



Avaya Solution & Interoperability Test Lab

Application Notes for VTech NG-S3411W Cordless SIP Hospitality Room Phone with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for VTech NG-S3411/NG-S3411W Cordless SIP Hotel Room Phones v3.2.4.5 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. VTech NG-S3411/NG-S3411W hospitality phones register with Avaya Aura® Session Manager as a SIP endpoint.

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 VTech NG-S3411/NG-S3411W Cordless SIP Hotel Room Phones to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. VTech SIP hospitality phones are available in 1- or 2-line styles with corded and cordless handsets. VTech NG-S3411/NG-S3411W Cordless SIP Hotel Room Phones register to Avaya Aura® Session Manager as a SIP endpoint. Compliance testing used the VTech NG-S3411W 1-line Cordless SIP Hotel Room Phone as a representative model. See **Attachment 1** which provides details of VTech NG-S3411W Cordless SIP Hotel Room Phone equivalency to the NG-S3411 SIP Hotel Phone model.

2. General Test Approach and Test Results

The general test approach was to place calls to and from VTech NG-S3411W and exercise basic telephone operations.

As the purpose of these phones is for hotel guest rooms, certain functionality considered to be standard on Avaya endpoints is not supported, and therefore, was not tested. For example, VTech NG-S3411W does not support transfers or conferences. More details on these limitations are described in the Test Results in **Section 2.2**.

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 Avaya systems and VTech NG-S3411W enabled capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

The following areas were evaluated in the interoperability compliance test:

- Registration of VTech NG-S3411W to Session Manager.
- Basic call features: Answer, Hold/Resume, Mute/Un-mute, Drop, Message Waiting Indicator, DTMF, Call Pickup, Call Waiting, and Call Forward.
- G.711 and G.729 codec negotiation, and Session Refresh Interval.
- Media (shuffling) enabled and disabled.
- TLS transport and SRTP media encryption.
- Hospitality features: Automatic Wakeup Call and Housekeeping status.
- Serviceability testing to validate recovery from network connectivity loss.

2.2. Test Results

All test cases were executed. The following observations were made during the testing:

- VTech NG-S3411W does not support the following features
 - Call Park/Unpark
 - Transfer
 - Conference
 - VTech NG-S3411W programmable buttons do not support feature access codes requiring secondary input.
- The VTech G.726 codec payload type of 2 is not supported by Communication Manager. This is acceptable to VTech.
- VTech NG-S3411W does not support SDP negotiation capabilities per (RFC5939) between SRTP and non-SRTP modes so codec sets for the phones must not offer both modes. Employing a separate codec set for the phones' encryption capabilities is a possible alternative to support endpoints that use SDP negotiation in a mixed environment.
- VTech NG-S3411W does not validate the offered identity certificate for Session Manager during TLS handshake. This is a known problem that will be fixed in a future release of VTech NG-S3411W firmware.
- A separate but related observation is that the web administration user interface setting **Only accept trusted certificates** must also be set for VTech NG-S3411W to validate Session Manager identity certificate during TLS session setup. Subsequent access to the web administration's **Trusted Certificates** page will not show that it has been set. This will be fixed in a future release of VTech NG-S3411W firmware.

2.3. Support

Technical support for VTech NG-S3411W SIP Hotel Phones can be obtained at:

- Phone: 1 (888) 907-2007
- <https://vtechhotelphones.com>

3. Reference Configuration

Figure 1 illustrates the test configuration diagram for VTech NG-S3411W integrated with Avaya Aura® Communication Manager and Avaya Aura® System Manager.

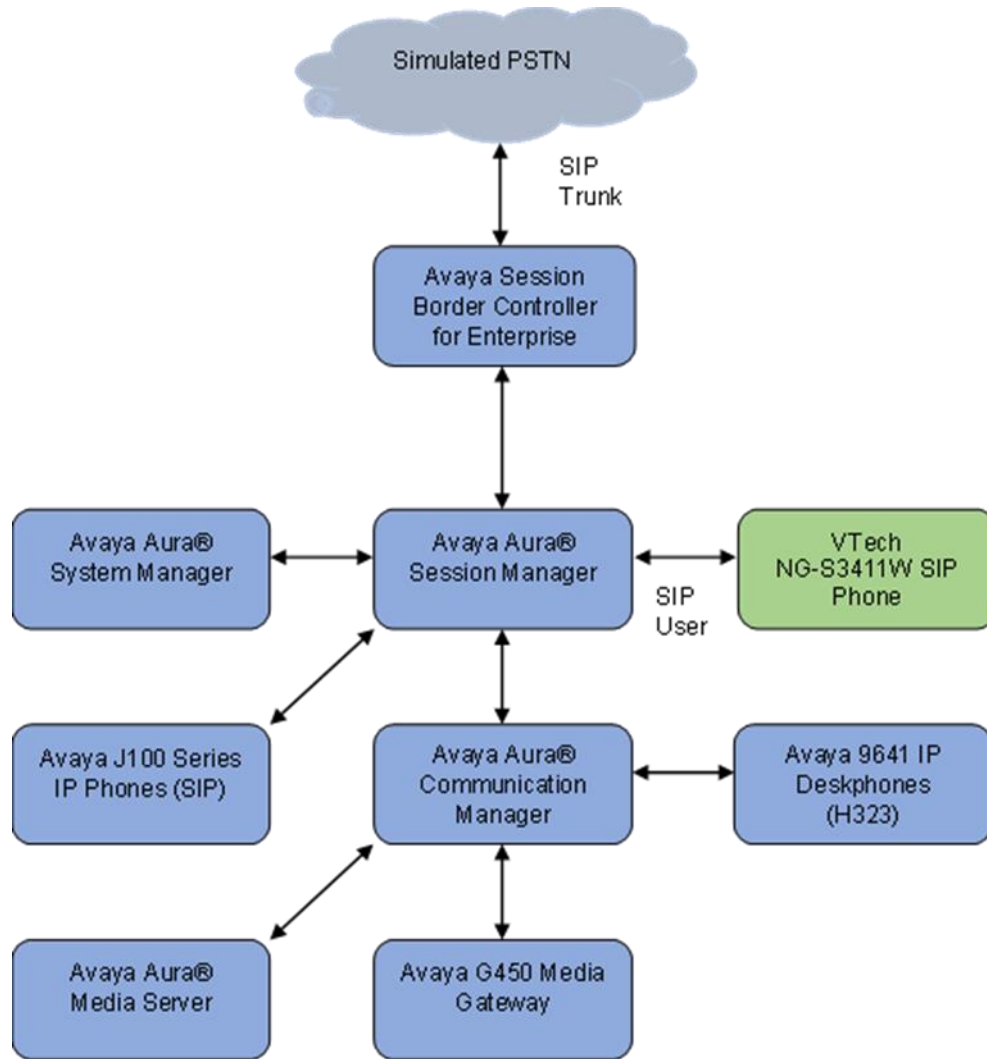


Figure 1: Avaya Test Configuration for VTech NG-S3411W Cordless SIP Hotel Room Phones

4. Equipment and Software Validated

The following equipment and software were used for the compliance test provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Machine	10.1.0.2-SP2 01.0.974.0-27607
Avaya Aura® System Manager running on Virtual Machine	10.1.0.2 Service Pack 2 10.1.0.2.0715160
Avaya Aura® Session Manager running on Virtual Machine	10.1.0.2 Service Pack 2 10.1.0.02.1010215
Avaya Session Border Controller for Enterprise running on Virtual Machine	10.1.1.0-35-21872
Avaya Aura® Media Server running on Virtual Machine	10.1.0.101
Avaya G450 Media Gateway	42.7.0
Avaya 9641G IP DeskPhone	6.8532 (H.323)
Avaya J179 IP Phone	4.0.13.0.6 (SIP)
VTech NG-S3411W Cordless 1-line SIP Hotel Phone	3.2.4.5

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager OPS Licensed Capacity
- Administer IP Network Region
- Administer IP Codec Set

Use the System Access Terminal (SAT) to configure Communication Manager and log in with the appropriate credentials. The configuration steps illustrate field values changed for this reference configuration. Default values were used for all other fields.

Note: It is assumed that basic configuration of the Communication Manager has already been completed, such as the SIP trunk to Session Manager. The SIP station configuration for VTech NG-S3411W is configured through System Manager in **Section 6.2**.

5.1. Verify Communication Manager OPS Licensed Capacity

Using the SAT, verify that the Off-PBX Stations (OPS) and SIP Trunks features are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

display system-parameters customer-options				Page 1 of 12	
OPTIONAL FEATURES					
G3 Version: V20			Software Package: Enterprise		
Location: 2			System ID (SID): 1		
Platform: 28			Module ID (MID): 1		
				USED	
Platform Maximum Ports:		48000	150		
Maximum Stations:		150	115		
Maximum XMOBILE Stations:		36000	0		
Maximum Off-PBX Telephones - EC500:		150	0		
Maximum Off-PBX Telephones - OPS:		150	62		
Maximum Off-PBX Telephones - PBFMC:		150	0		
Maximum Off-PBX Telephones - PVFMC:		150	0		
Maximum Off-PBX Telephones - SCCAN:		0	0		
Maximum Survivable Processors:		313	0		
(NOTE: You must logoff & login to effect the permission changes.)					

5.2. Administer IP Network Region

This IP network region is for the signaling group associated with the SIP trunk between Session Manager and Communication Manager. This form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. Verify the following values:

- **Authoritative Domain:** The applicable domain (e.g., *avaya.com*)
- **Codec Set:** The codec set number from **Section 5.3**

By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the G450 Media Gateway or Media Server.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avaya.com	
Name: Main		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? n
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

5.3. Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to VTech NG-S3411W. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set *1* is specified in **IP Network Region 1** from **Section 5.2**. The form shows the list of codecs tested. Enter values for the following:

- **Audio Codec:** The audio codecs tested
- **Media Encryption:** Do not include *none*

Note: Avaya endpoints supporting both RTP/SRTP may be administered in a separate codec set.

```
display ip-codec-set 1                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt     Size (ms)
1: G.711MU      n             2          20
2: G.711A      n             2          20
3: G.729       n             2          20
4:
5:
6:
7:
Media Encryption                               Encrypted SRTCP: best-effort
1:1-srtp-aescm128-hmac80
2:2-srtp-aescm128-hmac32
3:
4:
5:
```


6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The steps include the following areas.

- Launch System Manager
- Administer SIP Users

6.1. Launch System Manager

Access Session Manager Administration web interface by entering **http://<ip-address>/SMGR** in a web browser, where **<ip-address>** is the IP address of System Manager. Log in using the appropriate credentials.

The screenshot shows the login page for the Avaya Aura Session Manager Administration web interface. The page has a dark header bar. Below the header, there is a light gray sidebar on the left containing several paragraphs of text and a list of cases where IP address access might fail. The main content area on the right contains a login form with fields for 'User ID' and 'Password', 'Log On' and 'Cancel' buttons, and a 'Change Password' link. Below the login form, there is a blue box with a warning icon and text about supported browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

6.2. Administer SIP Users

VTech NG-S3411W is administered as a SIP user on Session Manager by the following steps. This configuration is automatically synchronized with Communication Manager. In Session Manager, select **Users → User Management → Manage Users** to display the **User Management** screen (not shown). Click + **New** to add a user.

6.2.1. Identity

Enter values for the following required attributes for a new SIP user in the **New User Profile** screen:

- **Last Name:** Enter the last name of the user, e.g., *VTech*
- **First Name:** Enter the first name of the user, e.g., *NG3411W*
- **Login Name:** Enter <extension>@<sip domain> of the user (e.g., *70124@avaya.com*)

The screenshot displays the Avaya Aura System Manager 10.1 interface for adding a new user profile. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile icon are also present. The main content area is titled 'User Profile | Add' and features a sidebar with 'Basic Info' selected. The main form area has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is active, showing fields for 'User Provisioning Rule', 'Last Name', 'First Name', 'Login Name', 'Description', 'Password', 'Confirm Password', 'Last Name (in Latin alphabet characters)', 'First Name (in Latin alphabet characters)', 'Middle Name', 'Email Address', 'User Type', and 'Localized Display Name'. The 'Login Name' field is populated with '70124@avaya.com'.

6.2.2. Communication Address

Select the **Communication Profile** tab. Select **Communication Address** in the left-hand side list and click + **New** (not shown).

Enter the following attributes for the **Communication Address**:

- **Type:** Select *Avaya SIP* from the drop-down list
- **Fully Qualified Address:** Enter the extension number (e.g., *70124*)
- **Domain:** Enter the domain (e.g., *avaya.com*)

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The main menu on the left shows 'Home', 'Session Manager', and 'User Management'. The 'User Management' section is active, showing a 'User Profile | Add' form with tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is selected, and the 'Communication Address' section is highlighted. A modal dialog box titled 'Communication Address Add/Edit' is open, featuring a dropdown for 'Type' (set to 'Avaya SIP') and a 'Fully Qualified Address' field with a text input for the extension '70124' and a dropdown for the domain 'avaya.com'. The dialog also includes 'Cancel' and 'OK' buttons.

6.2.3. Communication Profile Password

Click the **Communication Profile Password** tab and in the **Comm-Profile Password** and **Re-enter Comm-Profile Password** fields, enter a numeric password. This will be used to register the device. Click **OK**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The main content area shows the 'User Profile | Add' dialog with tabs for Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is selected, showing fields for 'Communication Profile Password' and 'Re-enter Comm-Profile Password'. A modal window titled 'Comm-Profile Password' is open, prompting for a password and its re-entry. The modal window has a close button (X) and 'Cancel' and 'OK' buttons at the bottom.

6.2.4. Session Manager Profile

Click on the **Session Manager Profile** slide button. For **Primary Session Manager**, **Origination Sequence**, **Termination Sequence**, and **Home Location** (not shown), select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user roles (Users, Elements, Services, Widgets, Shortcuts). The main header shows 'Home' and 'User Management'. The breadcrumb trail indicates 'Home / Users / Manage Users'. The 'User Profile | Add' form is open, with tabs for Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with a dropdown for 'PROFILE SET : Primary' and a 'Communication Address' field. Below this, the 'PROFILES' section has a 'Session Manager Profile' toggle switch turned on and a 'CM Endpoint Profile' toggle switch turned off. The 'SIP Registration' section contains fields for 'Primary Session Manager' (set to 'sm10'), 'Secondary Session Manager' (set to 'Start typing...'), 'Survivability Server' (set to 'Start typing...'), 'Max. Simultaneous Devices' (set to 'Select'), and a checkbox for 'Block New Registration When Maximum Registrations Active?'. The 'Application Sequences' section has dropdowns for 'Origination Sequence' (set to 'cm81') and 'Termination Sequence' (set to 'cm81'). Action buttons at the top right include 'Commit & Continue', 'Commit', and 'Cancel'.

6.2.5. CM Endpoint Profile

Click on the **CM Endpoint Profile** slide button. Fill in the following fields:

- **System:** Select the relevant Communication Manager SIP Entity (e.g., *cm10*)
- **Profile Type:** Select *Endpoint*
- **Template:** Select *J179_DEFAULT_CM_10_1*
- **Extension:** Enter the extension number (e.g., *70124*)

Click on the **Editor** icon in the Extension field to edit Communication Manager settings. Input the appropriate **Coverage Path 1** number (not shown) configured to route unanswered calls to voicemail. Click **Done** to close the Endpoint Editor. Click **Commit**.

The screenshot displays the Avaya Aura System Manager 10.1 User Management interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and user profile 'admin' are also visible. The main content area is titled 'User Profile | Add' and features four tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a form for adding a new profile. The form includes fields for 'System' (cm10), 'Profile Type' (Endpoint), 'Extension' (70124), 'Template' (J179_DEFAULT_CM_10_1), 'Set Type' (J179), 'Security Code' (Enter Security Code), 'Port' (IP), 'Voice Mail Number', 'Preferred Handle' (Select), 'Calculate Route Pattern' (checkbox), 'SIP URI' (Select), 'Delete on Unassign from User or on Delete User' (checkbox), 'Override Endpoint Name and Localized Name' (checkbox), and 'Allow H.323 and SIP Endpoint Dual Registration' (checkbox). The left sidebar shows a list of profiles, with 'CM Endpoint Profile' selected.

7. Configure VTech NG-S3411/NG-S3411W Cordless SIP Hotel Room Phones

The steps to configure VTech NG-S3411W to integrate with Communication manager are as follows:

- Configure IP Address
- Launch Web Interface
- Configure SIP Account
- Install CA Certificate
- Modify Codec Settings

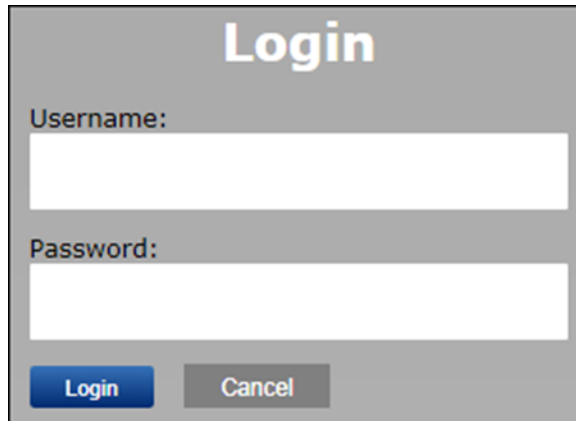
7.1. Configure IP Address

VTech NG-S3411W is configured for DHCP as a factory default. The following steps provide network connectivity and determine the phone IP address for use in launching administration detailed in **Section 7.2**:

- Connect the NET port of VTech NG-S3411W to a Power over Ethernet (PoE) switch
- Determine the assigned IP address. Use the built-in voice menu which will read out the IP address. The voice menu is accessed by pressing **SPEAKER * * * ***. For more information, refer to VTech NG-S3411W user manual obtained at <http://vtechhotelphones.com>.

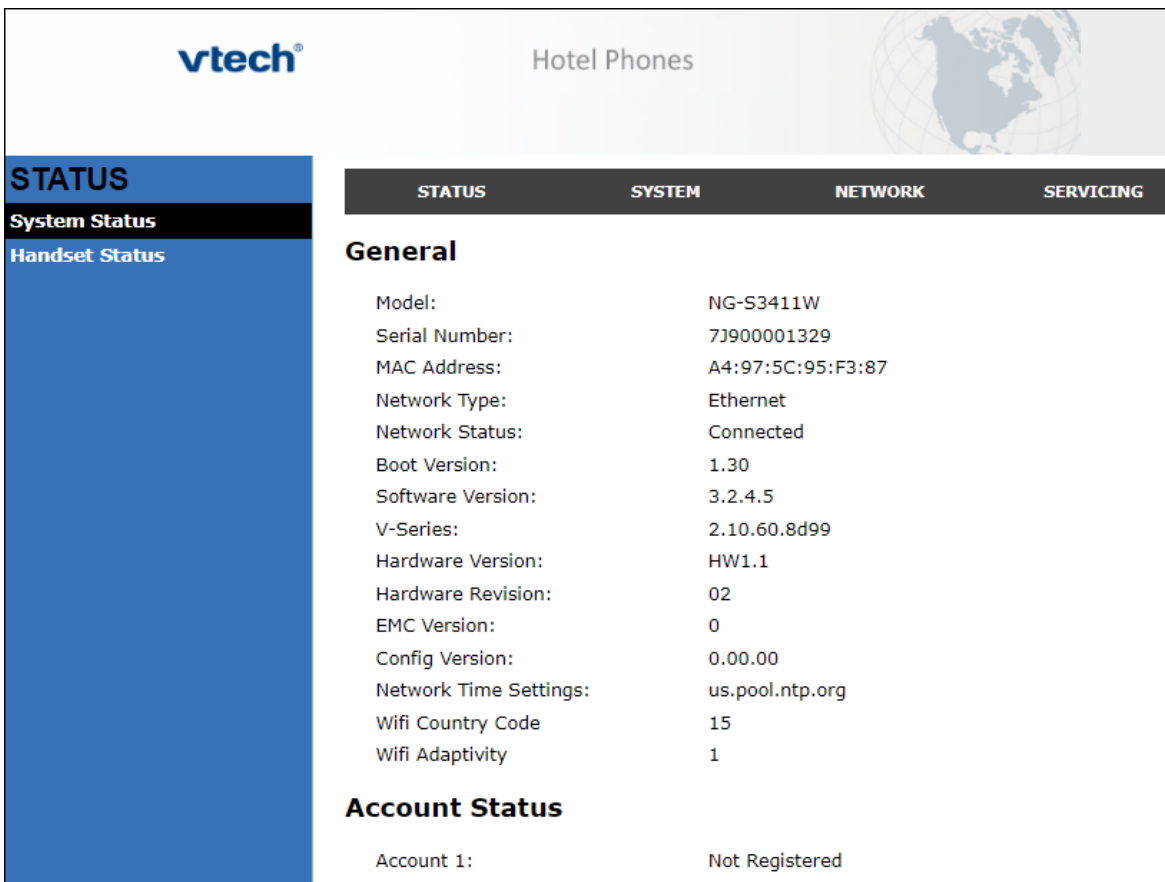
7.2. Launch Web Interface

The phone administration is done through a web interface. To access web administration, invoke the web login page using the **IP address** obtained from **Section 7.1** using the URL **https://<IP address>**. The login prompt is displayed.



The login form is titled "Login" in a large, bold, sans-serif font. Below the title, there are two input fields: "Username:" and "Password:". Each field is a simple white rectangle with a thin gray border. At the bottom of the form, there are two buttons: a blue "Login" button and a gray "Cancel" button.

Enter the appropriate **Username** and **Password**. Once logged in, the default settings display. The status for VTech NG-S3411W is shown.



The web interface for Vtech Hotel Phones is displayed. The header features the Vtech logo, the text "Hotel Phones", and a globe icon. The main content area is divided into a left sidebar and a main panel. The sidebar has a blue background and contains the "STATUS" section with "System Status" and "Handset Status" links. The main panel has a dark gray header with "STATUS", "SYSTEM", "NETWORK", and "SERVICING" tabs. The "STATUS" tab is active, showing a "General" section with various system details and an "Account Status" section.

STATUS	SYSTEM	NETWORK	SERVICING
General			
Model:	NG-S3411W		
Serial Number:	7J900001329		
MAC Address:	A4:97:5C:95:F3:87		
Network Type:	Ethernet		
Network Status:	Connected		
Boot Version:	1.30		
Software Version:	3.2.4.5		
V-Series:	2.10.60.8d99		
Hardware Version:	HW1.1		
Hardware Revision:	02		
EMC Version:	0		
Config Version:	0.00.00		
Network Time Settings:	us.pool.ntp.org		
Wifi Country Code	15		
Wifi Adaptivity	1		
Account Status			
Account 1:	Not Registered		

Note: If firmware upgrades are needed, consult the configuration guide for instructions Refer to <http://vtechhotelphones.com>.

7.3. Configure SIP Account

To register VTech NG-S3411W to Session Manager, Select **System** from the toolbar, then **Account 1** from the left-hand side list. Under the **General Account Settings** heading, input the following:

- **Enable Account:** Click the corresponding checkbox
- **Account Label:** A descriptive string (e.g., *NG3411W*)
- **Display Name:** The desired display name (e.g., *NG3411W SIP*)
- **User Identifier:** An appropriate string (e.g., *70124*)
- **Authentication Name:** Enter the extension number (e.g., *70124*)
- **Authentication Password:** Enter the password

The screenshot displays the VTech Hotel Phones configuration web interface. The top header features the 'vtech' logo and 'Hotel Phones' text, with a globe icon on the right. A navigation bar below the header contains four tabs: 'STATUS', 'SYSTEM' (which is active), 'NETWORK', and 'SERVICING'. On the left side, there is a blue sidebar menu with the following items: 'SYSTEM' (highlighted), 'SIP Account Management', 'Account 1' (highlighted), 'Call Settings', 'Account 1', 'User Preferences', 'Speed Dial Settings', 'Handset Settings', 'Account Assignments', 'Repeater Mode', 'RF Settings', 'Paging Zones', and 'Emergency Dialing Settings'. The main content area is titled 'SYSTEM ACCOUNT MANAGEMENT ACCOUNT 1' and contains a section for 'General Account Settings'. This section includes a checkbox for 'Enable Account' which is checked. Below this are several input fields and dropdown menus: 'Account label' (text box with 'NG3411W'), 'Display Name' (text box with 'NG3411W SIP'), 'User Identifier' (text box with '70124'), 'Authentication Name' (text box with '70124'), 'Authentication Password' (password field with masked characters), 'Dial Plan' (text box with 'x+P'), 'Call Restriction Dial plan' (empty text box), 'Inter-Digit Timeout (secs)' (dropdown menu with '3' selected), 'Line Type' (dropdown menu with 'Private' selected), 'DTMF Method' (dropdown menu with 'Auto' selected), 'Unregister After Reboot' (dropdown menu with 'Disable' selected), and 'Call Rejection Response Code' (dropdown menu with '486' selected).

Under the **SIP Server** heading, enter the following:

- **Server Address:** Session Manager IP address (e.g., *10.64.110.212*)
- **Port:** *5061*

Under the **Registration** heading, enter the following:

- **Server Address:** Session Manager IP address (e.g., *10.64.110.212*)
- **Port:** *5061*

	SIP Server	
	Server Address:	<input type="text" value="10.64.110.212"/>
	Port:	<input type="text" value="5061"/>
	Registration	
	Server Address:	<input type="text" value="10.64.110.212"/>
	Port:	<input type="text" value="5061"/>
	Expiration (secs):	<input type="text" value="3600"/>
	Registration Freq (secs):	<input type="text" value="10"/>
	Outbound Proxy	
	Server Address:	<input type="text"/>
	Port:	<input type="text" value="5060"/>
	Backup Outbound Proxy	
	Server Address:	<input type="text"/>
	Port:	<input type="text" value="5060"/>
	Caller Identity	
Source Priority 1:	<input type="text" value="PAI"/>	
Source Priority 2:	<input type="text" value="RPID"/>	
Source Priority 3:	<input type="text" value="From"/>	

Continuing on the same page, under the **Audio** heading, select **Enable Voice Encryption (SRTP)**. Under the **Signaling Settings** heading, input the following:

- **Local SIP Port:** *5061*
- **Transport:** *TLS*

Under the **Voicemail Settings** header, select **Enable MWI Subscription**. Click **Save** (not shown).

Audio	
Codec Priority 1:	<input type="text" value="G.711u"/>
Codec Priority 2:	<input type="text" value="G.711a"/>
Codec Priority 3:	<input type="text" value="G.729a/b"/>
Codec Priority 4:	<input type="text" value="G.726"/>
Codec Priority 5:	<input type="text" value="G.722"/>
Codec priority 6:	<input type="text" value="None"/>
Codec priority 7:	<input type="text" value="iLBC"/>
<input checked="" type="checkbox"/> Enable Voice Encryption (SRTP)	
<input type="checkbox"/> Enable G.729 Annex B	
Preferred Packetization Time (ms):	<input type="text" value="20"/>
DTMF Payload Type:	<input type="text" value="101"/>
Quality of Service	
DSCP (voice):	<input type="text" value="46"/>
DSCP (signaling):	<input type="text" value="26"/>
Signaling Settings	
Local SIP Port:	<input type="text" value="5061"/>
Transport:	<input type="text" value="TLS"/>
Voice	
Min Local RTP Port:	<input type="text" value="18000"/>
Max Local RTP Port:	<input type="text" value="19000"/>
Voicemail Settings	
<input checked="" type="checkbox"/> Enable MWI Subscription	

7.4. Install CA Certificate

Note: VTech NG-S3411W currently does not validate the server certificate during TLS handshake as noted in **Section 2.2**. This will be fixed in a future firmware release. As such, CA Certificate installation is not needed but is documented here.

Note: The Session Manager CA certificate file must be installed in the VTech NG-S3411W Trusted Certificate store for validation of the Session Manager identity certificate offered during the TLS handshake.

Note: After **Only accept trusted certificates** has been set and saved, subsequent access to the **Trusted Certificates** page will not show that it has been set. The setting can be verified by exporting the phone configuration to a text file in **Provisioning → Export Configuration**.

Review the file and verify the entry *provisioning.check_trusted_certificate = 1* exists.

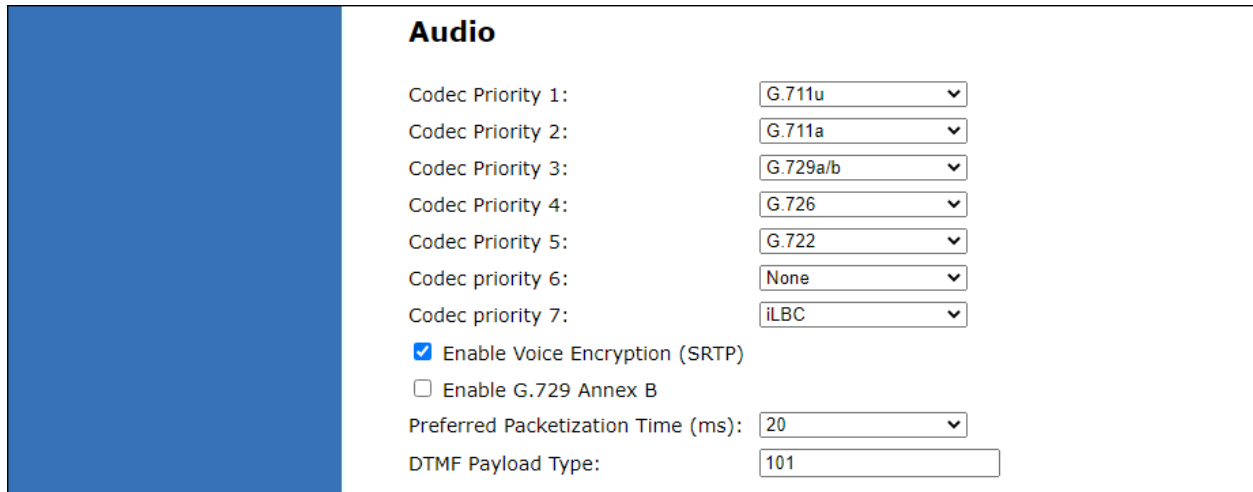
To install the CA certificate, select **SERVICING** from the toolbar, then **Trusted Certificates** from the left-hand side list. Click on **Choose File** and select the CA certificate. Select **Only accept trusted certificates** (not shown). Click **Import** (not shown). The CA should appear in the **Trusted Certificate** list.

The screenshot displays the VTech Hotel Phones web interface. On the left is a blue sidebar menu with options: Reboot, Time and Date, Firmware Upgrade (with sub-options Auto Upgrade and Manual Upgrade), Provisioning, Security, Certificates, Device, **Trusted Certificates** (highlighted), Tr069, and System Logs. The main content area has a top navigation bar with STATUS, SYSTEM, NETWORK, and SERVICING tabs. Below this is the 'Trusted Certificate' section, which includes a 'Select All' checkbox and a table of certificates. The table has columns for 'Total: 5', 'Issue to', 'Issue by', 'Expiration', and 'Protected'. It lists five certificates: Vtech Business Phone Intermediate CA, thawte Primary Root CA - G3, VeriSign Universal Root Certification Authority, DigiCert High Assurance EV Root CA, and System Manager CA. The first four are protected (checkbox checked), while the last is not. Below the table are buttons for 'Delete Selected Entries' and 'Protect Selected Entries', followed by the 'Only accept trusted certificates' checkbox and a 'Save' button. At the bottom, there is an 'Import Trusted Certificate:' section with a 'No file chosen' text box, a 'Choose File' button, and an 'Import' button.

Total: 5	Issue to	Issue by	Expiration	Protected
<input type="checkbox"/>	Vtech Business Phone Intermediate CA	Vtech Business Phone Root CA	Feb 28 07:26:03 2036 GMT	<input checked="" type="checkbox"/>
<input type="checkbox"/>	thawte Primary Root CA - G3	thawte Primary Root CA - G3	Dec 1 23:59:59 2037 GMT	<input checked="" type="checkbox"/>
<input type="checkbox"/>	VeriSign Universal Root Certification Authority	VeriSign Universal Root Certification Authority	Dec 1 23:59:59 2037 GMT	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	<input checked="" type="checkbox"/>
<input type="checkbox"/>	System Manager CA	System Manager CA	May 19 14:55:39 2047 GMT	<input type="checkbox"/>

7.5. Modify Codec Settings

Modify the codec settings by selecting **SYSTEM** in the toolbar and **Account 1** in the left hand side selections. Under the **Audio** heading, select the desired codecs in priority.



Audio	
Codec Priority 1:	G.711u ▼
Codec Priority 2:	G.711a ▼
Codec Priority 3:	G.729a/b ▼
Codec Priority 4:	G.726 ▼
Codec Priority 5:	G.722 ▼
Codec priority 6:	None ▼
Codec priority 7:	iLBC ▼
<input checked="" type="checkbox"/> Enable Voice Encryption (SRTP)	
<input type="checkbox"/> Enable G.729 Annex B	
Preferred Packetization Time (ms):	20 ▼
DTMF Payload Type:	101

Click **Save**.

8. Verification Steps

The proper configuration of VTech NG-S3411W with Avaya Session Manager and Avaya Communication Manager is verified by the following steps.

8.1. View Session Manager Status

Verify VTech NG-S3411W has successfully registered with Session Manager. In System Manager, Navigate to **Elements** → **Session Manager** → **System Status** → **User Registrations**. Check the registration status by the following:

- Verify VTech NG-S3411W (here 70124) is registered with Session Manager by noting the registered users include 70124.

AVAYA

Aura® System Manager 10.1

Users

Elements

Services

Widgets

Shortcuts

Search

admin

Home

Session Manager

S...

Help?

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

Customize

ViewDefaultExportForce UnregisterAST Device Notifications:RebootReloadFailbackAs of 5:11 PMAdvanced Search

13 ItemsShowAllFilter: Enable

<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered				
											Prim	Sec	3rd	4th	Surv
<input type="checkbox"/>	Show	70124@avaya.com	NG3411W	VTech	---	192.168.4.9	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8.2. Call Verification

Verify that basic calls can be made from and to VTech NG-S3411W and another telephone registered to Session Manager.

9. Conclusion

These Application Notes describe the configuration steps required to integrate VTech NG-S3411/NG-S3411W Cordless SIP Hotel Room Phones with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The VTech NG-S3411/NG-S3411W Cordless SIP Hotel Room Phones register to Avaya Aura® Session Manager. Calls were then established with Avaya H.323 / SIP desk phones and the PSTN. In addition, basic telephony features were verified. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

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

Avaya product documentation is available at <https://support.avaya.com>.

[1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 6, Release 10.1, September 2022.

[2] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022.

[3] *Administering Avaya Aura® System Manager*, Issue 7, Release 10.1.x, September 2022.

VTech NG-S3411/NG-S3411W SIP Hotel Phones product documentation is available at <https://vtechhotelphones.com>.

[4] *VTech SIP Next Gen Series NG3411 User's Guide*, October 24, 2022.

©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.



VTech Technologies Canada Ltd.

Date: October 12, 2022

Declaration of Conformance

We, VTech Technologies Canada LTD., declare under sole responsibility that product series NG-S3411 and NGS3411W all share the same hardware circuitry, software, SIP stack, and firmware version. Therefore the products are expected to behave in the same manner. Furthermore, these products are a functional superset of the other products in the NG series. The differences between the different models in the series are detailed in the table below.

Product Name	Model	Description
NG-S3411	NG-S3411	Next Gen Cordless SIP Hospitality Room Phone
NG-S3411W	NG-S3411W	Next Gen Cordless Wi-Fi Enabled SIP Hospitality Room Phone

Please do not hesitate to contact should you require further information.
Thank you,

A handwritten signature in black ink, appearing to read "R. Tischler".

Ralph Tischler
Director of Engineering
VTech Technologies Canada LTD.
604-273-5131
ralphtischler@vtech.ca