Avaya Solution & Interoperability Test Lab

Application Notes for SecureLogix Enterprise Telephony Management (ETM) SIP Proxy with Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the SecureLogix Enterprise Telephone Management (ETM) SIP Proxy with Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise. SecureLogix ETM SIP Proxy helps protect enterprise voice networks from VoIP attacks and service abuse in real-time by controlling network access and service use via Voice Firewall policies. In addition, it provides real-time detection and prevention of fraudulent, abusive, or operationally relevant call patterns, including voice fraud, excessive unanswered/busy calls, and voice spam via Voice Intrusion Protection System (IPS) policies. SecureLogix ETM SIP Proxy monitors all inbound and outbound SIP calls between the enterprise and SIP service provider / PSTN. SecureLogix ETM SIP Proxy connects to Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise via a SIP trunk.

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 configuration steps required to integrate the SecureLogix Enterprise Telephone Management (ETM) SIP Proxy with Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise (SBCE). SecureLogix ETM SIP Proxy helps protect enterprise voice networks from VoIP attacks and service abuse in real-time by controlling network access and service use via Voice Firewall policies. In addition, it provides real-time detection and prevention of fraudulent, abusive, or operationally relevant call patterns, including voice fraud, excessive unanswered/busy calls, and voice spam via Voice Intrusion Protection System (IPS) policies. SecureLogix ETM SIP Proxy monitors all inbound and outbound SIP calls between the enterprise and SIP service provider / PSTN. SecureLogix ETM SIP Proxy connects to Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise via a SIP trunk.

2 General Test Approach and Test Results

Interoperability compliance testing covered feature and serviceability testing. The feature testing focused on placing inbound and outbound calls between the enterprise voice network and the simulated SIP service provider (i.e., PSTN), and verifying that SecureLogix ETM SIP Proxy monitored and controlled call activity via voice firewall and IPS policies. The enterprise voice network was comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise with SecureLogix ETM SIP Proxy connected between Session Manager and SBCE via a SIP trunk.

The serviceability testing focused on verifying that SecureLogix ETM SIP Proxy came back into service after re-establishing IP network connectivity and after a reboot.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and SecureLogix ETM SIP Proxy did not include use of any specific encryption features as requested by SecureLogix.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing SIP trunk between Session Manager and ETM and verifying the exchange of SIP Options messages.
- Establishing voice calls between the enterprise voice network and the PSTN with all calls being monitored and controlled by ETM via Voice Firewall and Voice IPS policies.
- Verifying call attributes, such as call direction, source, destination, and duration, in the ETM Policy Logs and Call Monitor.
- Enforcing Voice Firewall policies to allow or deny individual calls based on call direction (inbound, outbound, or both), source, destination, call duration, and call frequency.
- Enforcing Voice IPS policies to detect and protect against anomalous call patterns over time that could indicate toll fraud or intrusion attempts.
- Proper system recovery after reconnecting ETM to the IP network and after a reboot.

2.2 Test Results

All test cases passed with the following observation:

- SecureLogix ETM SIP Proxy detects call type from the codec. Since Media Proxy was not enabled on ETM (i.e., media not anchored), the Call Type was displayed as "undetermined" for answered calls.

2.3 Support

For technical support on SecureLogix ETM SIP Proxy, contact SecureLogix via phone or website.

- **Phone:** 1 (877) SLC-4HELP (1-877-752-4435)
- **Web:** https://support.securelogix.com/index.htm

3 Reference Configuration

The network diagram below illustrates the test configuration. In this configuration, all inbound and outbound calls between the enterprise voice network and the PSTN traverse SecureLogix ETM SIP Proxy, which applies voice firewall and IPS policies. The SecureLogix ETM System Console is used to configure ETM. ETM connects to Session Manager and SBCE via a SIP trunk.

The enterprise voice network consists of a SIP trunk between Communication Manager and Session Manager, media resources in the G450 Media Gateway and Media Server, and 96x1 H.323 and SIP deskphones. All PSTN calls were routed through SBCE.

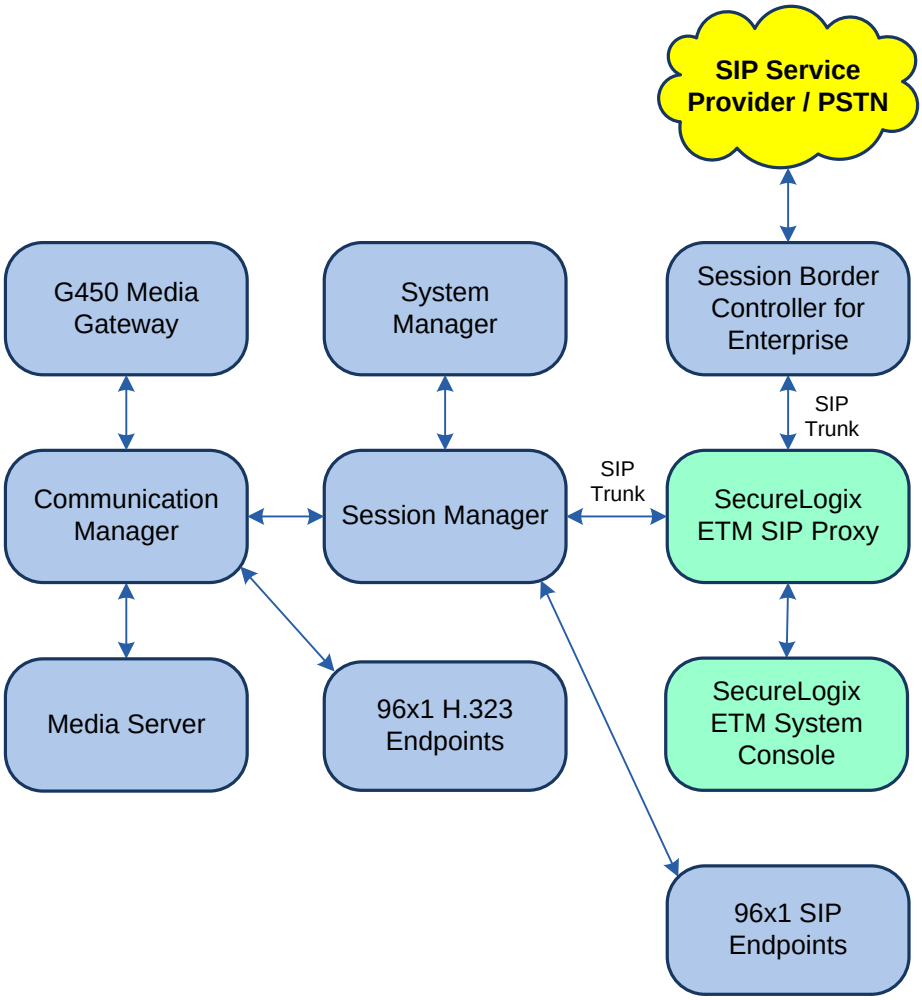


Figure 1: Avaya Enterprise Voice Network with SecureLogix ETM SIP Proxy

4 Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager	8.0.1.1.0-FP1SP1 (R018x.00.0.822.0 with Patch 25183)
Avaya G450 Media Gateway	FW 40.25.0
Avaya Aura® Media Server	v.8.0.0.173
Avaya Aura® System Manager	8.0.1.1 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.1.039340 Service Pack 1
Avaya Aura® Session Manager	8.0.1.1.801103
Avaya Session Border Controller for Enterprise	8.0.0.0-19-16991
Avaya 96x1 Series IP Deskphones	6.8003 (H.323) 7.1.5.0.11 (SIP)
SecureLogix Enterprise Telephony Management (ETM) SIP Proxy	7.1.79
SecureLogix ETM System Console	7.1.2_x64 build 92

5 Configure Avaya Aura® Session Manager

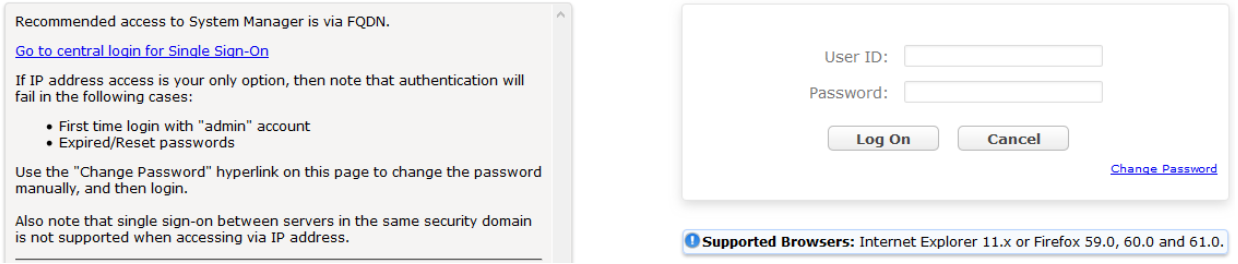
This section provides the procedure for configuring Session Manager. The procedure includes adding the following items:

- Launch System Manager
- SIP Entities corresponding to Session Manager, Communication Manager, and ETM
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies
- Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

Note: It is assumed that basic configuration of Session Manager has already been completed. This section will focus on the configuration of the SIP trunk to ETM and routing calls to it.

5.1 Launch System Manager

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



5.2 Add SIP Entities

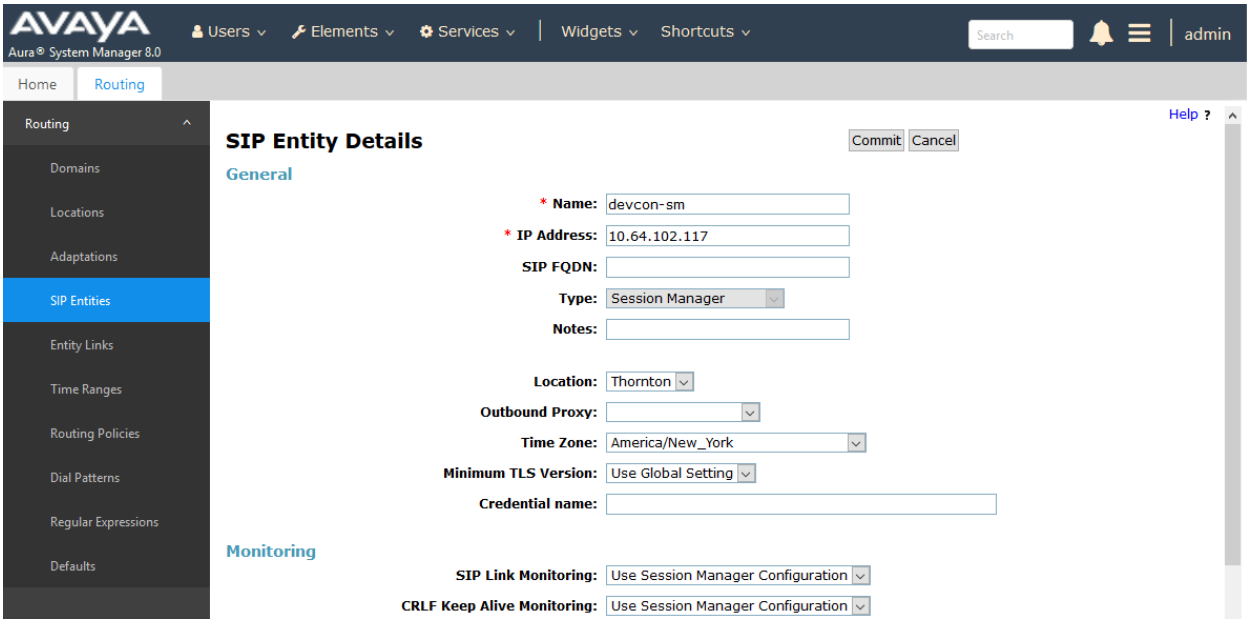
This section covers the configuration of SIP entities for Session Manager and ETM. It is assumed that the Communication Manager SIP entity has already been configured.

5.2.1 Avaya Aura® Session Manager

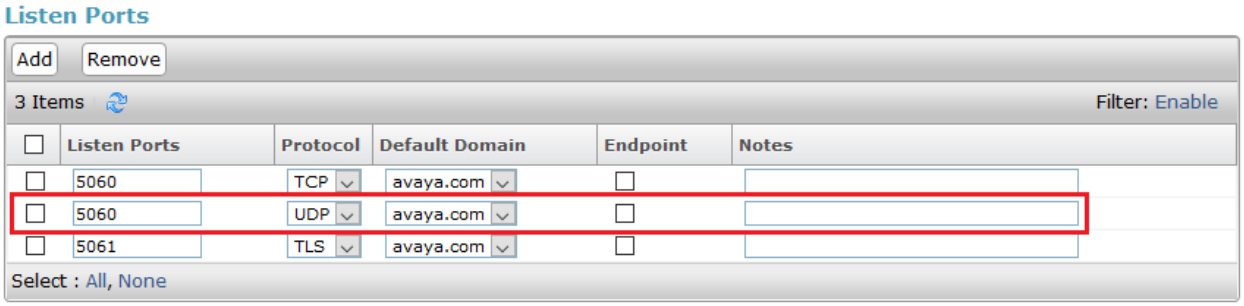
From the System Manager **Home** screen, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select one of the locations defined.
- **Time Zone:** Time zone for this location.



Scroll down to the **Listen Ports** section and verify that the UDP transport network protocol used by ETM is specified as shown below.



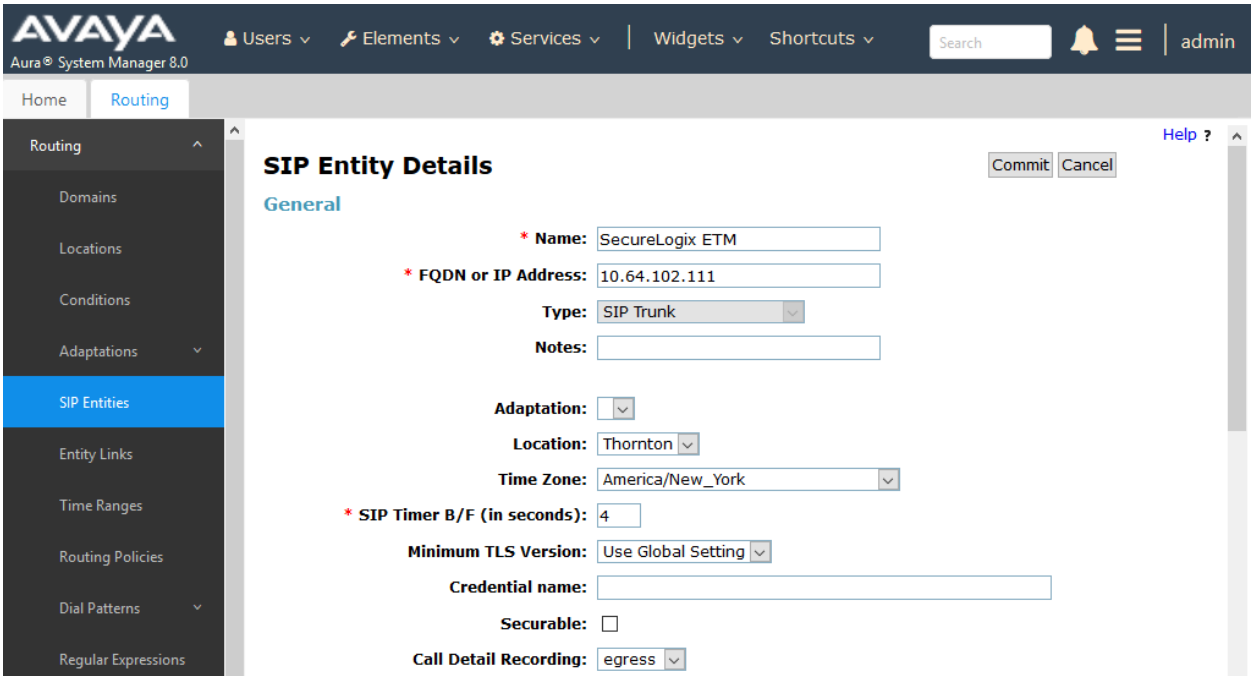
5.2.2 SecureLogix ETM SIP Proxy

A SIP Entity must be added for ETM. To add a SIP Entity, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** ETM IP address.
- **Type:** Select *SIP Trunk*.
- **Location:** Select one of the locations previously defined.
- **Time Zone:** Time zone for this location.

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.



5.3 Add Entity Links

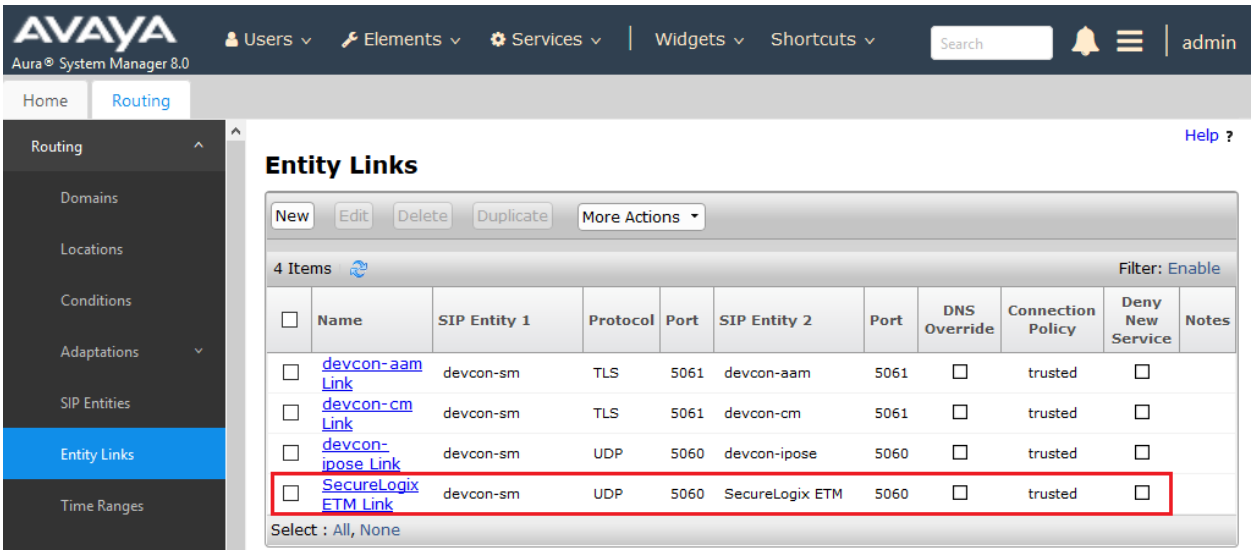
This section covers the configuration of Entity Links for ETM. It is assumed that the Communication Manager entity link has already been configured.

5.3.1 SecureLogix ETM SIP Proxy Entity Link

The SIP trunk between Session Manager and ETM is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *SecureLogixETM Link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select UDP transport protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the *SexureLogix ETM* SIP entity.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Selected *trusted*. *Note: If the link is not trusted, calls from the associated SIP Entity specified in* ***Section 5.2.2*** *will be denied.*

Click **Commit** to save the Entity Link definition.



5.4 Add Routing Policies

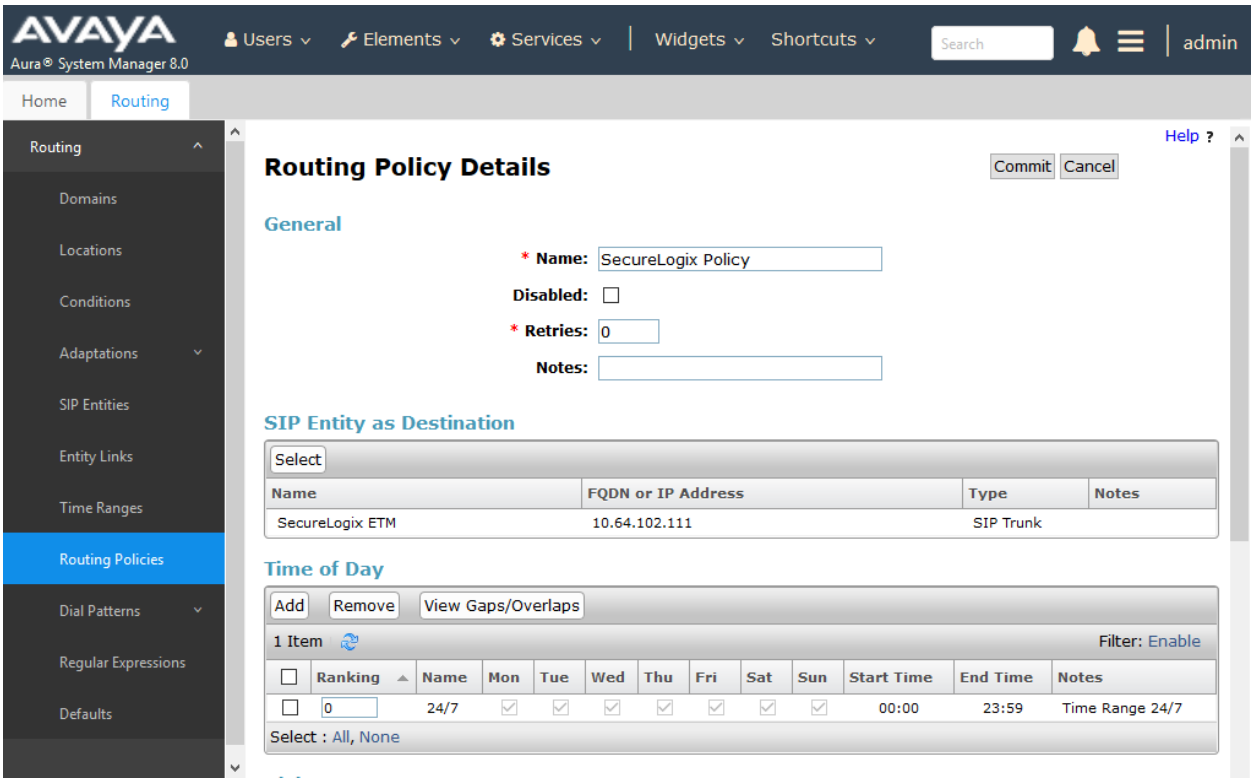
Routing policies describe the conditions under which calls are routed to Communication Manager and ETM SIP entities. To add a routing policy, navigate to **Elements → Routing → Routing Policies** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition.

The following screen shows the Routing Policy for ETM. It is assumed that the Routing Policy for Communication Manager has already been configured.



5.5 Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, 10-digit numbers starting with 73277 are routed to Communication Manager and calls to 900, 908, or 976 area codes are routed to ETM.

To add a dial pattern, navigate to **Elements → Routing → Dial Patterns** and click on the **New** button (not shown). Fill in the following:

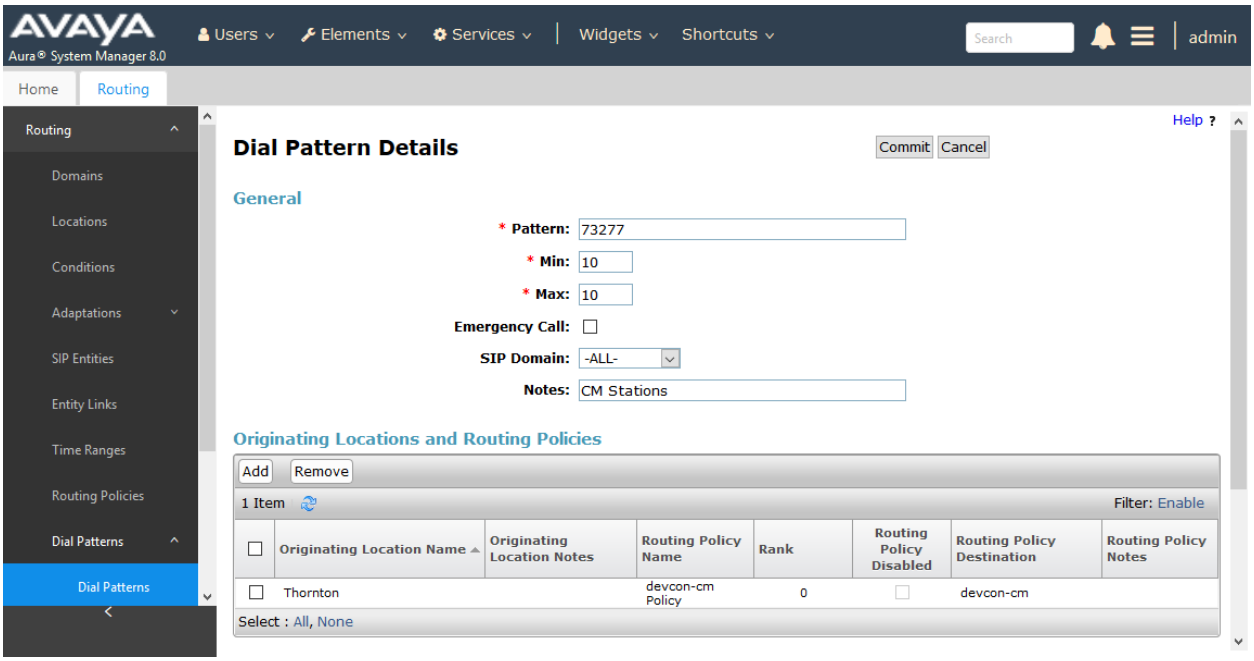
Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

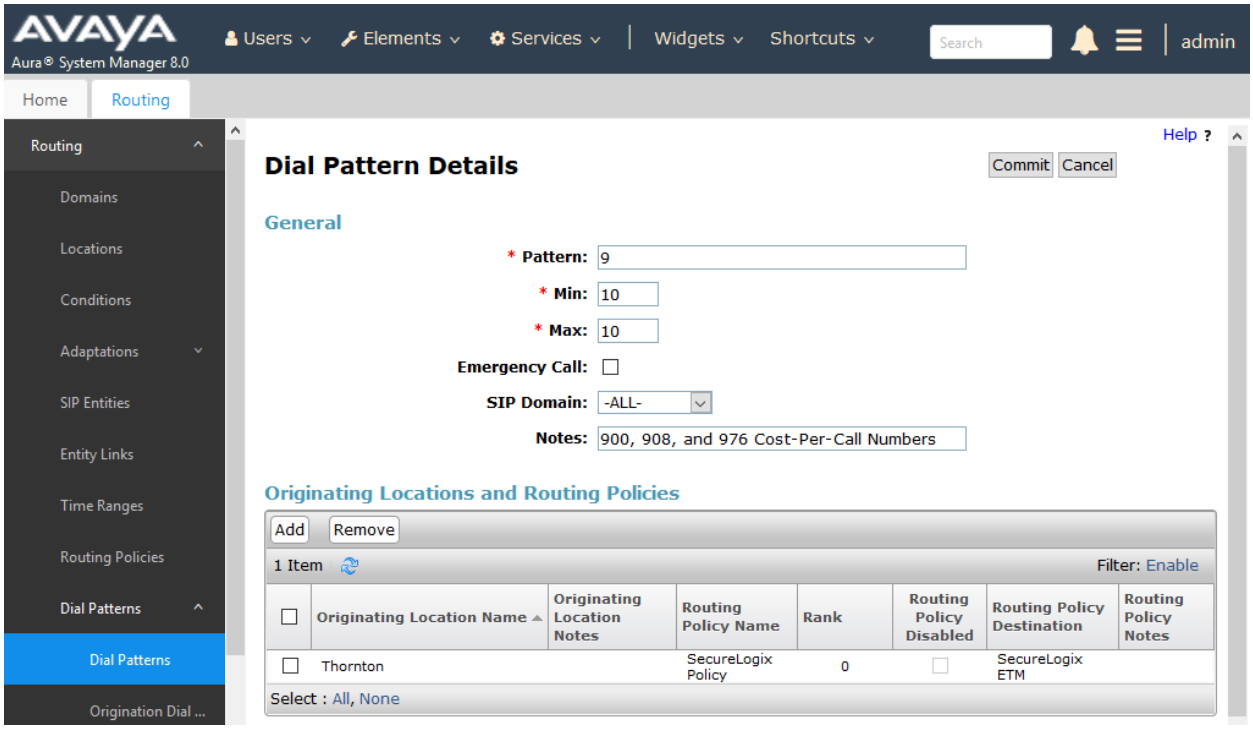
Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.

The following **Dial Pattern** shows the dial pattern definition for 73277 being routed to Communication Manager.



The following **Dial Pattern** shows the dial pattern definition for calls in the 900, 908, and 976 area codes being routed to ETM.



5.6 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

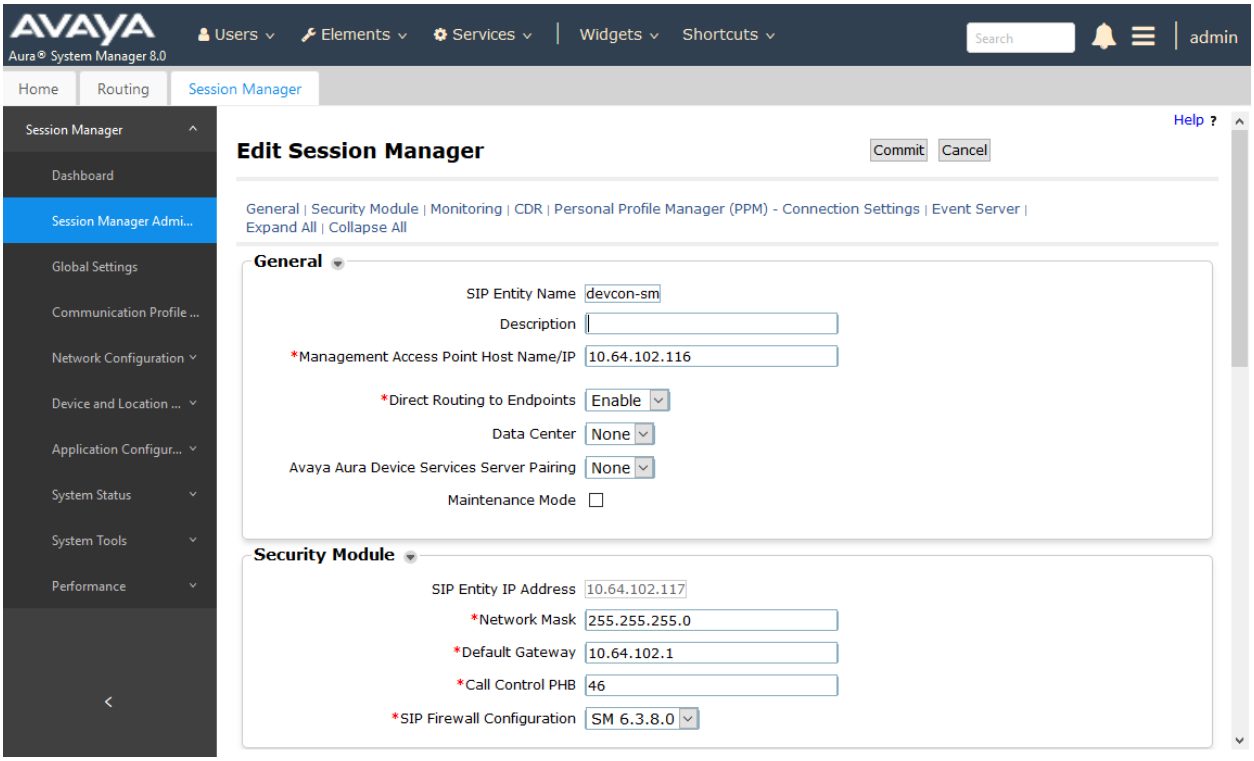
Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

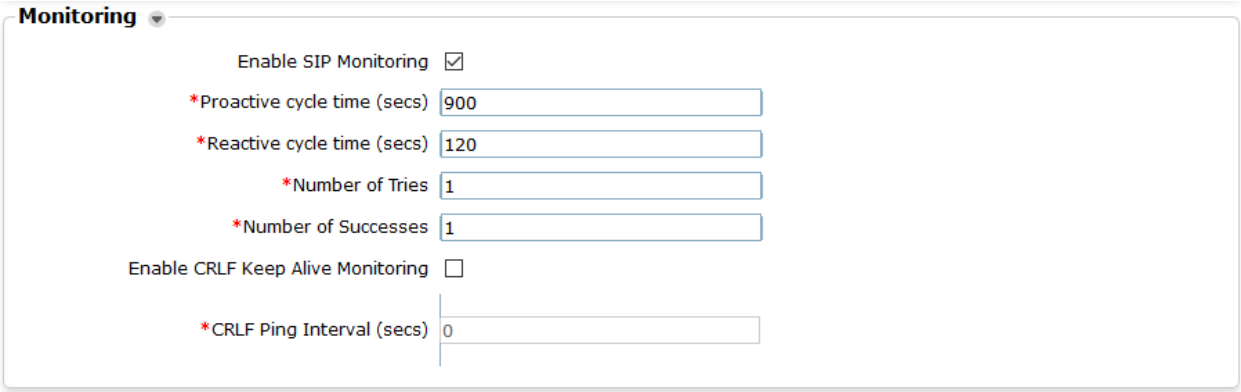
Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.



The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to ETM. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 900 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.



6 Configure Avaya Session Border Controller for Enterprise

This section provides the procedure for configuring SBCE, which includes creating a SIP trunk and routing to ETM. This section covers the following configuration areas:

- Log into the EMS Web Interface
- Configure Server Interworking
- Configure SIP Servers
- Configure Routing Profile
- Configure End Point Flows

Note: It is assumed that Avaya Session Border Controller for Enterprise has already been commissioned and the private and public interfaces, the media and signaling interfaces, and the SIP trunk and routing to the SIP service provider / PSTN have already been configured.

6.1 Log into the EMS Web Interface

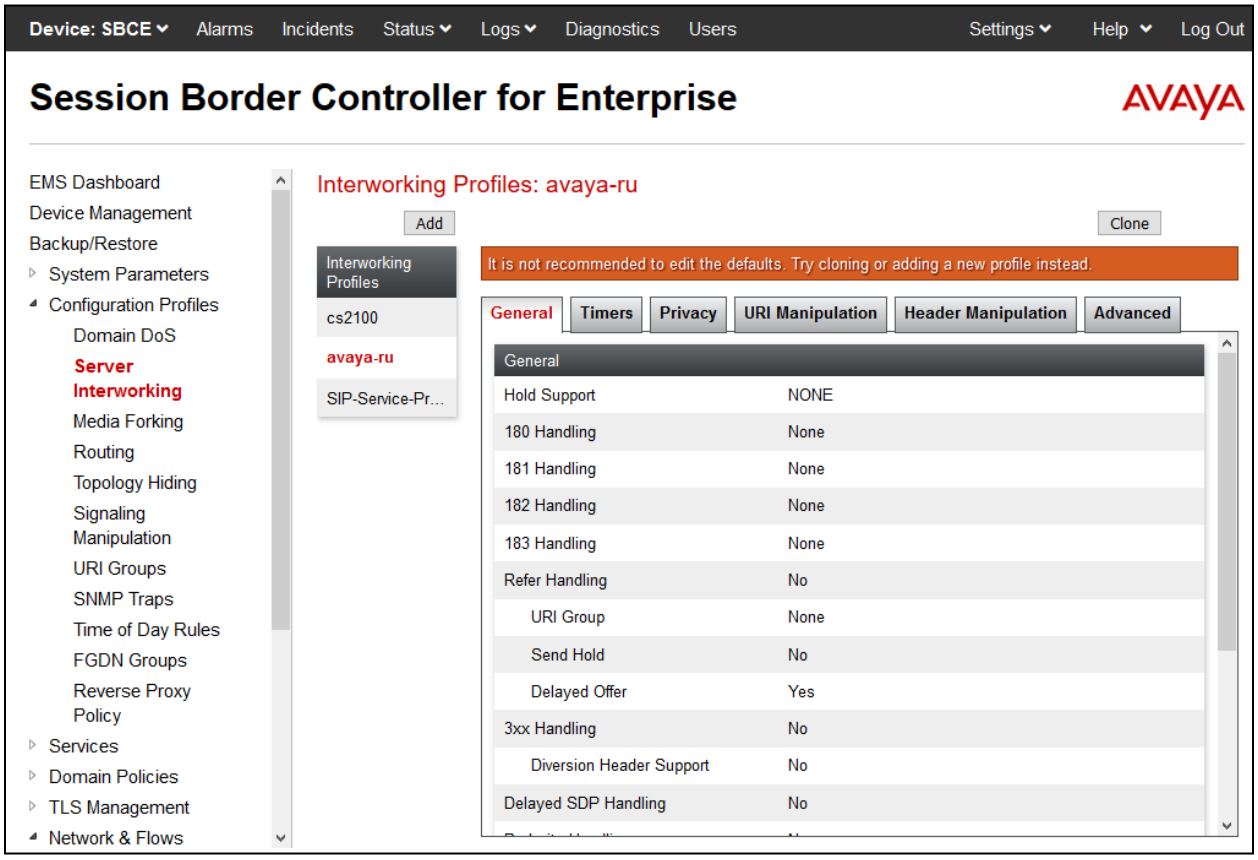
Access the EMS web interface by using the URL "https://ip-address/sbc" in a compatible browser, where "ip-address" is the management IP of the EMS server. Log in using the appropriate credentials.

Note: Select the SBCE in the navigation pane at the top of the browser as indicated by **Device: SBCE** in the window displayed after logging into the EMS Server.

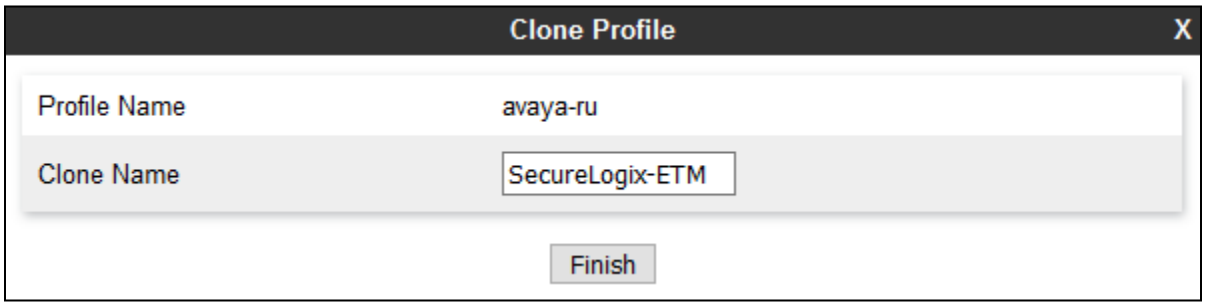
6.2 Configure Server Interworking

Under **Configuration Profiles**, configure a **Server Interworking** profile to specify the SIP protocol implementation used with ETM. Note that an **Interworking Profile** was already configured for the SIP service provider / PSTN side (i.e., public interface).

Navigate to **Configuration Profiles → Server Interworking**. The EMS server displays the **Interworking Profiles** page. Click on **avaya-ru** profile and then click the **Clone** button.



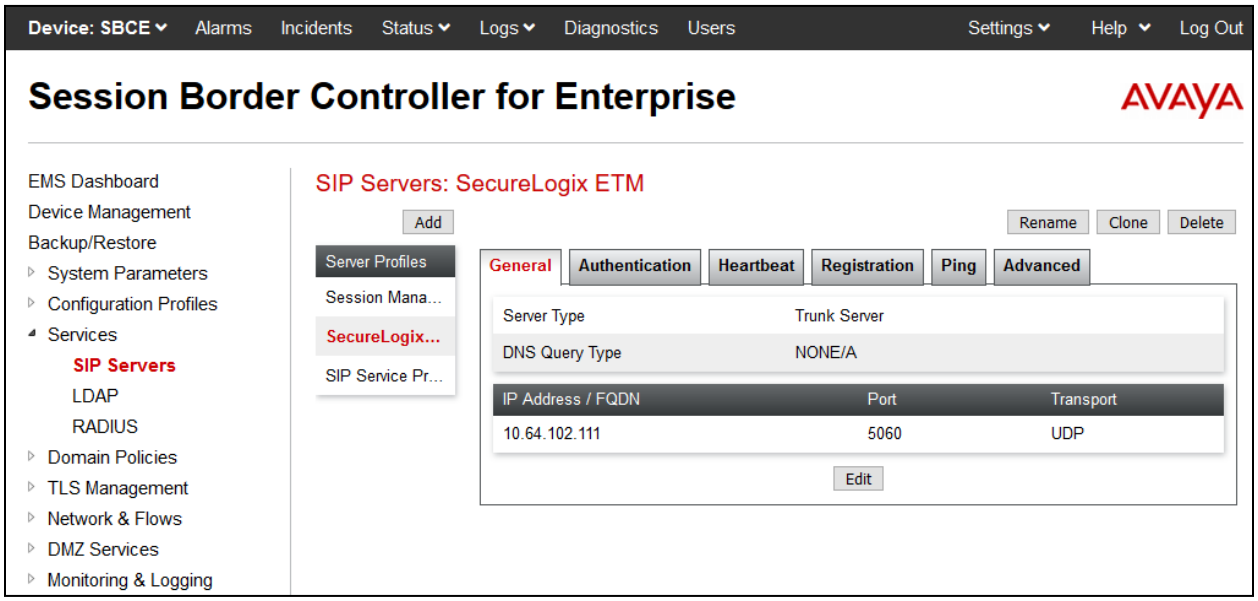
In the **Clone Profile** window, type the profile name in the **Clone Name** field as shown below. Click **Finish**.



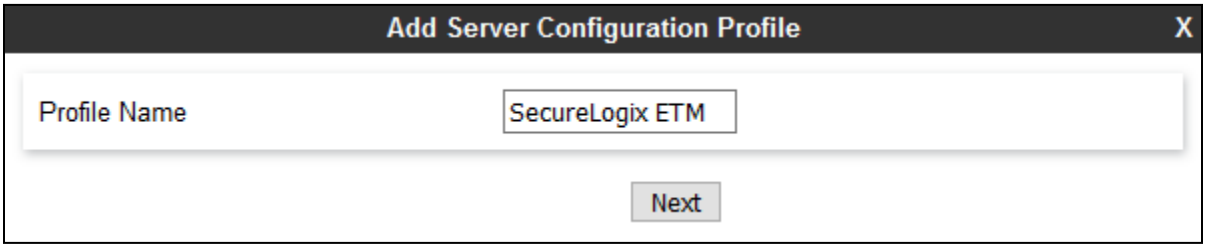
6.3 Configure SIP Servers

Under **Services**, configure **SIP Servers** to create the SBCE SIP trunk to ETM. SIP Servers were created for ETM and the SIP service provider / PSTN (not shown).

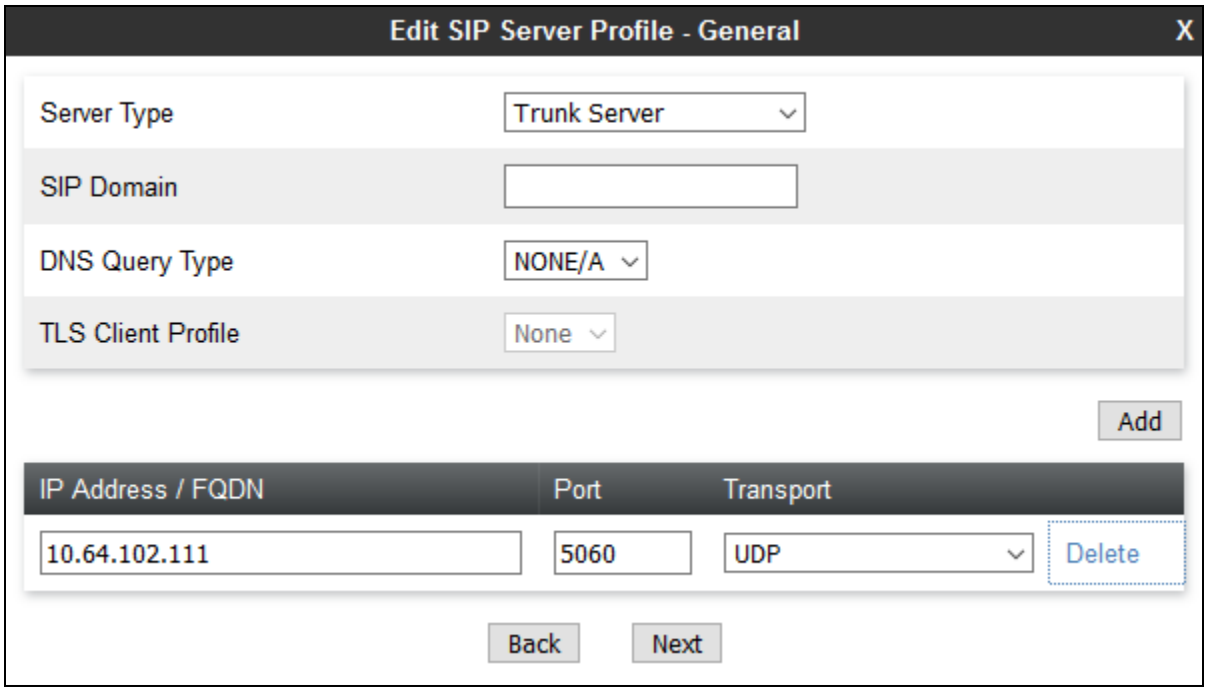
Navigate to **Services → SIP Servers** and then click **Add** to add the ETM SIP trunk.



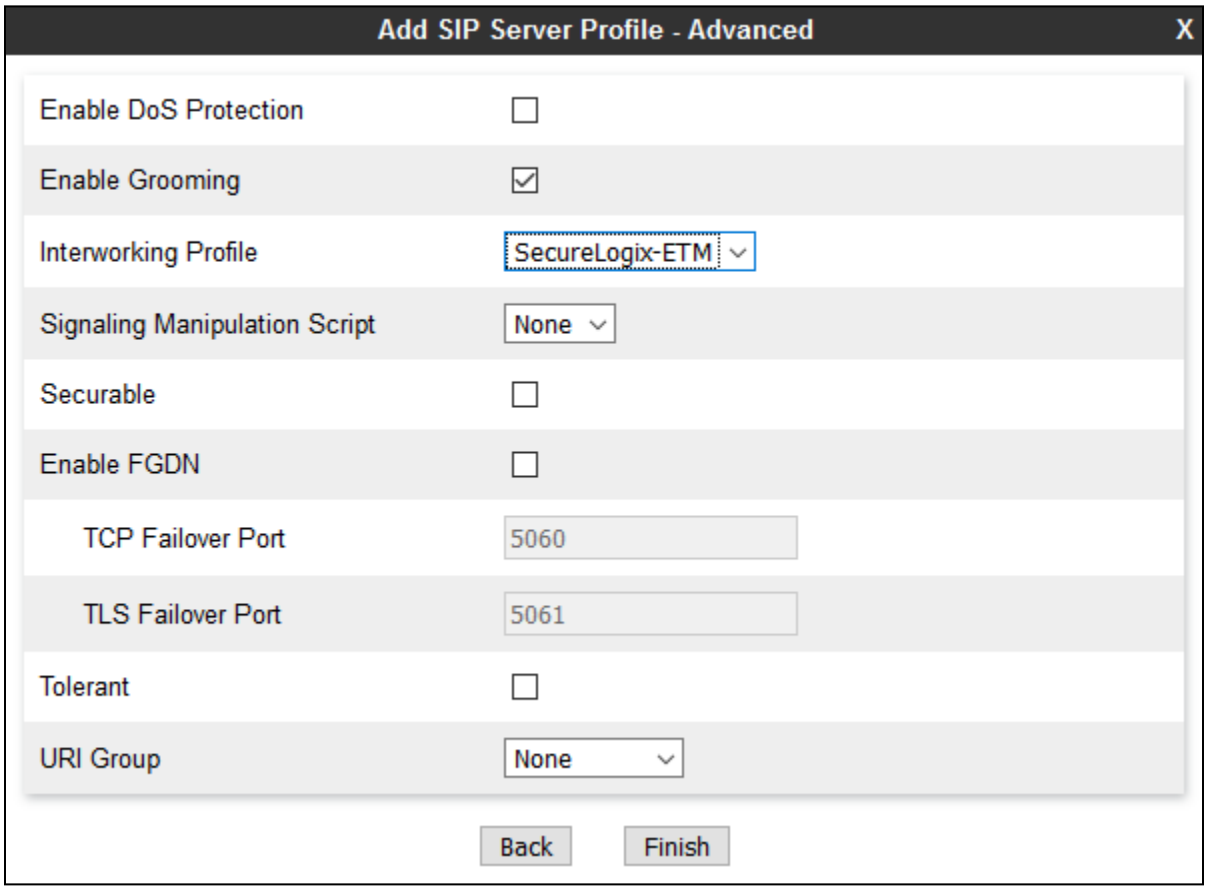
In the **Add Server Configuration Profile** window, type a distinctive **Profile Name** as shown below. Click **Next**.



In the **Edit SIP Server Profile – General** window, set **Server Type** to *Trunk Server* and click **Add**. Set **IP Address / FQDN** to the ETM signaling IP address (e.g., *10.64.102.111*) and the **Transport/Port** fields to *UDP/5060*. Click **Next**. Continue to click **Next** until the **Add SIP Server Profile – Advanced** window is displayed.



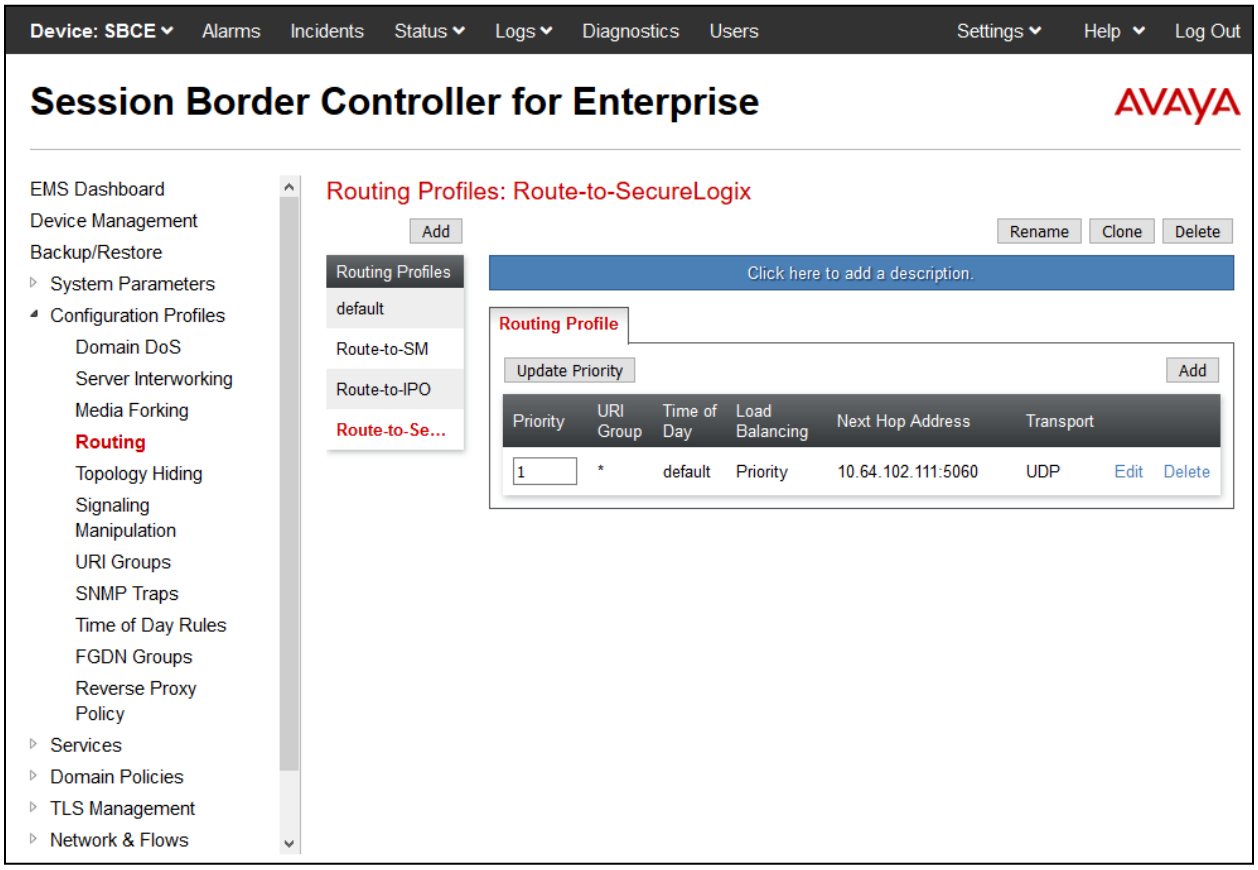
In the **Add SIP Server Profile – Advanced** window, set **Interworking Profile** to the one configured in **Section 6.2**. Click **Finish**.



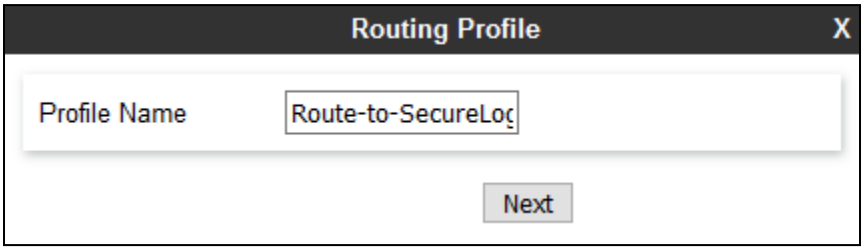
6.4 Configure Routing Profile

Routing profiles define a specific set of routing criteria that is used to determine the path that the SIP traffic will follow as it flows through the SBCE interfaces. **Routing Profiles** were created for ETM and the SIP service provider / PSTN (not shown).

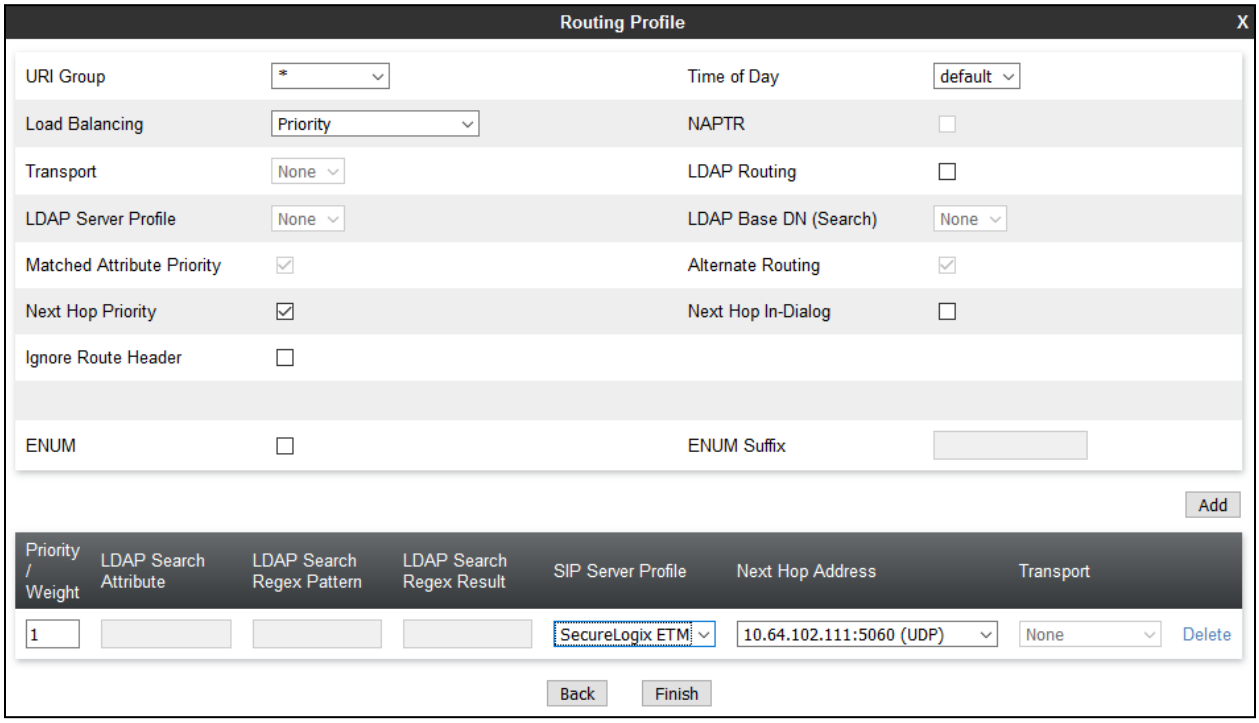
Navigate to **Configuration Profiles → Routing** and click **Add**.



In the **Routing Profile** window, type a distinctive name for the new routing profile. Click **Next**.



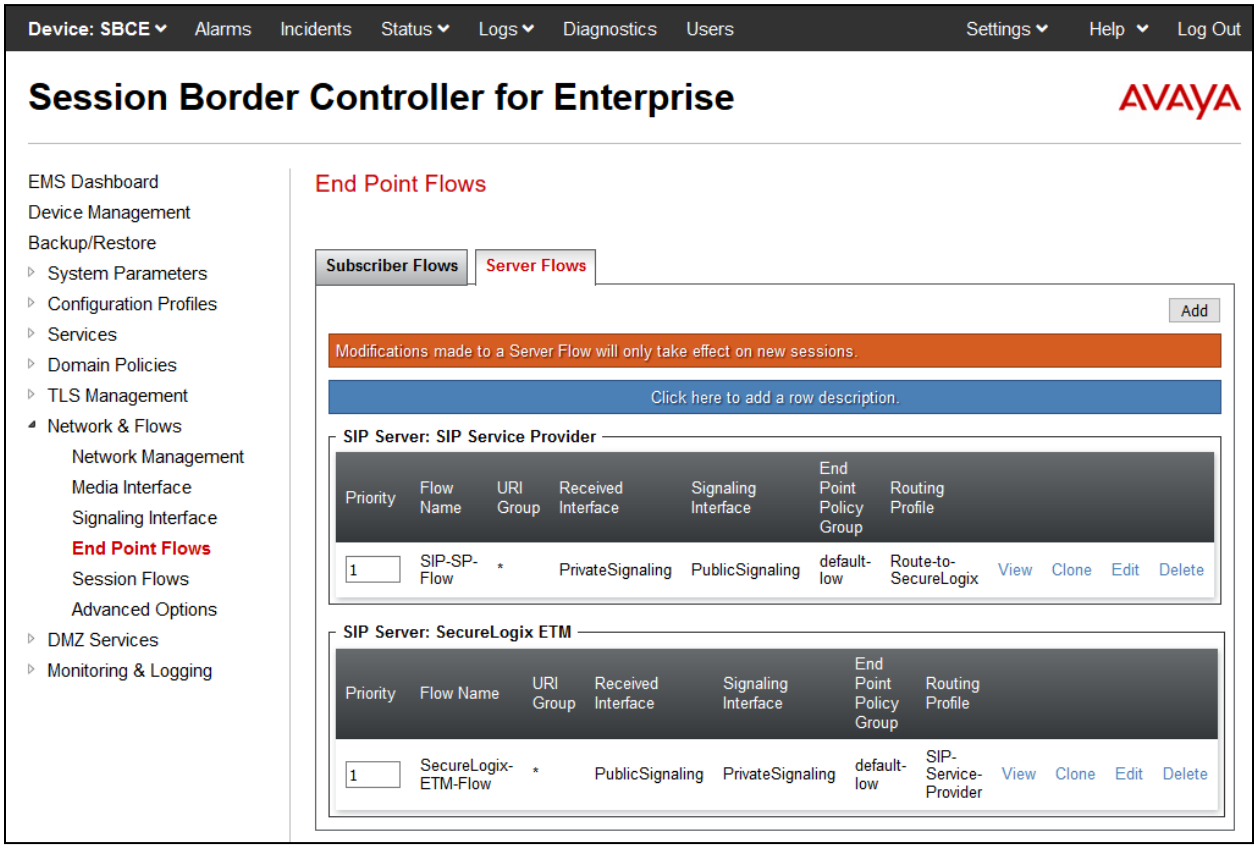
In the **Routing Profile** window, click **Add** to specify the next hop routing information. Specify a **Priority/Weight** and set **SIP Server Profile** to the ETM SIP Server configured in **Section 6.3**. The **Next Hop Address** field is automatically populated. Click **Finish**.



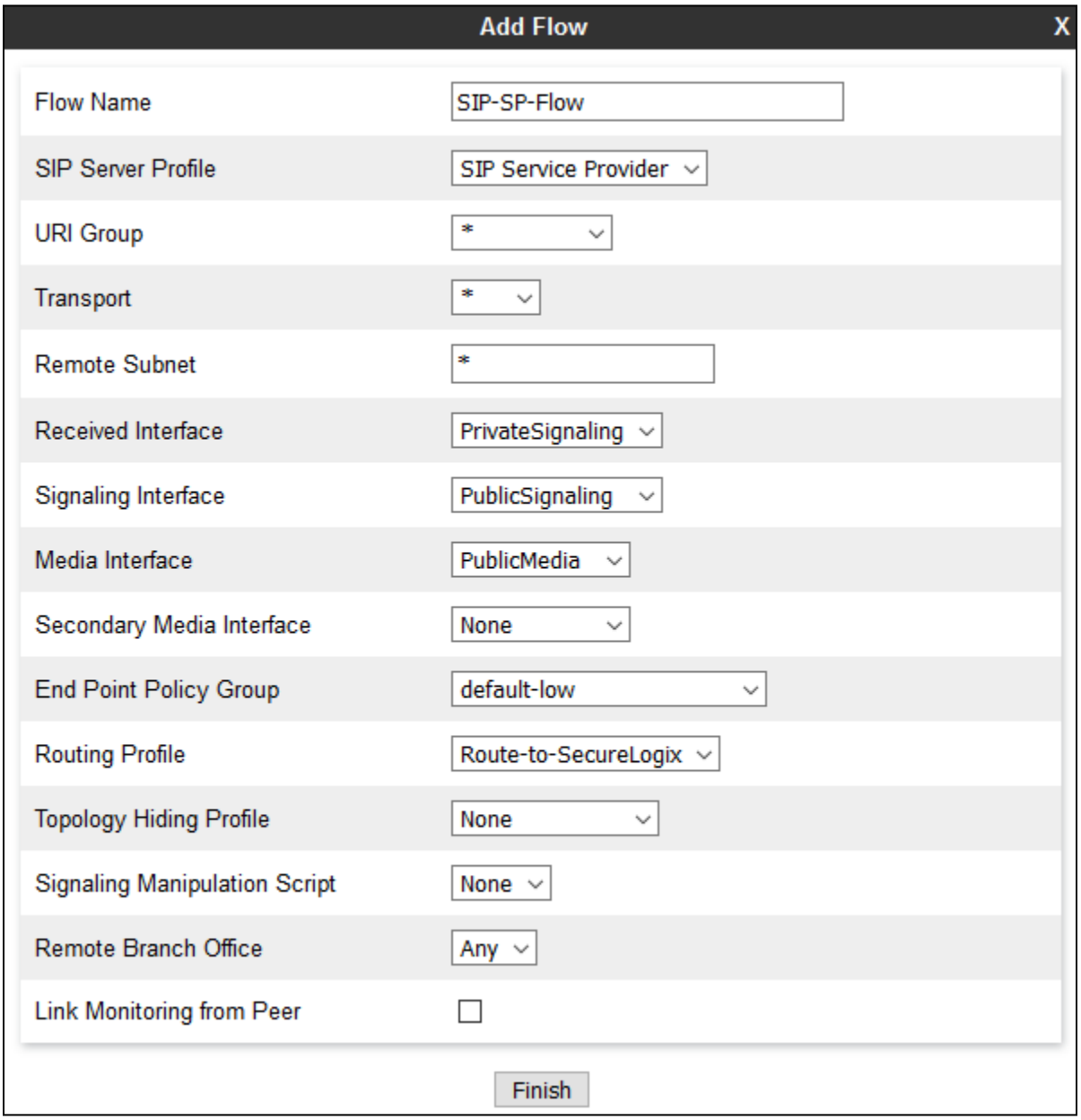
6.5 Configure End Point Flows

With **End Point Flows**, certain parameters that pertain to the signaling and media portions of a call are defined. The call can originate from within the enterprise or outside the enterprise. **End Point Flows** characterize a call through the network. Two **End Point Flows** were created, one for a call flow towards the enterprise or ETM and one for a call flow towards the SIP service provider / PSTN.

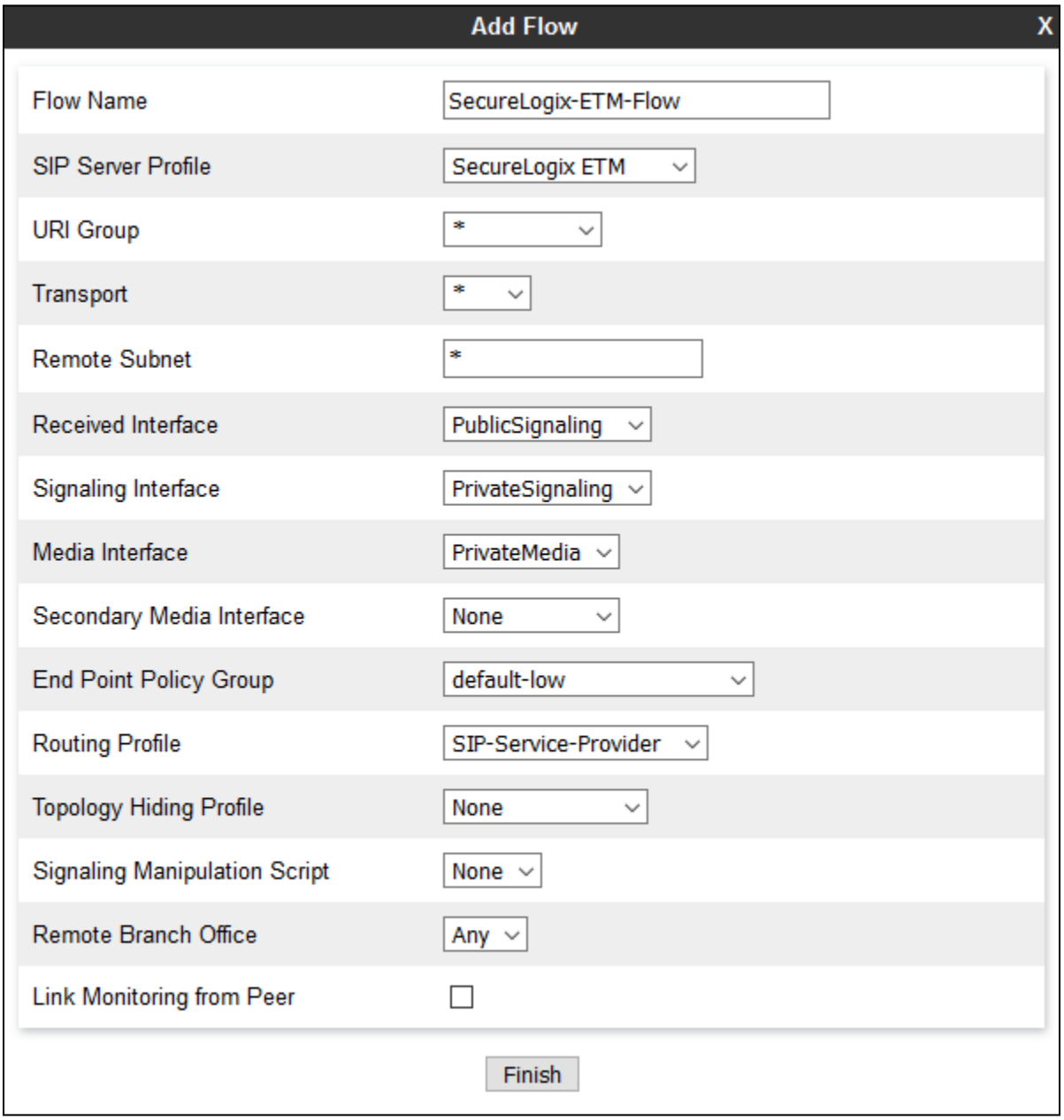
Navigate to **Network & Flows → End Point Flows**. Select the **Server Flows** tab and click **Add** to create a server flow.



The following configuration is for a call flow towards the enterprise. In the **Add Flow** window, specify a **Flow Name** and set **SIP Server Profile** to the one pertaining to the SIP service provider. In the **Received Interface** field, specify the SBCE private signaling interface. Set the **Signaling Interface** and **Media Interface** fields to the SBCE public signaling and public media interfaces, respectively. These SBCE private and public interfaces were not configured as part of these Application Notes. It was assumed that these were already configured. Set the **Routing Profile** to the SecureLogix route configured in **Section 6.4**. Click **Finish**.



The following configuration is for a call flow towards the SIP service provider / PSTN. In the **Add Flow** window, specify a **Flow Name** and set **SIP Server Profile** to the one pertaining to the ETM server. In the **Received Interface** field, specify the SBCE private signaling interface. Set the **Signaling Interface** and **Media Interface** fields to the SBCE public signaling and public media interfaces, respectively. These SBCE private and public interfaces were not configured as part of these Application Notes. It was assumed that these were already configured. Set the **Routing Profile** to the SIP service provider route configured in **Section 6.4**. Click **Finish**.



7 Configure SecureLogix ETM SIP Proxy

This section covers the initial configuration of the ETM Appliance and the SIP trunk configuration via the ETM System Console.

7.1 Initial Configuration of ETM Appliance

The initial configuration of the ETM Appliance is accomplished using the **ETM_5000_configure.pl script**. The function of the script is to create an ETM configuration file based on user responses to questions regarding system configuration. To begin the script execution, log into the ETM Appliance as **root**, change into the **/opt/slc** directory, then execute the main configuration script by typing **./ETM_5000_configure.pl**. The script allows basic host and network configuration information to be specified, such as host name, ETM management IP, ETM signaling IP, and IP address of the ETM Management Server. Below is the **etm_5000_config.txt** configuration file created by the script for the compliance test. Refer to **[5]** for additional information.

```
%CONFIG = (
            'N-ETM.avaya.com' => {
                                    '5100' => '',
                                    'cap' => 'n',
                                    'cm' => 'n',
                                    'cp' => 'y',
                                    'crc' => 'n',
                                    'eth0' => {
                                                'assigned' => 'private #1 eth0',
                                                'ip' => '10.64.102.111',
                                                'ipv6' => 'n',
                                                'ipv6autoconf' => 'n',
                                                'netmask' => '255.255.255.0',
                                                'route' => {}
                                              },
                                    'eth2' => {
                                                'assigned' => 'public #1 eth2',
                                                'ip' => '10.64.102.112',
                                                'ipv6' => 'n',
                                                'ipv6autoconf' => 'n',
                                                'netmask' => '255.255.255.0',
                                                'route' => {}
                                              },
                                    'ha' => 'n',
                                    'mp' => 'y',
                                    'mpha' => 'n',
                                    'ms' => 'y',
                                    'nodenum' => 1,
                                    'priv' => 'eth0',
                                    'publ' => 'eth2',
                                    'sp' => 'y',
                                    'spha' => 'n',
                                    'vlan' => {}
                                  },
            'cpnodename' => 'N-ETM.avaya.com',
            'gateway' => '10.64.102.1',
            'hostname' => 'ETM.avaya.com',
            'ipsec' => 'n',
            'msip' => '52.0.207.36',
            'msport' => 33813,
```

```
            'nameserver' => '0.0.0.0',
            'nonhampnode' => 'N-ETM.avaya.com',
            'nonhaspnode' => 'N-ETM.avaya.com',
            'numhosts' => 1
          );
```

Note: Although ETM was installed as a virtual server, it will be referred to as a *virtual appliance* or simply *appliance* throughout this section.

7.2 SIP Trunk Confguration via ETM System Console

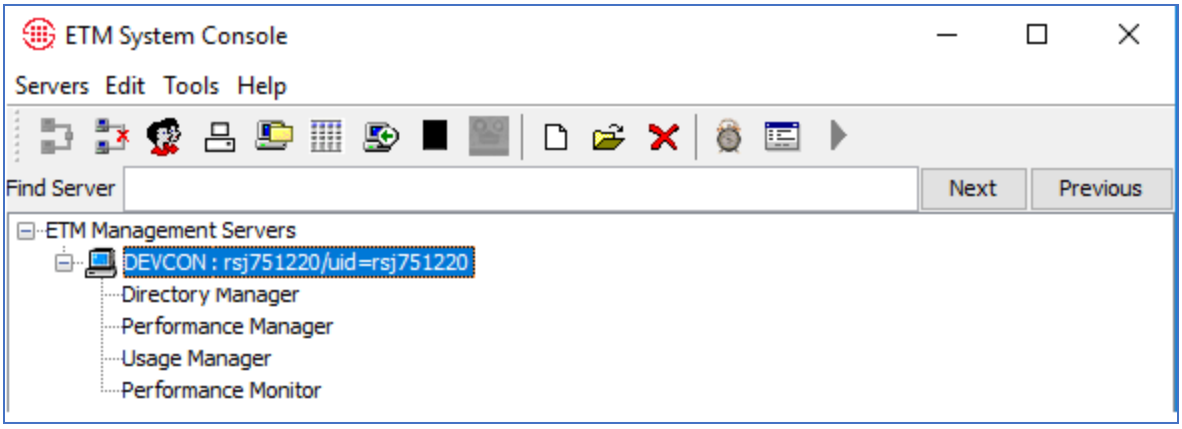
This section covers the SIP trunk configuration via the ETM System Console. This procedure covers the following areas:

- Launch ETM System Console
- Card Configuration
- Span Configuration
- Telco Configuration

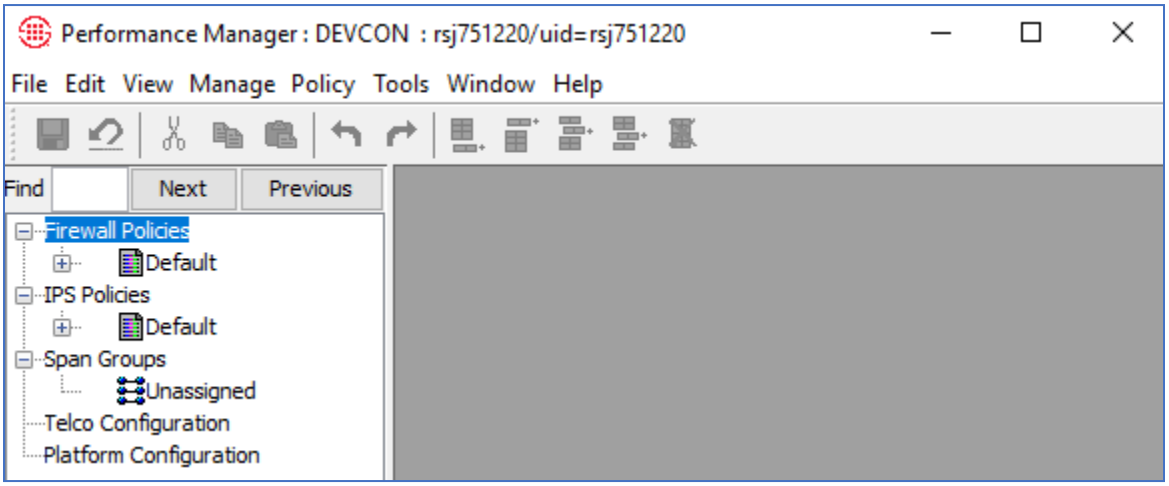
7.2.1 Launch ETM System Console

Launch the **ETM System Console**. The **ETM System Console** window is displayed as shown below. It is assumed that the ETM management server object (e.g., *DEVCON*) has already been created. Connect to the selected ETM management server and log in with the appropriate credentials (not shown).

From the **ETM System Console**, open the **Performance Manager**.

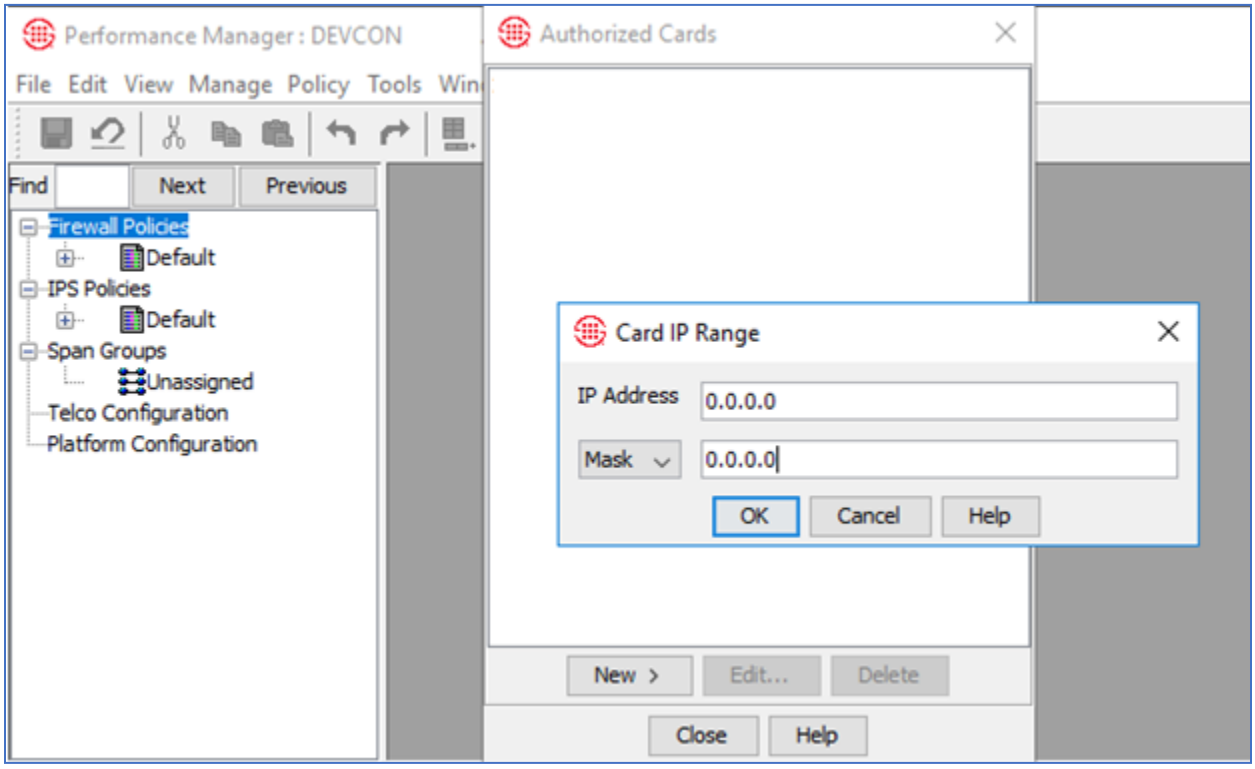


In the **Performance Manager** window, right-click on **Platform Configuration** and select **Manage → Authorized Cards** from the pop-up menu (not shown) to configure the ETM Appliance Card.

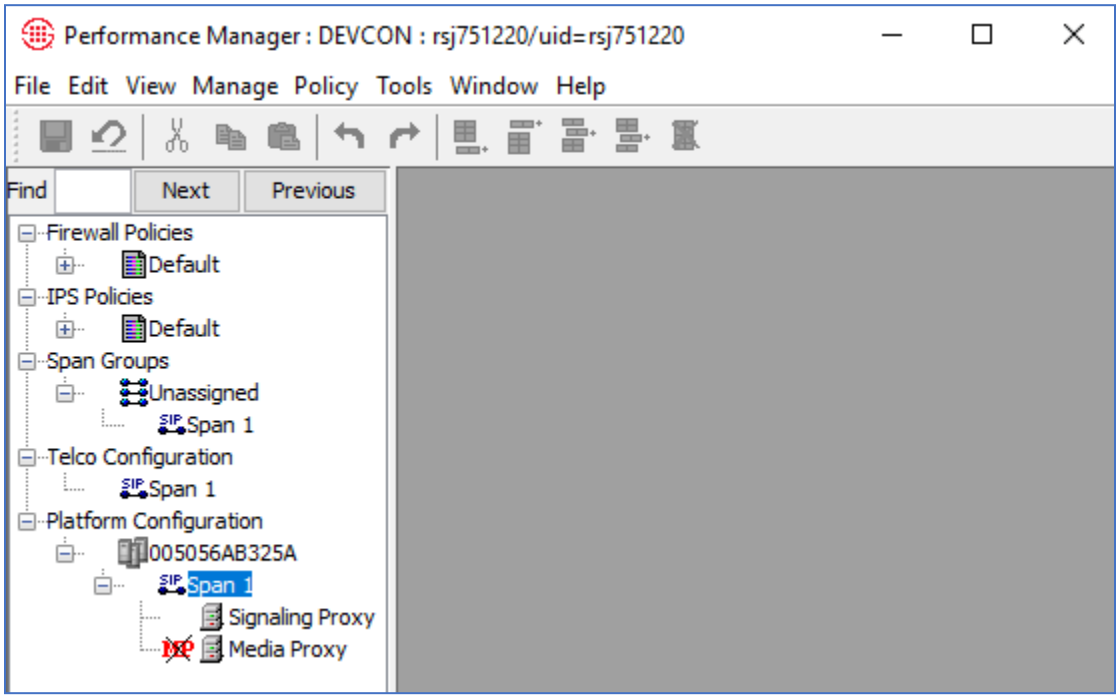


7.2.2 Card Configuration

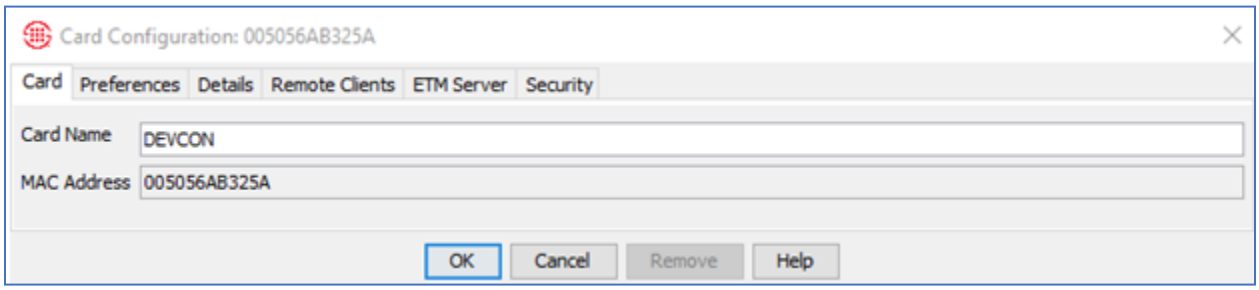
In the **Authorized Cards**, click **New** and select **IP Range** (not shown). By configuring an IP Range as shown below, it allows all ETM Appliances to connect to the ETM Management Server. Alternatively, a specific subnet or individual device IP address could have been specified to restrict access.



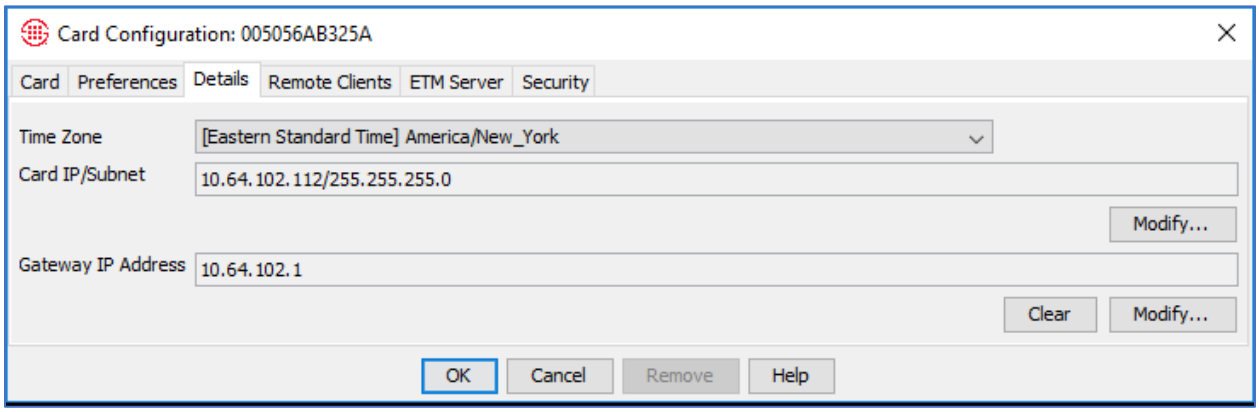
Once the **Authorized Card** is configured, the ETM Appliance can connect to the ETM Management Server. The ETM Appliance Card appears under **Platform Configuration** and is labeled with a MAC address as shown below.



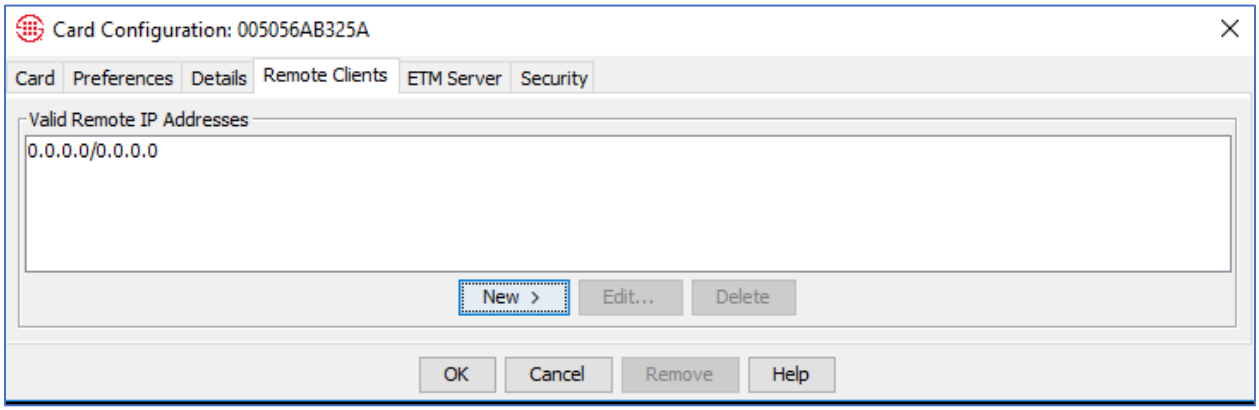
Right-click on the Card and select **Edit Card(s)** to configure the Card (not shown). In the **Card** tab, a **Card Name** can be provided as shown below.



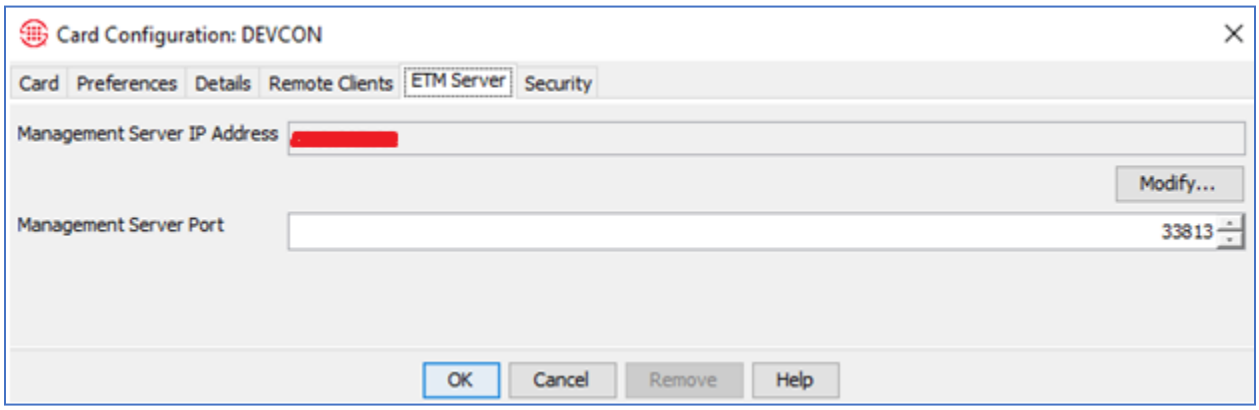
In the **Details** tab, specify the time zone. The **Card IP/Subnet** displays the management IP of the ETM Appliance configured in **Section 7.1**.



In the **Remote Clients** tab, provide remote IP addresses or IP range to allow SSH to ETM Appliances.

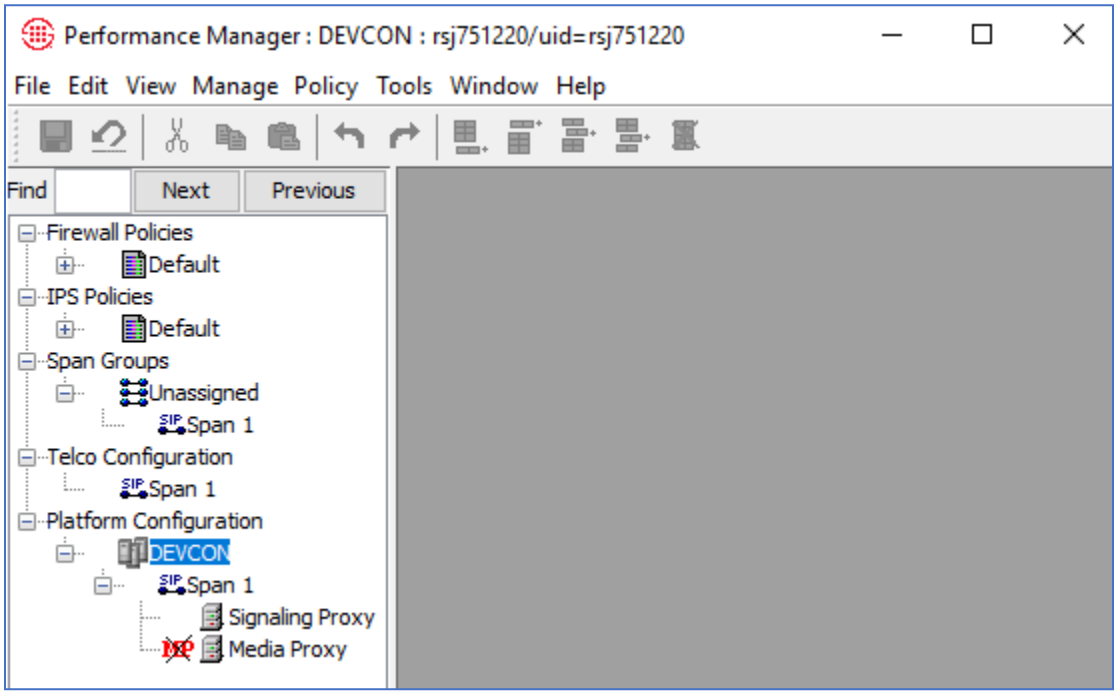


The ETM Server tab, shows the Management Server IP Address, which was configured in the ETM Appliance in **Section 7.1**. No configuration is required. The IP address is masked for security reasons.

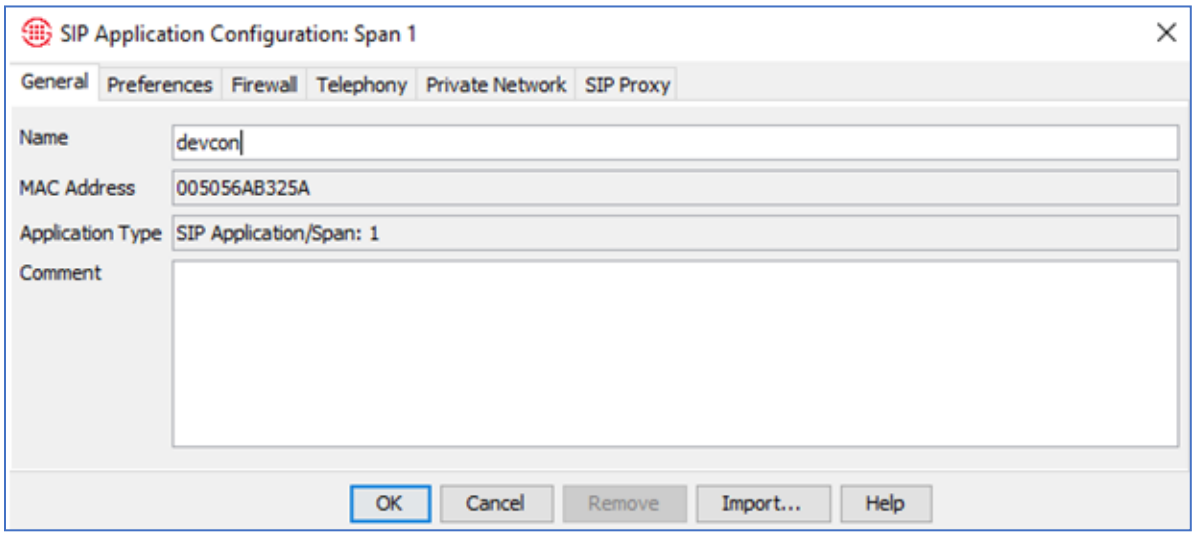


7.2.3 Span Configuration

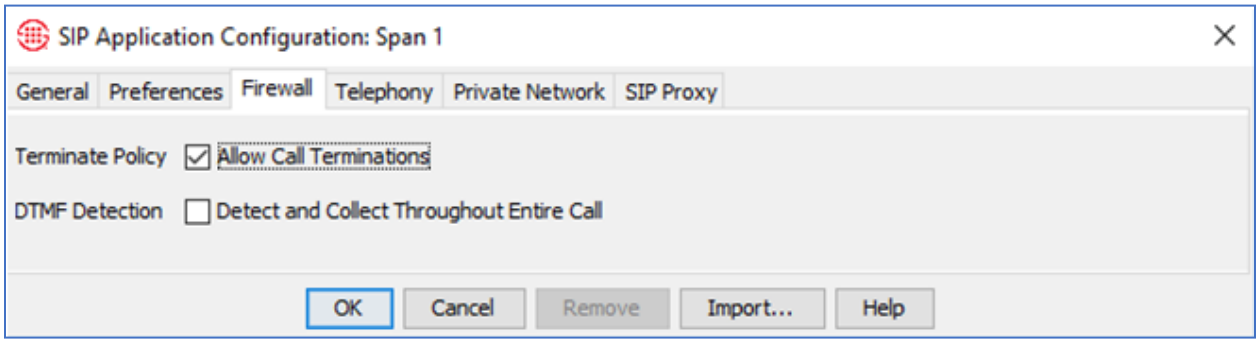
Right-click on **Span 1** under **Platform Configuration** and select **Edit Span(s)** from the pop-up menu (not shown) to configure the SIP trunk.



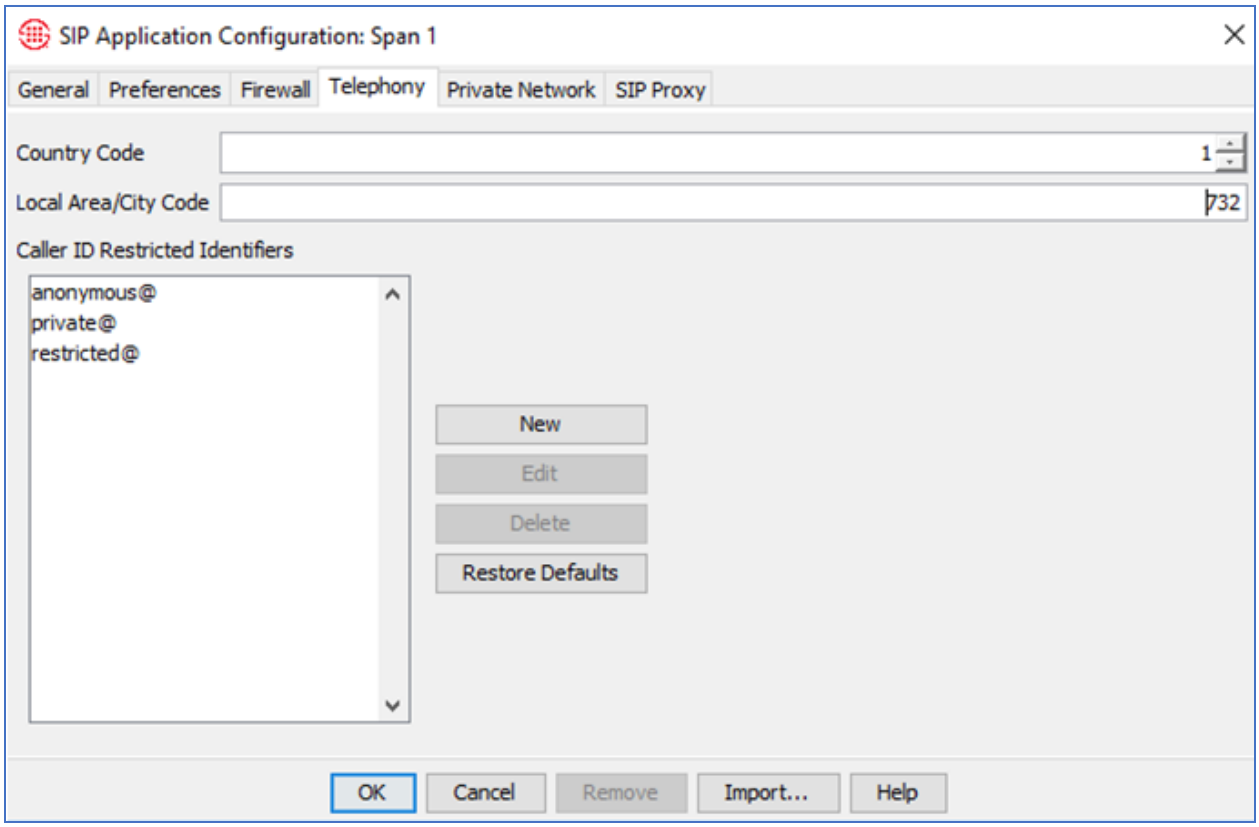
The **SIP Application Configuration: Span 1** window is displayed. In the **General** tab, provide a descriptive name for the span.



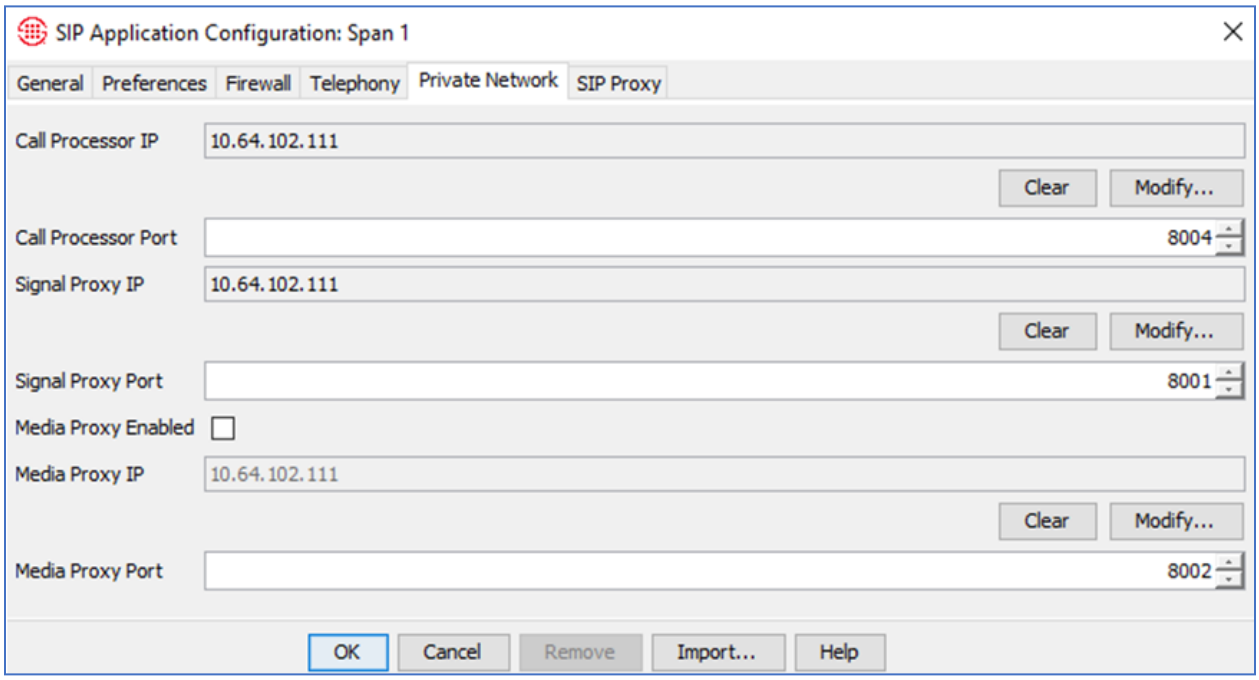
In the **Firewall** tab, enable **Allow Call Terminations** to allow firewall policies to terminate calls when necessary.



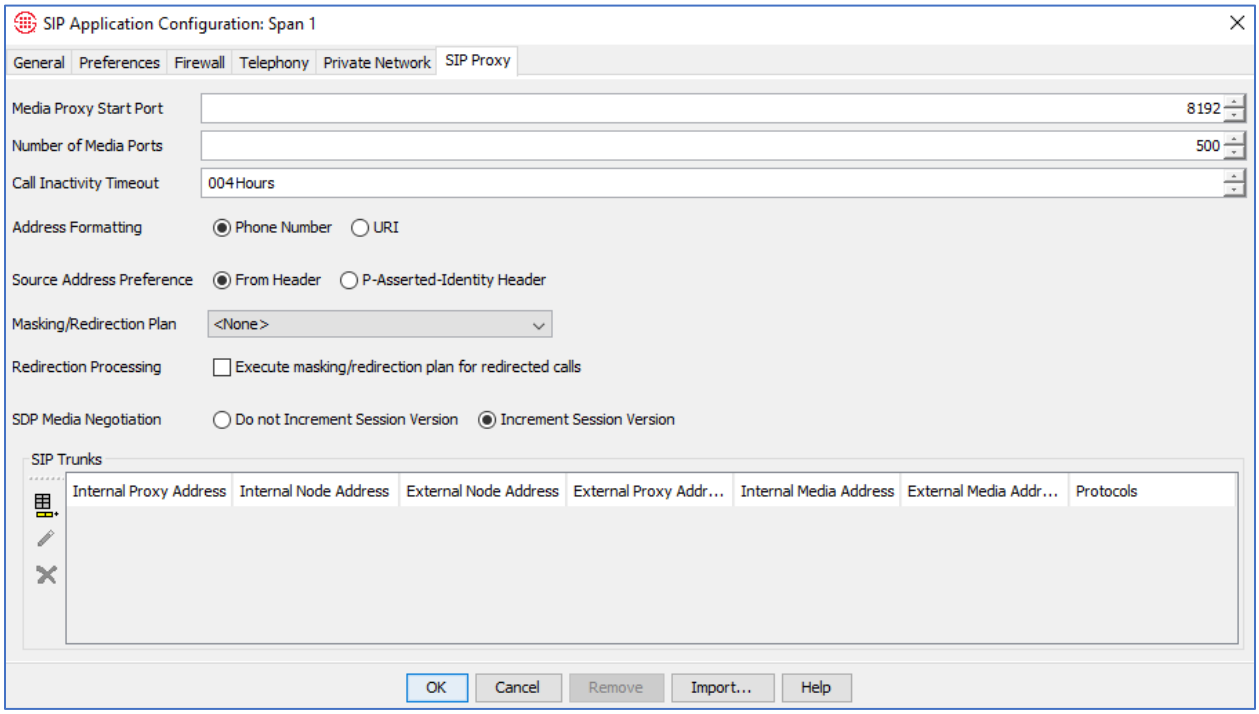
In the **Telephony** tab, enter the **Local Area/City Code**.



In the **Private Network** tab, verify that the settings were successfully received from the ETM Appliance. No configuration required.



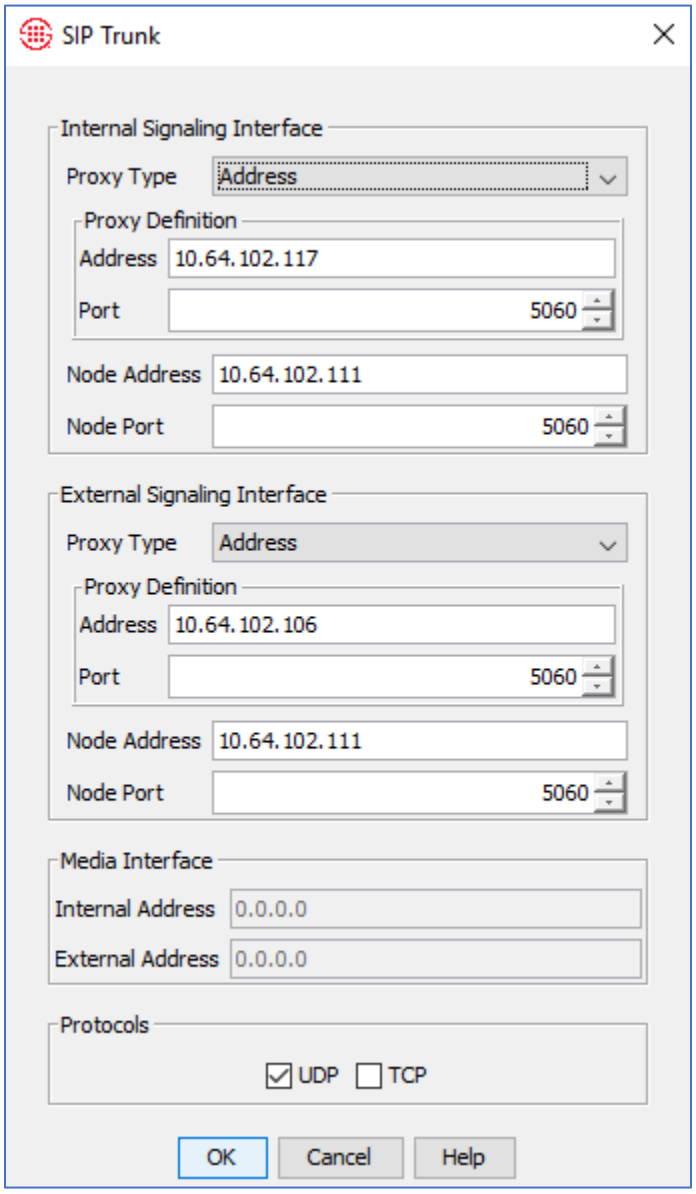
In the **SIP Proxy** tab, accept the default values shown below and configure the SIP trunk by clicking on the **Add trunk** icon in the **SIP Trunks** section.



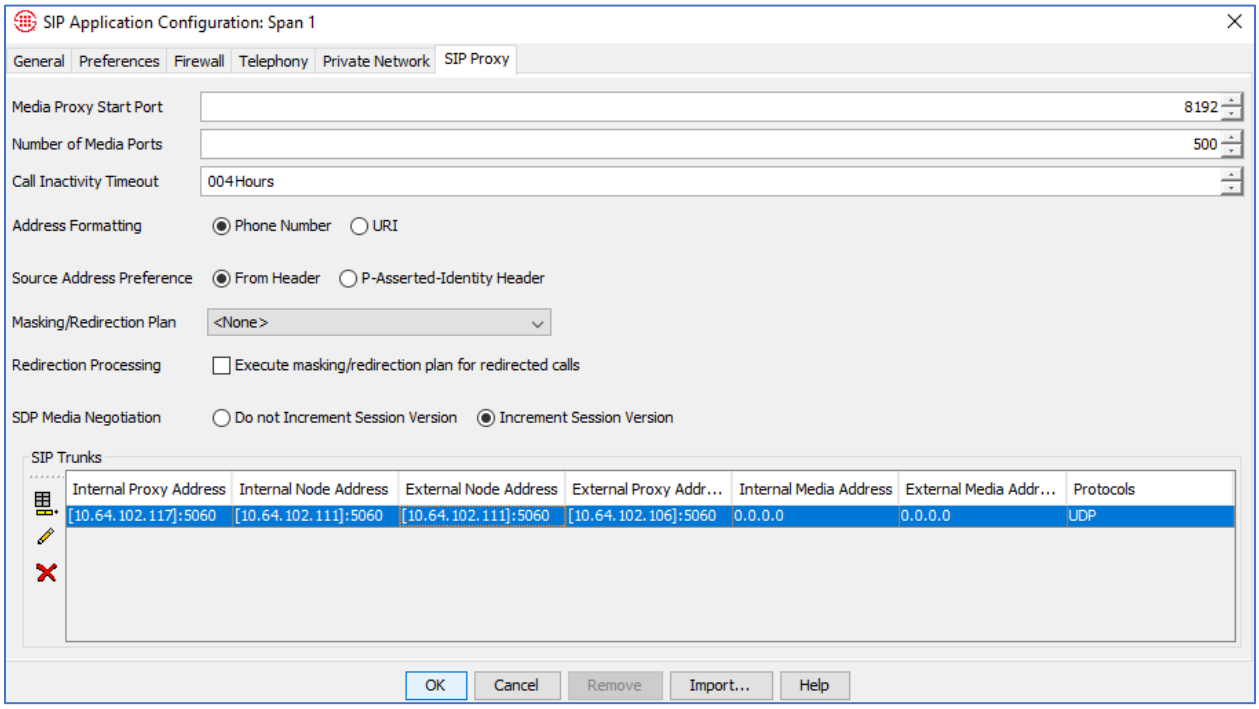
Configure the **SIP Trunk** as follows. In the **Internal Signaling Interface** section, configure the Session Manager side of the SIP trunk. Under **Proxy Definition**, set the **Address** to the Session Manager signaling IP address (e.g., *10.64.102.117*) and the **Port** to *5060*. Set the **Node Address** to the ETM Appliance signaling IP address and the **Node Port** to *5060*.

In the **External Signaling Interface** section, configure the SBCE side of the SIP trunk. Under **Proxy Definition**, set the **Address** to the SBCE private IP address (e.g., *10.64.102.106*) and the **Port** to *5060*. Set the **Node Address** to the ETM Appliance signaling IP address and the **Node Port** to *5060*.

In the **Protocols** section, select *UDP*.

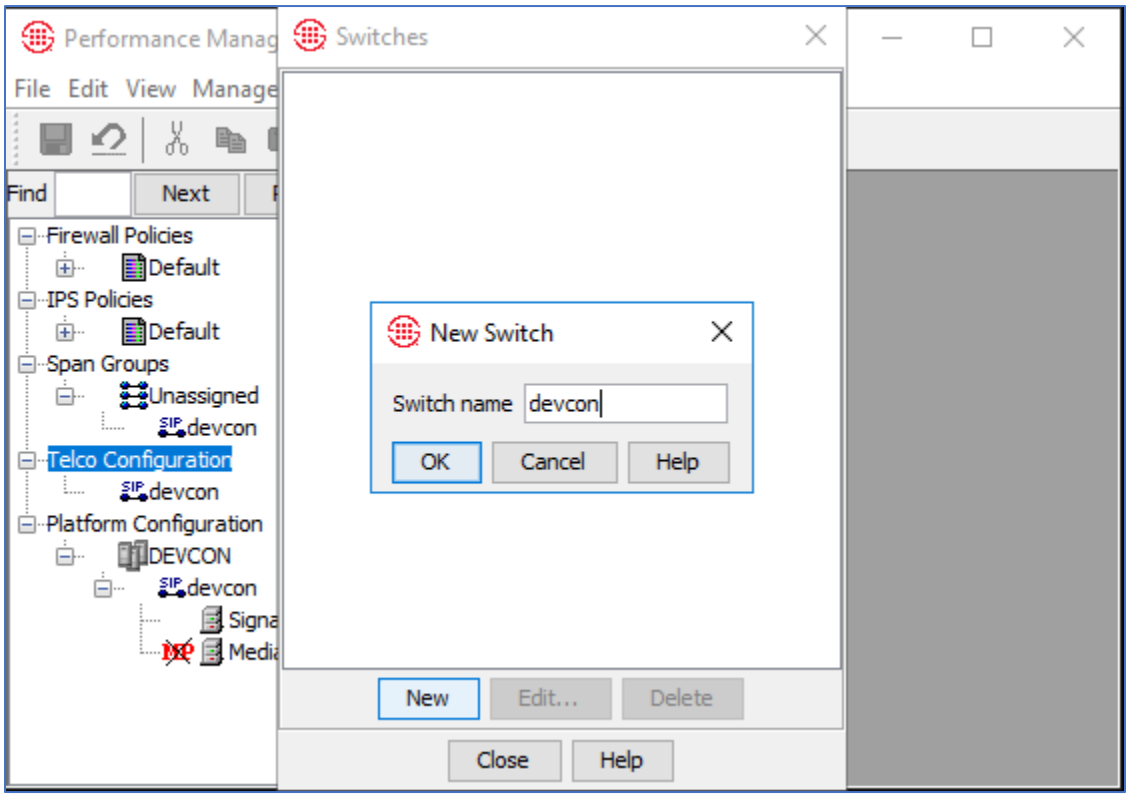


The configured SIP trunk is shown below.

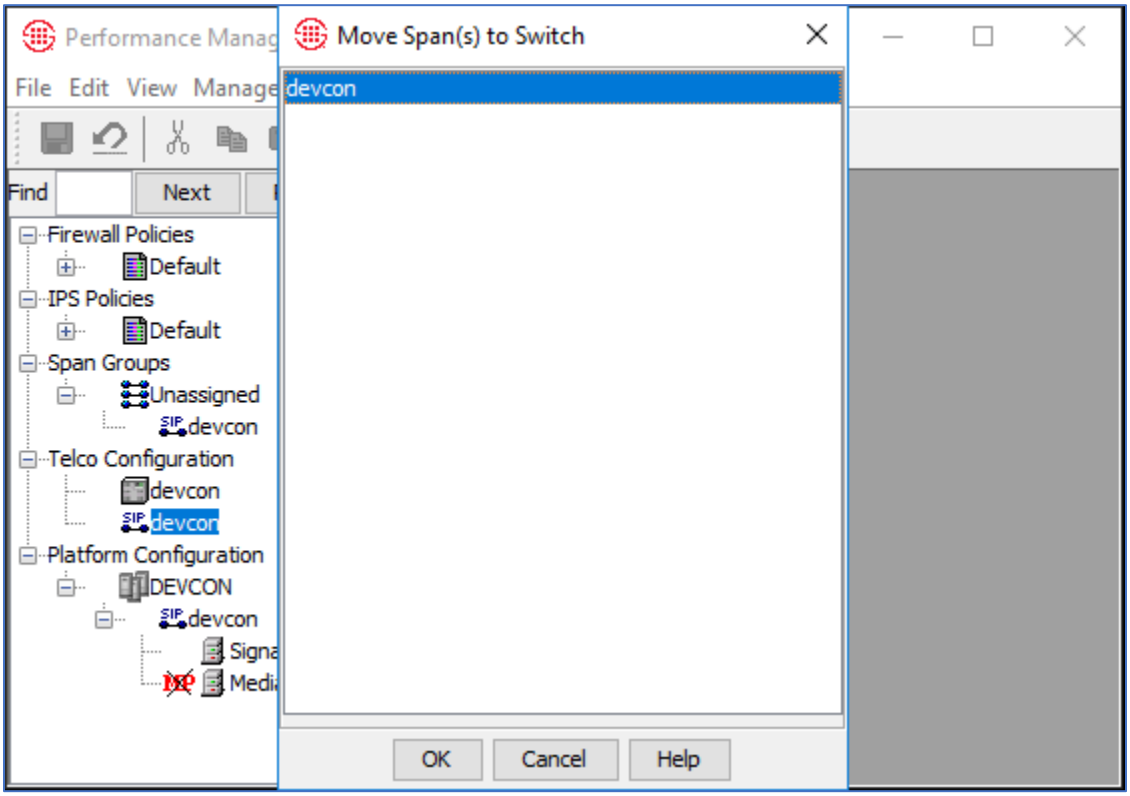


7.2.4 Telco Configuration

In the **Performance Manager** window, right-click on **Telco Configuration** and select **Manage Switches** (not shown). In the **Switches** window, click **New** and enter a switch name (e.g., *devcon*) as shown below.

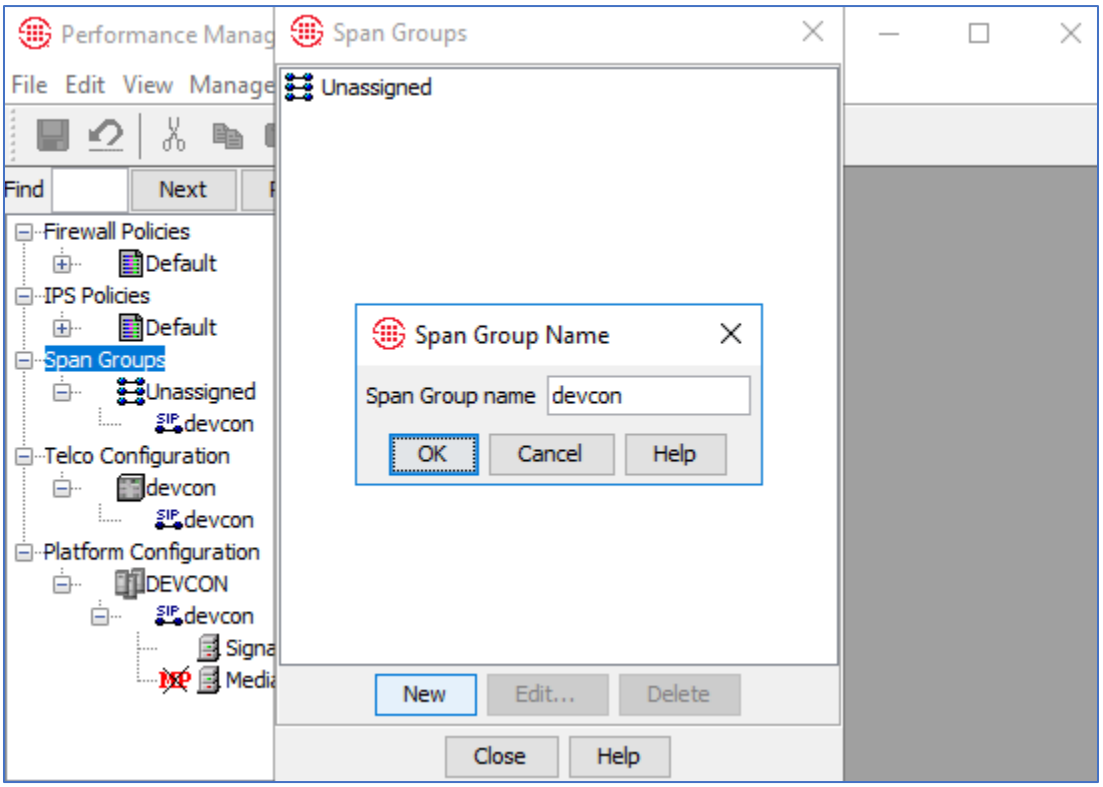


Under **Telco Configuration**, right-click on the *devcon* span and select **Move Span(s) → To Switch** (not shown) to move the span to the switch that was created above. In the **Move Span(s) to Switch** window, select the *devcon* switch.

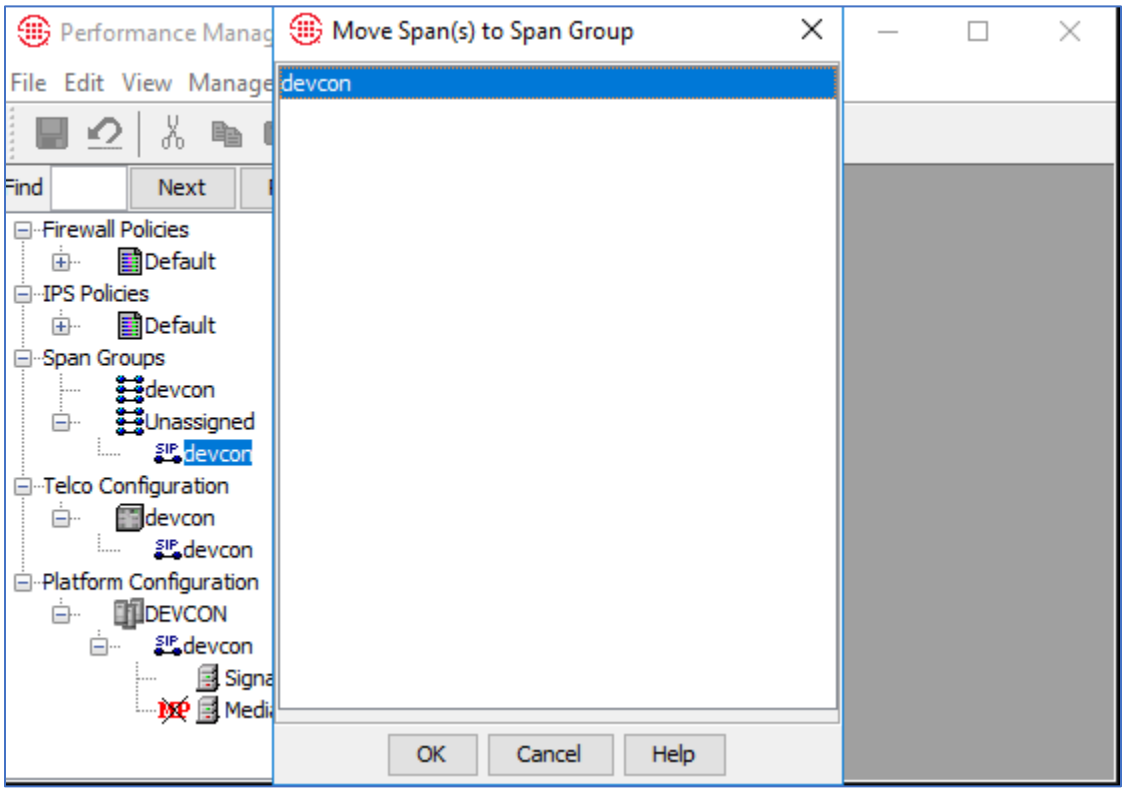


7.2.5 Span Group Configuration

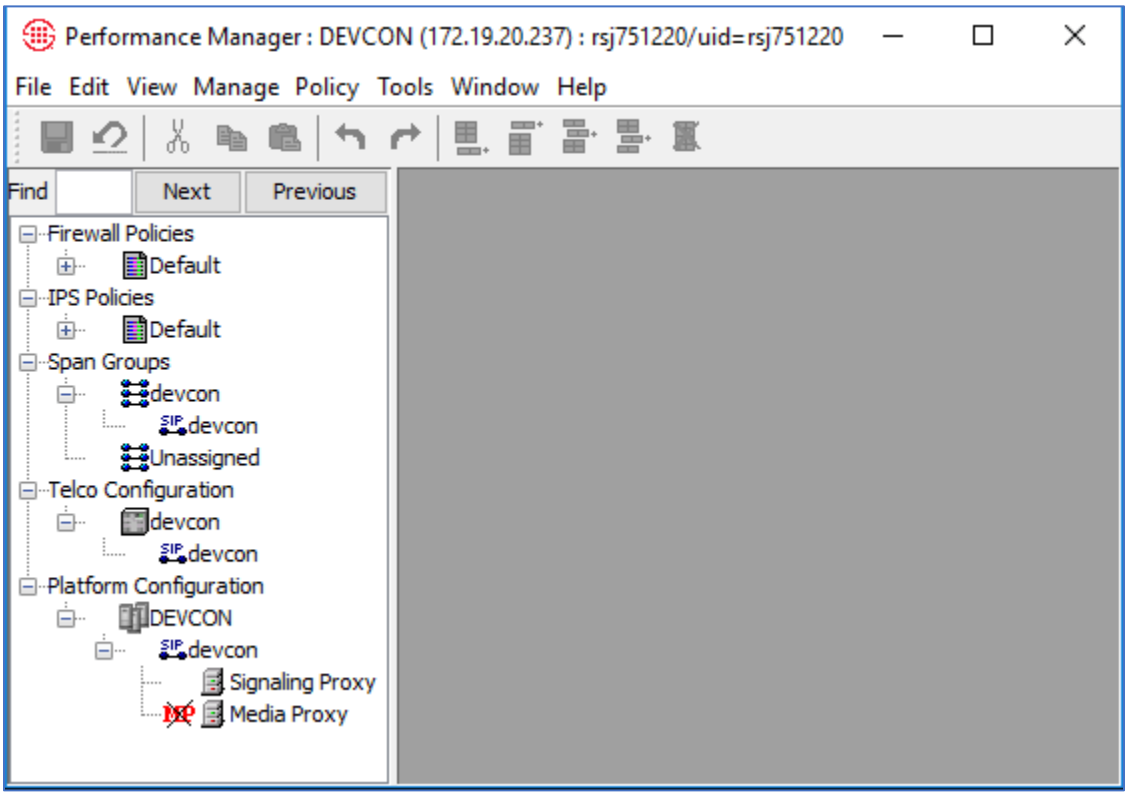
Right-click on **Span Groups** in the **Performance Manager** and select **Manage Span Groups** (not shown) to create a span group. In the **Span Groups** window, click **New**. Enter a **Span Group name** as shown below.



Move the *devcon* span to the **Span Group**. Right-click on span and select **Move Span(s)** (not shown). In the **Move Span(s) to Span Group** window, select the *devcon* span.



After the **Span** (i.e., SIP trunk), **Telco** switch, and **Span Group** have been configured, the **Performance Manager** appears as shown below.



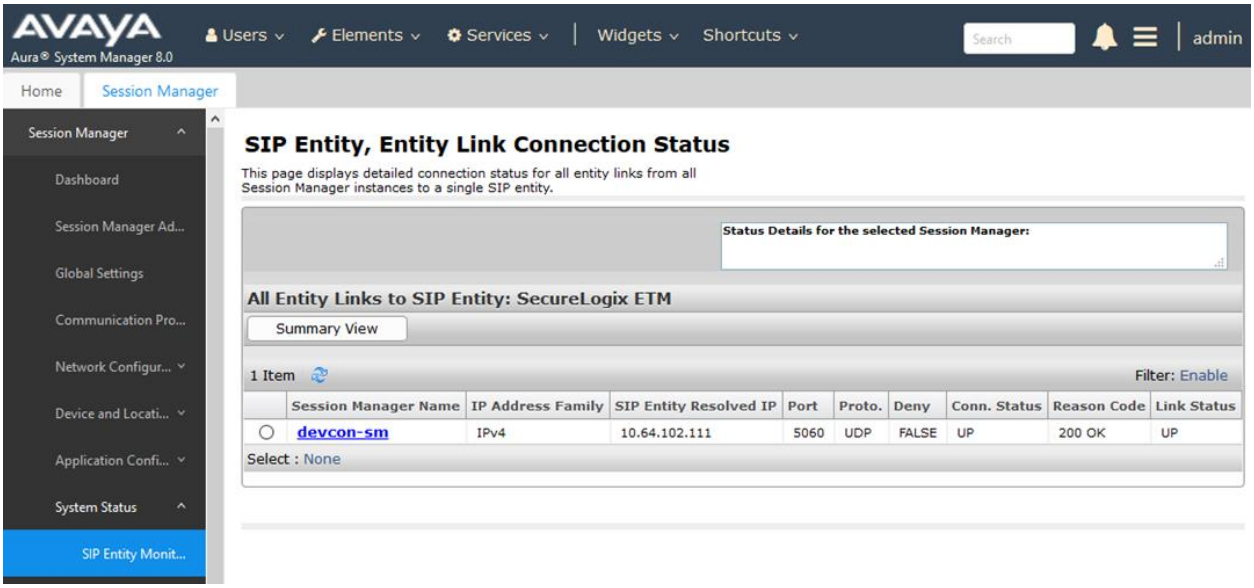
7.2.6 Firewall and IPS Policy Configuration

Firewall and IPS Policy configuration is outside the scope of these Application Notes. Refer to **[7]** for configuration information.

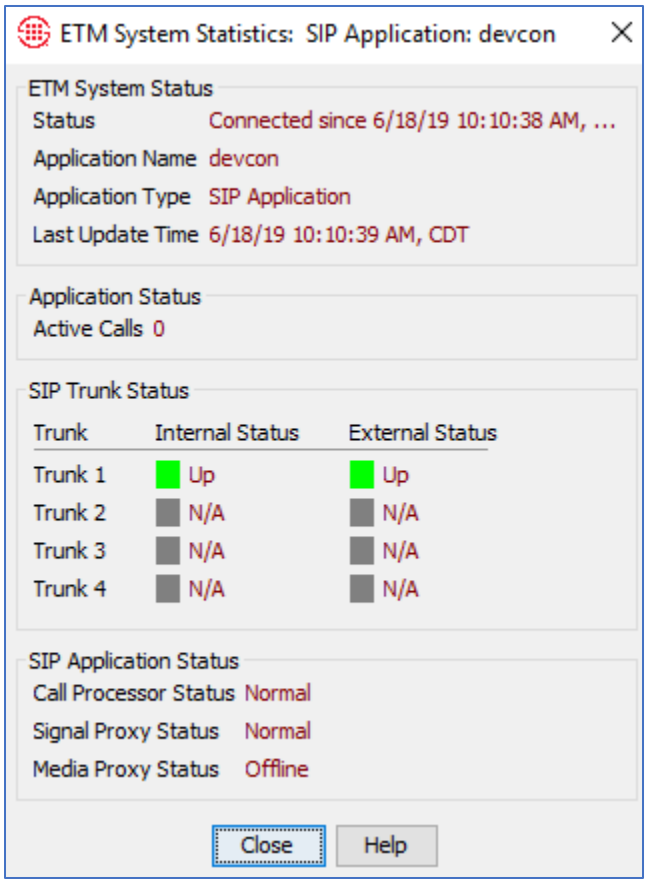
8 Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Session Manager, Avaya Session Border Controller for Enterprise, and SecureLogix ETM SIP Proxy.

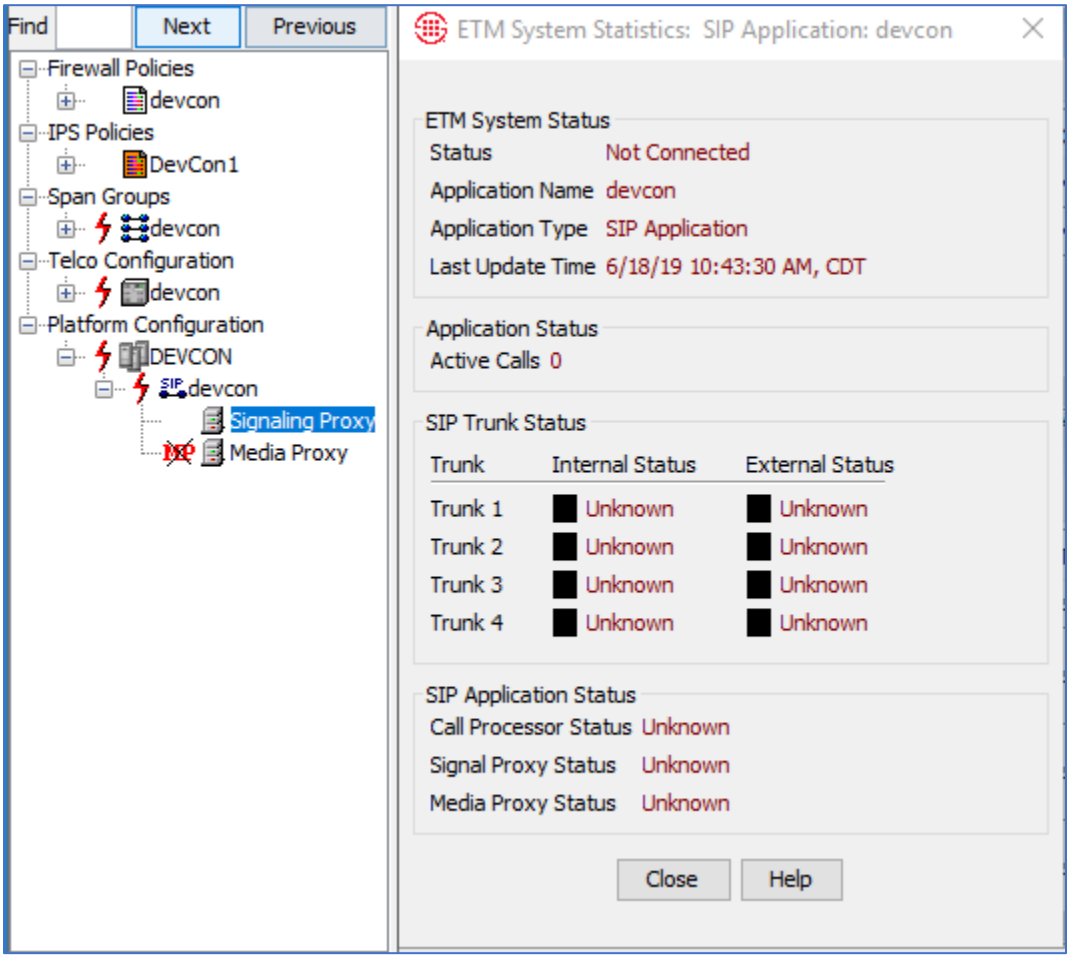
1. The connection status of the SIP trunk between Session Manager and ETM may be viewed on System Manager by navigating to **Elements → Session Manager → System Status → SIP Entity Monitoring** and clicking on the appropriate SIP entity. Below is the status of the SIP trunk to ETM. The **Conn. Status** should be *UP*.



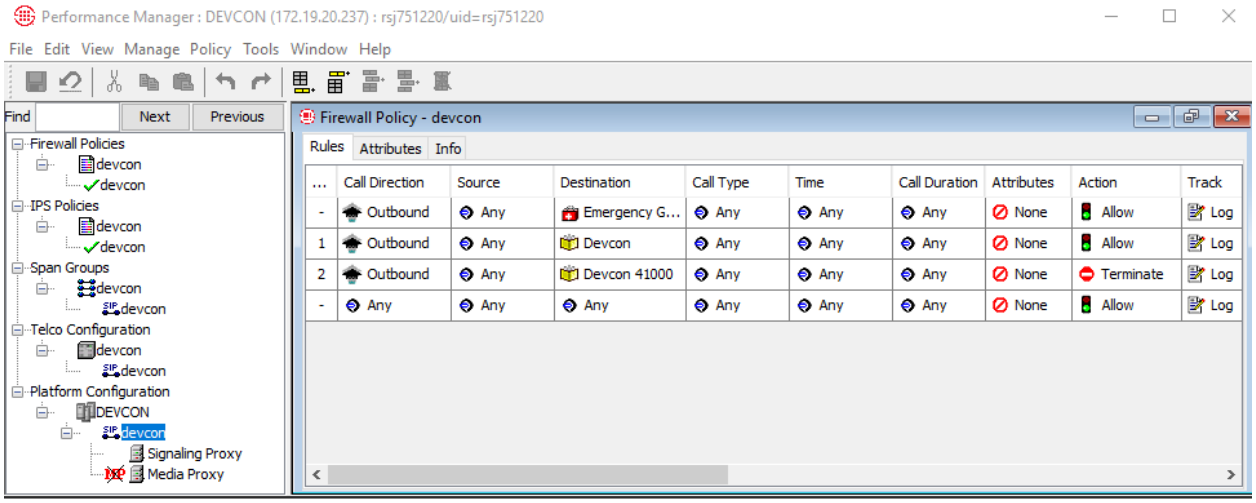
2. Alternatively, the SIP trunk status may be viewed on the **ETM System Console**. From the **Performance Manager**, right-click on the span (i.e., SIP trunk) under **Platform Configuration** and select **Health & Status**. The **Internal Status** and **External Status** should be *Up*.

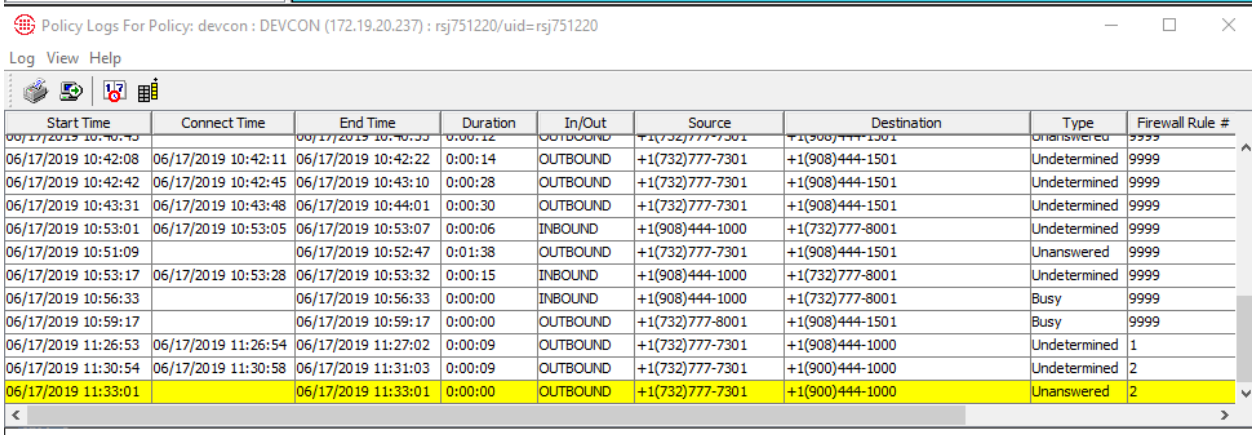


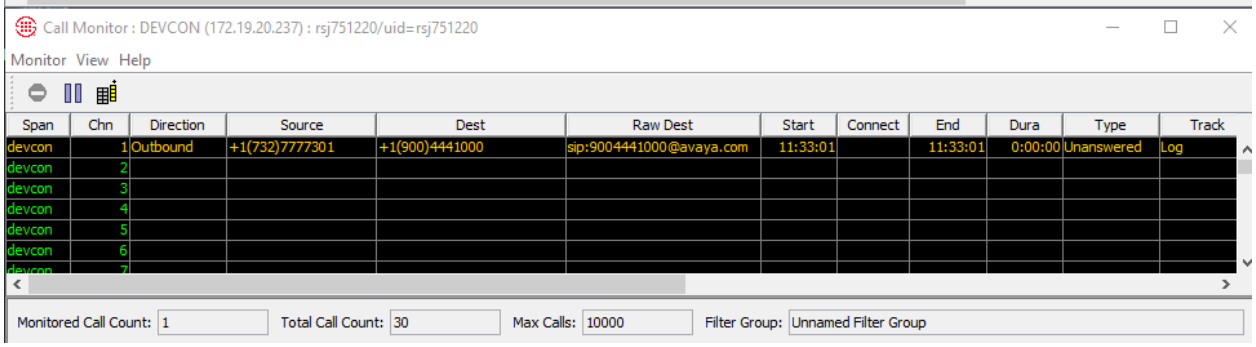
Note that if the ETM Appliance is not connected to the ETM Management Server, a red lightning bolt will appear in the navigation pane of the ETM System Console and the SIP trunk status would be *Unknown* as shown below.



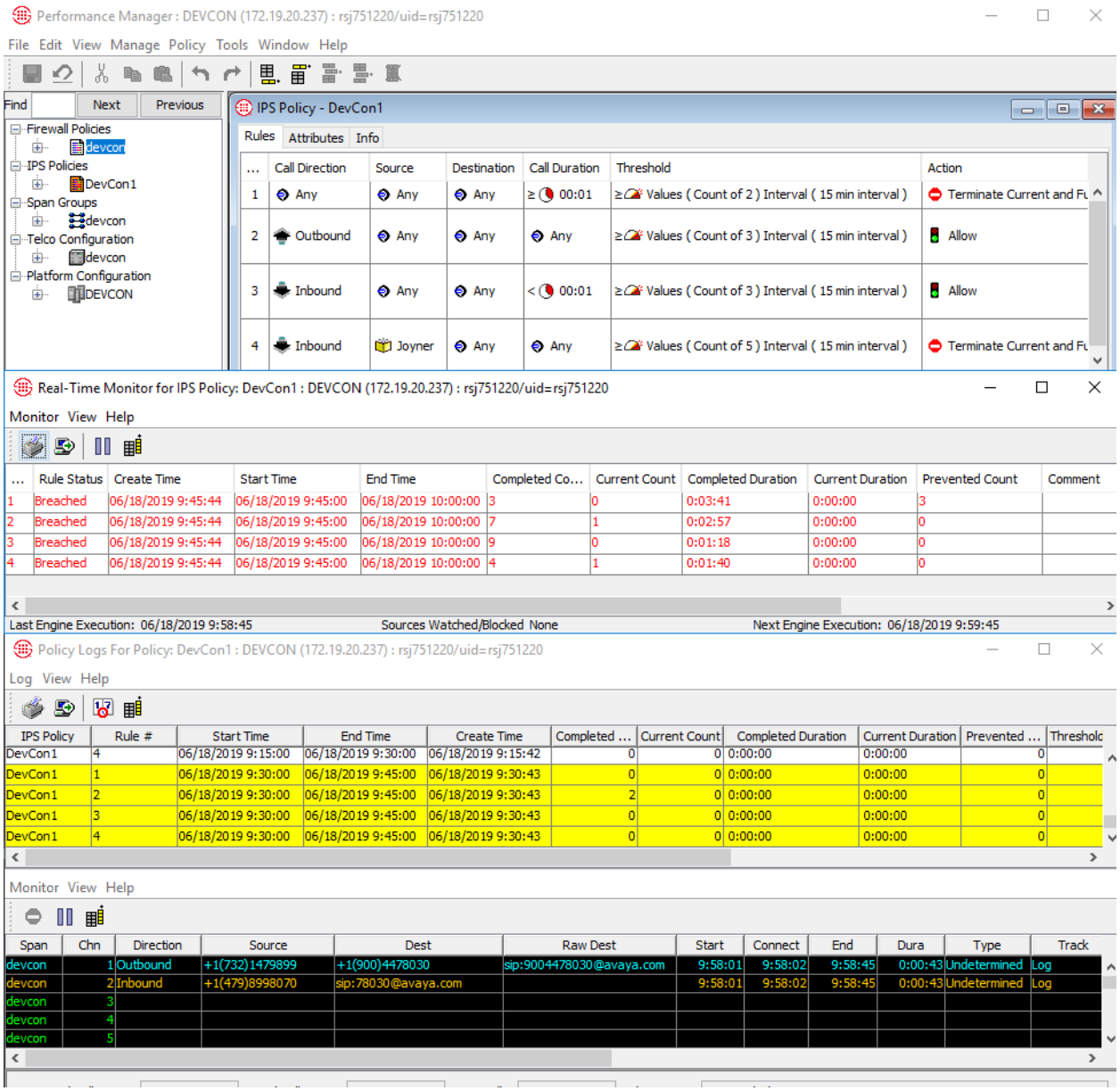
3. Place inbound and outbound calls that trigger **Voice Firewall** policies and verify that calls are properly detected and appropriate actions are taken as reflected in the **Policy Logs** and **Call Monitor** shown below.







4. Place inbound and outbound calls that trigger **Voice IPS** policies and verify that calls are properly detected and appropriate actions are taken as shown in the **Real-Time Monitor for IPS Policy**, **Policy Logs** and **Call Monitor**.



9 Conclusion

These Application Notes describe the configuration steps required to integrate the SecureLogix ETM SIP Proxy with Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise. Inbound and outbound calls were placed and SecureLogix ETM SIP Proxy successfully detected the calls, triggered the appropriate Voice Firewall and Voice IPS policies, and took the appropriate action. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10 References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 8.0.1, Issue 3, December 2018, available at http://support.avaya.com.

[2] *Administering Avaya Aura® System Manager for Release 8.0.1*, Release 8.0.x, Issue 7, January 2019, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018, available at http://support.avaya.com.

[4] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Issue 1, February 2019, available at http://support.avaya.com.

[5] *SecureLogix ETM 5000-Series SIP Appliance Installation and Configuration*, DOC-INSSIP-ETM6x7x-2014—0506.

[6] *SecureLogix ETM (Enterprise Telephone Management) Installation Guide v7.1.2*, DOC-IN-712-09242018.

[7] *SecureLogix ETM (Enterprise Telephone Management) System Administration and Maintenance Guide v7.1.2*, DOC-SA-712-09242018.

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.