



Application Notes for Spectralink 84-Series Wireless Telephones with a Duplicated Avaya Aura® Communication Manager in an Enterprise Survivable Server Environment with Primary and Secondary Avaya Aura® Session Managers – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Spectralink 84-Series Wireless SIP Telephones to interoperate with a duplicated Avaya Aura® Communication Manager in an Enterprise Survivable Server (ESS) environment including primary and secondary Avaya Aura® Session Managers.

The overall objective of the interoperability compliance testing is to verify Spectralink 84-Series Telephones functionalities in an environment comprised of duplicated Avaya Aura® Communication Managers in an ESS environment, primary and secondary Avaya Aura® Session Managers, and various Avaya telephones (analog, digital, H.323, and SIP).

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 procedures for configuring Spectralink 84-Series Wireless SIP Telephones to interoperate with a duplicated Avaya Aura® Communication Manager in an Enterprise Survivable Server (ESS) environment including primary and secondary Avaya Aura® Session Managers. These Application Notes assume that each Communication Manager and Session Manager has already been installed and basic configuration steps have been performed. Only the steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult the references in **Section 11**.

The Spectralink phones register with Avaya Aura® Session Manager as SIP endpoints. In addition to testing basic SIP functionality, the Spectralink phones were also tested to ensure that they could failover and failback between primary and secondary Session Managers. It is important to note that the Spectralink phones do not support the same simultaneous and alternate registration mechanisms that are utilized by the Avaya 9600 Series SIP phones for failover and failback. Rather, the Spectralink phones were configured to use a combination of configuration file parameters and DNS SRV records to implement their own alternate registration strategy for failover and failback.

During compliance testing, the Spectralink phones received their IP address via Dynamic Host Configuration Protocol (DHCP). As part of the DHCP message exchange between the phones and the DHCP server, the DHCP server was configured to return the Domain Name System (DNS) server IP address to the DHCP clients (i.e., the phones). Using the SIP domain configured in the Spectralink **site.cfg** file, the phones would then attempt to discover any SIP servers (e.g. Avaya Aura® Session Managers) that they could register to by querying the DNS server for `_sip` service DNS SRV records within that domain. In the tested configuration, the DNS server was configured with two DNS SRV records: one for the primary Session Manager and one for the secondary Session Manager (refer to **Appendix C** for the DNS server configuration). As a result, the DNS server responded to the phones' queries with two DNS SRV records, each containing the Session Manager's hostname (FQDN), priority, protocol (TCP), and port (5060) to be used for SIP communication.

Note, if for any reason the DNS server became unreachable, or could not find/respond with DNS SRV records, then the Spectralink phones would attempt to use any static record values configured in their **site.cfg** file, as shown in **Section 8.2.2** of this document.

The default registration period requested by the 84-Series handsets is 3600 seconds (i.e., 1 hour). However, by shortening this interval, the Avaya Aura® system and the handset can more quickly detect outages and take appropriate actions for failover/failback. The trade-off is that requiring re-registration too often can create extra traffic on the network. For compliance testing, 2 minutes was the time used to require re-registration.

2. General Test Approach and Test Results

The overall objective of the interoperability compliance testing was to verify Spectralink 84-Series Telephone functionalities in an environment comprised of duplicated Avaya Aura® Communication Managers in an ESS environment, primary and secondary Avaya Aura® Session Managers, and various Avaya telephones (analog, digital, H.323, and SIP).

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.

DevConnect Compliance Testing for this Application Note focused on the features and functionality listed, however Spectralink labs also performs independent testing. Avaya DevConnect cannot warrant that the features and functionality described in these independent tests function correctly, however users seeking additional configuration assistance and feature interoperability details may wish to consult the following Interoperability Notes document available on the Spectralink Support site:

http://support.spectralink.com/sites/default/files/resource_files/1725-86991-000_A.pdf

2.1. Interoperability Compliance Testing

For basic SIP functionality, the general test approach was to place calls to and from Spectralink 84-Series and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711MU)
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- Transfer with Shuffling enabled (origination/destination/ attended/unattended)
- Transfer with Shuffling disabled (origination/destination/ attended/unattended)
- Three party conference (origination/destination)
- Avaya Feature Name Extension (FNE)
 - Call Park
 - Call Pickup
 - Call Forward (Unconditional, Busy/no answer)
- MWI
- Voicemail
- Multi-Device Access

- Serviceability

The next test approach was to verify the phones could failover and failback between Session Managers, and recover from various failure scenarios, including:

- Failure of the Active duplicated Communication Manager in an ESS environment, causing the Standby server to become Active, and failback
- Failure of both the Active and Standby duplicated Communication Manager in an ESS environment, causing the Survivable Server to be Active, and failback
- Failure of the primary Session Manager, causing failover to the secondary Session Manager, and failback
- Failure of the DNS server
- Failure of the wireless network

2.2. Test Results

The test objectives were verified. All test cases passed with the tested features working as expected with the following observations.

The Spectralink 8400 phones were able to handle the failure of the Active duplicated Communication Manager server, as well as the Main Server (i.e., both the Active and Standby pair that make of the Main Server in an ESS environment) with no loss of registration to Session Manager. The phones were able to place and receive calls regardless of which Communication Manager server was Active.

The Spectralink phones were able to maintain audio for calls that had been established with the media shuffled between the endpoints, even if the Session Manager or Communication Manager/media gateway became unavailable during the course of the call. When the media has been shuffled between endpoints, a failure of the Communication Manager/media gateway should not cause a call in progress to lose audio since the Communication Manager/media gateway is no longer in the audio path (note, Session Manager is not in the audio path regardless of whether the media is shuffled or not). For established calls without the media shuffled, a failure of the Communication Manager/media gateway in the audio path can cause a loss of audio.

If a Session Manager becomes unavailable during an established call, and the Spectralink phones failover or failback to the other Session Manager, even though the audio for a call with shuffled media is maintained, any actions that require signaling (e.g., placing the call on hold or hanging up) should not be relied on. These actions may result in failure of the call with the call not being completely torn down if only one endpoint hangs up. To completely terminate the call, both endpoints should hang up.

Based on the `reg.1.server.1.expires="120"` parameter that was used during compliance testing (see **Section 8.2.2**), the Spectralink phones were able to detect a Session Manager failure within two minutes, and then failover or failback within another two minutes.

If the phones booted when the DNS server was unavailable, they were able to utilize static DNS cache values to determine the Primary and Secondary Session Manager addresses and achieve registration. Testing also covered DNS record renewals when the DNS TTL had expired. Example static DNS cache values are shown in **Section 8.2.2** of this document.

Without wireless access, the test phones cannot communicate with the Avaya Aura environment and will not be able to place or receive calls. In the test environment, when the wireless network was restored, the phone successfully re-established connection with the Session Manager.

The Spectralink phones do not support display updates via the UPDATE SIP message. As a result, the Spectralink phones didn't show the number of parties in a conference via the display name, and the phones didn't always accurately reflect the name/number of the party on the other end of the line following transfers and/or conferences.

2.3. Support

Support for the Spectralink 84-Series can be obtained through the following:

- **Customer Support Hotline** at 1-800-775-5330. The hotline is open Monday through Friday, 6 a.m. to 6 p.m. Mountain Time.
- **Technical Support:** technicalsupport@Spectralink.com
- **Knowledge Base:** <http://support.Spectralink.com>

3. Reference Configuration

Figure 1 illustrates a sample configuration with a duplicated Communication Manager Server with an Avaya G450 Media Gateway in an Enterprise Survivable Server (ESS) environment, including redundant Session Managers. Site 1 consists of a duplicated Communication Manager Main Server and the primary Session Manager. Site 2 consists of a duplicated Communication Manager Survivable Server and the secondary Session Manager. The Spectralink 84-Series Wireless Telephones are connected to a Spectralink approved Access Point (AP) and registered with Session Manager as SIP users.

Also shown in the figure below are the Avaya Aura® System Manager used to configure each Session Manager, the Avaya Aura® Messaging server used for voicemail, and Avaya endpoints (analog, digital, H.323 and SIP) used for testing various call flows. Not shown in the figure below are the DHCP, FTP, and DNS servers that were utilized during testing.

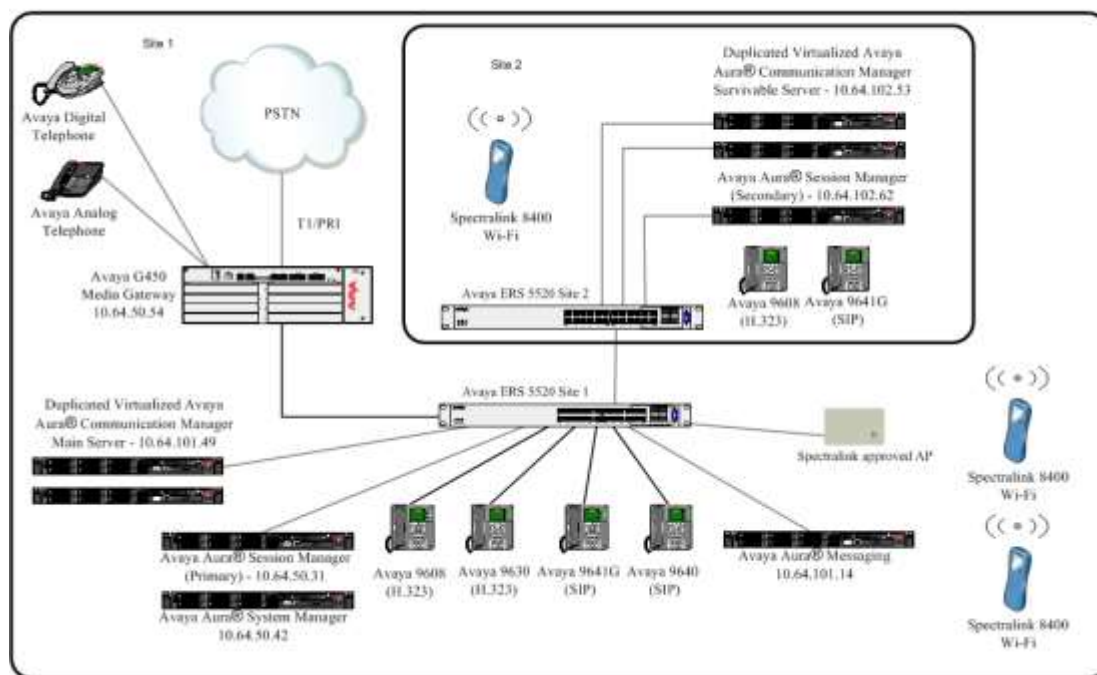


Figure 1: Spectralink 84-Series Wireless Telephones in Avaya Aura® SIP Environment

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 w/ G450 Media Gateway	6.3.10
Avaya Aura® System Manager	6.3.13
Avaya Aura® Session Manager	6.3.13
Avaya Aura® Messaging	6.3
Avaya 9600 Series IP Deskphones (H323 and SIP)	various
Avaya Analog Telephone	-
Avaya Digital Telephone	-
Spectralink 84-Series Wireless Telephones	4.11.0.2041

5. General Configuration for Duplication & Redundancy

The configuration of a duplicated Communication Manager server, an Enterprise Survivable Server (ESS), and redundant Session Managers is outside the scope of this document. No special or additional configuration was required in these areas to specifically support the Spectralink 84-Series Wireless Telephones. However, some explanation and configuration has been provided below as a reference and for the convenience of the reader. For more information on duplicated Communication Managers, ESS environments, and Session Manager redundancy, please consult references [1] and [2] in **Section 11**.

For compliance testing, four virtualized Communication Manager servers (two duplicated pairs) were utilized. Within each pair, one Communication Manager served as the Active server and the other as the Standby server. The pair at Site 1 in **Figure 1** represented the “Main Server” in the ESS environment. The **Main Server** consisted of the following two Communication Managers (where the Active server was reachable via IP address **10.64.101.49**):

Main Server (10.64.101.49):

- Communication Manager #1
- Communication Manager #2

The pair of servers at Site 2 in **Figure 1** were configured as the “Survivable Server” in the ESS environment. The **Survivable Server** consisted of the following two Communication Managers (where the Active server was reachable via IP address **10.64.102.53**):

Survivable Server (10.64.102.53):

- Communication Manager #3
- Communication Manager #4

Using the System Access Terminal (SAT) to configure Communication Manager, SIP trunks were created to both the primary and secondary Session Managers. Likewise, the System Manager web interface was used to create Entity Links (i.e. SIP Trunks) from each Session Manager to Communication Manager. The following steps were taken to create the Entity Links.

1. The **Local Host Name Resolution** table was modified to map FQDN **cm.d4f27.com** to both the **Main Server** and **Survivable Server** addresses of Communication Manager (10.64.101.49 and 10.64.102.53) as shown below. Note that the Main Server was given a higher priority than the Survivable Server. The lowest value has the highest priority.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar contains a navigation menu with categories like Session Manager, Network Configuration, and Device and Location Configuration. The main content area is titled 'Local Host Name Resolution' and includes a table of entries. A red box highlights three entries for 'cm.d4f27.com' with IP addresses 10.64.101.179, 10.64.101.49, and 10.64.102.53. The entry with IP 10.64.101.49 has a priority of 100, while the entry with IP 10.64.102.53 has a priority of 200. Below the table, there is a 'Background Job Status' section showing 0 items.

Local Host Name Resolution

This page allows you to add, edit, or remove local host name entries. Host name entries on this page will override information provided by DNS.

Local Host Name Entries

New Edit Delete More Actions

3 Items Filter: Enable

<input type="checkbox"/>	Host Name (FQDN)	IP Address	Port	Priority	Weight	Transport
<input type="checkbox"/>	cm.d4f27.com	10.64.101.179	5061	100	100	TLS
<input type="checkbox"/>	cm.d4f27.com	10.64.101.49	5060	100	100	TCP
<input type="checkbox"/>	cm.d4f27.com	10.64.102.53	5060	200	100	TCP

Select: All, None

Background Job Status

View Failures Stop Job

0 Items Show ALL Filter: Enable

Start Time	Status	Percent Completed	Total Entries to Process	Failed Entries	Last Updated	Job Name
No jobs have been queued since System Manager was last started.						

- Communication Manager SIP Entity **cmd4f27** was created and assigned the **cm.d4f27.com** FQDN. Additionally, Entity links were configured from the primary and secondary Session Managers SIP Entities, **sm5031** and **sm10262** respectively, to the Communication Manager SIP Entity.

AVAYA
Aura® System Manager 6.3

Last Logged on at July 22, 2015 12:30 PM
Go... Log off admin

Home Session Manager User Management Session Manager Routing

Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: cmd4f27

* FQDN or IP Address: cm.d4f27.com

Type: CM

Notes:

Adaptation: CM Adapter

Location: d4f27_l1

Time Zone: America/Denver

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* sm10262_cmd4f27_5061	sm10262	TLS	* 5061	cmd4f27	* 5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	* sm5031_cmd4f27_5061	sm5031	TLS	* 5061	cmd4f27	* 5061	trusted	<input type="checkbox"/>

Select: All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

6. Configure Avaya Aura® Communication Manager

This document assumes that a duplicated Communication Manager has already been installed in an ESS environment and that basic configuration exists for the reference configuration shown in **Figure 1**, including:

- All Avaya endpoints
- Signaling/Trunk Groups
- Dial Plans and Routing
- Feature Access Codes

Since the Spectralink phones register with a Session Manager, there is no specific configuration required on Communication Manager to support the Spectralink phones, other than the creation of the SIP stations on Communication Manager which will be created automatically in the next section.

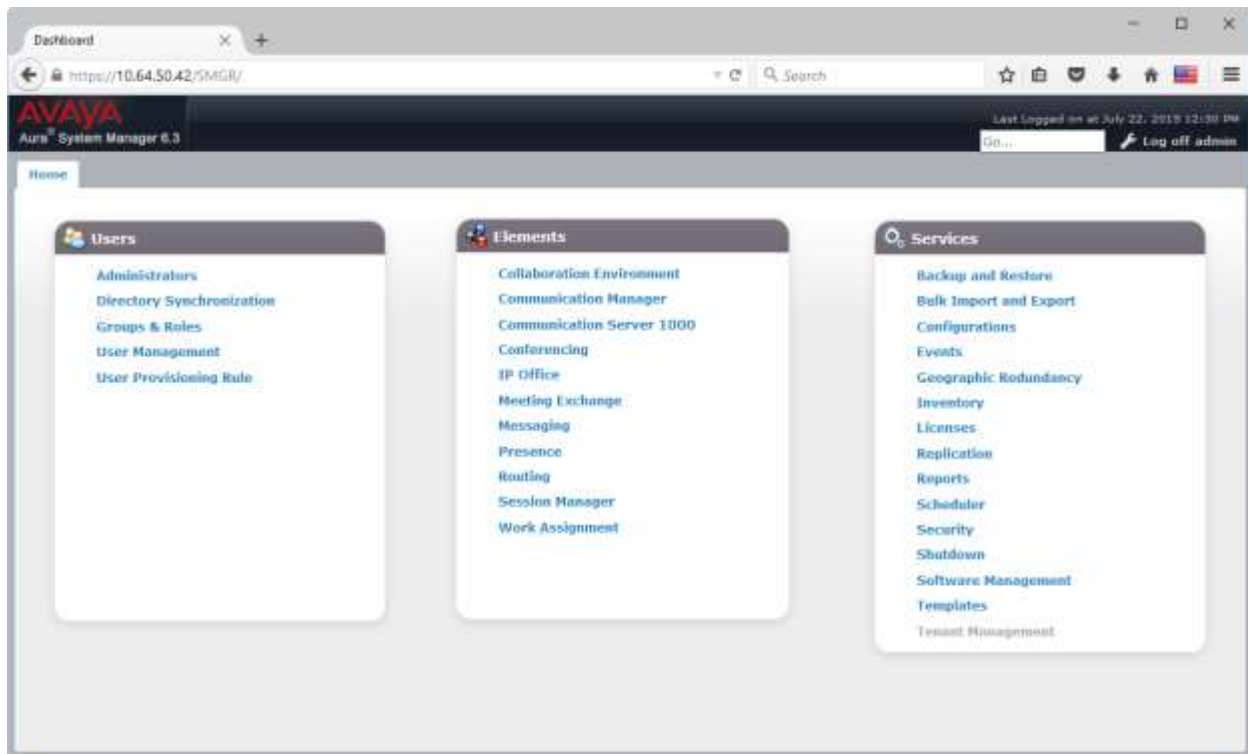
7. Configure Avaya Aura® Session Manager

This section provides the procedures needed to allow a Spectralink 84-Series Wireless Telephone to register with the primary and secondary Session Managers shown in the reference configuration (**Figure 1**).

The following sub-sections assume that both Session Managers and System Manager have been installed and that basic configuration already exists, including the following:

- **A SIP Domain**
- **A Location**
- **SIP Entities** for the Communication Manager, the two Session Managers and Avaya Aura® Messaging
- **Entity Links** between the two Session Managers, each Session Manager and Communication Manager, and each Session Manager and the Messaging server
- **Time Ranges**
- **Routing Policies**
- **Dial Patterns**
- **Applications and Application Sequences**

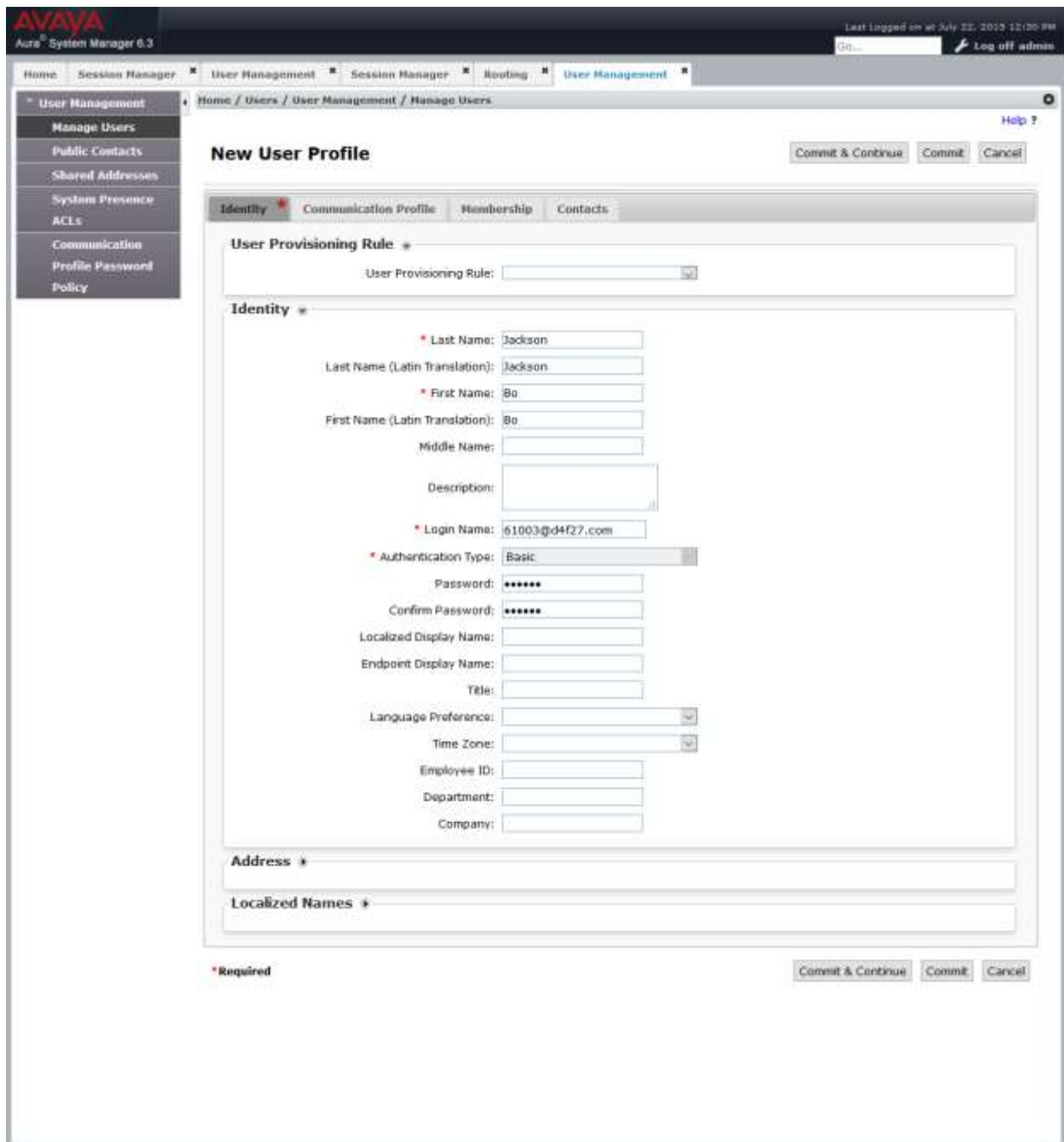
Provisioning for Session Manager is performed through the System Manager Web interface. To access System Manager, launch a web browser, enter <https://<IP address of System Manager>> in the URL, and log in with the appropriate credentials. The following home page is displayed.



7.1. Configure SIP User

To add a new SIP user for a Spectralink phone, Navigate to **Home → Users → User Management → Manage Users**. Click **New** (not shown) and provide the following information:

- Identity tab
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.
 - **Login Name** – Enter extension number@sip_domain name.
 - **Authentication Type** – Verify **Basic** is selected.
 - **Password** and **Confirm Password** – Enter password of user.



- Communication Profile tab

Provide the following information:

- **Communication Profile Password** – Enter a numeric value used for the SIP user to register with Session Manager.
- **Confirm Password** – Repeat numeric password.

Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name** – Enter **Primary**.
- **Default** – Enter ☒

The screenshot displays the 'New User Profile' page in the Avaya Aura System Manager 6.1. The 'Communication Profile' tab is active. The 'Communication Profile' section contains two password fields, both masked. Below them is a table with one entry, 'Primary', which is selected. The 'Default' checkbox for this entry is checked. At the bottom, the 'Communication Address' section shows an empty table with the message 'No Records found'.




- Communication Address sub-section

Select **New** to define a **Communication Address** for the new SIP user, and provide the following information:

- **Type** – Select **Avaya SIP** using drop-down menu.
- **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

Click the **Add** button to save the Communication Address for the new SIP user.

Communication Address ▼



<input type="checkbox"/>	Type	Handle	Domain
No Records found			

Type:

* Fully Qualified Address: @

Add

Cancel

- Session Manager Profile section
 - **Primary Session Manager** – Select primary Session Manager SIP Entity from the drop-down menu.
 - **Secondary Session Manager** – Select secondary Session Manager SIP Entity from the drop-down menu.
 - **Max. Simultaneous Devices** – Select desired number from drop-down menu.
 - **Origination Application Sequence** – Select the Application Sequence created to route calls to Communication Manager
 - **Termination Application Sequence** – Select Application Sequence created to route calls to Communication Manager.
 - **Block New Registration When Maximum Registrations Active** – If desired, check the box to block any new registration requests when the current number of maximum registrations has already been reached.
 - **Home Location** – Select Location previously configured on Session Manager.

☒ **Session Manager Profile** ▼

SIP Registration

* Primary Session Manager ▼

Secondary Session Manager ▼

Survivability Server ▼

Max. Simultaneous Devices ▼

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence ▼

Termination Sequence ▼

Call Routing Settings

* Home Location ▼

Conference Factory Set ▼

Call History Settings

Enable Centralized Call History? ☐

- Endpoint Profile section
 - **System** – Select Managed Element defined in **System Manager** (not shown) for Communication Manager.
 - **Profile Type** – Select **Endpoint**.
 - **Use Existing Endpoints** - Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created or check the box if endpoint is already defined in Communication Manager.
 - **Extension** - Enter same extension number used in this section.
 - **Template** – Select template for type of SIP phone. During the compliance test, **9608SIP_DEFAULT_CM_6_3** was selected.
 - **Security Code** – Enter numeric value used to log on to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.)
 - **Port** – Select **IP**
 - **Voice Mail Number** – Enter **Pilot Number** for Avaya Modular Messaging if installed or leave field blank. This feature was not used during the compliance test.
 - **Delete Station on Unassign of Endpoint from User or on Delete User** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

☒ **CM Endpoint Profile** ▼

* System ▼

* Profile Type ▼

Use Existing Endpoints ☐

* Extension

* Template ▼

Set Type

Security Code

Port

Voice Mail Number

Preferred Handle ▼

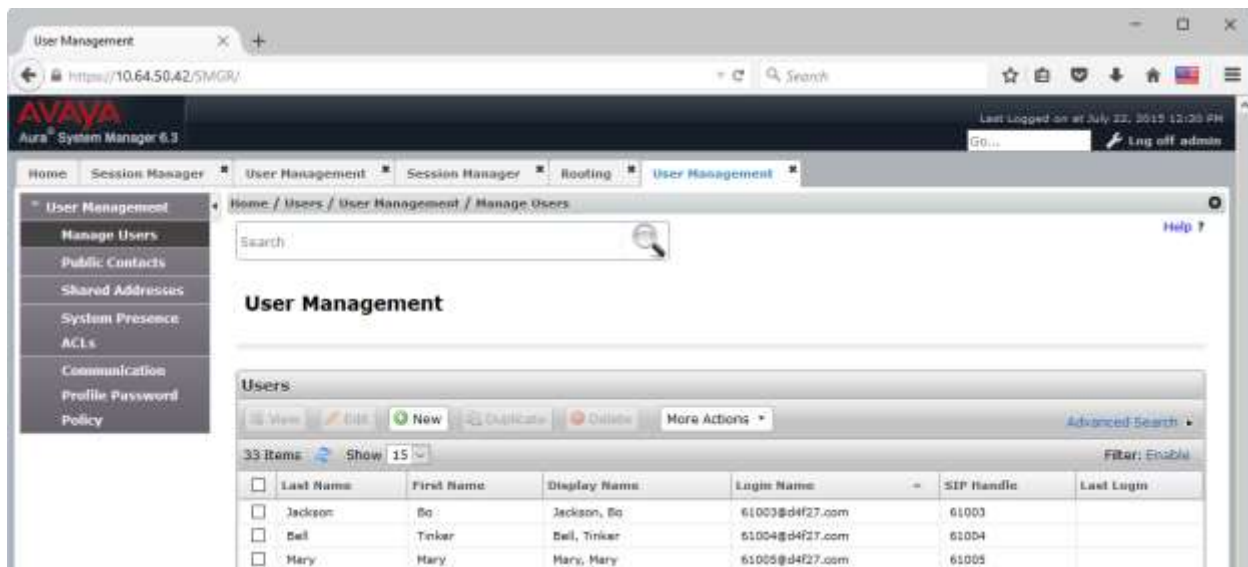
Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☒

Override Endpoint Name and Localized Name ☒

Click the **Commit** button (not shown) to save the user. This will automatically create a SIP station on Communication Manager. The creation of the SIP station on Communication Manager can be verified by performing a **list station** command from the Communication Manager System Access Terminal (SAT).

Repeat these steps to add any additional users. The following screen shows the users created during compliance testing.



8. Configure Spectralink 84-Series Wireless Telephones

This section provides steps required to configure a Spectralink 84-Series handset to register with the primary Avaya Aura® Session Manager, failover to the secondary Session Manager, and failback to the primary Session Manager. There are two ways to configure the Spectralink 84-Series handsets:

1. Using the configuration files [recommended]
2. Using the WEB user interface [deprecated]

For compliance testing, configuration files were used, and the Flat Deployment Scenario template was followed and tested, though Spectralink has stated that any of the supported configuration template formats should function. The important thing to ensure is that the phones receive all of the recommended configuration values when contacting their provisioning server. Refer to Spectralink documentation for more information on template formats.

8.1. Connect the Handsets to the Wireless LAN

The first step in connecting the Spectralink 84-Series handset to an Avaya Aura® SIP environment is to get the handset connected to the wireless LAN. The wireless LAN

configuration is outside the scope of this document; however detailed discussions of this topic are available through the Spectralink support web site:

<http://support.Spectralink.com/products/wi-fi/Spectralink-84-series-wireless-telephone>

See *Spectralink 84-Series Wireless Telephone Deployment Guide* or the *Spectralink 84-Series SLIC Administration Guide*.

Note that a Spectralink approved Access Point (AP) is required. Please consult the Spectralink support site for the most up-to-date list of Spectralink VIEW certified Access Points:

<http://support.spectralink.com/view>

8.2. Configure Per-phone and Site-Wide Parameters

The following configuration files were modified during compliance testing: **site.cfg** and **<macaddress>-ext.cfg**, where **<macaddress>** is the 12 digit MAC address of the handset without any separators. One **<macaddress>-ext.cfg** file is created for each handset that is deployed.

8.2.1. Extension Configuration File

The **<macaddress>-ext.cfg** file provides per-handset parameters. The following parameters and values were used for user 61003 during compliance testing. Refer to **Appendix A** for the complete extension configuration file used.

Registration Parameters	
reg.1.address="61003 "	Specifies the SIP username to be used for registration. This value will typically correspond with the extension number.
reg.1.auth.userID="61003"	Specifies the authentication user ID to be used for response to digest authentication challenges. The value of this parameter should correspond with the Login Name field of the User in System Manager
reg.1.auth.password="123456"	Specifies the authentication password to be used for responses to digest authentication challenges. This value should correspond with the Communication Profile Password created for the User in System Manager.
Voicemail Integration Parameters	
msg.mwi.1.subscribe=""	Specifies the value to use in SIP Subscribe messages for this registration when requesting to be notified of Voice Mail Message Waiting Messages. If non-Null, the handset will send a SUBSCRIBE request to this contact after boot-up. This value will typically correspond to the extension number; however, no value was needed in the compliance tested configuration for MWIs (with Avaya Aura® Messaging). Previous testing found it necessary to populate this field with the extension number in order to

	achieve successful MWIs with Communication Manager Messaging.
--	---

8.2.2. Site-wide configuration

The **site.cfg** file provides global or site-wide parameters. One file is configured for the facility. The following parameters and values were used during compliance testing. Note that the *Optional Parameters* specified in the table below are simply matters of personal preference, and not necessary for basic registration or functionality. Refer to **Appendix B** for the complete site configuration file used during testing.

<i>reg.1.x parameters replace the SIPserver volpProt.x parameters</i>	
reg.1.server.1.address="d4f27.com"	Specifies the address of the proxy server that the handset will register with (i.e. the Avaya Aura® Session Manager). This value should correspond with the Domain name specified for Session Manager's Signaling Group created in the Communications Manager.
reg.1.server.1.transport="TCPonly"	Specifies the transport the handset will use to attempt registrations.
reg.1.server.1.expires="120"	Specifies the desired registration interval. Note that this value significantly reduces the default interval and is recommended to help minimize the amount of time a phone may take to achieve failover or fallback. This value is in seconds.
volpProt.server.1.failOver.reRegisterOn="1"	When set to 1, the handset will attempt to register with the secondary server. If the registration succeeds (a 200 OK response with valid expires), signaling will proceed with the secondary server
volpProt.server.1.failOver.failRegistrationOn="1"	When set to 1, and the reRegisterOn parameter is enabled, the handset will silently invalidate an existing registration (if it exists), at the point of failing over
volpProt.server.1.failOver.failBack.mode="duration"	When set to duration, the primary server is retried after the amount of time defined by the timeout parameter (as shown in the next row)
volpProt.server.1.failOver.failBack.timeout="120"	When failBack.mode is set to "duration", the time in seconds after failing over to the current working server before the primary server becomes the first server to forward new requests to. If you set a value between 1 and 59, the timeout will be 60 seconds. If you set a value of 0, the primary server won't be selected as the first server to forward new requests to until a failover event occurs with the current working server.
volpProt.SIP.failoverOn503Response="1"	Specifies the handset should attempt to failover upon receiving a 503 response. If a primary Session Manager is in the "Deny New Service" service state (e.g. for maintenance purposes), it will send 503 responses to endpoints that contact it. Utilizing this parameter allows the Spectralink 8400 phones to redirect their messaging to the

	secondary Session Manager when this occurs.
Call Forwarding / DND Parameters	
volpProt.SIP.serverFeatureControl.dnd="0"	If set to 1, server-based DND is enabled. The call server has control of DND. If set to 0, server-based DND is not enabled
volpProt.SIP.serverFeatureControl.cf="0"	Enable or disable server-based call forwarding
volpProt.SIP.use486forReject="1"	Specifies the handset should send 486, rather than 603 messages when rejecting a call
Static DNS Parameters that are utilized if the DNS SRV query fails or returns no DNS SRV records	
dns.cache.SRV.1.name="_sip._tcp.d4f27.com"	The domain name string with SRV prefix.
dns.cache.SRV.1.ttl="300"	The TTL describes the time period the handset will use the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record will retry a dynamic network request before falling back on the static entry and its reset TTL timer again.
dns.cache.SRV.1.priority="1"	The priority of this target host.
dns.cache.SRV.1.weight="1"	A server selection mechanism.
dns.cache.SRV.1.port="5060"	The port on this target host of this service.
dns.cache.SRV.1.target="sm5031.d4f27.com"	The domain name of the target host.
dns.cache.A.1.name="sm5031.d4f27.com"	Hostname
dns.cache.A.1.ttl="300"	The TTL describes the time period the handset will use the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record will retry a dynamic network request before falling back on the static entry and its reset TTL timer again.
dns.cache.A.1.address="10.64.50.31"	IP Address
dns.cache.SRV.2.name="_sip._tcp.d4f27.com"	The domain name string with SRV prefix.
dns.cache.SRV.2.ttl="300"	The TTL describes the time period the handset will use the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record will retry a dynamic network request before falling back on the static entry and its reset TTL timer again.
dns.cache.SRV.2.priority="2"	The priority of this target host.
dns.cache.SRV.2.weight="1"	A server selection mechanism.
dns.cache.SRV.2.port="5060"	The port on this target host of this service.
dns.cache.SRV.2.target="sm10262.d4f27.com"	The domain name of the target host.
dns.cache.A.2.name="sm10262.d4f27.com"	Hostname
dns.cache.A.2.ttl="300"	The TTL describes the time period the handset will use the configured static cache record. If a dynamic network request receives no response, this timer begins on first access of the static record and once the timer expires, the next lookup for that record will retry a dynamic network request before falling back on the static entry and its reset TTL timer again.
dns.cache.A.2.address="10.64.102.62"	IP Address

<i>Voicemail Integration Parameters</i>	
up.oneTouchVoicemail="1"	enables one-touch voicemail dialing
up.mwiVisible="1"	
msg.mwi.1.callBackMode="contact"	specifies the handset will dial the "msg.mwi.1.callBack" value rather than the phones' own extension in order to access the Voicemail system
msg.mwi.1.callBack="69999"	specifies the number the handset will dial when attempting to contacting the Voicemail system (e.g. the Voicemail pilot number)
<i>Optional Parameters</i>	
dialplan.digitmap=""	Nulls the existing dialplan
dialplan.impossibleMatchHandling="2"	Forces the phone to wait for the user to press the send key before delivering digits to the reg.1.server

9. Verification Steps

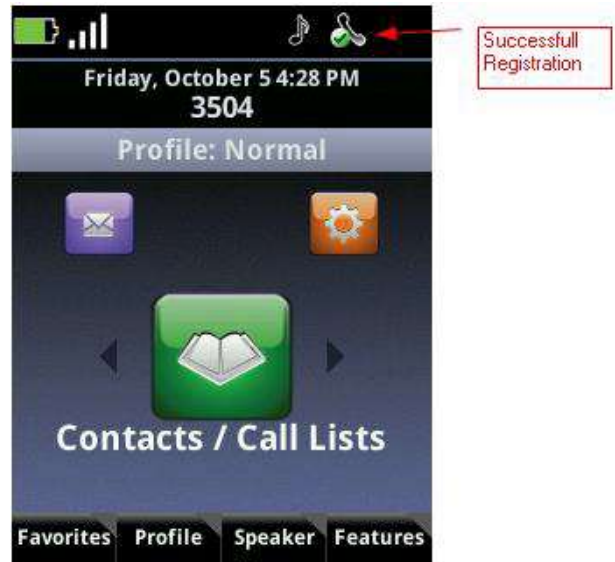
The following steps may be used to verify the configuration:

9.1. Verify the Configuration files are received by the handset

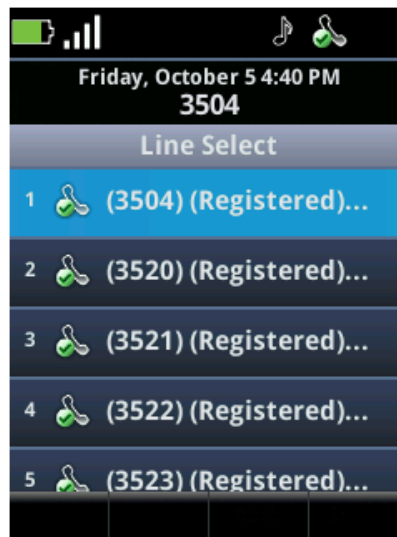
- 1 On the Handset, Navigate to **Settings > Status > Platform > Configuration**.
The configuration screen displays the IP address of the FTP server, the provisioning protocol being used, the .cfg files it is using, and detailed information about the number of parameters accepted from each configuration file, any duplicate parameters, and any errors.
- 2 Ensure that any errors or unintended duplicate parameters are corrected. Also ensure that the number of parameters accepted from each file aligns with the number of parameters expected.

9.2. Verify the handset is registered

- 1 Verify Registration Status on the handset by checking to see if the Spectralink 84-Series has successfully registered all configured line appearances.
- 2 Look in the upper right hand corner of the idle screen for the green checkmark. This indicates the handset believes it has successfully registered all lines:



You can also see the status of each individual line registered (useful for multi-line handsets) by Navigating to **Settings > Status > Lines**.



- Verify that Spectralink 84-Series successfully registers with Session Manager by following the **Session Manager → System Status → User Registrations** link on the System Manager Web Interface.

9.3. Test the Solution

Once the device's registration has been confirmed, a basic functionality test should be performed:

- Place a call to and from the 84-Series handset to another Avaya device. While calls are established, enter **status trunk <t/r>** command, where **t** is the SIP trunk group configured, and **r** is trunk group member. This will verify whether the call is shuffled or not. If the call is shuffled, then the **Audio Connection Type** field shows “ip-direct”. Otherwise, the call is not shuffled, by showing “ip-tdm”.
- Call Transfer the 84-Series handset to another device, and use the 84-Series handset to conduct a transfer.
- Perform a conference with the 84-Series handset, using the 84-Series handset as the conference initiator and test using the 84-Series handset as a conference participant
- Hold and resume a call.
- Leave a voicemail for the 84-Series handset (if equipped) – Ensure message Waiting Indication is delivered. Call the voicemail system from the 84-Series handset and retrieve the call.
- Place a call to a PSTN number equipped with a menu system and verify the functionality of DTMF tones to navigate the menus.
- Verify other any other functionality of interest.

10. Conclusion

Spectralink 84-Series was compliance tested with Communication Manager (Version 6.3) and Session Manager (Version 6.3). Spectralink 84-Series (UCS 4.11.0.2041) functioned properly for feature and serviceability. During compliance testing, Spectralink 84-Series successfully registered with Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like three-way conference, transfers, hold, etc. The phones are able to failover and back between primary and secondary Session Managers as well as recover from various outages such as DNS, wireless network, and Communication Manager failures.

11. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, August 2015, Release 6.3, Document Number 03-300509.
- [2] *Administering Avaya® Session Manager*, September 2014, Release 6.3.
- [3] *Administering Avaya® System Manager*, July 2015, Release 6.3.13.
- [4] *Application Notes for Spectralink 84-Series Wireless Telephones and Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0*

Spectralink product documentation is available at <http://support.Spectralink.com>. Spectralink has provided the following references:

- [5] *Spectralink 84-Series SLIC Administration Guide* - The SLIC tool provides step-by-step instructions for configuring wireless settings required for the handsets to associate with the wireless LAN.

- [6] *Spectralink 84-Series Wireless Telephone Deployment Guide* - The Deployment Guide provides sequential information for provisioning and deploying the handsets. It covers deployment using the SLIC tool as well as manual deployment.
- [7] *Spectralink 84-Series Wireless Telephone Administration Guide* - The Admin Guide is a companion guide to the Deployment Guide. It provides detailed information about settings and options available to the administrator through configuration files and through the handsets. Time-saving shortcuts, troubleshooting tips and other important maintenance instructions are also found in this document.
- [8] *Spectralink 84-Series Wireless Telephone User Guide* - The User Guide provides detailed information about using the features of the 84-Series handsets.
- [9] *Spectralink 84-Series Wireless Telephones Web Developer's Guide* - The Web Developer's Guide provides Web application creators with information for developing and deploying Web applications that interface with Spectralink handsets.
- [10] http://support.spectralink.com/sites/default/files/resource_files/1725-86991-000_A.pdf

12. Appendix A – Extension Configuration File (*<macaddress>-ext.cfg*) for User 61003 Used During Compliance Testing

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<handsetConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="handsetConfig.xsd">
<!-- ***** -->
<!-- * Sample per-phone Configuration File for FLAT DEPLOYMENTS * -->
<!-- * * -->
<!-- * This file contains the user-specific information for the user of a * -->
<!-- * specific handset identified by its MAC address. In particular it * -->
<!-- * contains the user name and extension for that user. * -->
<!-- * -->
<!-- * -->
<!-- * -->
<!-- * This file MUST be named as <macaddress>-ext.cfg where <macaddress> is the * -->
<!-- * 12 digit MAC address of the handset without : separators. The MAC * -->
<!-- * address is printed on the label in the battery well of each handset. * -->
<!-- * For example if the handset label reads MAC: 00:90:7A:0E:7F:E%, this file* -->
<!-- * should be named 00907a0e7fe5-ext.cfg * -
->
<!-- ***** -->

<LineRegistration>

    <!-- * -->
    <!-- * -->
    <!-- The information below is the user-specific information. The global server
settings are in -->
    <!-- the SystemParameters->TelephonyParameters->SIPserver -->
    <openSIPTelephony
        call.callsPerLineKey="24" >
        <TelephonyLine1
            reg.1.address="61003"
            reg.1.auth.password="123456"
            reg.1.auth.userID="61003"
            reg.1.label=""
            reg.1.displayName=""
            msg.mwi.1.subscribe="">
        </TelephonyLine1>
        <!-- Additional lines: -->
        <!-- * -->
        <!-- Additional telephony lines can be added (reg.3, etc...) by copying the
TelephonyLine1 group above and -->
        <!-- editing appropriately-->
    </openSIPTelephony>

</LineRegistration>

<qbc
    qbc.connect.ipAddress-hostname="">
    <!-- This is the IP address or hostname of the computer the phone should connect
to in single mode. -->
    <!-- See the QBC Admin Guide for detailed information. -->
</qbc>

</handsetConfig>
```

13. Appendix B – Site Configuration file (site.cfg) Used During Compliance Testing

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<handsetConfig xsi:noNamespaceSchemaLocation="handsetConfig.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <!--*****-->
  <!--site.cfg template for FLAT DEPLOYMENT-->
  <!--*****-->
  <!--Site Parameters configured in this file apply to all phones.-->
  <!--*****-->
  <!--Only those parameters that apply to ALL phones should be in this file.-->
  <!--DELETE THOSE PARAMETERS THAT YOU DO NOT DEPLOY.-->
  <!--DO NOT deploy duplicate parameters.-->
  <!--*****-->
  <!--System Parameters are network parameters that all phones use.-->
  <!--*****-->
  <SystemParameters>
    <!--Unless otherwise specified, all values are recommended settings and do not
need to be changed.-->
    <log
      log.render.file.upload.period="7200"
      log.render.file.size="180"
      log.render.file.upload.append="1"
      log.render.file.upload.append.sizeLimit="65535"
      log.render.level="0"
      log.render.stdout="0"
      log.level.change.wlan="2"
      log.level.change.sip="0"
      log.level.change.app1="1" />
    <!--The syslog server name can be an IP address or fqdn (fully qualified domain
name)-->
    <prov.polling
      prov.polling.enabled="1"
      prov.polling.mode="abs"
      prov.polling.period="86400"
      prov.polling.time="03:00"
      prov.polling.timeRandomEnd="">
    </prov.polling>
    <syslog
      device.set="1"
      device.syslog.serverName="mysyslogserver.domain.com"
      device.syslog.serverName.set="1"
      device.syslog.renderLevel="3"
      device.syslog.renderLevel.set="1" />
  </SystemParameters>
  <!--*****-->
  <!--Telephony Parameters are those that are dependent on the Call Server.-->
  <!-- * -->
  <!-- * -->
  <!--*****-->
  <TelephonyParameters>
    <!-- * -->
    <!-- * -->
    <!-- * -->
    <!-- * -->
    <!-- * -->
    <!-- * -->
    <!-- * -->
    <!-- * -->
```

```

        <!-- device.set="1" only needed if previous device.set in syslog is not used -
->
        <!-- * -->
<openSIP>
  <SIPserver
    reg.1.server.1.address="d4f27.com"
    reg.1.server.1.transport="TCPOnly"
    reg.1.server.1.expires="120"
    voIpProt.server.1.failOver.reRegisterOn="1"
    voIpProt.server.1.failOver.failRegistrationOn="1"
    voIpProt.server.1.failOver.failBack.mode="duration"
    voIpProt.server.1.failOver.failBack.timeout="120"
    voIpProt.SIP.failoverOn503Response="1"
    dns.cache.SRV.1.name="_sip._tcp.d4f27.com"
    dns.cache.SRV.1.ttl= "300"
    dns.cache.SRV.1.priority="1"
    dns.cache.SRV.1.weight="1"
    dns.cache.SRV.1.port="5060"
    dns.cache.SRV.1.target="sm5031.d4f27.com"
    dns.cache.A.1.name="sm5031.d4f27.com"
    dns.cache.A.1.ttl="300"
    dns.cache.A.1.address="10.64.50.31"
    dns.cache.SRV.2.name="_sip._tcp.d4f27.com"
    dns.cache.SRV.2.ttl= "300"
    dns.cache.SRV.2.priority="2"
    dns.cache.SRV.2.weight="1"
    dns.cache.SRV.2.port="5060"
    dns.cache.SRV.2.target="sm10262.d4f27.com"
    dns.cache.A.2.name="sm10262.d4f27.com"
    dns.cache.A.2.ttl="300"
    dns.cache.A.2.address="10.64.102.62"
  />

  <dialplan
    dialplan.impossibleMatchHandling="2"
    dialplan.digitmap="" />
  <DND_CallForwarding
    voIpProt.SIP.serverFeatureControl.dnd="0"
    voIpProt.SIP.serverFeatureControl.cf="0"
    voIpProt.SIP.use486forReject="1"
  >
</DND_CallForwarding>
<voicemail
  up.oneTouchVoicemail="1"
  up.mwiVisible="1"
  msg.mwi.1.callBackMode="contact"
  msg.mwi.1.callBack="69999">
</voicemail>
</openSIP>
</TelephonyParameters>
</handsetConfig>

```

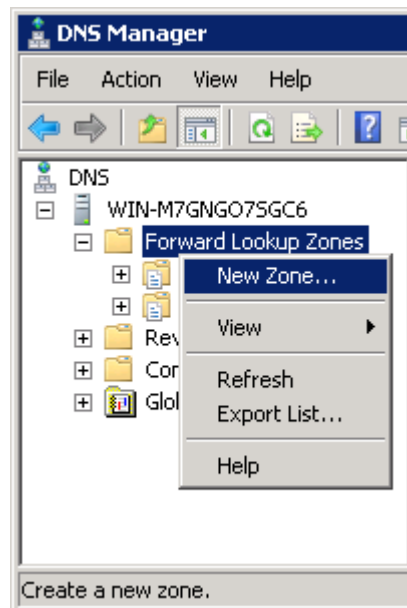
14. Appendix C – Creating a DNS SRV Record on a Windows Server

While a Windows 2008 Server was used during compliance testing, the steps for a Windows 2003 Server would be very similar. There are many different settings and options that can be set in a DNS server as a new SRV record is created that corresponds with the SIP Domain name. It is also possible that the DNS Forward Lookup Zone defined for the SIP Domain may already be defined. The information below provides an example of creating a new SIP Domain (Forward Lookup Zone) in the DNS server from scratch, but if the Domain already exists, skip past the step where the original SIP Domain is created and follow the rest of the steps in sequence.

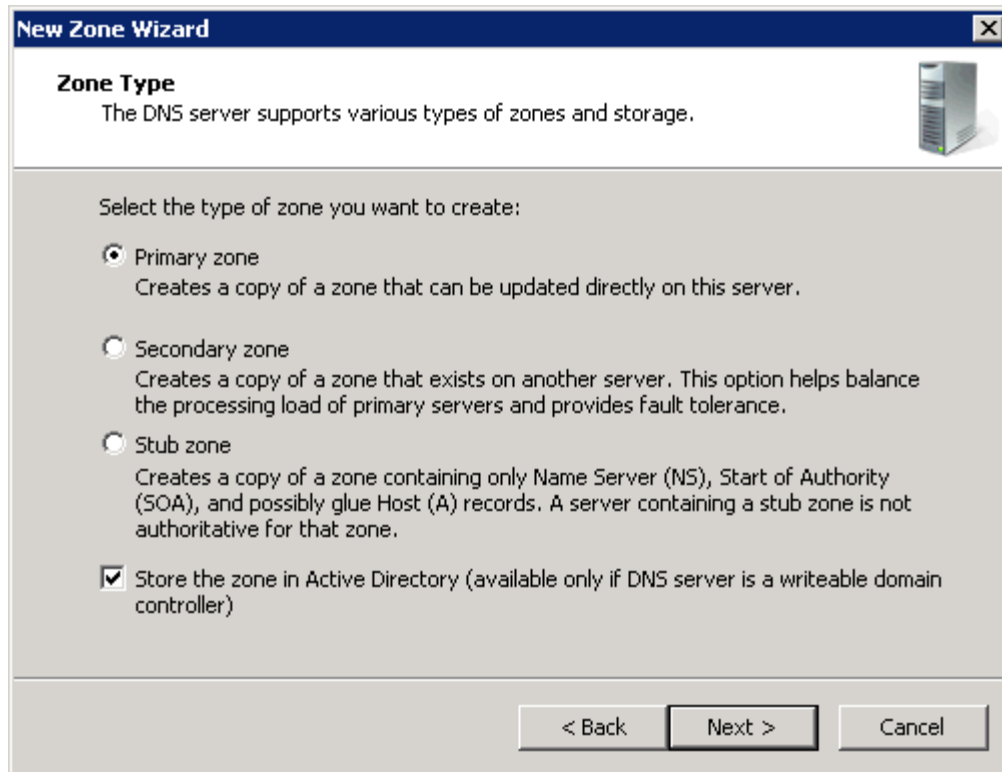
On the DNS Server, navigate to the Forward Lookup Zones and look for a Zone with the name of your SIP Domain, if it already exists, skip down to the “Create DNS A Name Records for the Avaya Aura® Session Managers” section of this document. Otherwise follow the steps below to create a new Forward lookup zone using the SIP Domain name:

Create a New Forward Lookup Zone using the SIP Domain Name (or Verify a Zone Exists with the SIP Domain name)

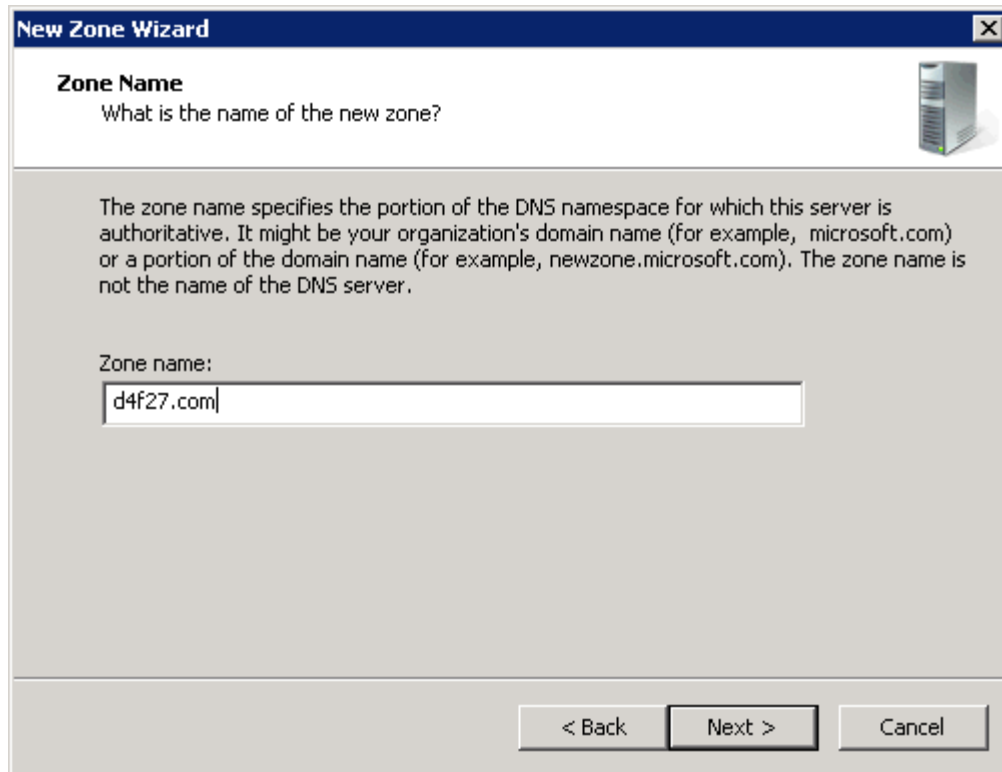
1. Right click on the **Forward Lookup Zones** field, and select **New Zone**



2. Select **Next** at the **Welcome to the New Zone Wizard** page
3. In this example, a **Primary Zone** was chosen. Selected Next, and also selected Next on the following page, using the default of: **To all DNS servers running on domain controllers in this domain:d4f27.com.**



4. In the **Zone Name** field, type the name of the domain (e.g., **d4f27.com**), and then select **Next** again:



New Zone Wizard

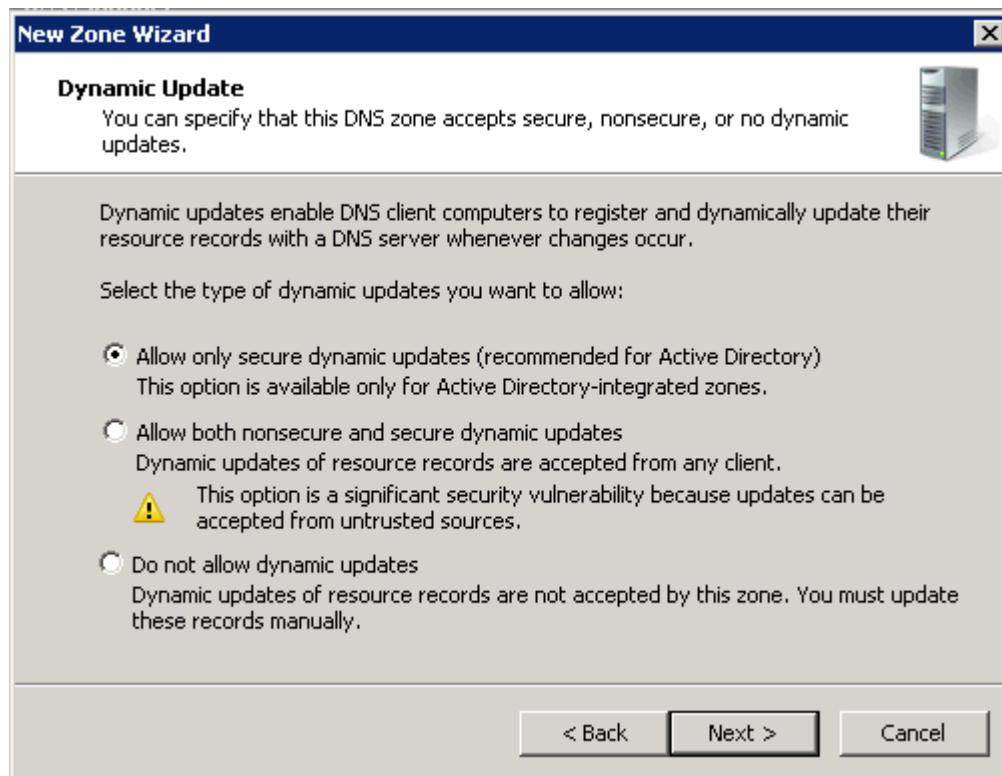
Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

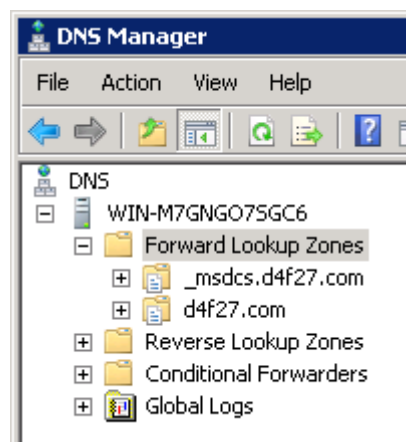
Zone name:
d4f27.com

< Back Next > Cancel

5. On the **Dynamic Update** page, select the option that is in accordance with the local policy. Then select **Next** again, and finally, select **Finish**.



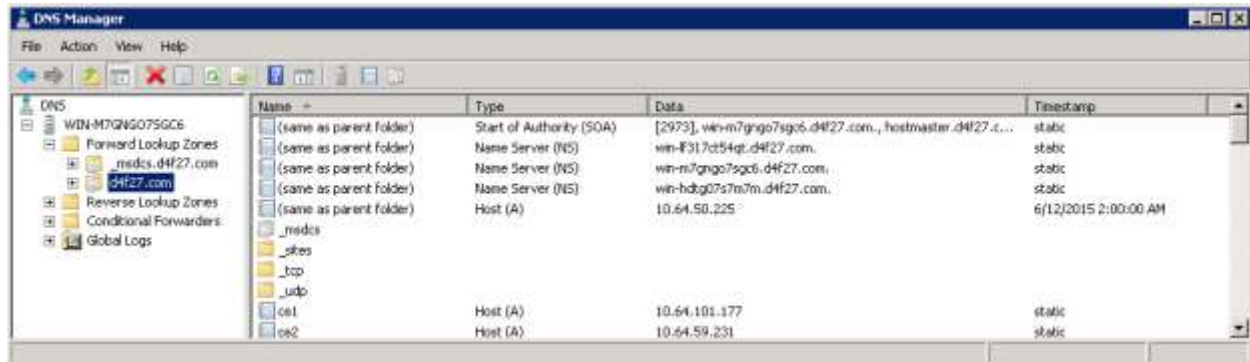
6. Now, verify the domain name just created (i.e. **d4f27.com**) appears a Forward Lookup Zone:



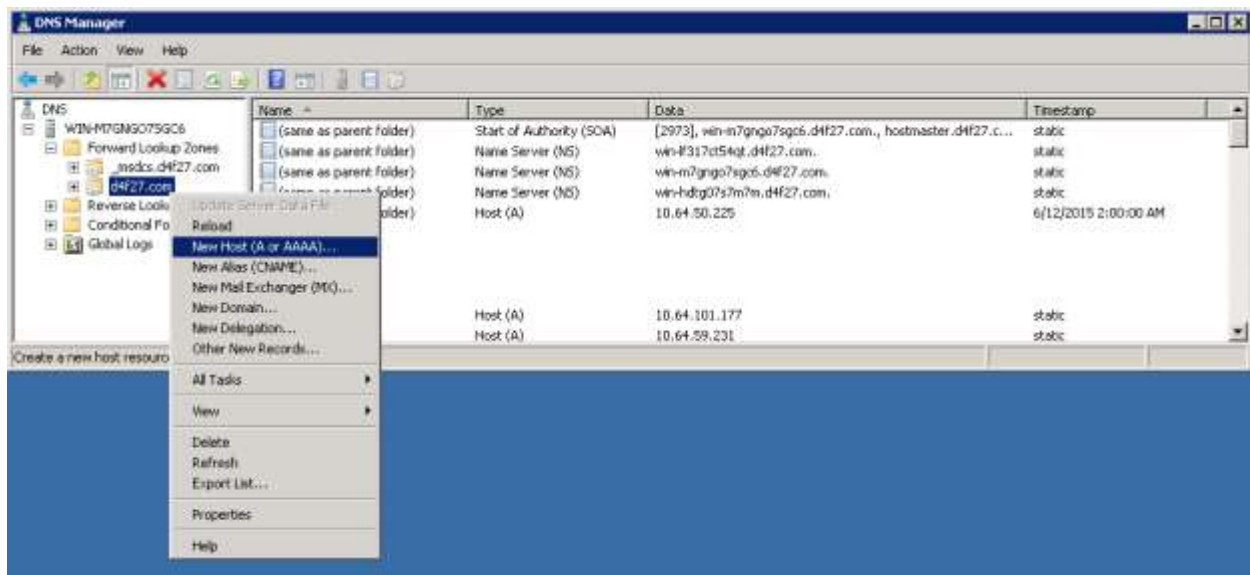
Create DNS A Name Records for the Avaya Aura® Session Managers (or Verify the A name records already exists for the Session Managers)

On the DNS Server, navigate to the Forward Lookup Zone that corresponds to the SIP Domain and highlight it. Now look for A name records that correspond to the primary and secondary Session Managers the phones will point to. If the host A Name records already exists, skip down to the “Create a SRV records for the Avaya Aura® Session Managers” section of this Appendix.

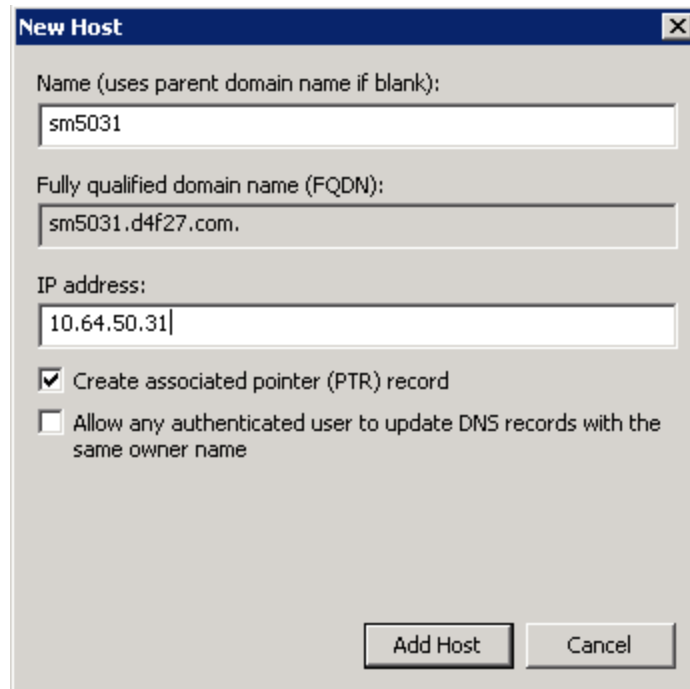
Otherwise follow the steps below to create a new DNS A name record for the primary Session Manager.



1. Right click on the Forward Lookup Zone just created and select **New Host (A or AAAA)...**

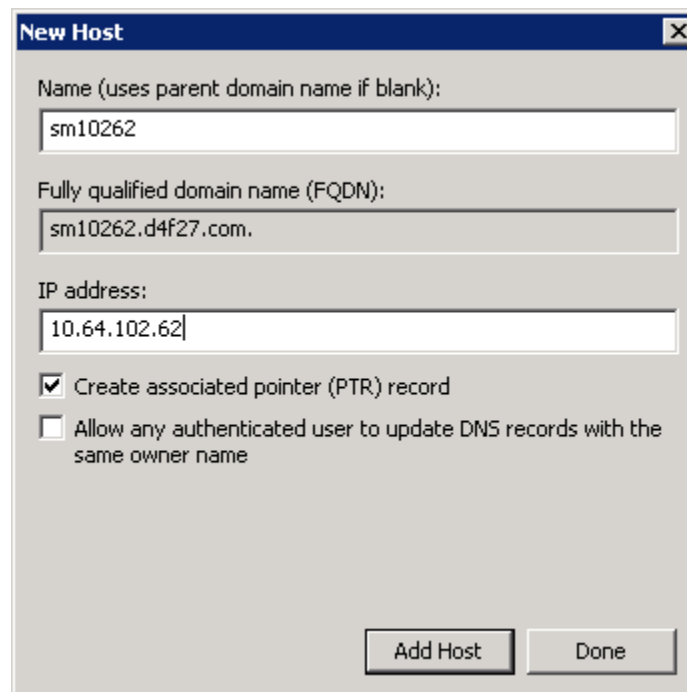


2. Now enter the primary Session Manager's name in the **Name** field. It can be named anything that would help to identify it as the primary Session Manager. This record is used to resolve the primary Session Manager's IP Address. For this example, **sm5031** is used. The Session Manager's IP address must also be provided. This is the signaling address that SIP REGISTRATIONS and INVITES should be directed to. Then select **Add Host**.

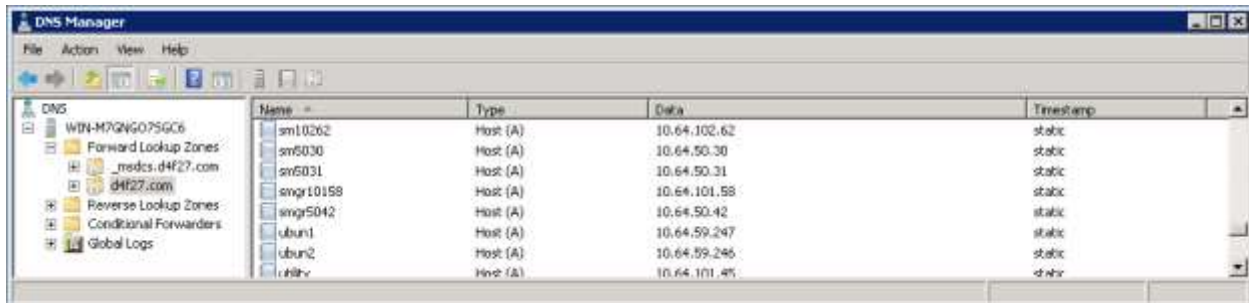
A screenshot of a 'New Host' dialog box. It has a title bar with 'New Host' and a close button. The dialog contains three text input fields: 'Name (uses parent domain name if blank):' with 'sm5031', 'Fully qualified domain name (FQDN):' with 'sm5031.d4f27.com.', and 'IP address:' with '10.64.50.31'. Below these fields are two checkboxes: 'Create associated pointer (PTR) record' which is checked, and 'Allow any authenticated user to update DNS records with the same owner name' which is unchecked. At the bottom right are two buttons: 'Add Host' and 'Cancel'.

Note: If there is an error message about the associated PTR record NOT being created, it simply means the reverse lookup zone is not specified. If the customer is not familiar with how to resolve this error or is not concerned about it, it can be safely ignored.

Now repeat this step to create the secondary Session Manager's A name Host record.

A screenshot of a 'New Host' dialog box, similar to the one above but with different values. The title bar says 'New Host'. The 'Name' field contains 'sm10262', the 'Fully qualified domain name (FQDN)' field contains 'sm10262.d4f27.com.', and the 'IP address' field contains '10.64.102.62'. The 'Create associated pointer (PTR) record' checkbox is checked, and the 'Allow any authenticated user to update DNS records with the same owner name' checkbox is unchecked. At the bottom right are two buttons: 'Add Host' and 'Done'.

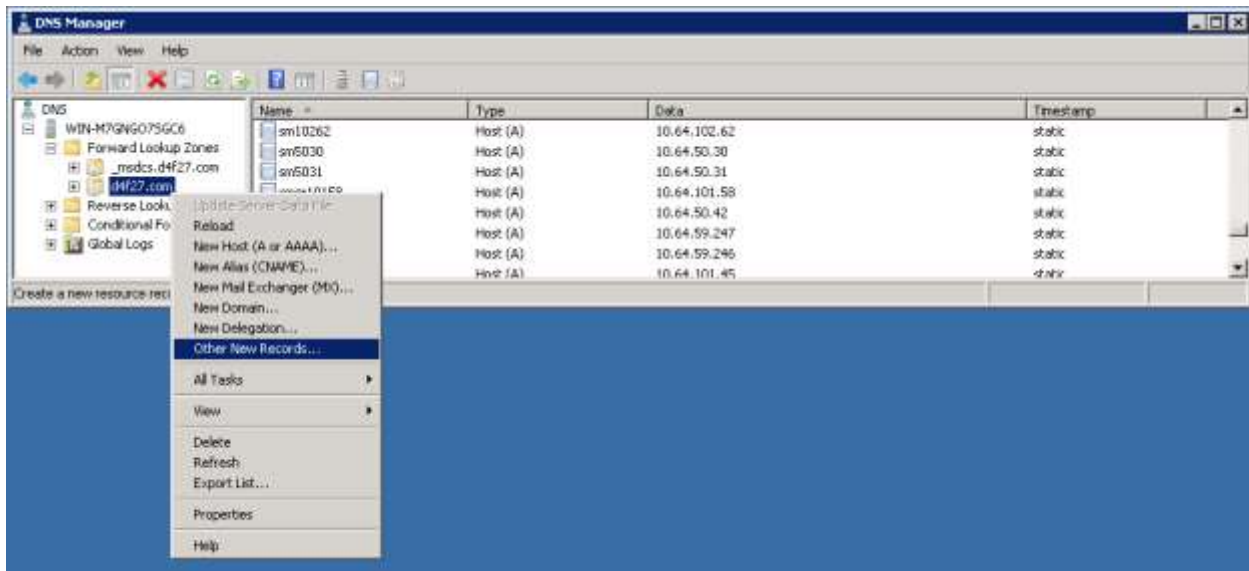
3. Select **Done** to finish creating the A name Host records. Verify the A name records appear linking each Session Manager's name to its IP address:



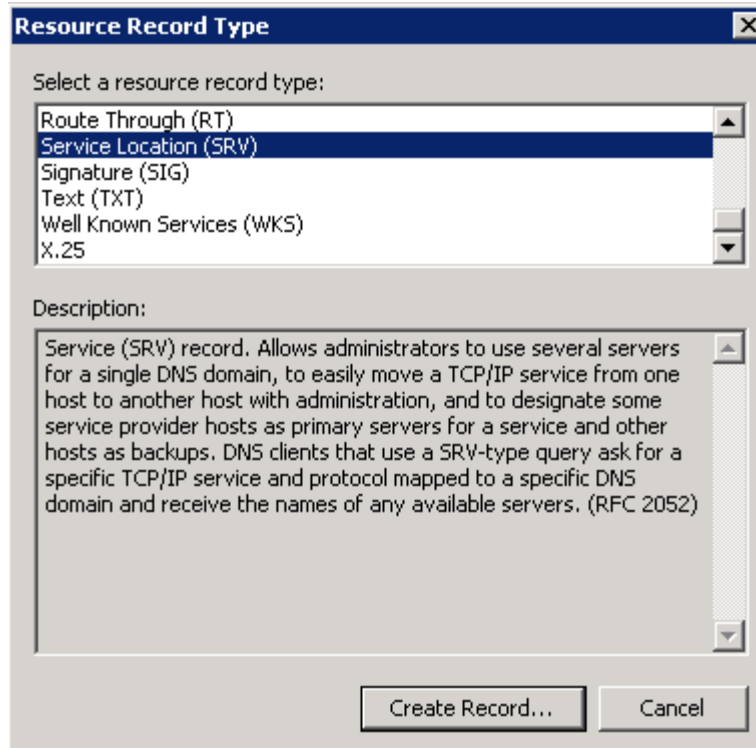
Name	Type	Data	Timestamp
sm10262	Host (A)	10.64.102.62	static
sm5030	Host (A)	10.64.50.30	static
sm5031	Host (A)	10.64.50.31	static
smgr10158	Host (A)	10.64.101.58	static
smgr5042	Host (A)	10.64.50.42	static
ubunt1	Host (A)	10.64.59.247	static
ubunt2	Host (A)	10.64.59.246	static
ubuntv	Host (A)	10.64.101.45	static

Create SRV Records for the Avaya Aura® Session Managers

1. Right click on the forward lookup zone created that corresponds to the SIP Domain and select **Other New Records**.



2. In the resource record type window, scroll down to the **Service Location (SRV)** field and highlight it, then select **Create Record**.



In the **New Resource Record** window, a record will be created that will point to the primary Session Manager, **sm5031.d4f27.com**, and program it to use the tcp protocol on port 5060. To do so, modify the following fields:

Service: **_sip**

Protocol: **_tcp**

Priority: **1** (This server have the highest priority in the phone's list)

Port Number: **5060**

Host Offering This Service: **sm5031.d4f27.com**.

New Resource Record

Service Location (SRV)

Domain: d4f27.com

Service: _sip

Protocol: _tcp

Priority: 1

Weight: 0

Port number: 5060

Host offering this service:
sm5031.d4f7.com.

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

Select **OK** and then **Create Record** again to create similar record for the secondary Session Manager. Note the Priority of 2 which means this server will have the second highest priority on the phone's list. Select **OK**.

New Resource Record

Service Location (SRV)

Domain: d4f27.com

Service: _sip

Protocol: _tcp

Priority: 2

Weight: 0

Port number: 5060

Host offering this service:
sm10262.d4f27.com.

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

3. Select **Done** to close the Resource Record Type window that remains. Verify SRV records exist that point to each Session Manager's name using port 5060 in the Forward Lookup Zone that corresponds to the SIP Domain.

DNS Manager

File Action View Help

DNS

- WIN-M7GNGO75GC6
 - Forward Lookup Zones
 - _msdcs.d4f27.com
 - _msdcs
 - _lites
 - _ldap
 - DomainDnsZones
 - ForestDnsZones
 - Reverse Lookup Zones
 - Conditional Forwarders
 - Global Logs

| Name | Type | Data | Timestamp |
|-----------|------------------------|---|-----------------------|
| _gc | Service Location (SRV) | [0][100][3268] win-m7gngo7sgc6.d4f27.com. | 7/23/2015 2:00:00 PM |
| _gc | Service Location (SRV) | [0][100][3268] win-f317ct54qt.d4f27.com. | 9/17/2014 8:00:00 PM |
| _kerberos | Service Location (SRV) | [0][100][88] win-m7gngo7sgc6.d4f27.com. | 5/20/2013 10:00:00 AM |
| _kerberos | Service Location (SRV) | [0][100][88] win-f317ct54qt.d4f27.com. | 5/21/2013 11:00:00 AM |
| _lites | Service Location (SRV) | [0][100][464] win-m7gngo7sgc6.d4f27.com. | 5/20/2013 10:00:00 AM |
| _lites | Service Location (SRV) | [0][100][464] win-f317ct54qt.d4f27.com. | 5/21/2013 11:00:00 AM |
| _ldap | Service Location (SRV) | [0][100][389] win-m7gngo7sgc6.d4f27.com. | 5/20/2013 10:00:00 AM |
| _ldap | Service Location (SRV) | [0][100][389] win-f317ct54qt.d4f27.com. | 5/21/2013 11:00:00 AM |
| _sip | Service Location (SRV) | [2][0][5060] sm10262.d4f27.com. | static |
| _sip | Service Location (SRV) | [1][0][5060] sm5031.d4f27.com. | static |

DNS Verification and Troubleshooting

After the SRV records and A name records on the DNS server have been built, ensure they can be queried. A regular Windows machine can be used, but it must be pointed to the DNS server (or have access to the DNS Server) where the records were created.

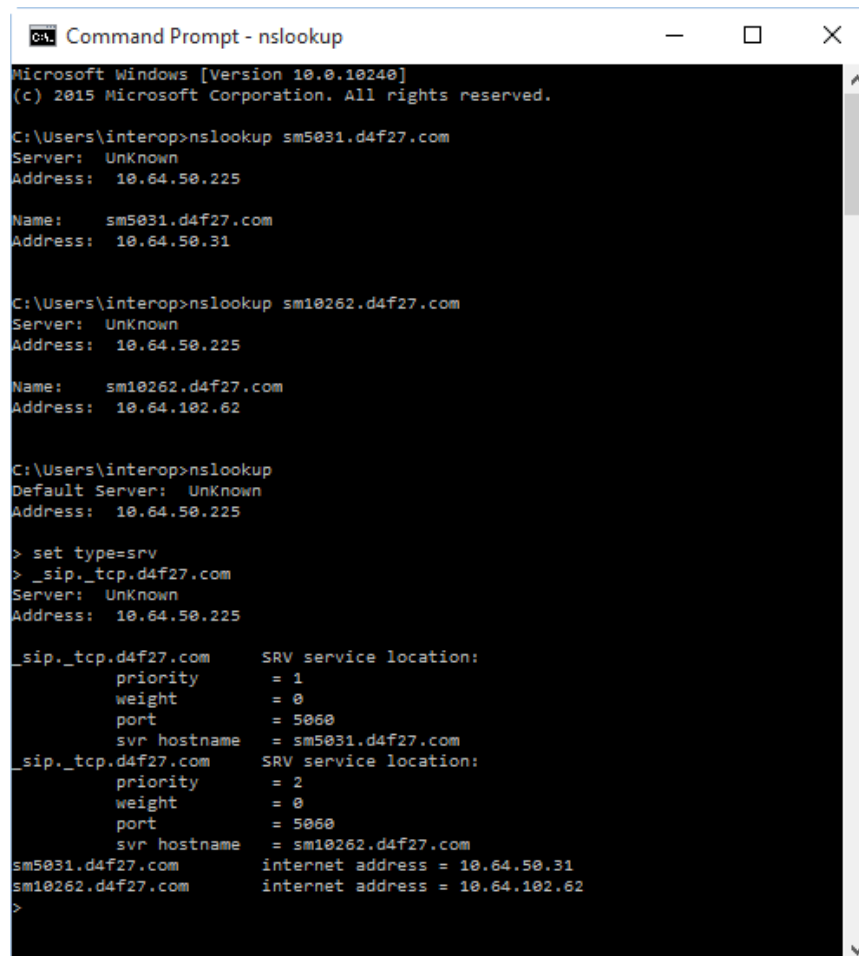
To Verify the A Record for the two Session Managers (**sm5031.d4f27.com** and **sm10262.d4f27.com**), from a Command Prompt:

1. type: **nslookup sm5031.d4f27.com**
2. type: **nslookup sm10262.d4f27.com**

To Verify the SRV record for d4f27.com, from a Command Prompt:

1. type: **nslookup** and press **return**
2. type: **set type=srv**
3. type: **_sip._tcp.d4f27.com**

The Output from the above tests should similar to the results shown below. If not, the phone won't work either:



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\interop>nslookup sm5031.d4f27.com
Server: UnKnown
Address: 10.64.50.225

Name:      sm5031.d4f27.com
Address: 10.64.50.31

C:\Users\interop>nslookup sm10262.d4f27.com
Server: UnKnown
Address: 10.64.50.225

Name:      sm10262.d4f27.com
Address: 10.64.102.62

C:\Users\interop>nslookup
Default Server: UnKnown
Address: 10.64.50.225

> set type=srv
> _sip._tcp.d4f27.com
Server: UnKnown
Address: 10.64.50.225

_sip._tcp.d4f27.com    SRV service location:
      priority         = 1
      weight           = 0
      port             = 5060
      svr hostname     = sm5031.d4f27.com
_sip._tcp.d4f27.com    SRV service location:
      priority         = 2
      weight           = 0
      port             = 5060
      svr hostname     = sm10262.d4f27.com
sm5031.d4f27.com       internet address = 10.64.50.31
sm10262.d4f27.com     internet address = 10.64.102.62
>
```

©2015 Avaya Inc. All Rights Reserved.

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

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