Application Notes for RedSky Technologies E911 Manager with Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of Avaya Aura® Session Manager and the RedSky E911 Manager.

RedSky E911 Manager provides an emergency numbering and location information solution for endpoints registered with Avaya Aura® Session Manager.

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 a compliance-tested configuration consisting of Avaya Aura® Session Manager and RedSky E911 Manager.

The purpose of RedSky E911 is to provide or update emergency numbering and location information for endpoints registered with Session Manager. When a Public Safety Answering Point (PSAP) receives a 911 call, the PSAP searches an Automatic Location Identifier (ALI) database to obtain the specific address/location associated with the Auto Number Identification (ANI) or the Emergency Location Identification Number (ELIN). ELINs are used to more precisely define the location of a device based on where the device is actually being used, rather than a static location that is generally associated with an ANI of an endpoint or trunk.

Session Manager offers a unique interface to ELIN servers, enabling an enterprise to manage emergency location information for users who register SIP endpoints. Though static definitions of emergency location information have been, and continue to be offered through the Avaya platforms, dynamic ELIN information permits enterprise users to register a SIP endpoint in alternate locations such as meeting rooms, and for the emergency location information to be updated to reflect the current location of the user should the endpoint need to place an emergency call.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between RedSky E911 Manager and Avaya Aura® Session Manager. Although other elements were present such as SIP Endpoints and Avaya Aura® Communication Manager, the configuration of these elements was not directly related to the interoperability of the tested solution and is therefore not covered in these notes.

The ALI database update function was not included in this compliance test. The compliance testing focused on verifying the internal generation of the ELIN information and not on the transfer of records to ALI databases.

2.1. Interoperability Compliance Testing

RedSky receives registration information from Session Manager when a SIP Entity Link is established, and when endpoints register with Session Manager. The registration information Session Manager provides contains the network address of the endpoint. RedSky compares this address to administered IP Address ranges and returns the ELIN associated with the current location of the endpoint. Session Manager uses the ELIN information obtained from RedSky in place of any it has associated with the device and stores this in the registration data for the endpoint. Should a 911 call be placed, the ELIN information stored in Session Manager would be included in the header of the invite sent to the far end of the Entity Link configured for handling emergency calls, this function is independent of the RedSky server meaning that in a worst case scenario, once ELIN information were provided to Session Manager, the RedSky server could be unreachable and the proper ELIN information would be sent.

Session Manager support for emergency calling is broader than the 911 service used in North America. Specifics and availability of products and capabilities beyond those used in North America are not covered in these Application Notes. More details can be obtained by consulting with RedSky, or the providers of emergency location solution offered in these other locations.

In addition to the sunny day scenarios described above, testing included disconnecting network cables and restarting Entity Links, as well as restarting Session Manager and RedSky servers to verify recoverability of the solution.

2.2. Test Results

The objectives described in **Section 2.1** were verified. For serviceability testing, the RedSky E911 Manager was able to supply station emergency numbering information to Session Manager after connection to the server was disconnected and reconnected, as well as after resets of Avaya Communication Manager, Session Manager and the RedSky E911 Manager server.

2.3. Support

Technical support for RedSky E911 Manager and other RedSky offers can be obtained at:

- Phone: (866) 778-2435
- Email: support@redskytech.com
- http://www.redskye911.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager on S8300 Server
- Avaya G450 Media Gateway
- Avaya SIP telephones registered alternately on two separate subnets
- RedSky E911 Manager server

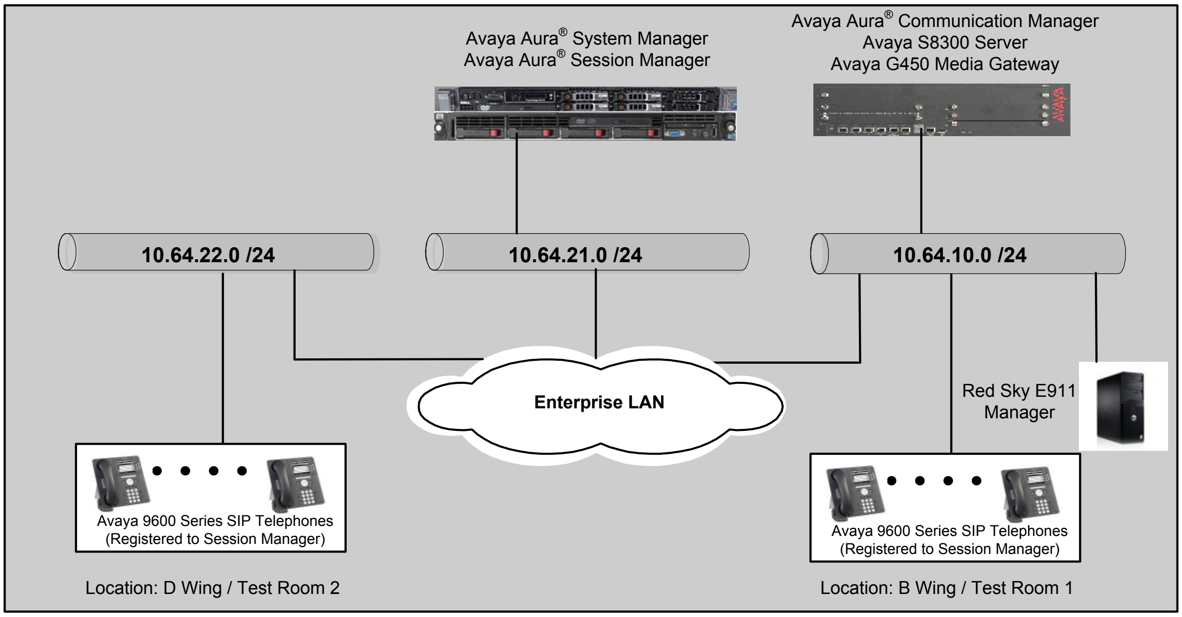

Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya Aura® Communication Manager
Avaya S8300 Server
Avaya G450 Media Gateway
10.64.22.0 /24
10.64.21.0 /24
10.64.10.0 /24
Enterprise LAN
Red Sky E911 Manager
Avaya 9600 Series SIP Telephones (Registered to Session Manager)
Avaya 9600 Series SIP Telephones (Registered to Session Manager)
Location: D Wing / Test Room 2
Location: B Wing / Test Room 1

Figure 1 – RedSky E911 Manager Configuration

4. Equipment and Software Validated

The following equipment and version were used for the sample configuration provided:

Equipment	Version
Avaya Aura® System Manager	6.1.0 (Build No. - 6.1.0.4.5072-6.1.4.11)
Avaya Aura® Session Manager	6.1.0 (Build No. - 6.1.0.0.610023)
Avaya Aura® Communication Manager - Avaya S8300D Server	6.0 (R016x.00.0.345.0 -18567)
Avaya G450 Media Gateway	30.14.0/1
Avaya 9600 Series SIP Phones	Avaya one-X® Deskphone Edition SIP 2.6
RedSky Technologies - E911 Manager	Version: 2.0 (20101216-0845 rev:9427)

5. Configure Avaya Aura® Communication Manager

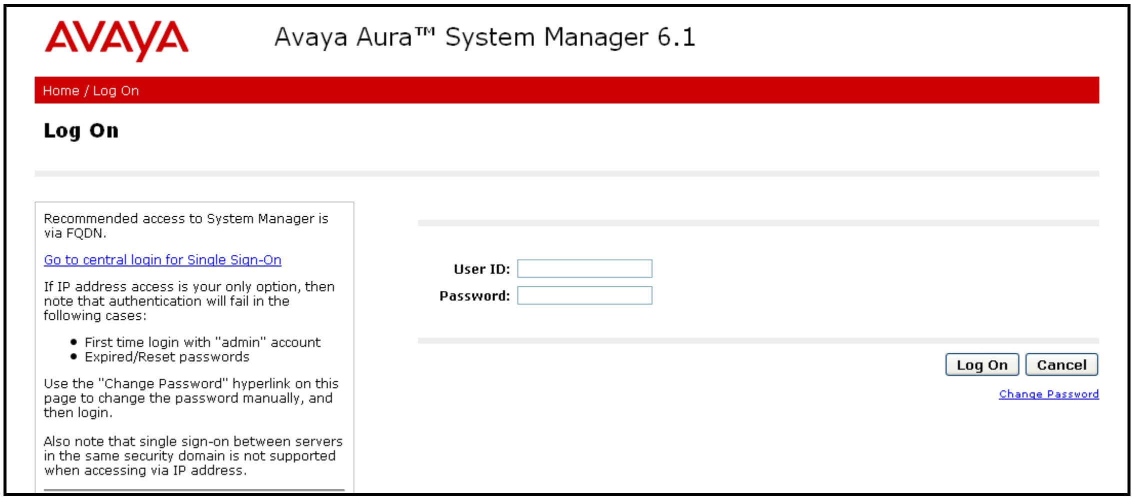
Communication Manager used an existing configuration with SIP trunks to connect to Avaya Aura® Session Manager. Configuration of this aspect of the integration was standard and not directly relevant to the interoperability of RedSky E911 Manager. These application notes will not cover this aspect of the configuration.

6. Configure Avaya Aura® Session Manager

This section provides the steps for configuring Session Manager to communicate with the RedSky E911 Manager. For more details, see the administration guide [1].

6.1. Session Manager Configuration Details

Session Manager is configured using browser access to System Manager. Enter the URL of System Manager such as https://<hostname>/network-login/SMGR where <hostname> is the ip address or qualified domain name of the System Manager. Login using appropriate credentials.



Avaya Aura™ System Manager 6.1

Home / Log On

Log On

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

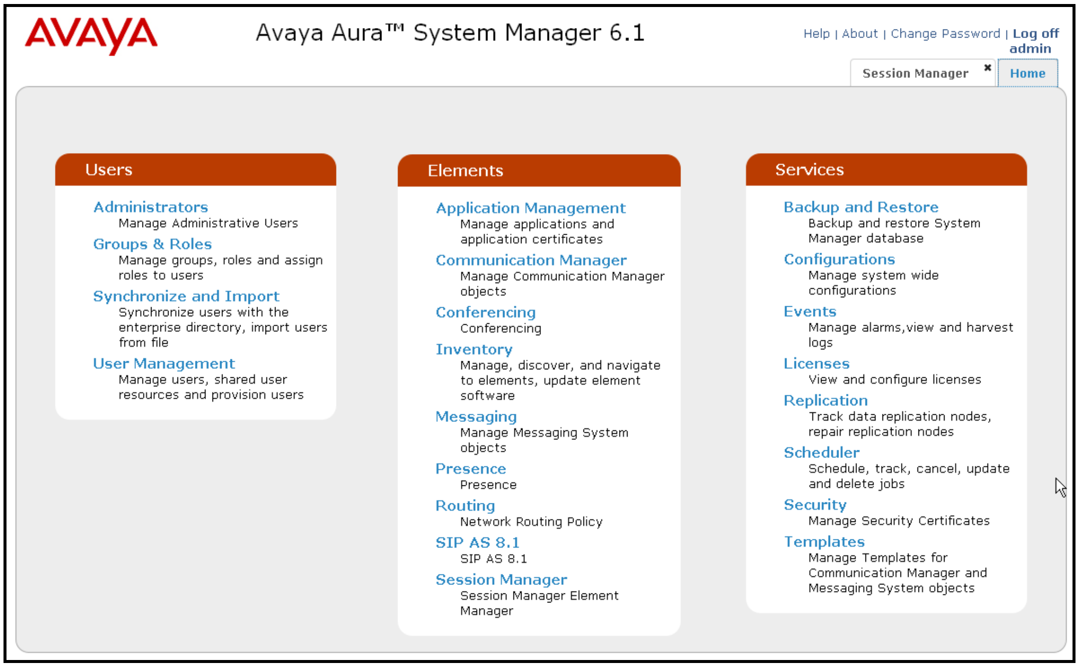
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

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

User ID:

Password:

The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment.


AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

SIP AS 8.1
SIP AS 8.1

Session Manager
Session Manager Element Manager

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

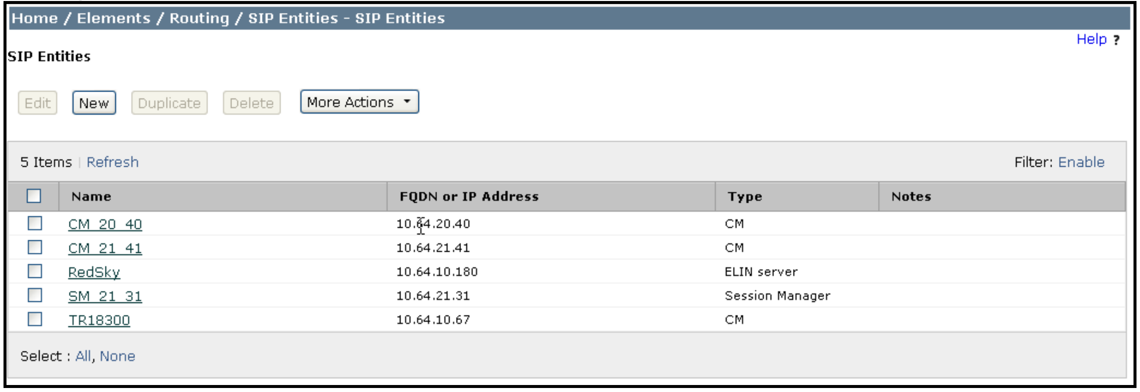
The steps required to enable RedSky E911 Manager to communicate with Session Manager are outlined as follows:

1. Create a SIP Entity and Entity Link
2. Associate the ELIN Server with the Session Manager
3. Configure Certificates for TLS - Import the RedSky Certificate
4. Configure Certificates for TLS - Export the Avaya (or Customer) Certificate

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

Create a SIP Entity and SIP Entity Link for the RedSky Server

Navigate to **Elements/Routing/SIP Entities** and click **New** to create an Entity definition. In the screenshot below, the Entity ***RedSky*** was previously created using the settings described below.



<table>
<tr><th>□</th><th>Name</th><th>FQDN or IP Address</th><th>Type</th><th>Notes</th></tr>
<tr><td>□</td><td>CM_20_40</td><td>10.64.20.40</td><td>CM</td><td></td></tr>
<tr><td>□</td><td>CM_21_41</td><td>10.64.21.41</td><td>CM</td><td></td></tr>
<tr><td>□</td><td>RedSky</td><td>10.64.10.180</td><td>ELIN server</td><td></td></tr>
<tr><td>□</td><td>SM_21_31</td><td>10.64.21.31</td><td>Session Manager</td><td></td></tr>
<tr><td>□</td><td>TR18300</td><td>10.64.10.67</td><td>CM</td><td></td></tr>
</table>

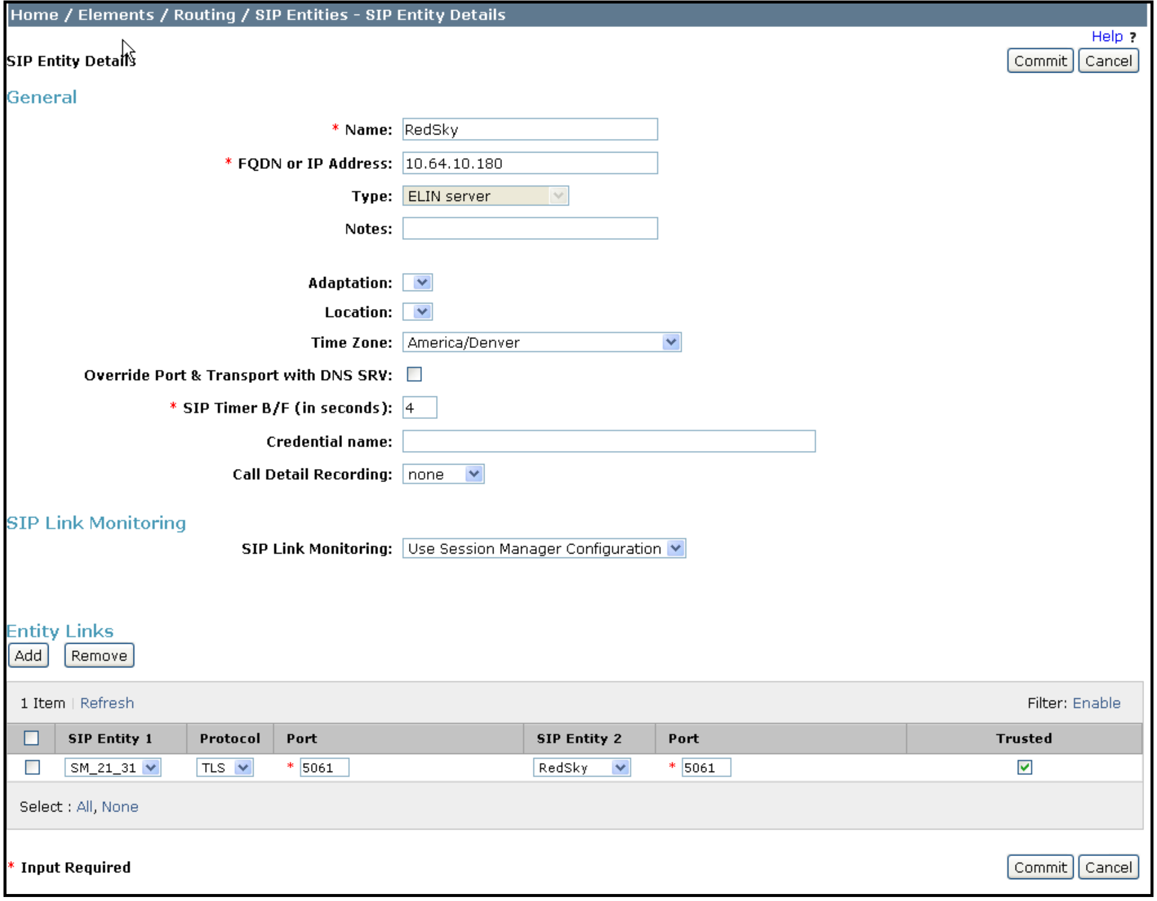
</td></tr>
</table>

Step	Description
	Create a SIP Entity and Entity Link for the RedSky Server (Continued)

Enter a descriptive **Name** such as ***RedSky*** and enter the **FQDN or IP Address** for the RedSky server as shown below. Select **ELIN server** for the Entity **Type**. All other settings in the General section were defaults. Click **Commit** to save the changes.

*Note, when deploying redundant RedSky servers, use the FQDN and create a host name resolution to the two IP Addresses using the **Elements/System Manager/Network Configuration/Local Host Name Resolution** form. The tested configuration was a single server, so this step is not covered in these application notes.*

Click **Add** under the **Entity Links** header to create an Entity link between Session Manager and RedSky. Select the Session Manger ***SM_21_31*** for **SIP Entity1**, and ***RedSky,*** (created above) for **SIP Entity 2**. For this test, ***TLS*** *was used for* the **Protocol** setting to secure the Entity Links, check the **Trusted** checkbox to create a trusted relationship. Click **Commit** to complete this step.


Home / Elements / Routing / SIP Entities - SIP Entity Details
Help ?
Commit
Cancel

SIP Entity Details

General

* Name: RedSky

* FQDN or IP Address: 10.64.10.180

Type: ELIN server

Notes:

Adaptation:

Location:

Time Zone: America/Denver

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

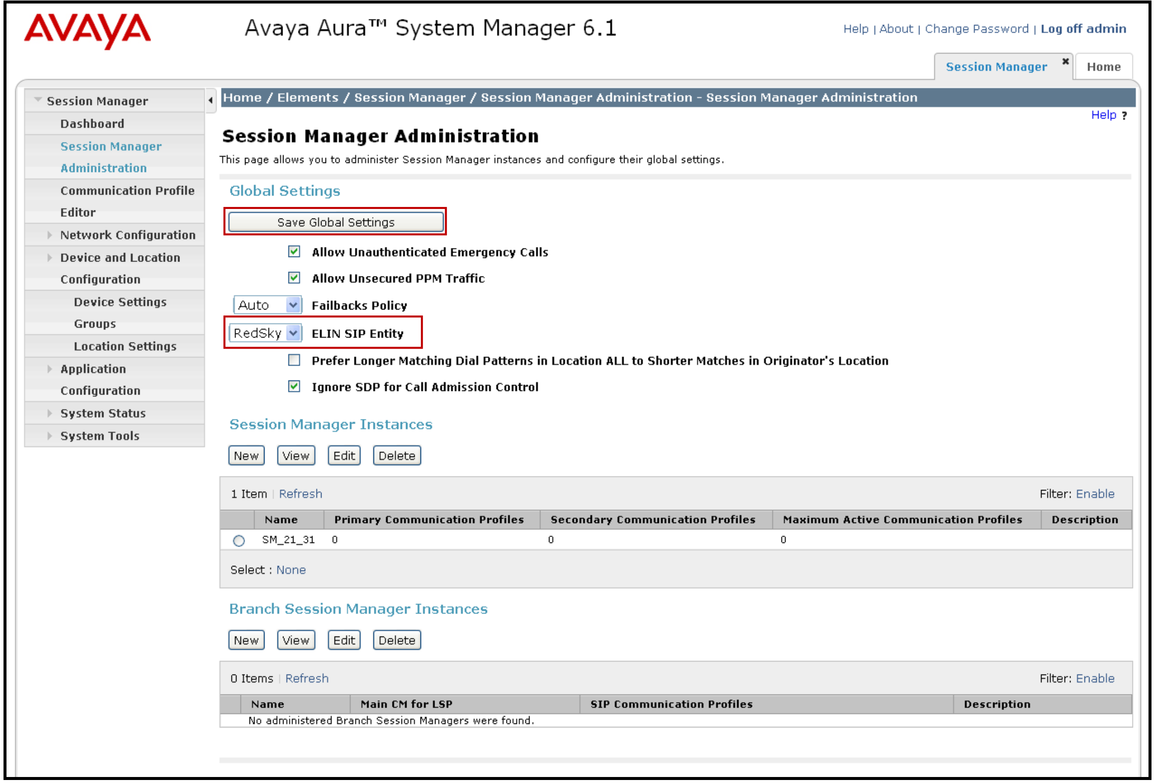
Entity Links

1 Item | Refresh   Filter: Enable

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	SM_21_31	TLS	* 5061	RedSky	* 5061	☑

Select : All, None

* Input Required

Step	Description
2.	**Associate the ELIN Server with the Session Manager** Session Manager treats ELIN server Entities uniquely, it is necessary to make an association with the ELIN server entity created above for the **ELIN SIP Entity** setting under **Session Manager Administration**, shown below. Click **Save Global Settings** to save this change. 

AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Device Settings
Groups
Location Settings
Application Configuration
System Status
System Tools
Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration
Help ?

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Global Settings

Save Global Settings

☑ Allow Unauthenticated Emergency Calls

☑ Allow Unsecured PPM Traffic

Auto Failbacks Policy

RedSky ELIN SIP Entity

□ Prefer Longer Matching Dial Patterns in Location ALL to Shorter Matches in Originator's Location

☑ Ignore SDP for Call Admission Control

Session Manager Instances

New View Edit Delete

1 Item | Refresh Filter: Enable

	Name	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
○	SM_21_31	0	0	0	

Select : None

Branch Session Manager Instances

New View Edit Delete

0 Items | Refresh Filter: Enable

Name	Main CM for LSP	SIP Communication Profiles	Description
No administered Branch Session Managers were found.			

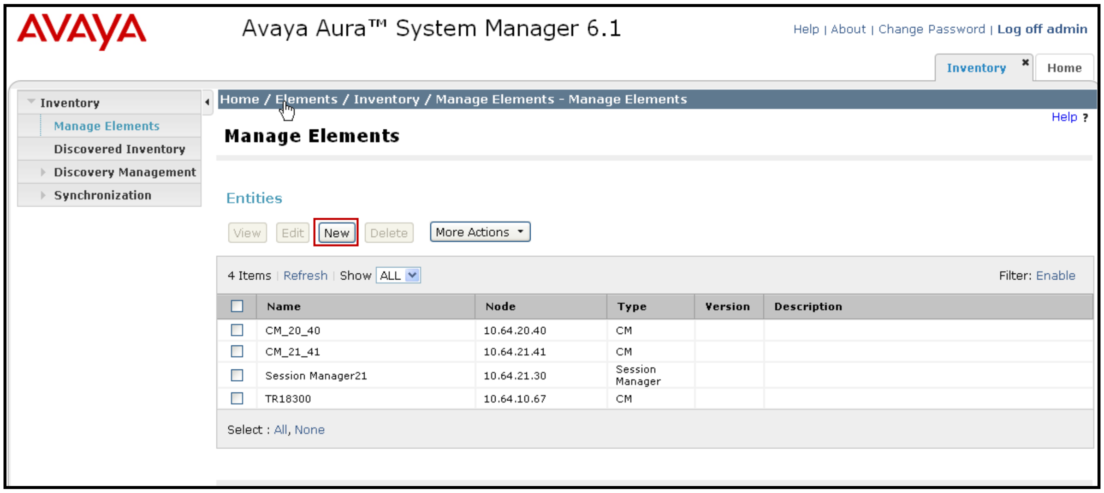
3.

Configure Certificates for TLS - Import the RedSky Certificate

In order for RedSky and Session Manager to use TLS to secure communications, a RedSky certificate must be installed on the Avaya equipment, and an Avaya (or Customer provided) certificate must be installed on the RedSky server.

Note: This step involves several subtasks which span several pages. The step is dependent on having completed the certificate export from the RedSky server described in Section 7.1 Step 1.

Navigate to **Inventory > Manage Elements** and click **New** (this step was previously completed, so Edit was used in the screenshots to demonstrate the settings)**:**



Manage Elements

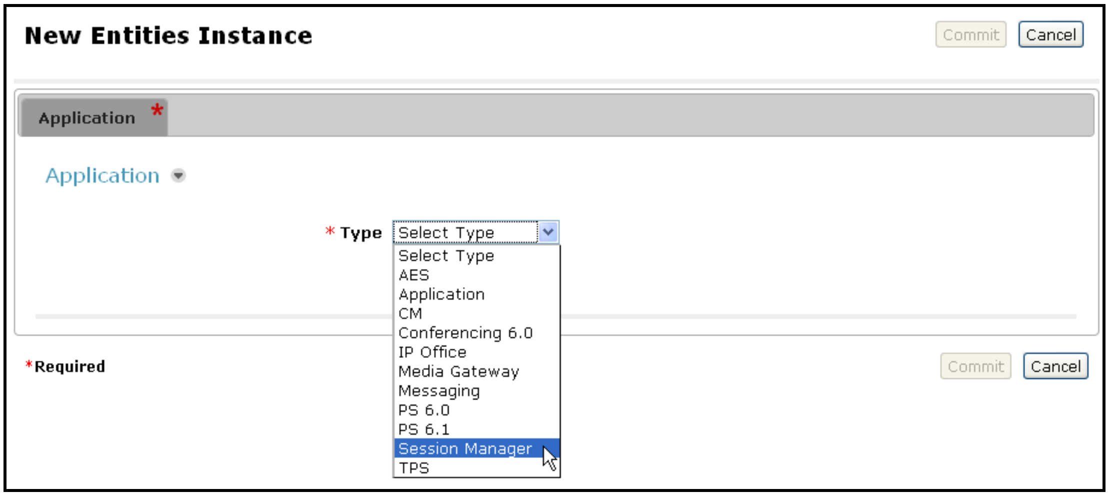
Entities

4 Items | Refresh | Show ALL

☐	Name	Node	Type	Version	Description
☐	CM_20_40	10.64.20.40	CM		
☐	CM_21_41	10.64.21.41	CM		
☐	Session Manager21	10.64.21.30	Session Manager		
☐	TR18300	10.64.10.67	CM		

Select : All, None

Select **Session Manager** for the **Type**:



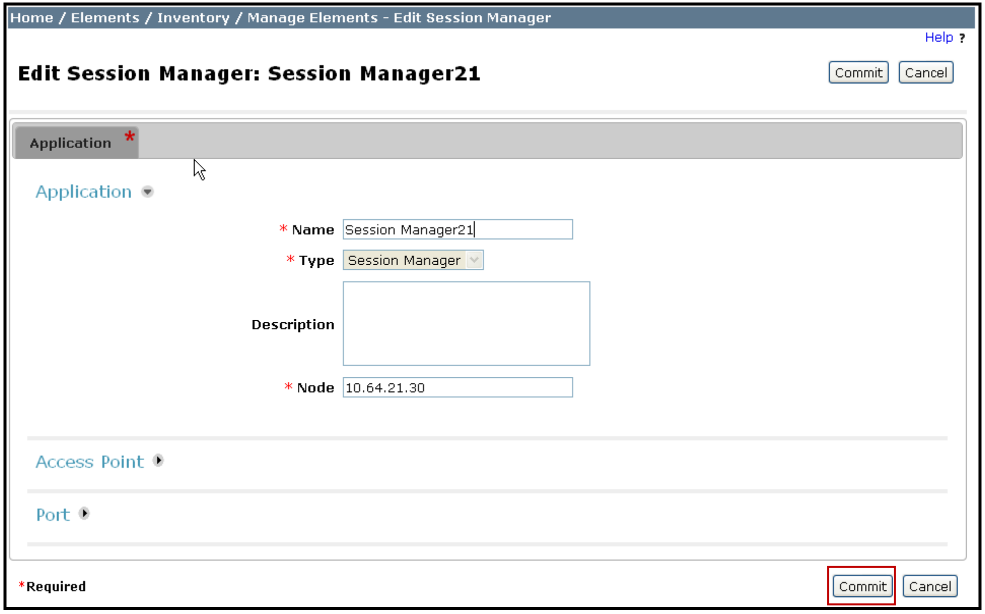
New Entities Instance

* Type: Select Type

*Required

Configure Certificates for TLS - Import the RedSky Certificate (continued)

Enter an appropriate **Name** for the Application. For the **Node**, use the Management Interface IP Address, ***10.64.21.30*** was used for the test.



Home / Elements / Inventory / Manage Elements - Edit Session Manager

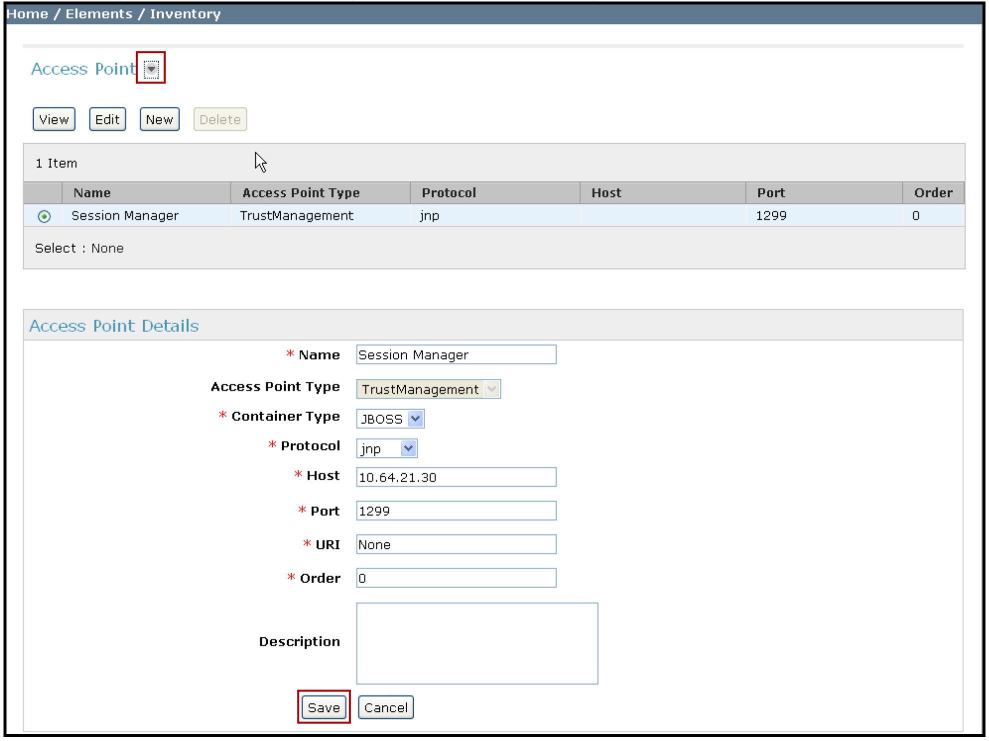
Help ?

Edit Session Manager: Session Manager21

Application

* Name	Session Manager21
* Type	Session Manager
Description	
* Node	10.64.21.30

Expand the **Access Point** heading and click **New**. In this screenshot, the entry had previously been completed providing ***Session Manager*** as the **Name** and using ***10.64.21.30*** which is the Management Interface IP Address of the Session Manager for the **Host** setting. The other settings should be exactly as entered below and click **Save**.



Home / Elements / Inventory

Access Point

1 Item

	Name	Access Point Type	Protocol	Host	Port	Order
●	Session Manager	TrustManagement	jnp		1299	0

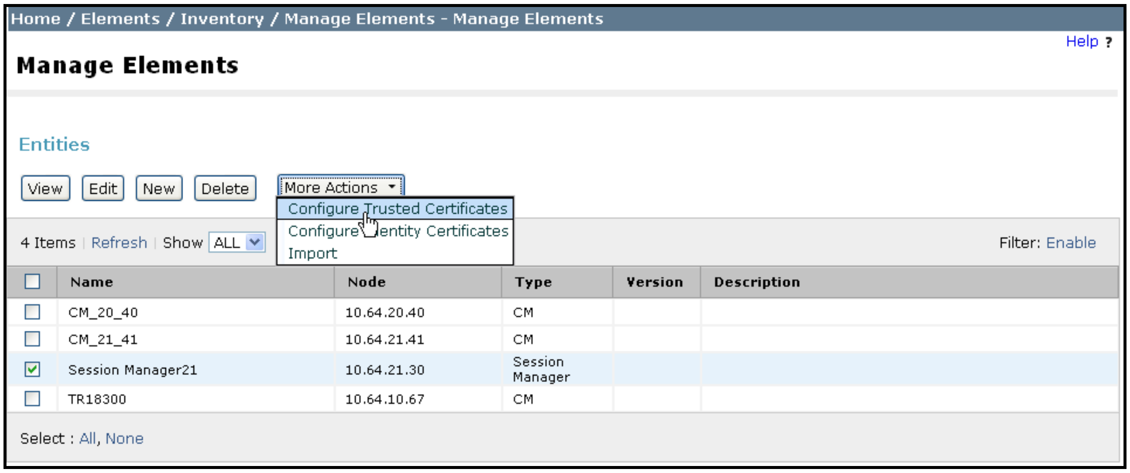
Select : None

Access Point Details

* Name	Session Manager
Access Point Type	TrustManagement
* Container Type	JBOSS
* Protocol	jnp
* Host	10.64.21.30
* Port	1299
* URI	None
* Order	0
Description	

Configure Certificates for TLS - Import the RedSky Certificate (continued)

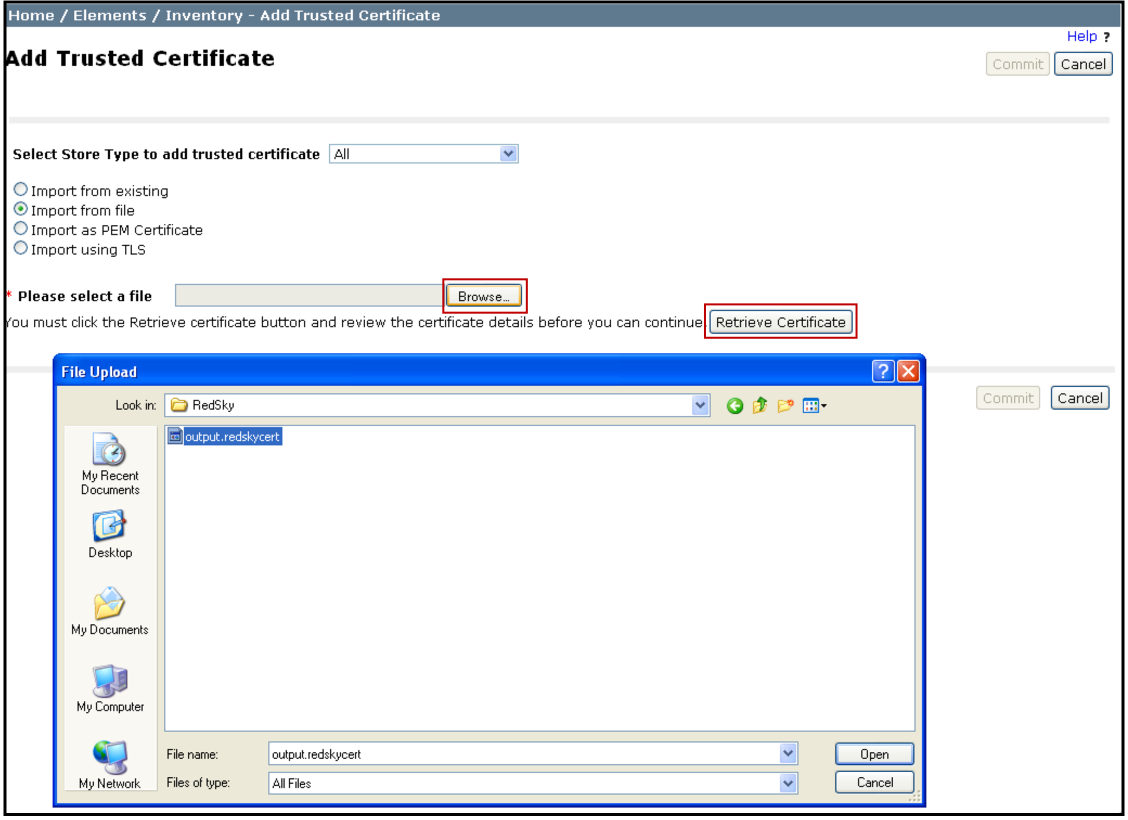
The **Manage Elements** form will appear, select the new Session Manager Element created above, select the **Configure Trusted Certificates** from the **More Actions** button.


Home / Elements / Inventory / Manage Elements - Manage Elements
Help ?
Manage Elements
Entities
View
Edit
New
Delete
More Actions
Configure Trusted Certificates
Configure Identity Certificates
Import
4 Items | Refresh | Show ALL
Filter: Enable

☐	Name	Node	Type	Version	Description
☐	CM_20_40	10.64.20.40	CM		
☐	CM_21_41	10.64.21.41	CM		
☑	Session Manager21	10.64.21.30	Session Manager		
☐	TR18300	10.64.10.67	CM		

Select : All, None

Select **Import from file** and **Browse** to find the RedSky certificate file created in **Section 7.1, Step 1** below, then click on the **Retrieve Certificate** button which activates the **Add Trusted Certificate** page shown on the following page:



Select Store Type to add trusted certificate: All

○ Import from existing
● Import from file
○ Import as PEM Certificate
○ Import using TLS

* Please select a file

You must click the Retrieve certificate button and review the certificate details before you can continue

Look in: RedSky

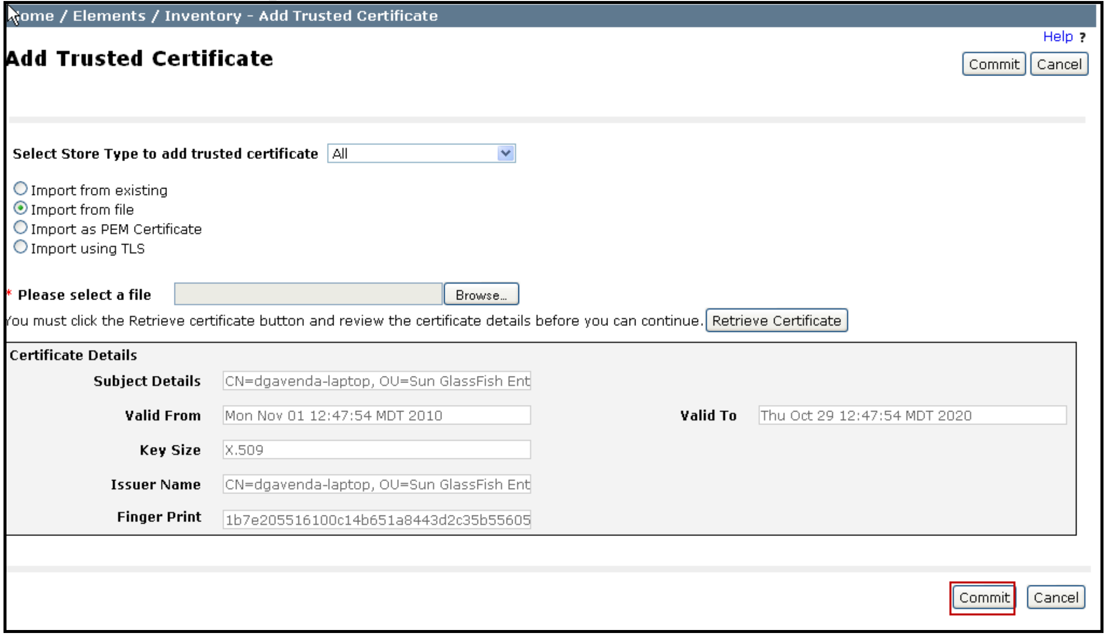
output.redskycert

File name: output.redskycert

Files of type: All Files

Configure Certificates for TLS - Import the RedSky Certificate (continued)

Click **Commit** to complete the task:



Home / Elements / Inventory - Add Trusted Certificate

Help ?

Add Trusted Certificate

Commit | Cancel

Select Store Type to add trusted certificate: All

○ Import from existing
● Import from file
○ Import as PEM Certificate
○ Import using TLS

* Please select a file [ ] Browse...

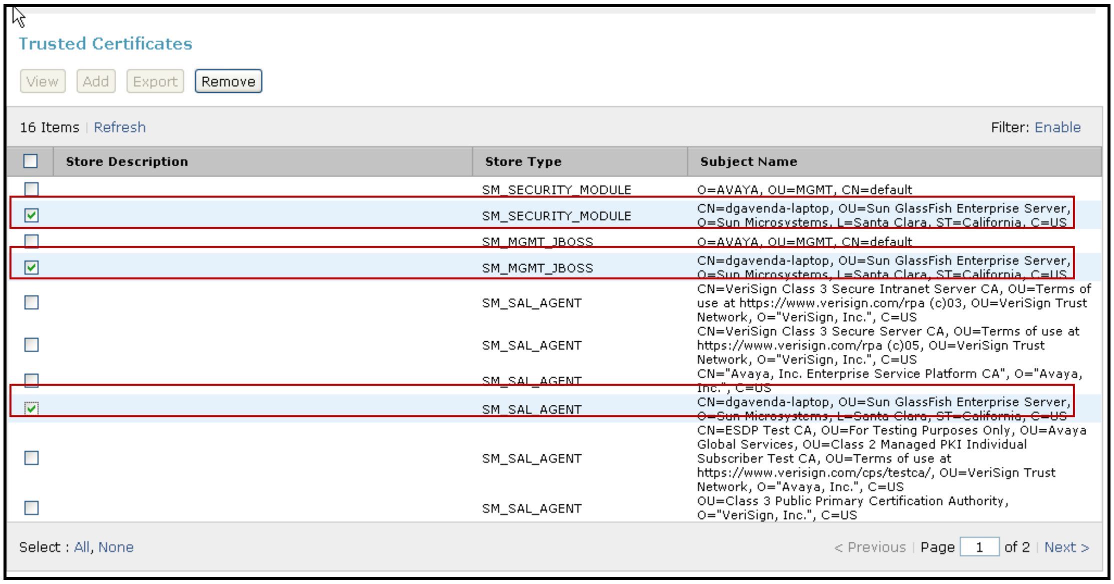
You must click the Retrieve certificate button and review the certificate details before you can continue. Retrieve Certificate

Certificate Details

Subject Details	CN=dgavenda-laptop, OU=Sun GlassFish Ent		
Valid From	Mon Nov 01 12:47:54 MDT 2010	Valid To	Thu Oct 29 12:47:54 MDT 2020
Key Size	X.509		
Issuer Name	CN=dgavenda-laptop, OU=Sun GlassFish Ent		
Finger Print	1b7e205516100c14b651a8443d2c35b55605		

Commit | Cancel

Returned to the **Manage Elements** form, select the new Session Manager Instance and select the **Configure Trusted Certificates** from the **More Actions** button as demonstrated earlier in this step. Confirm that the Certificates loaded properly (note the three highlighted entries below which may look different in your configuration).



Trusted Certificates

View | Add | Export | Remove

16 Items | Refresh

Filter: Enable

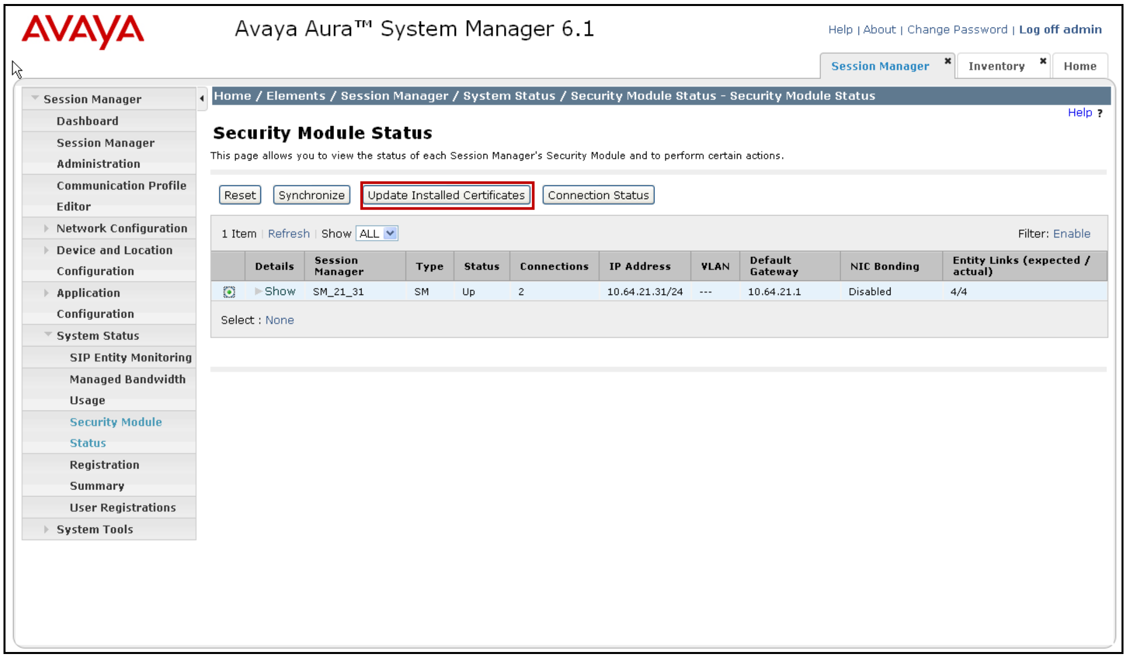
□	Store Description	Store Type	Subject Name
□		SM_SECURITY_MODULE	O=AVAYA, OU=MGMT, CN=default
☑		SM_SECURITY_MODULE	CN=dgavenda-laptop, OU=Sun GlassFish Enterprise Server, O=Sun Microsystems, L=Santa Clara, ST=California, C=US
□		SM_MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=default
☑		SM_MGMT_JBOSS	CN=dgavenda-laptop, OU=Sun GlassFish Enterprise Server, O=Sun Microsystems, L=Santa Clara, ST=California, C=US
□		SM_SAL_AGENT	CN=VeriSign Class 3 Secure Intranet Server CA, OU=Terms of use at https://www.verisign.com/rpa (c)03, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
□		SM_SAL_AGENT	CN=VeriSign Class 3 Secure Server CA, OU=Terms of use at https://www.verisign.com/rpa (c)05, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
□		SM_SAL_AGENT	CN="Avaya, Inc. Enterprise Service Platform CA", O="Avaya, Inc.", C=US
☑		SM_SAL_AGENT	CN=dgavenda-laptop, OU=Sun GlassFish Enterprise Server, O=Sun Microsystems, L=Santa Clara, ST=California, C=US
□		SM_SAL_AGENT	CN=ESDP Test CA, OU=For Testing Purposes Only, OU=Avaya Global Services, OU=Class 2 Managed PKI Individual Subscriber Test CA, OU=Terms of use at https://www.verisign.com/cps/testca/, OU=VeriSign Trust Network, O="Avaya, Inc.", C=US
□		SM_SAL_AGENT	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US

Select : All, None

< Previous | Page 1 of 2 | Next >

Configure Certificates for TLS - Import the RedSky Certificate (continued)

Navigate to **Elements > Session Manager > System Status > Security Module Status**, select the **Session Manager** (created earlier as part of the Session Manager installation), and click the **Update Installed Certificates** button.

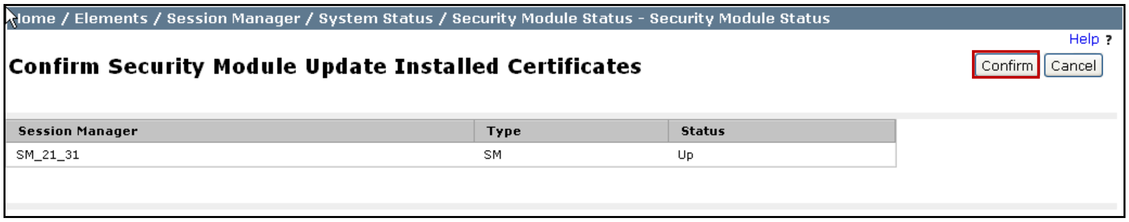

AVAYA
Avaya Aura™ System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Inventory
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
Registration Summary
User Registrations
System Tools
Home / Elements / Session Manager / System Status / Security Module Status - Security Module Status
Help ?
Reset
Synchronize
Update Installed Certificates
Connection Status
1 Item | Refresh | Show ALL
Filter: Enable
Select : None

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)
●	▶ Show	SM_21_31	SM	Up	2	10.64.21.31/24	---	10.64.21.1	Disabled	4/4

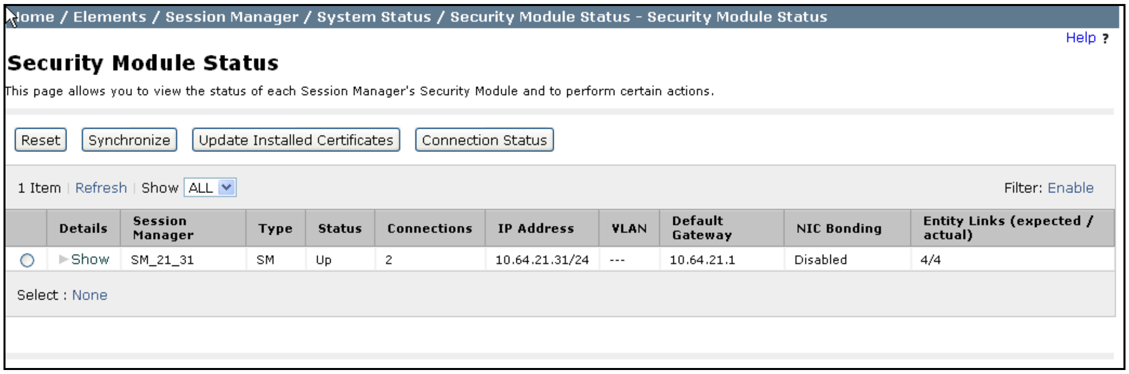
When prompted, select **confirm**


Home / Elements / Session Manager / System Status / Security Module Status - Security Module Status
Help ?
Confirm
Cancel

Confirm Security Module Update Installed Certificates

Session Manager	Type	Status
SM_21_31	SM	Up

The status page will appear:


Home / Elements / Session Manager / System Status / Security Module Status - Security Module Status
Help ?
Reset
Synchronize
Update Installed Certificates
Connection Status
1 Item | Refresh | Show ALL
Filter: Enable
Select : None

Security Module Status

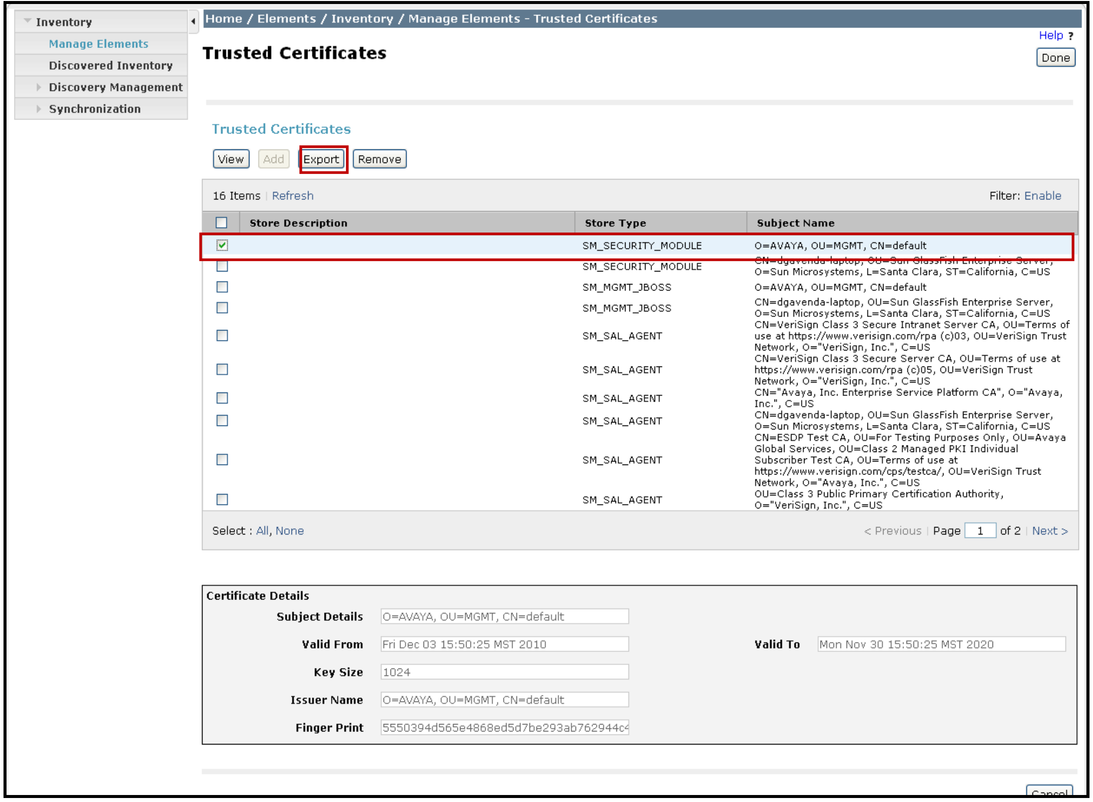
This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)
○	▶ Show	SM_21_31	SM	Up	2	10.64.21.31/24	---	10.64.21.1	Disabled	4/4

4. Configure Certificates for TLS - Export the Avaya (or Customer) Certificate

Returned to the **Manage Elements** form, select the new Session Manager Instance created in **Step 3** and select the **Configure Trusted Certificates** from the **More Actions** button as demonstrated in **Step 3**.

Select the **SM_Security_Module**and click **Export**:



Trusted Certificates

Trusted Certificates

16 Items | Refresh   Filter: Enable

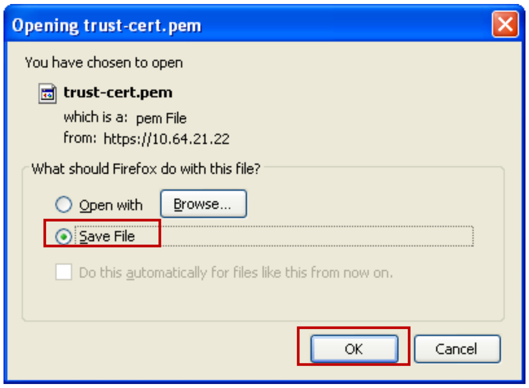
□	Store Description	Store Type	Subject Name
☑		SM_SECURITY_MODULE	O=AVAYA, OU=MGMT, CN=default
□		SM_SECURITY_MODULE	CN=dgavenda-laptop, OU=Sun GlassFish Enterprise Server, O=Sun Microsystems, L=Santa Clara, ST=California, C=US
□		SM_MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=default
□		SM_MGMT_JBOSS	CN=dgavenda-laptop, OU=Sun GlassFish Enterprise Server, O=Sun Microsystems, L=Santa Clara, ST=California, C=US
□		SM_SAL_AGENT	CN=VeriSign Class 3 Secure Intranet Server CA, OU=Terms of use at https://www.verisign.com/rpa (c)03, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
□		SM_SAL_AGENT	CN=VeriSign Class 3 Secure Server CA, OU=Terms of use at https://www.verisign.com/rpa (c)05, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
□		SM_SAL_AGENT	CN="Avaya, Inc. Enterprise Service Platform CA", O="Avaya, Inc.", C=US
□		SM_SAL_AGENT	CN=dgavenda-laptop, OU=Sun GlassFish Enterprise Server, O=Sun Microsystems, L=Santa Clara, ST=California, C=US
□		SM_SAL_AGENT	CN=ESDP Test CA, OU=For Testing Purposes Only, OU=Avaya Global Services, OU=Class 2 Managed PKI Individual Subscriber Test CA, OU=Terms of use at https://www.verisign.com/cps/testca/, OU=VeriSign Trust Network, O="Avaya, Inc.", C=US
□		SM_SAL_AGENT	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US

Select : All, None   < Previous | Page 1 of 2 | Next >

Certificate Details

Subject Details	O=AVAYA, OU=MGMT, CN=default		
Valid From	Fri Dec 03 15:50:25 MST 2010	Valid To	Mon Nov 30 15:50:25 MST 2020
Key Size	1024		
Issuer Name	O=AVAYA, OU=MGMT, CN=default		
Finger Print	5550394d565e4868ed5d7be293ab762944c4		

Choose **Save File** and **OK** which will save the PEM file in the browsers default location. This file will be used in **Step 2** in **Section 7.1**:



You have chosen to open

trust-cert.pem

which is a: pem File
from: https://10.64.21.22

What should Firefox do with this file?

○ Open with

● Save File

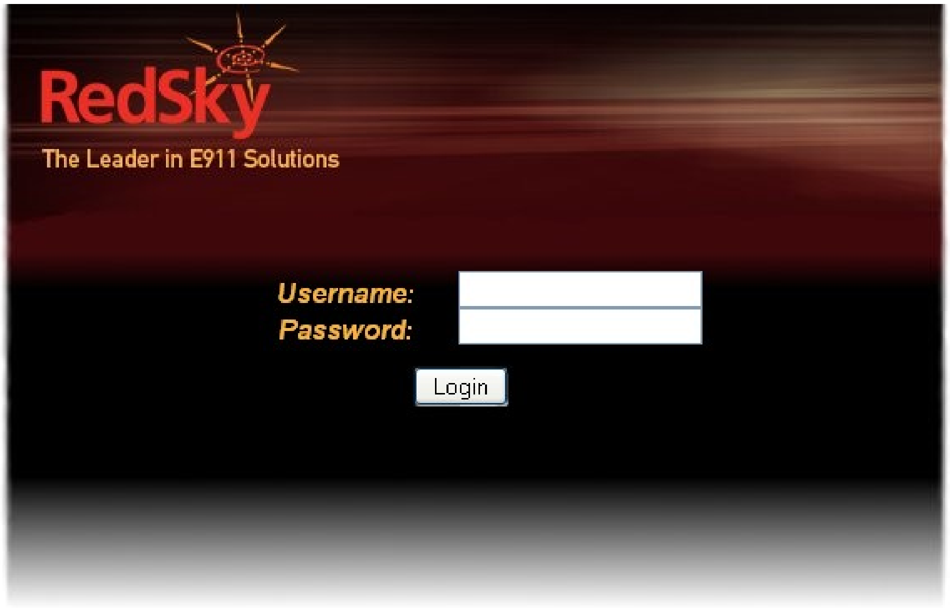
□ Do this automatically for files like this from now on.

7. Configure RedSky E911 Manager

This section provides the steps for configuring the RedSky E911 Manager to provide ELIN information to Avaya Aura® Session Manager.

7.1. RedSky E911 Configuration Details

RedSky E911 is configured using a web browser. Enter the URL of the RedSky E911 server such as http://<hostname>:8080/e911Anywhere where <hostname> is the ip address or fully qualified domain name of the RedSky server. Login using appropriate credentials.



In general, the steps were as follows:

- Configure Certificates for TLS - Export the RedSky Certificate
- Configure Certificates for TLS - Import the Avaya (or Customer) Certificate
- Verify the Company Name and Installed License Keys
- Administer the Session Manager link (Optional)
- Define the Company Locations (Buildings)
- Define the Company Locations (Locations)
- Define the ELIN for each Location
- Administer the IP Address Ranges

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

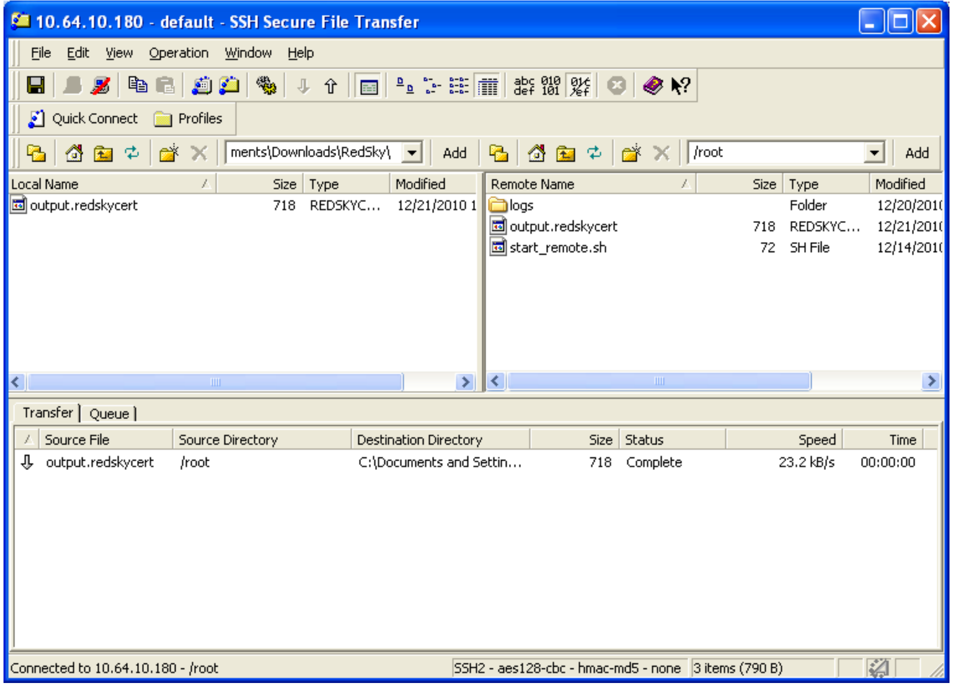
Configure Certificates for TLS - Export the RedSky Certificate

In order for RedSky and Session Manager to use TLS to secure communications, a RedSky certificate must be installed on the Avaya equipment, and an Avaya (or Customer provided) certificate must be installed on the RedSky server.

Start by exporting the certificate from the RedSky server using telnet to access the CLI on the RedSky server. Login using appropriate credentials and enter the highlighted command. For this test, **output.redskycert** was the name given to the output file, this can be any meaningful filename.

```
redsky:~# keytool -export -alias slas -file output.redskycert -keystore
/opt/sailfin/domains/domain1/config/keystore.jks -storepass changeit
Certificate stored in file <output.redskycert>
redsky:~#
```

Transfer the file using a file transfer utility. Note the location of the output.redskycert file is root in this example, but could have been specified to be a different directory if the command had included a path. This file will be used in **Step 3** in **Section 6.1**.



Local Name	Size	Type	Modified
output.redskycert	718	REDSKYC...	12/21/2010 1

Remote Name	Size	Type	Modified
logs		Folder	12/20/201(
output.redskycert	718	REDSKYC...	12/21/201(
start_remote.sh	72	SH File	12/14/201(

Source File	Source Directory	Destination Directory	Size	Status	Speed	Time
output.redskycert	/root	C:\Documents and Settin...	718	Complete	23.2 kB/s	00:00:00

Connected to 10.64.10.180 - /root SSH2 - aes128-cbc - hmac-md5 - none 3 items (790 B)

</td></tr>
</table>

Step	Description
2.	**Configure Certificates for TLS - Import the Avaya (or Customer) Certificate** Copy the .pem file that was created in **Section 6.1, Step 4**, over to the target server in the path shown below using a file transfer utility as demonstrated earlier in this Step. Enter the highlighted command (use the literal text) to import the certificate. When prompted, enter **y** and **Enter** to complete the task:

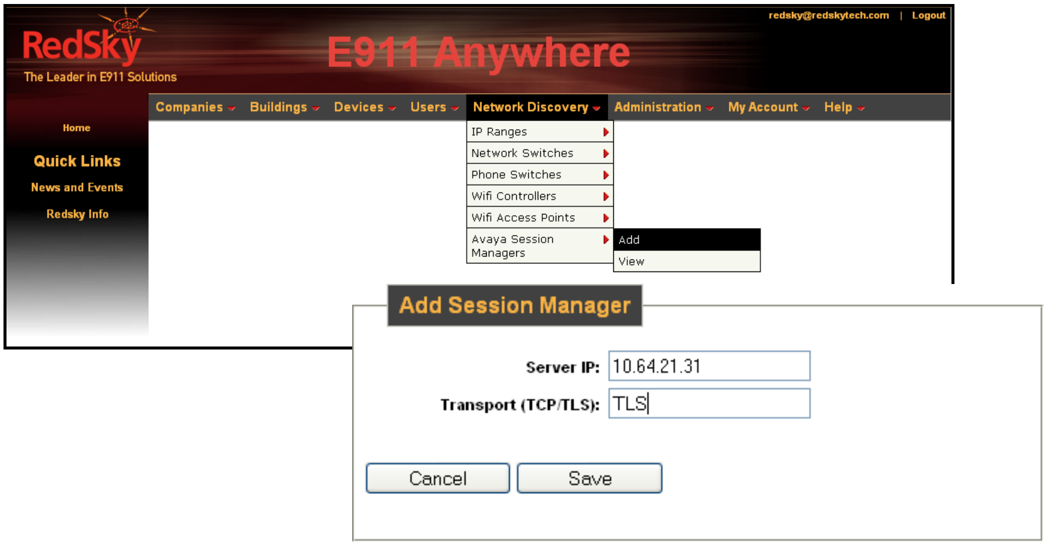
```
redsky:/opt/sailfin/domains/domain1/config# keytool -importcert -alias default
-file trust-cert.pem -keystore /opt/sailfin/domains/domain1/config/keystore.jks
-storepass changeit -trustcacerts
Owner: O=AVAYA, OU=MGMT, CN=default
Issuer: O=AVAYA, OU=MGMT, CN=default
Serial number: 33f15667345e076a
Valid from: Fri Dec 03 16:50:25 CST 2010 until: Mon Nov 30 16:50:25 CST 2020
Certificate fingerprints:
         MD5:  44:7A:BC:EF:37:36:EE:68:B4:11:C1:B9:A9:40:49:3D
         SHA1: 55:50:39:4D:56:5E:48:68:ED:5D:7B:E2:93:AB:76:29:44:C4:BF:9C
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1A 41 35 B3 BE BC B1 96   1A 43 C5 2E B9 DB 2C EF  .A5......C....,.
0010: 55 E5 47 B4                                        U.G.
]
]

#4: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 1A 41 35 B3 BE BC B1 96   1A 43 C5 2E B9 DB 2C EF  .A5......C....,.
0010: 55 E5 47 B4                                        U.G.
]

]

Trust this certificate? [no]:  y
Certificate was added to keystore
redsky:/opt/sailfin/domains/domain1/config#
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Administer the Session Manager link (Optional)

Select **Add** from the **Network Discovery > Avaya Session Managers** menu to administer the Session Manager(s). In the compliance test, a single Session Manager was used, however it is possible to administer more than one Session Manager by repeating the process. This step is optional, when Session Manager is administered properly, a connection will automatically be established between servers.

Enter the **Server IP** address of the Session Manager. Enter the **Transport** protocol to match the entry in the Session Manager configuration, **Step 2**. **TLS** is recommended for security reasons.

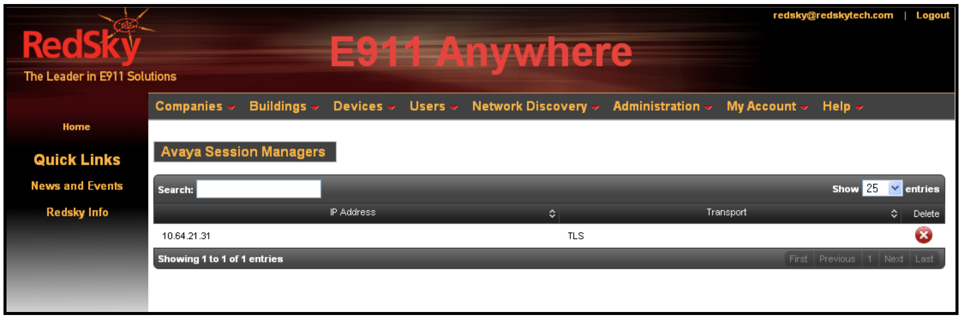


Add Session Manager

Server IP: 10.64.21.31

Transport (TCP/TLS): TLS

Select **View** from the **Network Discovery > Avaya Session Managers** menu to review the administered entries.



Avaya Session Managers

IP Address	Transport	Delete
10.64.21.31	TLS	⊗

Showing 1 to 1 of 1 entries

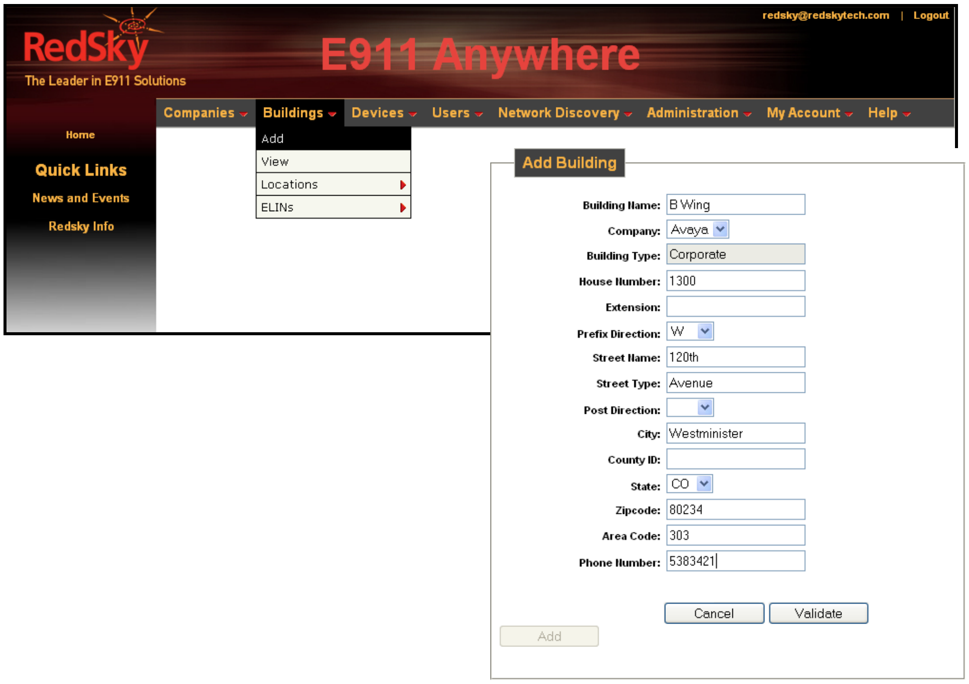
</td></tr>
</table>

Step **Description**

4. **Define the Company Locations (Buildings)**

Location administration involves defining one or more Buildings, one or more Locations within each building, and one or more network IP Ranges associated with each Location and assigning ELINs to each IP Range. It is also possible to define devices such as phones, however this is not necessary as this would be redundant with administration in CM and Session Manager. Device definitions are overridden with IP Address based location information if it differed from the statically defined device location information.

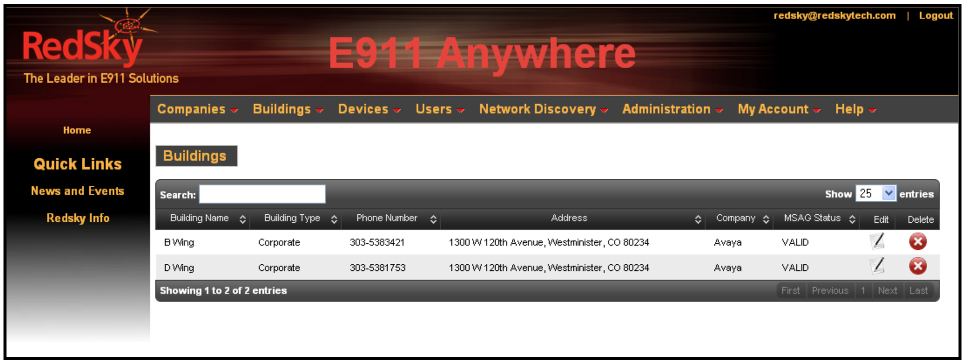
Select **Add** from the **Buildings** menu to administer general location information. Multiple Buildings may be administered by repeating the process. For the compliance test, two buildings were defined. Click **Validate** then **Add** to complete the entry.



Add Building

Building Name: B Wing
Company: Avaya
Building Type: Corporate
House Number: 1300
Extension:
Prefix Direction: W
Street Name: 120th
Street Type: Avenue
Post Direction:
City: Westminister
County ID:
State: CO
Zipcode: 80234
Area Code: 303
Phone Number: 5383421

Select **View** from the **Buildings** menu to see the administered entries.

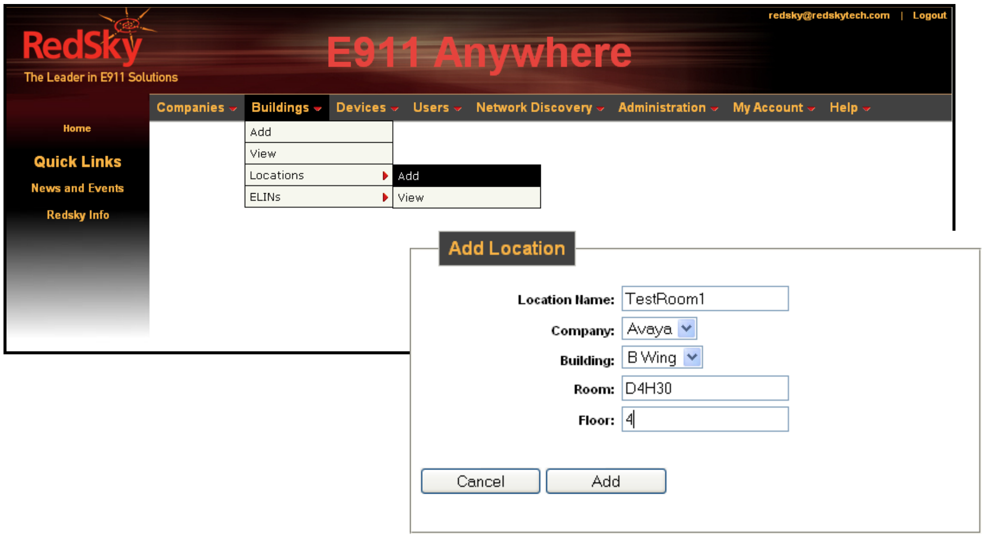


Building Name	Building Type	Phone Number	Address	Company	MSAG Status	Edit	Delete
B Wing	Corporate	303-5383421	1300 W 120th Avenue, Westminister, CO 80234	Avaya	VALID	✎	✖
D Wing	Corporate	303-5381753	1300 W 120th Avenue, Westminister, CO 80234	Avaya	VALID	✎	✖

Showing 1 to 2 of 2 entries

5. **Define the Company Locations (Locations)**

Select **Add** from the **Buildings > Locations** menu to administer refined location information. Multiple Locations may be administered by repeating the process. For the compliance test, two locations were defined, **TestRoom1** and **TestRoom2**.



Add Location

Location Name: TestRoom1

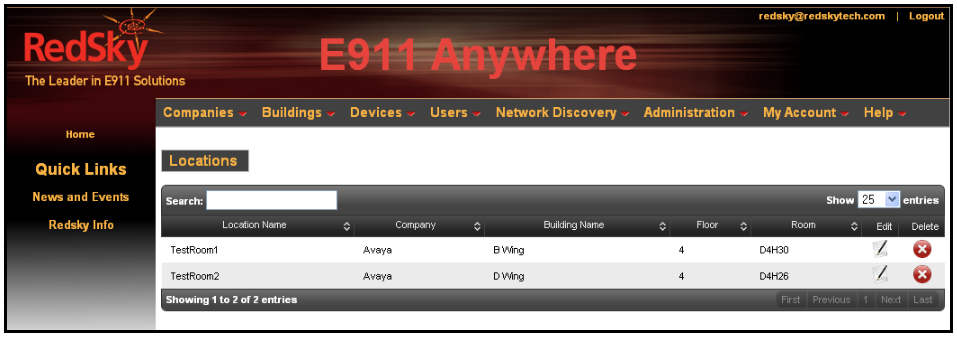
Company: Avaya

Building: B Wing

Room: D4H30

Floor: 4

Select **View** from the **Buildings > Locations** menu to see the administered entries.



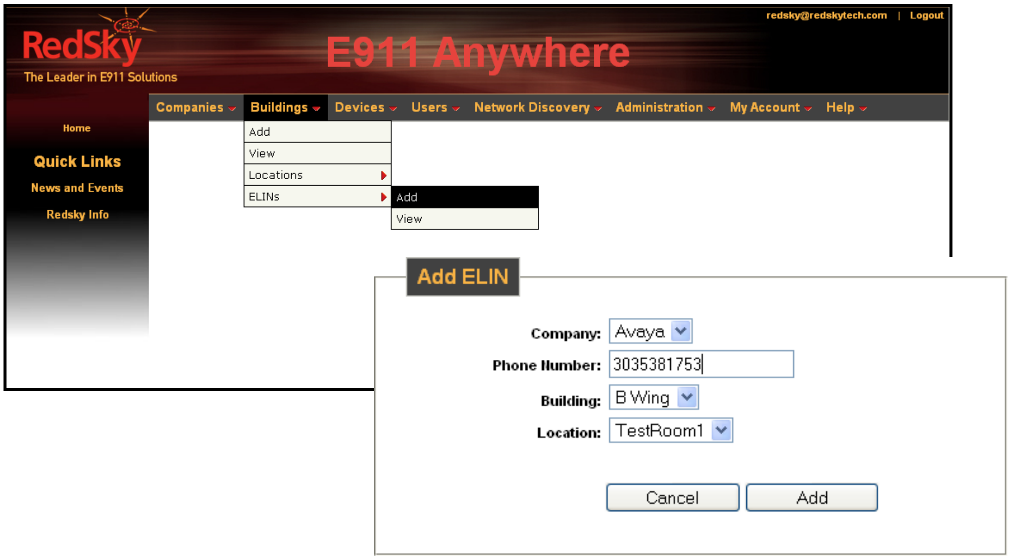
Locations

Location Name	Company	Building Name	Floor	Room	Edit	Delete
TestRoom1	Avaya	B Wing	4	D4H30		
TestRoom2	Avaya	D Wing	4	D4H26		

Showing 1 to 2 of 2 entries

6. **Define the ELIN for each Location**

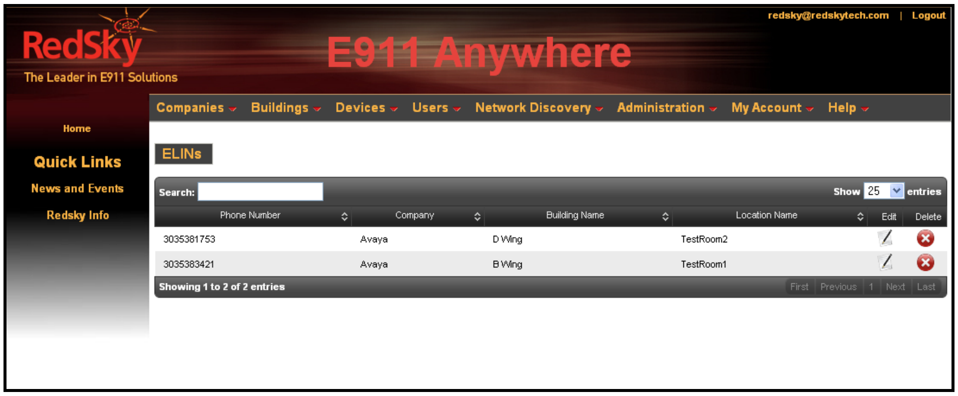
Select **Add** from the **Buildings > ELINs** menu to administer the ELIN that will be associated with each location. For the Compliance Test, an ELIN entry was created for each Location.



Add ELIN

Company: Avaya
Phone Number: 3035381753
Building: B Wing
Location: TestRoom1

Select **View** from the **Buildings > ELINs** menu to see the administered entries.



ELINs

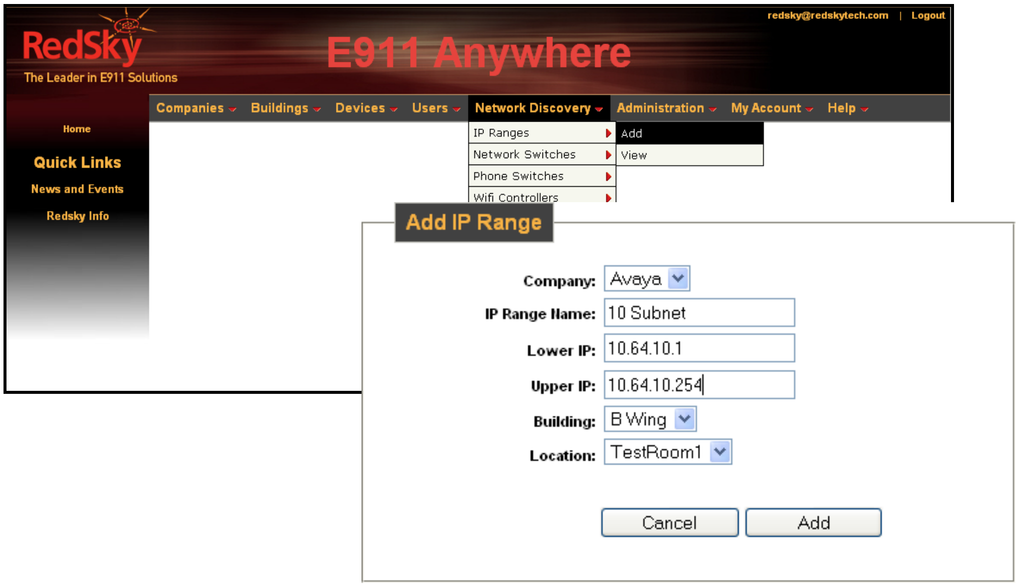
Show 25 entries

Phone Number	Company	Building Name	Location Name	Edit	Delete
3035381753	Avaya	D Wing	TestRoom2		
3035383421	Avaya	B Wing	TestRoom1		

Showing 1 to 2 of 2 entries

7. **Administer the IP Address Ranges**

Select **Add** from the **Network Discovery > IP Ranges** menu to administer the IP Address Ranges that will be associated with each location. For the Compliance Test, one address range entry was created for each Location.

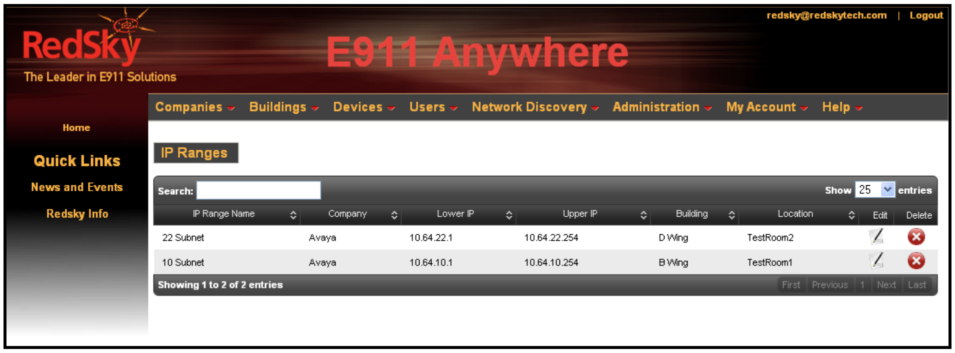


Add IP Range

Company: Avaya
IP Range Name: 10 Subnet
Lower IP: 10.64.10.1
Upper IP: 10.64.10.254
Building: B Wing
Location: TestRoom1

Cancel | Add

Select **View** from the **Network Discovery > IP Ranges** menu to see the administered entries.



IP Ranges

Search: Show 25 entries

IP Range Name	Company	Lower IP	Upper IP	Building	Location	Edit	Delete
22 Subnet	Avaya	10.64.22.1	10.64.22.254	D Wing	TestRoom2	✎	✖
10 Subnet	Avaya	10.64.10.1	10.64.10.254	B Wing	TestRoom1	✎	✖

Showing 1 to 2 of 2 entries | First Previous 1 Next Last

8. Verification Steps

The following command was executed on the command line of the Avaya Aura® Session Manager in order to validate the ELIN information provided by RedSky:

```
[root@SM21 craft]# sm cons get allreg
RegistrationKey[commProfileId:55, contactHashKey:sip:6012@10.64.22.204:5061;avaya-sc-
enabled;transport=tls]=RegistrationData[expirationTime=Wed Dec 22 13:57:57 MST 2010,
callId=25_15477c-44ed1a064d27961e_R@10.64.22.204, cSeq=56, elin=3035381753]
RegistrationKey[commProfileId:51, contactHashKey:sip:6010@10.64.22.202:5061;avaya-sc-
enabled;transport=tls]=RegistrationData[expirationTime=Wed Dec 22 14:28:46 MST 2010,
callId=17_154d226e0098314d279bbf_R@10.64.22.202, cSeq=28, elin=3035381753]
RegistrationKey[commProfileId:53, contactHashKey:sip:6011@10.64.22.203:5061;avaya-sc-
enabled;transport=tls]=RegistrationData[expirationTime=Wed Dec 22 14:15:27 MST 2010,
callId=1_1c9429-2c2220014d2ef57f_R@10.64.22.203, cSeq=2, elin=3035381753]
[root@SM21 craft]#
```

9. Conclusion

The RedSky E911 Manager successfully demonstrated the ability to retrieve the IP Address of SIP Endpoints registered with Avaya Aura® Session Manager and return the Emergency Location Identification Number (ELIN) corresponding to the network location of the Endpoint. While the general location information a company may have on file with the Automatic Location Identifier (ALI) database providers can be matched to an ANI from the calling party number sent over public networks, this information may not be precise, and could in fact be incorrect given the roaming nature of IP endpoints as well as the distributed nature of modern communications systems. The precision afforded to enterprises using a RedSky ELIN server solution can make a significant difference in response times in the event of an emergency.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.
[1] *Administering Avaya Aura™ SessionManager*, Document ID 03-603324, Issue 1, Release 6.1, November, 2010.

Product information for RedSky Technologies E911 Manager may be found at http://www.redskye911com.

©2011 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.