



Avaya Solution & Interoperability Test Lab

Application Notes for J&R Technology JR201-FK-VoIP SIP Phone with Avaya Aura® Session Manager 8.0 and Avaya Aura® Communication Manager 8.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for J&R Technology JR201-FK-VoIP SIP Phone to interoperate with Avaya Aura® Session Manager 8.0 and Avaya Aura® Communication Manager 8.0.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 steps required to integrate J&R Technology JR201-FK-VoIP SIP Phones as third-party SIP endpoints with Avaya SIP infrastructure consisting of Avaya Aura® Session Manager 8.0 and Avaya Aura® Communication Manager 8.0. Although the compliance test was completed with and without TLS/SRTP, these Application Notes will describe the configuration with TLS/SRTP enabled.

J&R Technology JR201-FK-VoIP SIP Phones are designed to meet the needs of clients who experience loss through vandalism. They are ideal for parking lots, prisons, railway / metro platforms, hospitals, police stations, ATM machines, stadiums, outside buildings, etc.

2. General Test Approach and Test Results

The general test approach was to configure the JR201-FK-VoIP SIP Phone to communicate with Session Manager as third-party SIP endpoints using TLS connection.

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 J&R Technology JR201-FK-VoIP SIP Phone utilized enabled capabilities of TLS/SRTP.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on carrying out different call scenarios with two-way audio. The tests included:

- Successful registration of JR201-FK-VoIP SIP Phones with Session Manager.
- Calls between JR201-FK-VoIP SIP Phones and Avaya SIP, H.323, digital telephones.
- Calls between JR201-FK-VoIP SIP Phones and PSTN.
- Calls with TLS/SRTP enabled and disabled.
- G.711, G.722 and G729 codec support and negotiation, with and without media shuffling.
- Basic features including audio call, answer, hang up, music on hold, DTMF transmission, and feature access code dialing.
- Proper system recovery after a JR201-FK-VoIP after removal and reconnection of LAN cable.

2.2. Test Results

The testing was successful. All the test cases passed with the following observations.

- JR201-FK-VoIP does not support display screen, Hold, Transfers or Conference.
- JR201-FK-VoIP does not support SIPS. Therefore, the **Enforce SIPS URI for SRTP** option in the SIP signalling group for the SIP trunk between Communication Manager and Session Manager should be disabled.
- JR201-FK-VoIP does not support SDP Capability Negotiation (RFC5939) so the **IP Codec Set** form on Communication Manager should only be set for one Media Encryption method and encrypted SRTCP (i.e., *1-srtp-aescm128-hmac80*); otherwise, SRTP would not be negotiated for the call. To support calls with other Avaya IP deskphones (e.g., Avaya H.323 1600/96x1 Series IP Deskphones) that don't support encrypted SRTCP, a separate IP Network Region with a different IP Codec Set should be used. In this case, the call leg between JR201-FK-VoIP and Communication Manager will have SRTP enabled with encrypted SRTCP and the call leg between the other party and Communication Manager will have SRTP enabled, but not encrypted SRTCP. In this case, the call is not shuffled (i.e., not direct IP-IP media). The Avaya H.323 phones could also support an Avaya proprietary encryption method, such as AES.
- If TLS/SRTP is enabled, the **Initial IP-IP Direct Media** option in the SIP signaling group of the SIP trunk group between Communication Manager and Session Manager

needs to be disabled to avoid failures in some blind transfer scenarios and to allow JR201-FK-VoIP to hear audio prompts from Avaya Aura® Messaging. If non-secure media is being used, the **Initial IP-IP Direct Media** option may be enabled.

2.3. Support

Technical support from J&R Technology Limited can be obtained through the following:

Tel: +86-755-27322952 Mobile: +86-135-1025-6386 (24-Hour Hotline)
Fax: +86-755-27322197 Contact email: info@jrtele.com

3. Reference Configuration

The configuration shown in **Figure 1** was used during the compliance test of JR201-FK-VoIP with Avaya Aura® Session Manager and Communication Manager.

JR201-FK-VoIP SIP Phone interoperates with Avaya Aura® Session Manager using TLS signaling and SRTP for media.

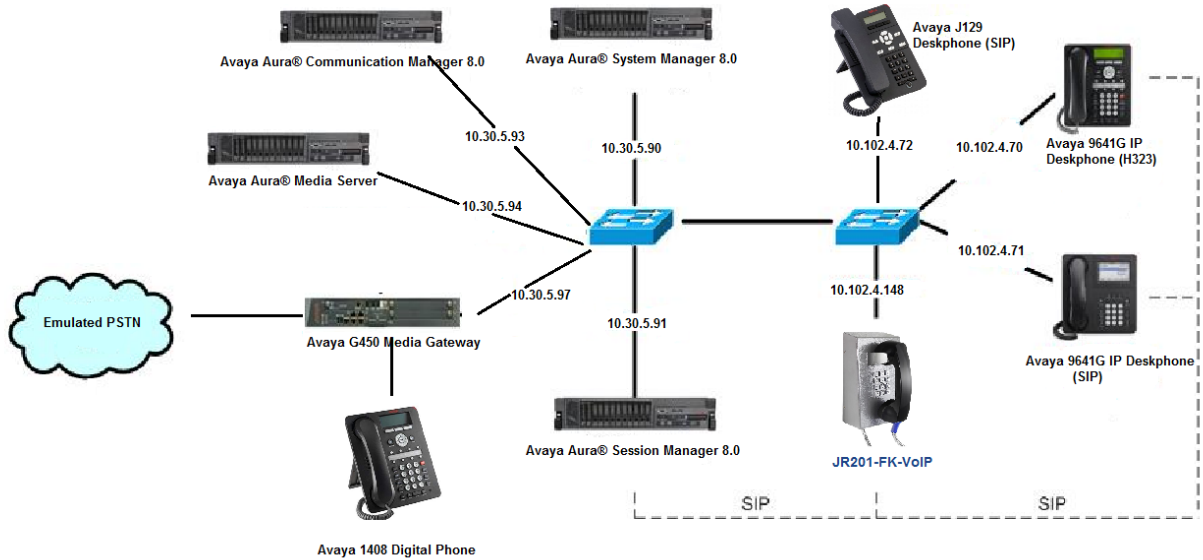


Figure 1: J&R Technology JR201-FK-VoIP SIP Phone with Avaya Aura® Session Manager and Avaya Aura® Communication Manager

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 on VMware	8.0.1.0.0 (8.0 FP1)
Avaya Aura® Session Manager on VMware	8.0.1
Avaya Aura® System Manager	8.0.1
Avaya G450 Media Gateway	40.10.1
Avaya Aura® Media Server	8.0 SP2
Avaya 9641 Deskphones (SIP)	7.1.4.0
Avaya 9621 Deskphones (SIP)	7.1.4.0
Avaya 9641 Deskphones (H323)	6.8.0
Avaya J129 SIP Deskphones	3.0.0.1.6
Avaya Equinox Client for Windows (SIP)	3.4.10.10.2
J&R Technology JR201-FK-VoIP SIP Phone	1.3.37

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Avaya Aura® Communication Manager. The procedures include the following areas:

- Verify Communication Manager License
- Administer IP Network Region and IP Codec Set
- Administer SIP Trunk to Session Manager

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that Communication Manager license has proper permissions for features illustrated in these Application Notes. Using the *display system-parameters customer-options* command, go to **Page 1** and check that the system is sufficiently licensed for **Off-PBX Telephones -OPS**:

```
Page 1 of 12
OPTIONAL FEATURES

G3 Version: V18                      Software Package: Enterprise
Location: 2                          System ID (SID): 1
Platform: 28                          Module ID (MID): 1

                                         USED
Platform Maximum Ports: 6400    546
Maximum Stations: 2400    13
Maximum XMOBILE Stations: 2400    0
Maximum Off-PBX Telephones - EC500: 9600    0
Maximum Off-PBX Telephones - OPS: 9600    10
Maximum Off-PBX Telephones - PBFMC: 9600    0
Maximum Off-PBX Telephones - PVFMC: 9600    0
Maximum Off-PBX Telephones - SCCAN: 2400    0
Maximum Survivable Processors: 313    1

(NOTE: You must logoff & login to effect the permission changes.)
```

On Page 5, verify that the **Media Encryption Over IP** option is enabled.

```
change system-parameters customer-options                               Page 5 of 12

                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                           ISDN Feature Plus? n
  Enhanced EC500? y                                                  ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n                                       ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                       ISDN-PRI? y
  ESS Administration? y                                               Local Survivable Processor? n
  Extended Cvg/Fwd Admin? y                                           Malicious Call Trace? y
  External Device Alarm Admin? y                                       Media Encryption Over IP? y
Five Port Networks Max Per MCC? n                                     Mode Code for Centralized Voice Mail? n
  Flexible Billing? n
Forced Entry of Account Codes? y                                       Multifrequency Signaling? y
  Global Call Classification? y                                       Multimedia Call Handling (Basic)? y
  Hospitality (Basic)? y                                               Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y                                   Multimedia IP SIP Trunking? y
  IP Trunks? y

IP Attendant Consoles? y

                                (NOTE: You must logoff & login to effect the permission changes.)
```


5.2. Administer IP Network Region and IP Codec Set

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. 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 Avaya G450 Media Gateway or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **Codec Set** to be used for calls routed over the SIP trunk to Session Manager.

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
  Region: 1          NR Group: 1
Location: 1        Authoritative Domain: devconnect.com
  Name: SaiGon      Stub Network Region: n
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
```

Use the “**change ip-codec-set n**” command, where **n** is the existing codec set number associated with the SIP trunk group to Session Manager. Update the audio codec types in the **Audio Codec** fields as necessary to include G.711MU, G.711A, G.722 and G.729. To enable SRTP, set **Media Encryption** to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** to *enforce-enc-srtp*.

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

                                IP Codec Set

Codec Set: 1

Audio          Silence      Frames      Packet
Codec          Suppression Per Pkt      Size(ms)
1: G.711A      n              2           20
2: G.711MU      n              2           20
3: G.722-64K   n              2           20
4: G.729        n              2           20
5:
6:
7:

Media Encryption          Encrypted SRTCP: enforce-enc-srtp
1: 1-srtp-aescm128-hmac80
2:
3:
```

Note: To support calls with other IP endpoints (e.g., Avaya H.323 1600/96x1 Series IP Deskphones) that don’t support this Media Encryption/ encrypted SRTCP, these IP endpoints should join a different IP Network Region associated with an IP Codec Set that includes no media encryption or media encryption methods supported by the IP endpoints. For example, for the Avaya H.323 1600/96x1 Series IP Deskphones, the IP Codec Set included *1-srtp-aescm128-hmac80*, *aes* and *none* under Media Encryption and set **Encrypted SRTCP** to *best-effort*. The **IP Network Map** form may be used to associate certain IP endpoints with a specific IP Network Region.

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

                                IP Codec Set

Codec Set: 2

Audio          Silence      Frames      Packet
Codec          Suppression Per Pkt      Size(ms)
1: G.711A      n              2           20
2: G.711MU      n              2           20
3: G.722-64K   n              2           20
4: G.729        n              2           20
5:
6:
7:

Media Encryption          Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
```

5.3. Administer SIP Trunk to Session Manager

JR201-FK-VoIP does not support SIPS. Therefore, the **Enforce SIPS URI for SRTP** option in the SIP signaling group for the SIP trunk between Communication Manager and Session Manager should be disabled. Disable **Initial IP-IP Direct Media** to avoid failures in some blind transfer scenarios.

```
change signaling-group 1                               Page 1 of 3
              SIGNALING GROUP

Group Number: 1          Group Type: sip
  IMS Enabled? n        Transport Method: tls
    Q-SIP? n
    IP Video? y          Priority Video? y          Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? n Peer Server: SM          Clustered? n
  Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
  Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
  Alert Incoming SIP Crisis Calls? n
    Near-end Node Name: procr          Far-end Node Name: smsip92
    Near-end Listen Port: 5061          Far-end Listen Port: 5061
                                          Far-end Network Region: 1

Far-end Domain: devconnect.com

Incoming Dialog Loopbacks: eliminate          Bypass If IP Threshold Exceeded? n
      DTMF over IP: rtp-payload          RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3          Direct IP-IP Audio Connections? y
      Enable Layer 3 Test? y          IP Audio Hairpinning? y
H.323 Station Outgoing Direct Media? y          Initial IP-IP Direct Media? n
                                          Alternate Route Timer(sec): 6
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol for JR201-FK-VoIP IP Phones
- Administer Users

6.1. Launch System Manager

Access the System Manager Web interface by using the URL “<https://<IP Address>/SMGR>” in an internet browser window, where <IP Address> is the IP address of the System Manager server. Log in using the appropriate credentials.

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: Internet Explorer 11.x or Firefox 59.0, 60.0 and 61.0.

6.2. Set Network Transport Protocol for JR201-FK-VoIP IP Phones

From the System Manager Home screen, select **Elements** → **Routing** → **SIP Entities** and edit SIP Entity for Session Manager shown below.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The left sidebar shows a navigation tree with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. The 'General' section includes fields for Name (SMSIP92), IP Address (10.30.5.92), SIP FQDN, Type (Session Manager), Notes, Location (SaiGon), Outbound Proxy, Time Zone (Asia/Ho_Chi_Minh), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' section includes SIP Link Monitoring (Link Monitoring Enabled), Proactive Monitoring Interval (900 seconds), Reactive Monitoring Interval (120 seconds), Number of Tries (1), and Number of Successes (1). 'Commit' and 'Cancel' buttons are located at the top right of the form.

Field	Value
Name	SMSIP92
IP Address	10.30.5.92
SIP FQDN	
Type	Session Manager
Notes	
Location	SaiGon
Outbound Proxy	
Time Zone	Asia/Ho_Chi_Minh
Minimum TLS Version	Use Global Setting
Credential name	
SIP Link Monitoring	Link Monitoring Enabled
Proactive Monitoring Interval (in seconds)	900
Reactive Monitoring Interval (in seconds)	120
Number of Tries	1
Number of Successes	1

Scroll down to the **Listen Ports** section and verify that the transport network protocol used by JR201-FK-VoIP IP Phones is specified in the list below. For the compliance test, the solution used TLS network transport.

Listen Ports

Add		Remove				
3 Items						
<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes	
<input type="checkbox"/>	5060	TCP	devconnect.com	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	5061	TLS	devconnect.com	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	5061	UDP	devconnect.com	<input checked="" type="checkbox"/>		

Select : All, None

6.3. Administer Users

From the dashboard, select **Users** → **User Management** → **Manage Users**.

The screenshot shows the Avaya Aura System Manager 8.0 dashboard. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A dropdown menu is open under 'Users', showing options like 'Administrators', 'Directory Synchronization', 'Groups & Roles', 'User Management', and 'User Provisioning Rule'. The 'User Management' option is further expanded to show 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile Password Policy'. The 'Manage Users' option is highlighted. In the background, there are widgets for 'System Resource Utilization' (a bar chart), 'Alarms' (a table with a 'Severity' dropdown), 'Notifications' (showing 'No data'), and 'Information' (a table listing system elements and their status).

Click **New**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows 'User Management' with 'Manage Users' selected. The main content area displays a table of users with columns for 'First Name', 'Surname', 'Display Name', and 'Login Name'. A '+ New' button is highlighted in the table's action bar.

<input type="checkbox"/>	First Name	Surname	Display Name	Login Name
<input type="checkbox"/>	2010006	TE	2010006 TE	2010006@h
<input type="checkbox"/>	2010007	TE	2010007 TE	2010007@h
<input type="checkbox"/>	2010008 duy	TE duy	2010008 TE duy	2010008@h
<input type="checkbox"/>	2010020	TE	2010020 TE	2010020@h
<input type="checkbox"/>	2012311	TE	2012311 TE	2012311@h
<input type="checkbox"/>	2012312	TE	2012312 TE	2012312@h
<input type="checkbox"/>	2012313	TE	2012313 TE	2012313@h

On the **Identity** tab enter an identifying **Last Name** and **First Name**, enter an appropriate **Login Name**, set **Authentication Type** to **Basic** and administer a password in the **Password** and **Confirm Password** fields.

The screenshot shows the 'User Profile | Add' form in the Avaya Aura System Manager 8.0 interface. The 'Identity' tab is selected. The form includes fields for 'Last Name', 'First Name', 'Login Name', 'Description', 'Password', 'Confirm Password', 'Last Name (Latin Translation)', 'First Name (Latin Translation)', 'Middle Name', 'Email Address', 'User Type', and 'Localized Display Name'. The 'User Provisioning Rule' is set to a dropdown menu. The 'User Type' is set to 'Basic'.

User Profile | Add

Identity | Communication Profile | Membership | Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [Dropdown]

* Last Name: [JR201] Last Name (Latin Translation): [JR201]

* First Name: [Phone1] First Name (Latin Translation): [Phone1]

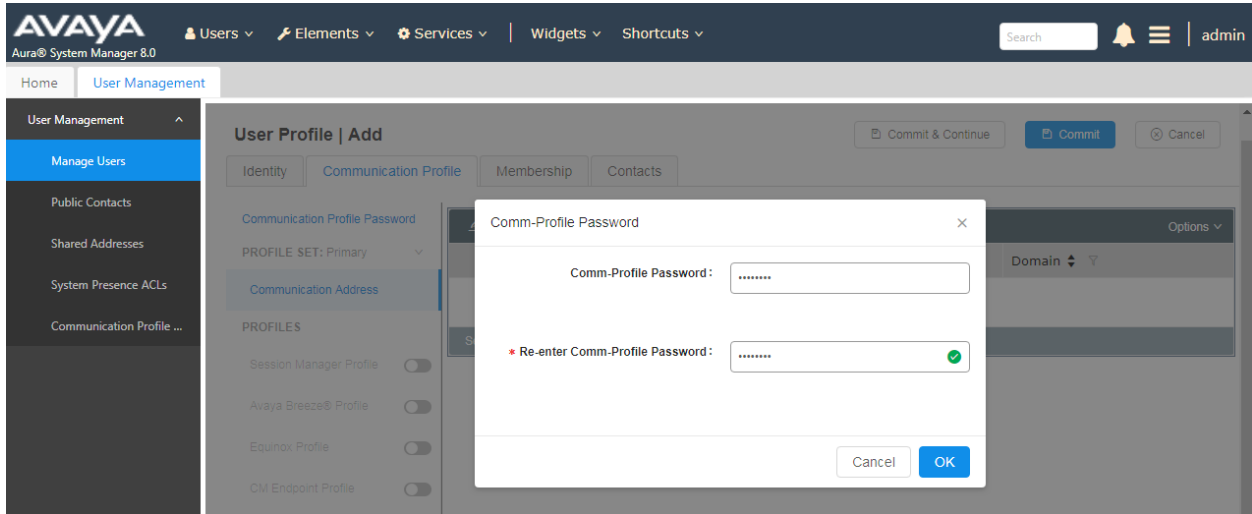
* Login Name: [70003@devconnect.com] Middle Name: [Middle Name Of User]

Description: [Description Of User] Email Address: [Email Address Of User]

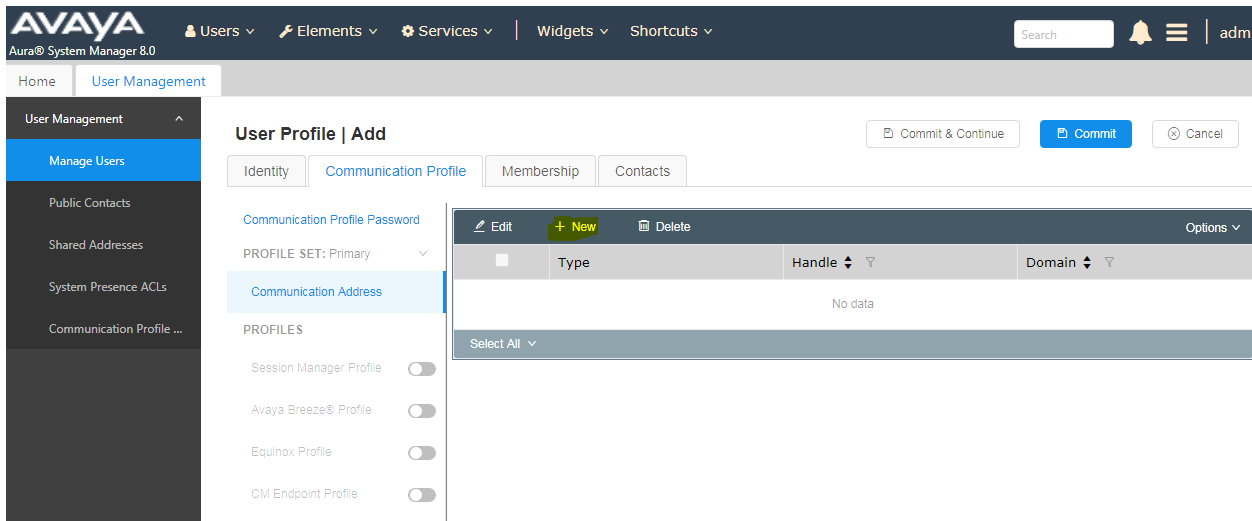
Password: [*****] User Type: [Basic]

* Confirm Password: [*****] Localized Display Name: [Localized Display Name C]

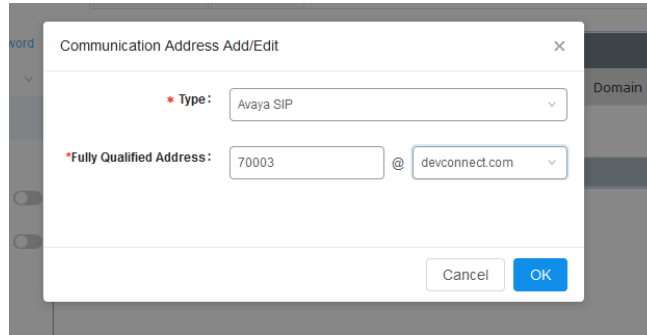
Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.



Click on the **Communication Address**, select **New**.



Select **Avaya SIP** from the **Type** drop down box and enter the **Fully Qualified Address** of the new SIP user. Click **Ok** when done.



Scroll down on the same page. Enable **Session Manager Profile** and enter the **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence** and **Home Location** relevant to the implementation.

Communication Address

PROFILES

- Session Manager Profile
- Avaya Breeze® Profile
- Equinox Profile
- CM Endpoint Profile
- Presence Profile
- Conferencing Profile

* Primary Session Manager: ⓘ

Secondary Session Manager: ⓘ

Survivability Server: ⓘ

Max. Simultaneous Devices:

Block New Registration When Maximum Registrations Active?:

Application Sequences

Origination Sequence:

Termination Sequence:

Emergency Calling Application Sequences

Emergency Calling Origination Sequence:

Emergency Calling Termination Sequence:

Call Routing Settings

* Home Location:

Scroll down the page and enable **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box, select **Endpoint** as the **Profile Type**, enter the **Extension** number you wish to use, select **9641SIP_DEFAULT_CM_8_0** as the **Template** and ensure **IP** is configured as the **Port**, click **Commit & Continue** (not shown) when finished.

Click on **Endpoint Editor** in the **CM Endpoint Profile** and on the General options tab set the **Coverage Path 1** field to a coverage path that routes the call to an alternate destination, if necessary. Click **Done** (not shown) to return to the previous web page.

Click on **Commit** to save the user. The user is now listed.

<input type="checkbox"/>	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	Phone1	JR201	JR201, Phone1	70003@devconnect.com	+8483970003

Select All

Total Users : 1 10 / page Goto

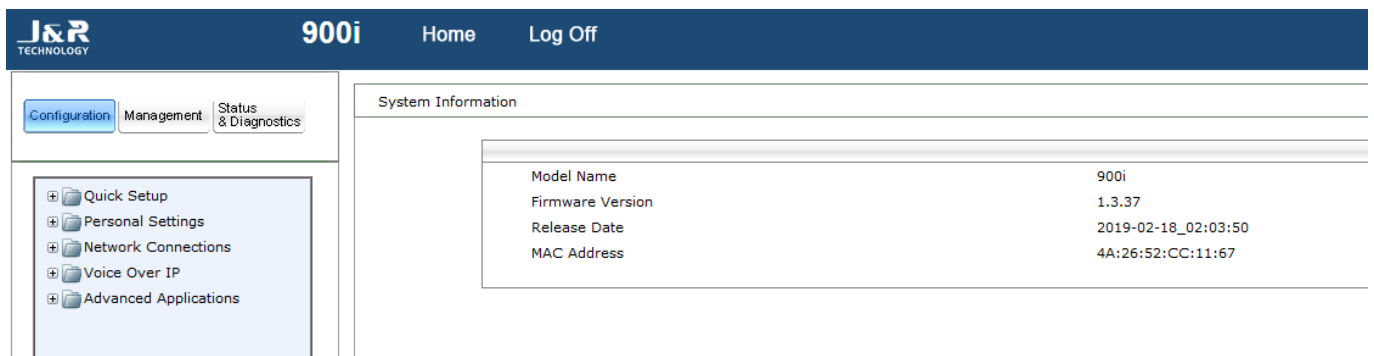
7. Configure JR201-FK-VoIP SIP Phones

This section provides the procedures for configuring JR201-FK-VoIP SIP Phones. The procedures include the following areas:

- Access Web Interface
- Configure Network Connections
- Configure Voice Over IP

7.1. Access Web Interface

Enter <http://<ip-addr>/>, where <ip-addr> is the IP address of the JR201-FK-VoIP phone, into the address bar of web browser and log in using a valid account. The **System Information** screen is displayed on the Home page.



The screenshot shows the J&R Technology 900i web interface. The top navigation bar includes the logo, the model name '900i', and links for 'Home' and 'Log Off'. Below the navigation bar, there are three tabs: 'Configuration', 'Management', and 'Status & Diagnostics'. The 'Configuration' tab is selected. On the left side, there is a menu with the following items: 'Quick Setup', 'Personal Settings', 'Network Connections', 'Voice Over IP', and 'Advanced Applications'. The main content area displays 'System Information' with the following details:

Model Name	900i
Firmware Version	1.3.37
Release Date	2019-02-18_02:03:50
MAC Address	4A:26:52:CC:11:67

7.2. Configure Network Connections

Select **Configuration** tab (top left) in the left pane for configuration settings. Select the **Network Connections** → **Network Settings** from the left menu (not shown)

In the **Network Settings**, choose **Static IP** for the **IP_Type** field as static IP is used in this testing. Enter the appropriate **Domain Name**, **IP Address**, **Subnet Mask**, **Default Gateway_Address** and **Primary DNS**. Leave the rest as default. Click **Submit** to save settings. The phone will reboot to update new configuration settings.

▼Network Settings	
IP_Type:	<input checked="" type="radio"/> Static IP <input type="radio"/> Automatic IP (DHCP)
Domain Name:	devconnect.com <input checked="" type="checkbox"/> Manual
IP Address:	10.102.4.148 <input checked="" type="checkbox"/> Manual
Subnet Mask:	255.255.255.0 <input checked="" type="checkbox"/> Manual
Default Gateway_Address:	10.102.4.1 <input checked="" type="checkbox"/> Manual
Primary DNS:	10.128.224.79 <input checked="" type="checkbox"/> Manual
Secondary DNS:	0.0.0.0 <input checked="" type="checkbox"/> Manual
MAC Address:	4A:26:52:CC:11:67
LAN Port Mode:	Auto Negotiation ▼
PC Port Mode:	Auto Negotiation ▼
▼Port Mirroring	
Activate:	Disable ▼
▼VLAN Settings	
VLAN Discovery Mode:	Automatic Configuration of VLAN (CDP+LLDP) ▼
Period:	30 Seconds
PC Port VLAN Activate:	Disable ▼



7.3. Configure Voice Over IP

Log into the JR201-FK-VoIP phone web interface again with new static IP address.

7.3.1. Signaling Protocols

From **Configuration** tab, select **Voice Over IP → Signaling Protocols**. Select **TLS** as **SIP Transport Protocol**, enter **TLS Port** and **SIP Local Port** you wish to use, enter the SIP domain in the **Gateway Name** field.

<ul style="list-style-type: none"> Configuration Management Status & Diagnostics 	<p>Signaling Protocols</p> <p>▼ SIP General</p> <p>SIP Transport Protocol: TLS ▼</p> <p>TLS Port: 5061</p> <p>SIP Local Port: 5060</p> <p>Gateway Name: devconnect.com</p> <p>PRACK Mode: Enable ▼</p> <p>Enable RPORT: Enable ▼</p> <p>Include PTIME in SDP: Enable ▼</p> <p>Enable Keep Alive using OPTIONS: Disable ▼</p> <p>Connect Media on 180 Response: Disable ▼</p> <p>Block Caller ID on Outgoing Calls: Disable ▼</p> <p>Incoming Anonymous Call Blocking: Disable ▼</p>
---	---

Scroll down the page and select **Enable** for **Use SIP Proxy** and **Use SIP proxy IP and Port for Registration** fields, enter **5061** for **Proxy Port**. Leave the rest as default. Click **Submit** to save settings (not shown).

▼SIP Proxy and Registrar	
Use SIP Proxy:	Enable ▾
Proxy IP Address or Host Name:	10.30.5.92
Proxy Port:	5061
Enable Registrar Keep Alive:	Enable ▾
Keep Alive Period:	60 Seconds
Maximum Number of Authentication Retries:	4
Use SIP Proxy IP and Port for Registration:	Enable ▾
Use SIP Registrar:	Disable ▾
Registration Expires:	3600 Seconds
Registration Failed Expires:	300 Seconds
Use SIP Outbound Proxy:	Disable ▾
Use Redundant Outbound Proxy:	Disable ▾
Redundant Proxy Mode:	Disable ▾

7.3.2. Media Streaming

From **Configuration** tab, select **Voice Over IP → Media Streaming**.

Select **101** for **DTMF Relay RFC 2833 Payload Type**. In **Codecs** table, select the appropriate codec to be supported for the phone in the order listed. In the screen shown below, **G711 A-Law** is set as first preference, **G711 u-Law** is set as second preference, **G729** is set as 3rd preference and **G722** is set as 4th preference. Select **Enable** for **Enable SRTP Encryption and Authentication** and **AES_CM_128_ALL_METHODS** for **Method**. Click **Submit** to save settings (not shown).

Media Streaming			
▼Media Streaming Parameters			
RTP Port Range - Contiguous Series of 4 Ports Starting From:	4000		
DTMF Relay RFC 2833 Payload Type:	101		
▼Quality of Service Parameters			
Type of Service (ToS):	0xb8 Hex		
▼Codecs			
Codec Priority	Codec Type	Packetization Time (milliseconds)	
1st Codec	G.711, 64 Kbps, A-Law ▾	20 ▾	
2nd Codec	G.711, 64 Kbps, u-Law ▾	20 ▾	
3rd Codec	G.729, 8 Kbps ▾	20 ▾	
4th Codec	G.722/16000 ▾	20 ▾	
5th Codec	None ▾	30 ▾	
▼SRTP			
Enable SRTP Encryption and Authentication:	Enable ▾		
Method:	AES_CM_128_ALL_METHODS ▾		
ARIA:	Disable ▾		

7.3.3. Line Settings

From **Configuration** tab, select **Voice Over IP → Line Settings**.

Select **Line Number 1**, select **Enable** for **Line 1 Activate** field, enter **Line 1 User ID**, **Line 1 Authentication User Name** and **Line 1 Authentication Password** with the account details as shown below to match the user settings in Session Manager added in **Section 6.2**. Repeat with the same user settings for **Line Number 2**. For a different user account, a new user must be created in Session Manager as in **Section 5.2**.

Line Settings

▼Line Settings

Line Number: 1 ▾

Line 1 Activate: Enable ▾

Line 1 Display Name: JPhone

Line 1 User ID: 70003

Line 1 Authentication User Name: 70003

Line 1 Line 1 Authentication Password: ●●●●●●●●

Line 1 Line 1 Label:

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Session Manager and JR201-FK-VoIP SIP Phones.

From the main System Manager dashboard, select Session Manager from the **Elements** section (not shown). Select **System Status → User Registrations** from the left-hand menu (not shown). The JR201-FK-VoIP user is listed and will show a tick in the **Prim** box under **Registered**.

User Registrations

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

Cu											
View ▾		Default		Export		Force Unregister		AST Device Notifications:		Reboot	
								Reload ▾		Failback	
										As of 6:41 PM	
											Advanced
19 Items Filter											
Show		15 ▾									
<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered Prim ▾
<input type="checkbox"/>	▶ Show	70001@devconnect.com	Viet	Nam	---	10.128.224.212	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	▶ Show	70003@devconnect.com	Phone1	JR201	---	10.102.4.147	<input type="checkbox"/>	<input type="checkbox"/>	1/2	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Establish a call between JR201-FK-VoIP and a local Avaya SIP deskphone. The **status trunk** command may be used to view the active call status. The trunk that is being monitored here is the trunk to Session Manager. This command should specify the trunk group and trunk member used for the call. On **Page 2**, **Audio Connection Type** will set to *ip-direct* if the call is shuffled. The **Codec Type** is also displayed.

```

status trunk 1/40                                     Page 2 of 3
CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
  Near-end: 10.30.5.93                               : 5061
  Far-end: 10.30.5.92                               : 5061
H.245 Near:
H.245 Far:
H.245 Signaling Loc:                               H.245 Tunneled in Q.931? no
Audio Connection Type: ip-direct           Authentication Type: None
Near-end Audio Loc:                               Codec Type: G.711MU
  Audio       IP Address                               Port
  Near-end: 10.102.4.147                             : 4018
  Far-end: 10.128.224.223                             : 5004
Video Near:
Video Far:
Video Port:
Video Near-end Codec:                               Video Far-end Codec:

```

9. Conclusion

These Application Notes describe the configuration steps required for J&R Technology JR201-FK-VoIP SIP Phones to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and J&R Technology Ltd product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- i. *Administering Avaya Aura® Communication Manager, Release 8, Issue 2.0, Nov 2018*
- ii. *Administering Avaya Aura® Session Manager, Release 8, Issue 2, August 2018*
- iii. *Administering Avaya Aura® System Manager, Release 8, Issue 4, September 2018*

Information regarding Product documentation for JR201-FK-VoIP SIP Phones can be obtained by contacting the Support email in **Section 2.3**.

©2019 Avaya Inc. All Rights Reserved.

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

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