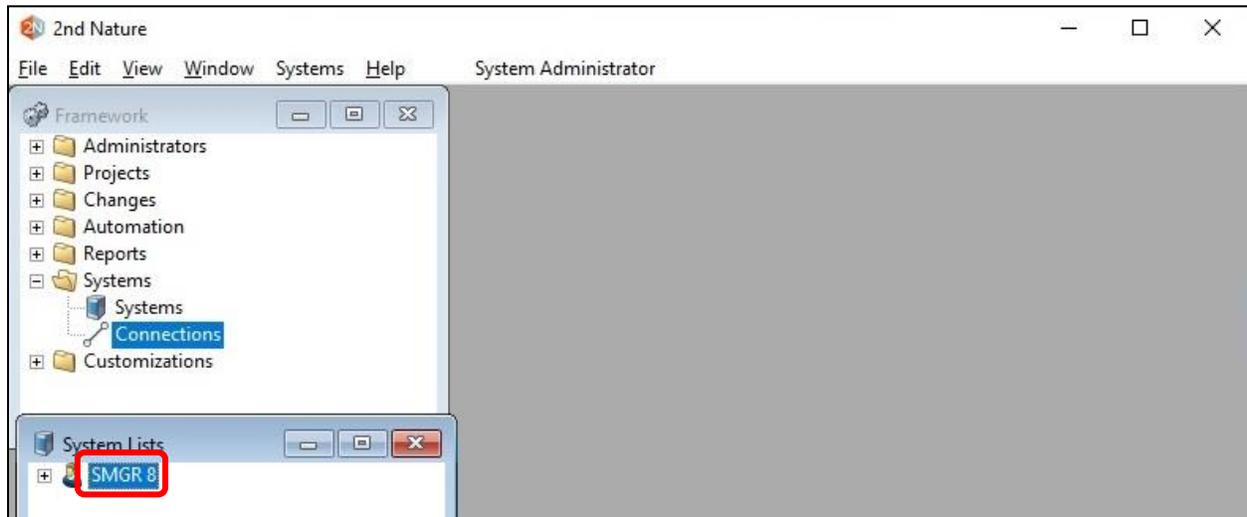
The screenshot shows the 'Multiple Record Editor' window for a 'System Connection SMGR-HTTP'. The left pane shows a tree view with 'Main' selected under 'User defined fields'. The right pane is a table with the following fields and values:

Field	Value
System name*	SMGR
Type*	HTTP
Name*	HTTP
Description	
Communication server*	TLT-W2019
Active	<input checked="" type="checkbox"/>
Priority	High
Host name*	10.64.101.235
Use encryption	<input checked="" type="checkbox"/>
Port number*	0
Username*	admin
Password	*****

At the bottom of the window are 'Save' and 'Cancel' buttons. The fields for 'Host name*', 'Use encryption', 'Username*', and 'Password' are highlighted with red boxes in the original image.

6.4. 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 6.2** and select **Modify** (not shown).



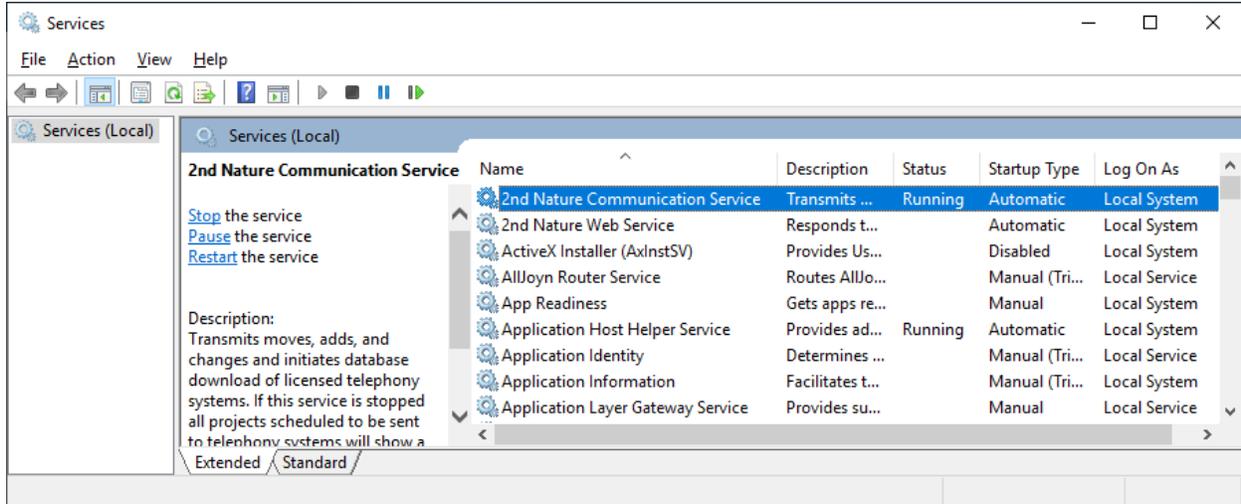
The **Multiple Record Editor** screen below is displayed. For **Release**, select **10.1** from the drop-down list. Retain the default values in the remaining fields.

The screenshot shows the 'Multiple Record Editor' window. On the left is a tree view with 'System SMGR' expanded, showing sub-items like 'System information', 'System hierarchy', 'Number inventory member', 'User defined fields', 'System parameters', 'Communication profile pas', and 'Number options'. The main area is a table with 'Field' and 'Value' columns. Several fields are highlighted with red boxes: 'Name*' (SMGR), 'Release' (10.1), and 'Number inventory system' (NI). At the bottom are 'Save', 'Send Now...', and 'Cancel' buttons.

Field	Value
ID	2
Name*	SMGR
Abbreviated name*	SM
Category	Directory Service
Type	Avaya Aura System Mana...
Make	Avaya
Model	
Release	10.1
Last successful download	5/18/2023 2:00:14 AM
Last download duration	00:00:13
Maximum concurrent connections*	1
Write communication log when down	<input checked="" type="checkbox"/>
Write communication log when sendi	<input checked="" type="checkbox"/>
Prevent download with too many recd	
Prevent download with too many recd	50
Number inventory system	NI
2nd Nature licenses used	9

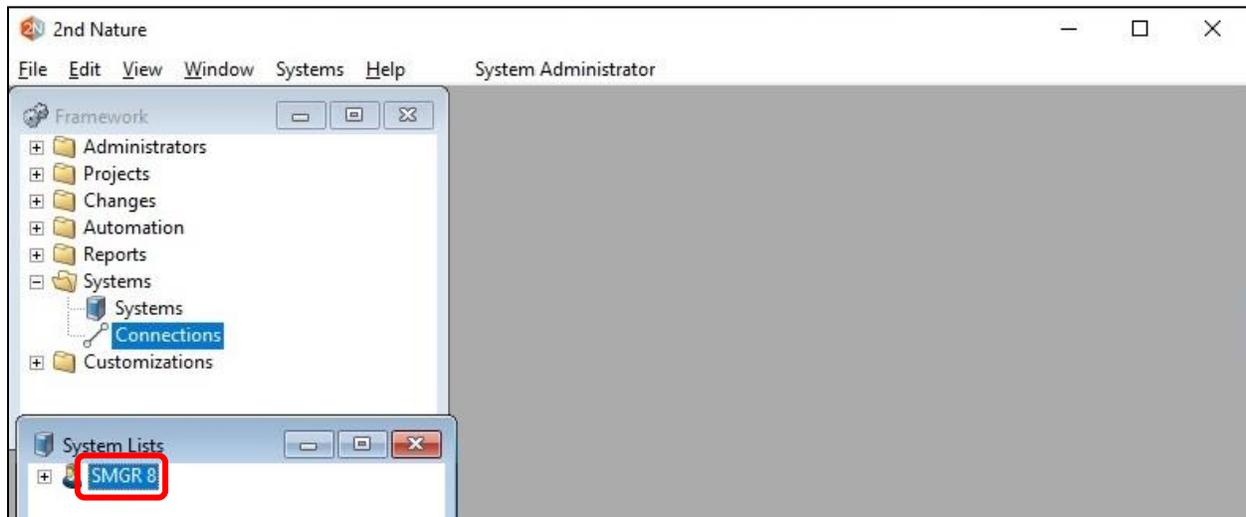
6.5. Start Communication Service

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

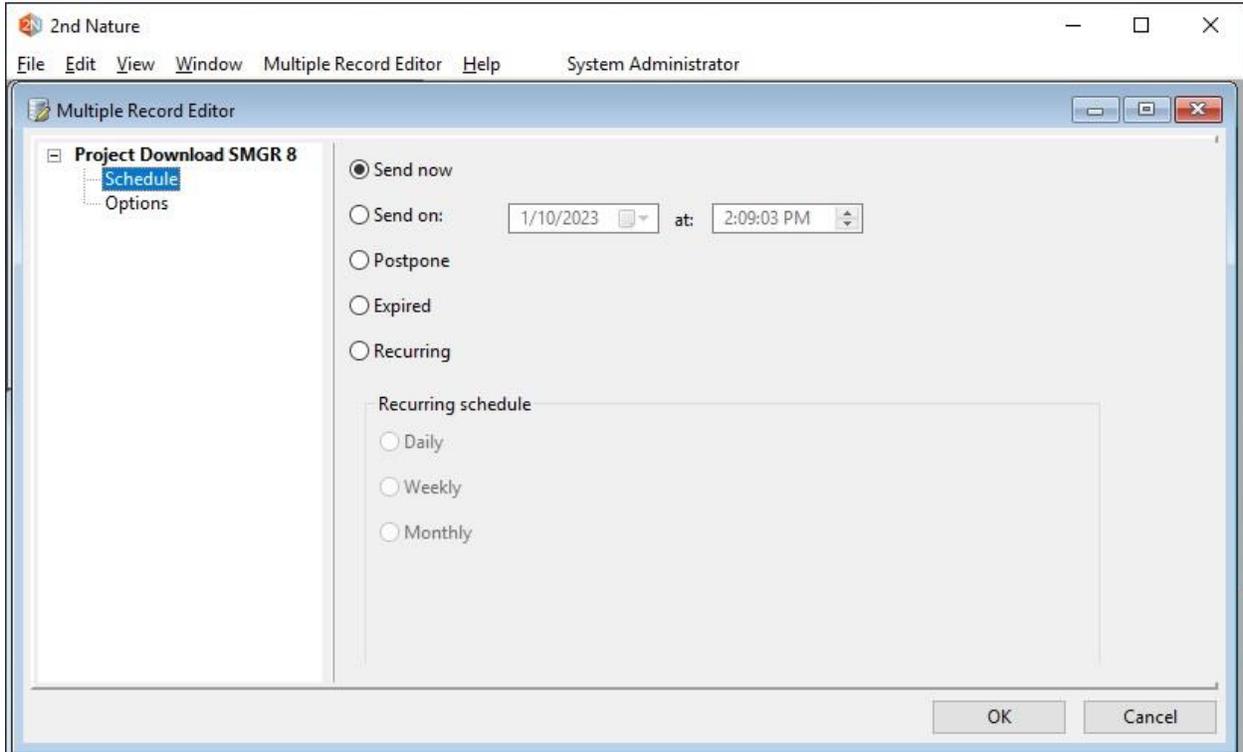


6.6. Download Data

From the **2nd Nature** screen below, right click on the entry in the **System Lists** pane and select **Download** (not shown) 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.

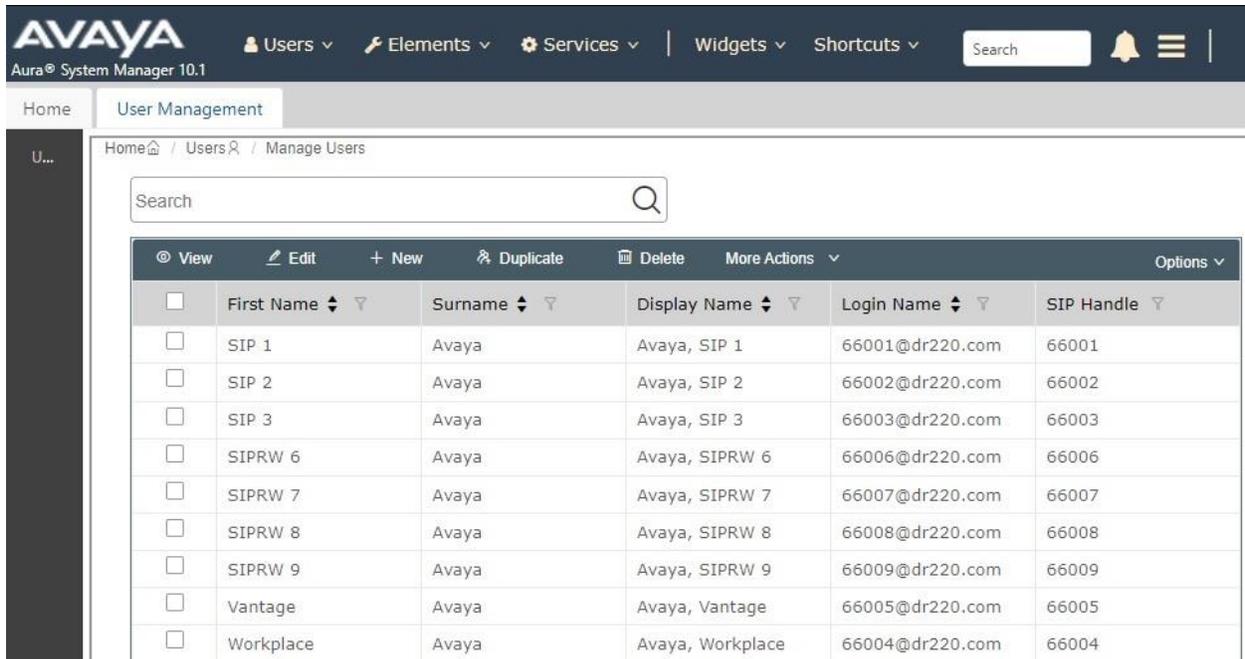


7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of System Manager and 2nd Nature.

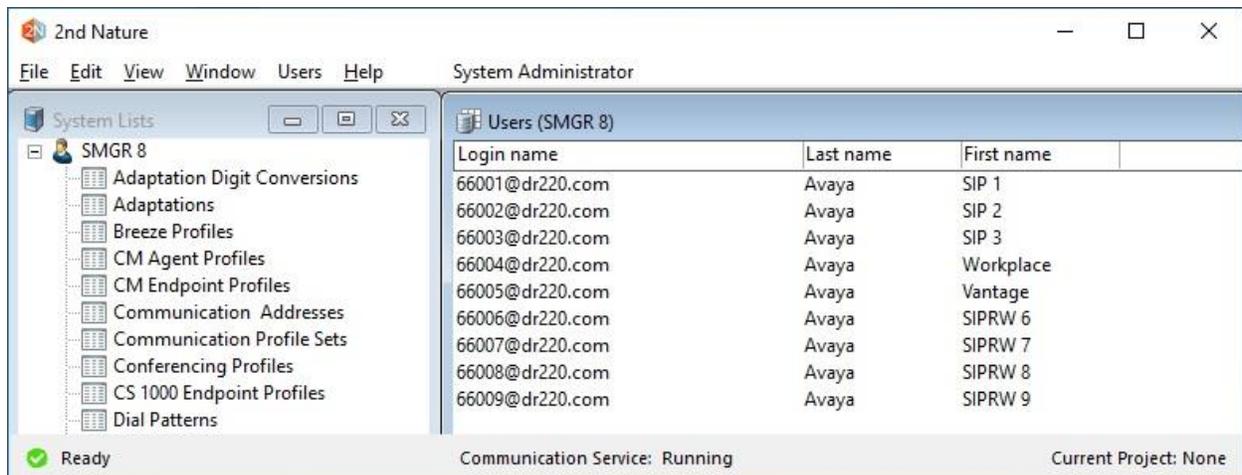
7.1. Verify EMWS

From the System Manager web interface from **Section 5.2**, select **Users → User Management → Manage Users** from the top menu to display a list of users configured on System Manager.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001
<input type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
<input type="checkbox"/>	SIP 3	Avaya	Avaya, SIP 3	66003@dr220.com	66003
<input type="checkbox"/>	SIPRW 6	Avaya	Avaya, SIPRW 6	66006@dr220.com	66006
<input type="checkbox"/>	SIPRW 7	Avaya	Avaya, SIPRW 7	66007@dr220.com	66007
<input type="checkbox"/>	SIPRW 8	Avaya	Avaya, SIPRW 8	66008@dr220.com	66008
<input type="checkbox"/>	SIPRW 9	Avaya	Avaya, SIPRW 9	66009@dr220.com	66009
<input type="checkbox"/>	Vantage	Avaya	Avaya, Vantage	66005@dr220.com	66005
<input type="checkbox"/>	Workplace	Avaya	Avaya, Workplace	66004@dr220.com	66004

From the **2nd Nature** screen, expand the entry in the **System Lists** pane, and double click on **Users** (not shown). Verify that the **Users** pane is created, showing a list of users retrieved from System Manager via UMWS, as shown below.



Login name	Last name	First name
66001@dr220.com	Avaya	SIP 1
66002@dr220.com	Avaya	SIP 2
66003@dr220.com	Avaya	SIP 3
66004@dr220.com	Avaya	Workplace
66005@dr220.com	Avaya	Vantage
66006@dr220.com	Avaya	SIPRW 6
66007@dr220.com	Avaya	SIPRW 7
66008@dr220.com	Avaya	SIPRW 8
66009@dr220.com	Avaya	SIPRW 9

7.2. Verify EMWS

From the System Manager web interface, select **Elements** → **Routing** → **Dial Pattern** from the top menu to display a list of dial patterns configured on System Manager.

The screenshot shows the Avaya System Manager web interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Dial Patterns' and shows a list of 38 items. The table below is a summary of the data shown in the screenshot:

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
#	3	3	<input type="checkbox"/>			-ALL-	
*	3	3	<input type="checkbox"/>			-ALL-	
1	3	3	<input type="checkbox"/>			-ALL-	To CM FAC
+1212663	12	12	<input type="checkbox"/>			-ALL-	To SBCE
+13035321	12	12	<input type="checkbox"/>			-ALL-	To IPO2-IPOSE from SBCE external
+13035322	12	12	<input type="checkbox"/>			-ALL-	To IPO2-IP500V2 from SBCE external
+1303533	12	12	<input type="checkbox"/>			-ALL-	To IPO2-IPOSE for ACCS from SBCE external
+1303534	12	12	<input type="checkbox"/>			-ALL-	To CM/PC from SBCE external
+1303535	12	12	<input type="checkbox"/>			-ALL-	To CM for calls to member applications 5xxxx
+1303536	12	12	<input type="checkbox"/>			-ALL-	To CM from SBCE external
+13035377	12	12	<input type="checkbox"/>			-ALL-	To CM for calls from external SBCE to AAC
+13035378	12	12	<input type="checkbox"/>			-ALL-	To CM for calls from external SBCE to EP
1425553	11	11	<input type="checkbox"/>			-ALL-	To SBCE from EP POM for SIP PSTN
+1703703	12	12	<input type="checkbox"/>			-ALL-	to SBCE
+1732852	12	12	<input type="checkbox"/>			-ALL-	To IPO1 from SBCE external

From the **2nd Nature** screen, expand the entry in the **System Lists** pane, and double click on **Dial Patterns**. Verify that the **Dial Patterns** pane is created, showing a list of dial patterns retrieved from System Manager via RWS, as shown below.

The screenshot shows the 2nd Nature application interface. The 'System Lists' pane on the left shows 'Dial Patterns' expanded under 'SMGR 8'. The main pane displays a table of dial patterns with columns for Pattern, Min, Max, Emergency, and Notes. The table lists various dial patterns including #, *, and several numbers starting with +1212663 and +13035321.

Pattern	Min	Max	Emergency	Emergency	Emergenc	Notes
#	3	3	No	-	-	
*	3	3	No	-	-	
+1212663	12	12	No	-	-	To SBCE
+13035321	12	12	No	-	-	To IPO2-IPOSE from SBCE external
+13035322	12	12	No	-	-	To IPO2-IP500V2 from SBCE external
+1303533	12	12	No	-	-	To IPO2-IPOSE for ACCS from SBCE extern
+1303534	12	12	No	-	-	To CM/PC from SBCE external
+1303535	12	12	No	-	-	To CM for calls to member applications 5x:
+1303536	12	12	No	-	-	To CM from SBCE external
+13035377	12	12	No	-	-	To CM for calls from external SBCE to AAC
+13035378	12	12	No	-	-	To CM for calls from external SBCE to EP
+1703703	12	12	No	-	-	to SBCE

8. Conclusion

These Application Notes describe the configuration steps required for Unimax 2nd Nature 9.6 to successfully interoperate with Avaya Aura® System Manager 10.1 using UMWS and RWS. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

9. Additional References

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

1. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 25, May 2023, available at <http://support.avaya.com>.
2. *2nd Nature Installation Guide*, Version 9.6, November 2021, available as part of 2nd Nature installation.

©2023 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.