



Avaya Solution & Interoperability Test Lab

Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3 - Issue 1.0

Abstract

These Application Notes describe the procedures necessary for configuring the Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Manager Rel. 6.3 to support Remote Workers on Avaya 96x1 SIP Deskphones, Avaya Flare® Experience for Windows and Avaya One-X® Communicator endpoints.

Testing was performed to verify basic functionalities of audio calls on the Avaya 96x1 SIP Deskphones and Avaya Flare® Experience for Windows, audio and video calls on Avaya One-X® Communicator. The calls were placed to and from Remote Worker users residing outside of the enterprise, across the public internet, to various Avaya endpoints located at the enterprise. For privacy, TLS for Signaling and SRTP for media encryption across the public internet were used. RTP, or non-encrypted media, was used inside of the enterprise (private network side).

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.

Table of Contents

1.	Introduction	4
2.	General Test Approach and Test Results	4
2.1.	Test Coverage	5
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Communication Manager	10
5.1.	Signaling Group	11
5.2.	IP Codec Set	12
6.	Configure Avaya Aura® Session Manager	13
6.1.	System Manager Login and Navigation	13
6.2.	Modify Session Manager Firewall	14
6.3.	Disable PPM Limiting	15
6.4.	HTTP Access from the Avaya SBCE to Avaya Aura® Session Manager for PPM data downloads.	17
6.4.1.	HTTP Access from the Avaya SBCE to Avaya Aura® Session Manager	17
6.5.	Enable video on Avaya SIP Softphones	18
7.	Configure the Avaya Session Border Controller for Enterprise (Avaya SBCE)	20
7.1.	Avaya Session Border Controller for Enterprise Configuration	20
7.2.	System Access	21
7.2.1.	Create Backup	24
7.3.	Network Management	25
7.4.	User Agents	27
7.5.	Global Profiles	29
7.5.1.	Server Interworking Profile	29
7.5.2.	Routing Profile	32
7.5.3.	Server Configuration	34
7.6.	SIP Cluster Proxy	38
7.7.	Domain Policies	42
7.7.1.	Application Rules	42
7.7.2.	Media Rules	44
7.7.3.	Signaling Rules	49
7.7.4.	End Point Policy Groups	50
7.8.	Device Specific Settings	53
7.8.1.	Media Interfaces	53
7.8.2.	Signaling Interfaces	55
7.8.3.	End Point Flows	58
7.8.4.	Relay Services	69
8.	Remote Worker IP Deskphones (96x1 SIP) Configuration	74

8.1.	ADDR Screen.....	74
8.2.	Set Group Number Screen.....	75
8.3.	Avaya IP Deskphones (96x1 SIP) 46xxsettings Configuration File	76
9.	Personal Computer (PC) Configuration.....	77
9.1.	Remote Worker Avaya Flare® Experience for Windows Configuration	78
9.2.	Remote Worker Avaya one-X® Communicator Configuration	81
10.	References.....	84

1. Introduction

These Application Notes describe the procedures necessary for configuring Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Manager Rel. 6.3 to support Remote Workers on Avaya 96x1 SIP Deskphones, Avaya Flare® Experience for Windows and Avaya One-X® Communicator endpoints.

Testing was performed to verify basic functionalities of audio calls on the Avaya 96x1 SIP Deskphones and Avaya Flare® Experience for Windows, audio and video calls on Avaya One-X® Communicator. The calls were placed to and from Remote Worker users residing outside of the enterprise, across the public internet, to various Avaya endpoints located at the enterprise.

The Avaya Session Border Controller for Enterprise (Avaya SBCE) authenticates SIP-based users/clients to the enterprise, securely proxy registrations and client device provisioning and securely manages communication without requiring the use of VPN. For privacy over the public internet, the public side of the Avaya SBCE facing the remote workers should be configured to use the recommended values of TLS for Signaling and SRTP for media encryption of audio and video. In the configuration depicted in these Application Notes, SRTP media encryption of audio and video was used across the public internet, and RTP, or non-encrypted media, was used inside of the enterprise (private network side)

The Avaya SBCE can effectively protect the enterprise network against all types of inadvertent and malicious intrusions and attacks. The Avaya SBCE two-wire-in-line topology performs border access control functionality such as Firewall/ Network Address Translation (NAT) traversal, access management and control based on user-configurable domain policies, and intrusion functionality to protect against DoS, spoofing, and stealth attacks, along with voice SPAM.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by configuring the Avaya SBCE, Communication Manager and Session Manager to support Remote Workers, allowing Remote Worker SIP endpoints residing outside of the enterprise to register to Session Manager, provide client device provisioning using HTTPS, and communicate effectively with enterprise endpoints using SRTP encryption of audio and video across the public internet without requiring the use of VPN, as depicted in **Figure 1**.

Currently there are several supported Avaya SIP endpoints for Remote Workers. Testing covered under these Application Notes only included the following SIP endpoints: Avaya 96x1 SIP deskphones, Avaya one-X® Communicator softphone (configured for SIP mode) and Avaya Flare® Experience for Windows SIP softphone. The Avaya 96x1 SIP Deskphones supports SRTP audio encryption, Avaya one-X® Communicator supports SRTP audio and video encryption, Avaya Flare® Experience for Windows softphone (as of Release 1.1.4.23) supports audio SRTP encryption, but currently does not support SRTP video encryption.

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 for 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.

2.1. Test Coverage

To verify Remote Worker basic functionality, the following areas were tested:

- Re-starting the 96x1 Deskphones, ensuring proper download and upgrade of new firmware. Also, proper download of settings defined in the configuration file (46xxsettings) via HTTPS.
- Making provisioning changes in Session Manager, ensuring proper download of PPM data.
- Remote Worker endpoint registrations to Session Manager, using the proper credentials.
- Basic audio calls to and from Remote Workers using 96x1 Deskphones, Avaya One-X® Communicator and Avaya Flare® Experience for Windows to various Avaya endpoint types located at the enterprise. SRTP media encryption of audio was used across the public internet. RTP, or non-encrypted media, of audio was used inside of the enterprise (private network side). For signaling, SIP over TLS was used across the public internet and inside of the enterprise (private network side).
- Basic audio calls, with video, to and from Remote Workers using Avaya One-X® Communicator to Avaya One-X® Communicator endpoints located at the enterprise. SRTP media encryption of audio and video was used across the public internet. RTP, or non-encrypted media, of audio and video was used inside of the enterprise (private network side). For signaling, SIP over TLS was used across the public internet and inside of the enterprise (private network side).
- Basic call handling features, such as Call hold, transfer, call forward, and conference were tested.
- Call coverage to Avaya Aura® Messaging and Message Waiting Indicator (MWI) activation/deactivation.

Note: The intent behind these Application Notes is not to perform Interoperability Compliance Testing or to test every supported Remote Worker SIP endpoint type, but simply to illustrate the provisioning steps that are required in order to support Remote Workers on Avaya enterprise solutions involving Communication Manager, Session Manager and the Avaya SBCE. Remote worker integration with SIP Trunking was not part of the reference configuration. Interoperability Compliance Testing of Remote Worker endpoints with SIP Trunking should be done independently with each Service Provider. Testing additional supported Remote Worker SIP endpoints, not listed under these Application Notes, is outside the scope of these Application Notes.

2.2. Test Results

Basic Remote Worker functionality was verified successfully with the following observations/limitations.

- **Avaya Flare® Experience for Windows SRTP video encryption** – SRTP video encryption is currently not supported on Avaya Flare® Experience for Windows (**Release 1.1.4.23**). Video has to be disabled on the Avaya Flare® Experience for Windows PC application if SRTP encryption is enabled in the Avaya SBCE for Avaya Flare® under **Subscriber Flows**. If video is enabled the user will receive busy signal when attempting to make calls.
- The inside IP address of the Avaya SBCE (private network side) used for Remote Workers needs to be “whitelisted” in the Session Manager Firewall.

2.3. Support

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

In the reference configuration, an existing Avaya SBCE is provisioned to support Remote Worker, allowing remote SIP endpoints, connected via the public Internet, access to the private enterprise without the use of VPN.

For Remote Workers, standard and Advanced Session Licenses are required on the Avaya SBCE. Contact an authorized Avaya representative for assistance if additional licensing is required. The settings presented here illustrate a sample configuration and are not intended to be prescriptive.

Figure 1 below illustrates the Remote Worker topology used in the reference configuration.

The Avaya components used to create the simulated enterprise site included:

- Avaya S8300 Server running Avaya Aura® Communication Manager.
- Avaya G450 Media Gateway.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- Dell R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 96x0-Series IP Deskphones (H.323 and SIP) at the enterprise site.
- Avaya 96x1-Series IP Deskphones (H.323 and SIP) at the enterprise site.
- Avaya 96x1-Series IP Deskphones (SIP) at the Remote Worker site.
- Avaya one-X® Communicator soft phones (H.323 and SIP) at the enterprise site.
- Avaya one-X® Communicator soft phones (SIP) at the Remote Worker site.
- Avaya Flare® Experience for Windows (SIP) at the enterprise site and at the Remote Worker sites.

- Desktop PC running a HTTPS file server at the enterprise site.

In the reference configuration, Remote Workers Internet access is simulated by a Router/NAT/Firewall/Default Gateway located at the Remote Worker site, between the Remote Worker private network side and the public Internet. The router also provides DHCP service to the SIP endpoints.

Located at the edge of the enterprise is a stand-alone Avaya SBCE. It has a public network side that connects to the public internet and a private network side that connects to the enterprise network. All SIP and media traffic entering or leaving the enterprise flows through the Avaya SBCE. This way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For privacy over the public internet, the Avaya SBCE was configured to use SRTP for media encryption of audio and video on its public network side. The Avaya SBCE was configured to use RTP, or non-encrypted media, for audio and video inside of the enterprise (private network side).

The transport protocol used between the Avaya SBCE and the Remote Workers across the public internet is SIP over TLS. The transport protocol used between the Avaya SBCE and Session Manager across the enterprise private network was also SIP over TLS.

For security reasons, any actual public IP addresses used in the configuration have been masked.

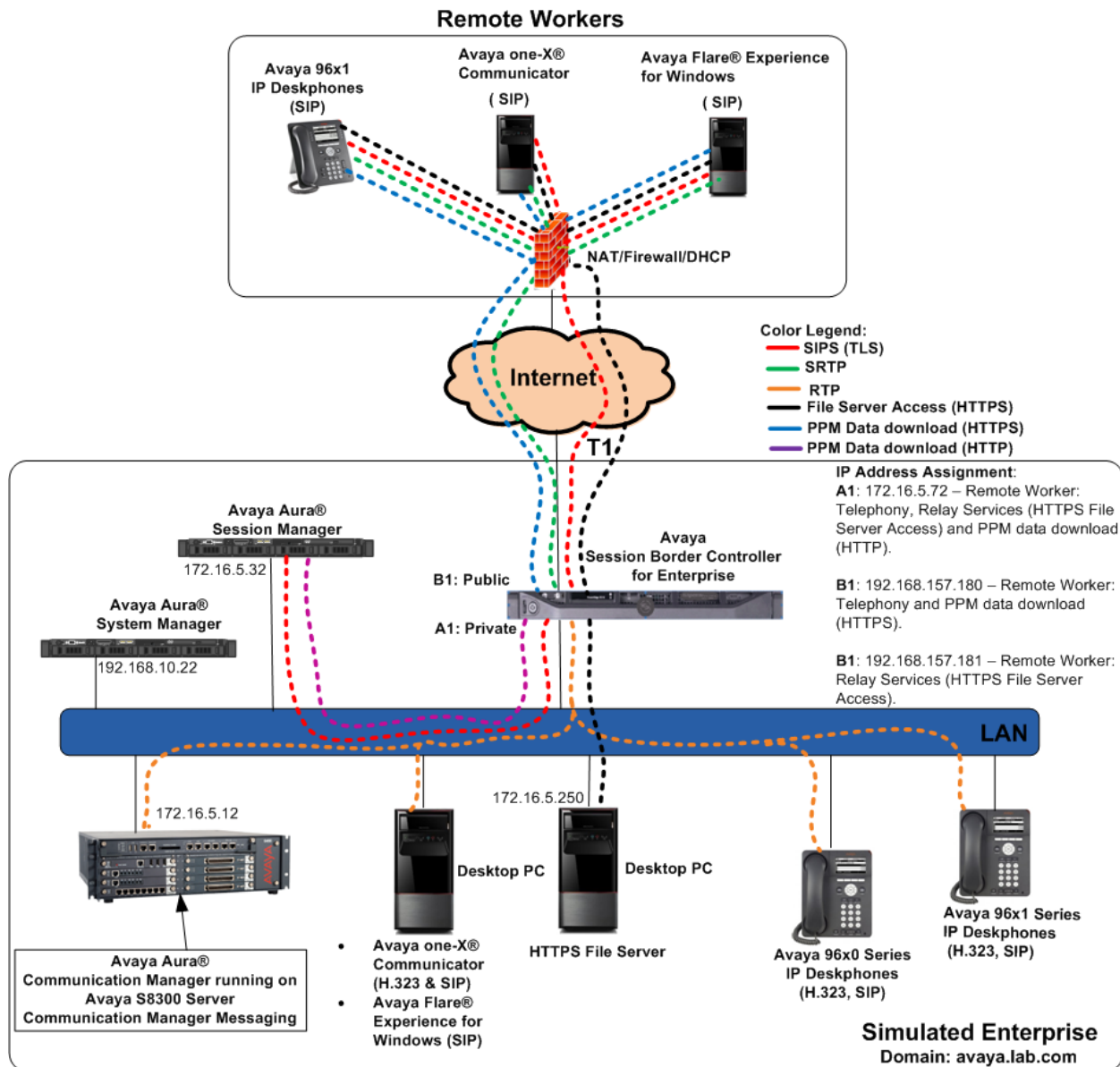


Figure 1: Remote Worker topology used in the reference configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on an Avaya S8300D Server	6.3.5 (Service Pack 5) (03.0.124.0-21460)
G450 Gateway	35.8.0
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server	6.3.7 (Service Pack 7) (6.3.7.0.637008)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server	6.3.7 Build No. 6.3.0.8.5682-6.3.8.3204 Software Update Rev. No. 6.3.7.7.2275
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.1.Q07
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya Aura® Communication Manager Messaging (CMM)	CMM 6.3 (Service Pack 2) (03.0.124.0-0202)
Avaya one-X® Communicator (SIP & H.323)	6.2.2.07-SP2
Avaya Flare® Experience for Windows (SIP)	1.1.4.23
Avaya 96x1 Series IP Deskphones (SIP)	Avaya one-X® Deskphone SIP Version 6.3.1.22
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone H.323 Version 6.3.0.37
Avaya 96x0 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition Version S3.212A
Avaya 96x0 Series IP Deskphones (SIP)	Avaya one-X® Deskphone SIP Version 2.6.11.4

Table 2 – Hardware and Software Components Tested

5. Configure Avaya Aura® Communication Manager

This section describes the required configuration of Communication Manager for video support on Avaya Softphones.

It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and Session Manager has been previously completed.

The Communication Manager configuration was performed using the Avaya Integrated Management Site Administrator.

Note: The Communication Manager Configuration shown under this section is **only** required if the customer is planning to use video on Avaya softphones.

On Avaya Flare® Experience for Windows, testing was done with video disabled since SRTP video encryption is not supported in the current release of Avaya Flare® Experience for Windows (**Release 1.1.4.23**). Please refer to the note in **Section 7.8.3.1** for additional information regarding video settings and using SRTP encryption for audio.

5.1. Signaling Group

Use the **change signaling-group** command to enable **IP Video** on the **Signaling Group** being used for calls within (inside) the enterprise. For the compliance test **Signaling Group 1** was used.

Use the **change signaling-group 1** command to enable **IP Video**, as follows:

- Set **IP Video?** to **y**.
- Leave remaining parameters with the existing values.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: <u>tls</u>	
Q-SIP? n		
IP Video? y	Priority Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: <u>procr</u>	Far-end Node Name: <u>Lab-HG-SM</u>	
Near-end Listen Port: <u>5061</u>	Far-end Listen Port: <u>5061</u>	
	Far-end Network Region: <u>1</u>	
Far-end Domain: <u>avaya.lab.com</u>		
Incoming Dialog Loopbacks: <u>eliminate</u>	Bypass If IP Threshold Exceeded? n	
DTMF over IP: <u>rtp-payload</u>	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): <u>3</u>	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): <u>6</u>	

5.2. IP Codec Set

Use the change **ip-codec-set** command to enable **Allow Direct-IP Multimedia** on the **IP Codec Set** being used for calls within (inside) the enterprise.

Use the **change ip-codec-set 1** command to enable **Allow Direct-IP Multimedia**, as follows:

On page 2 of 2:

- Set **Allow Direct-IP Multimedia?** to **y**.
- Set the **Maximum Call Rate for Direct-IP Multimedia** to a value specific for the enterprise, the default value of **384 Kbits** was used in the sample configuration.
- Set the **Maximum Call Rate for Priority Direct-IP Multimedia** to a value specific for the enterprise, the default value of **384 Kbits** was used in the sample configuration.
- Leave remaining parameters with the existing values.

change ip-codec-set 1 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? y
Maximum Call Rate for Direct-IP Multimedia: 384:Kbits
Maximum Call Rate for Priority Direct-IP Multimedia: 384:Kbits

	Mode	Redundancy	ECM: <u>y</u>	Packet Size(ms)
FAX	<u>t.38-standard</u>	<u>0</u>		
Modem	<u>off</u>	<u>0</u>		
TDD/TTY	<u>US</u>	<u>3</u>		
H.323 Clear-channel	<u>n</u>	<u>0</u>		
SIP 64K Data	<u>n</u>	<u>0</u>		<u>20</u>

Note: To save all Communication Manager provisioning changes, enter the command **save translations**.

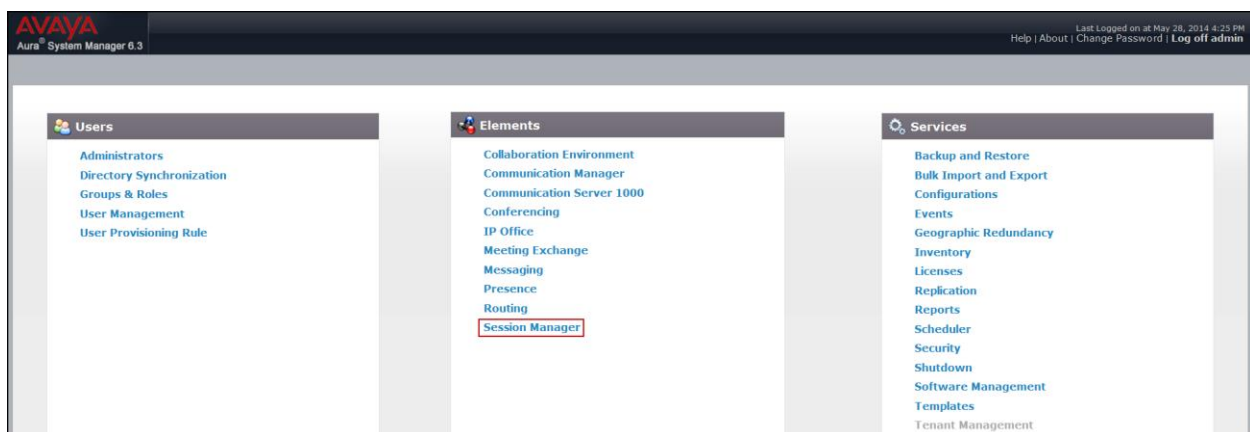
6. Configure Avaya Aura® Session Manager

This section describes the required configuring of Session Manager for the support of Remote Workers.

Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials (not shown). The screen shown below is then displayed. Click on **Session Manager**.

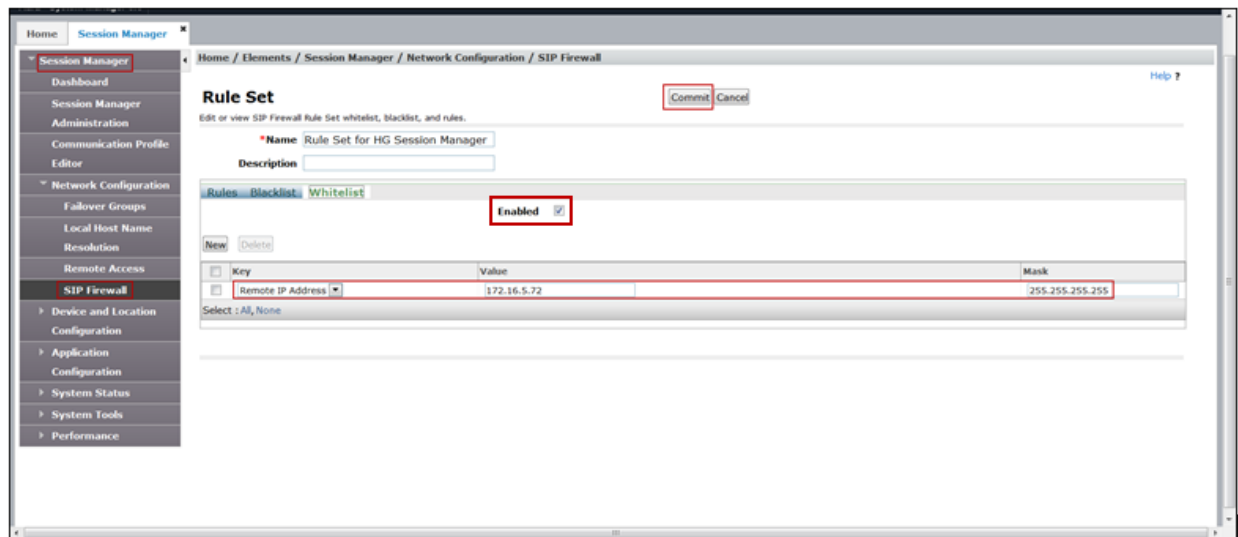


6.2. Modify Session Manager Firewall

Under **Elements** → **Session Manager** → **Network Configuration** → **SIP Firewall**, select the Session Manager instance (e.g., HG Session Manager) (not shown). Use values specific for the enterprise, the following values were used in the reference configuration:

- Select **Edit** (not shown).
- Select **Whitelist** tab.
- Verify **Enabled** is checked.
- Select **New**.
- Under the **Key** field select **Remote IP Address**.
- Under the **Value** field enter the internal (private network side) IP address of the Avaya SBCE used for Remote Worker (e.g., **172.16.5.72**) (see **Section 7.3**).
- Under the **Mask** field enter the appropriate mask (e.g., **255.255.255.255**).
- Click **Commit**.

The following screenshot show the values of the SIP Firewall after the changes were made.



Note: If this is a new Session Manager installation, you will need to create a rule set for the Session Manager. In later Session Manager software releases, the rule set is not created automatically; instead, the Session Manager is assigned to a default rule set which cannot be modified. Thus, the appropriate rule set must be copied, assigned to the Session Manager, and then modified using the procedure listed above.

6.3. Disable PPM Limiting

Under **Elements** → **Session Manager** → **Session Manager Administration**, Select the Session Manager instance (e.g., HG Session Manager).

- Select **Edit**.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left sidebar shows the navigation menu with 'Session Manager Administration' selected. The main content area is titled 'Session Manager Administration' and includes a 'Global Settings' section with various checkboxes and dropdowns for configuring Session Manager instances. Below this, the 'Session Manager Instances' section shows a table with 2 items. The first item, 'HG Session Manager', is highlighted, and the 'Edit' button is visible. The table columns are Name, Primary Communication Profiles, Secondary Communication Profiles, Maximum Active Communication Profiles, Description, and VMware. The second item is 'MA_Session Manager'.

Name	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description	VMware
HG Session Manager	6	0	6	Lab-HG SM	<input type="checkbox"/>
MA_Session Manager	12	0	12	SIL_MA SM	<input type="checkbox"/>

- AVAYA**
List Logged on at May 26, 2014 4:25 PM
Help | About | Change Password | Log off admin

[Home](#)

[Session Manager](#)

- [Session Manager Administration](#)
 - [Dashboard](#)
 - [Communication Profile Editor](#)
 - [Network Configuration](#)
 - [Failover Groups](#)
 - [Local Host Name Resolution](#)
 - [Remote Access](#)
 - [SIP Firewall](#)
 - [Device and Location Configuration](#)
 - [Application Configuration](#)
 - [System Status](#)
 - [System Tools](#)
 - [Performance](#)

Home / Elements / Session Manager / Session Manager Administration

Edit Session Manager

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
[Expand All](#) | [Collapse All](#)

[Commit](#)
[Cancel](#)

General

SIP Entity Name HG Session Manager

Description Lab-HG SM

*Management Access Point Host Name/IP 172.16.5.31

*Direct Routing to Endpoints Enable

VMware Virtual Machine ☐

Security Module

SIP Entity IP Address 172.16.5.32

*Network Mask 255.255.255.0

*Default Gateway 172.16.5.254

*Call Control PHB 46

*QOS Priority 6

*Speed & Duplex Auto

VLAN ID

*SIP Firewall Configuration Rule Set for HG Session Manager

NIC Bonding

Enable Bonding ☐

Driver Monitoring Mode ARP Monitoring

ARP Interval (msecs) 100

Link Monitoring Frequency (msecs) 100

ARP Target IP

Down Delay (msecs) 200

Up Delay (msecs) 200

Monitoring

Enable Monitoring ☒

*Proactive cycle time (secs) 900

*Reactive cycle time (secs) 120

*Number of Retries 1

CDR

Enable CDR ☐

User CDR_User

Password

Confirm Password

Data File Format Standard Flat File

Include User to User Calls ☐

Include Incomplete Calls ☐

Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection ☐

*Maximum Connection per PPM Client 3

PPM Packet Rate Limiting ☐

*PPM Packet Rate Limiting Threshold 200

Event Server

Clear Subscription on Notification Failure No

[Required](#)
[Commit](#)
[Cancel](#)

6.4. HTTP Access from the Avaya SBCE to Avaya Aura® Session Manager for PPM data downloads.

Remote Worker connection between the Avaya SBCE and Session Manager may use HTTPS or HTTP for PPM data download based on the **Allow Unsecured PPM Traffic** setting. In the reference configuration, HTTPS was used between the Remote Worker phones and the Avaya SBCE and HTTP was used between the Avaya SBCE and Session Manager.

6.4.1. HTTP Access from the Avaya SBCE to Avaya Aura® Session Manager

Under **Elements** → **Session Manager** → **Session Manager Administration**.

- Verify that **Allow Unsecured PPM Traffic** option is checked.
- Click **Save**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains navigation links: Home, Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Failover Groups, Local Host Name Resolution, Remote Access, SIP Firewall, Device and Location Configuration, Application Configuration, System Status, System Tools, and Performance. The main content area is titled 'Session Manager Administration' and includes a 'Global Settings' section with various checkboxes and dropdowns. The 'Allow Unsecured PPM Traffic' checkbox is checked. Below this is a 'Session Manager Instances' section with a table of 2 items.

Name	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description	VMware
HG Session Manager	6	0	6	Lab-HG SM	<input type="checkbox"/>
MA_Session Manager	12	0	12	SIL_MA SM	<input type="checkbox"/>

Note: In the reference configuration, **Allow Unsecured PPM Traffic** was checked, resulting in unsecured (HTTP) PPM traffic between the Avaya SBCE and Session Manager (private network side). Secured PPM traffic (HTTPS) was used between Remote Worker endpoints and the Avaya SBCE (public network side).

6.5. Enable video on Avaya SIP Softphones

This section describes the required configuration of Session Manager for video support on Avaya SIP Softphones, including Remote Worker SIP softphones (e.g., Avaya one-X® Communicator).

It is assumed that SIP user provisioning in Session Manager has been previously completed. Refer to item [12] in **Section 10** for instruction on how to add SIP users in Session Manager.

Under **Users** → **User Management**, select **Manage Users**. Select the user instance to enable video (not shown), click **Edit**. Under **CM Endpoint Profile**, click on **Endpoint Editor** (not shown). Under **Feature Options (F)**:

- Verify that **IP Softphone** is checked.
- Check **IP Video Softphone**.
- Click **Done**, then on **Commit** on the next screen (not shown).

7. Configure the Avaya Session Border Controller for Enterprise (Avaya SBCE)

This section describes the required configuring of the Avaya SBCE for the support of Remote Workers.

It is assumed that the Avaya SBCE was provisioned and the appropriate licenses were installed and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: During the next pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it.

7.1. Avaya Session Border Controller for Enterprise Configuration

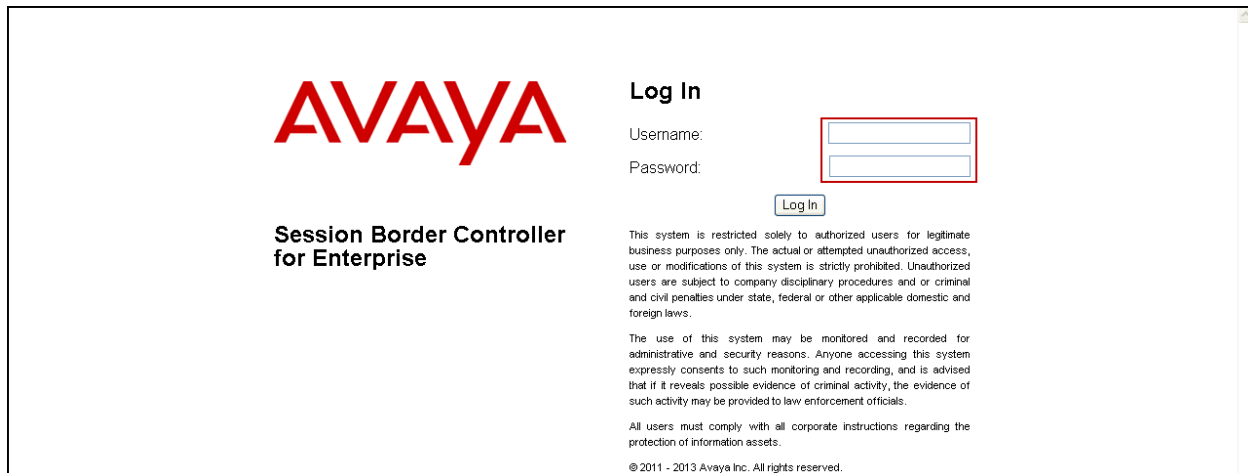
The configuration steps on the Avaya SBCE include the following:

- Add network interfaces.
- Create User Agents.
- Create Server Interworking Profile.
- Create Routing Profile.
- Create Server Configuration Profile.
- Create SIP Cluster Proxy.
- Create Application Rules.
- Create Media Rules.
- Create Signaling Rules.
- Create Endpoint Policy Group.
- Create Media and Signaling Interfaces.
- Create Endpoint Subscriber Flow.
- Create Endpoint Server flow.
- Create Relays Services.

7.2. System Access

Use a web browser to access the Avaya SBCE web interface, enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the management IP address of the Avaya SBCE.

Enter the appropriate credentials and then click **Log In**.



The image shows the Avaya SBCE Log In page. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right is the "Log In" section with fields for "Username:" and "Password:", a "Log In" button, and a disclaimer. The disclaimer states that the system is restricted to authorized users and that unauthorized access is prohibited. It also mentions that the use of the system may be monitored and recorded for administrative and security reasons. At the bottom, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

AVAYA

Session Border Controller for Enterprise

Log In

Username:

Password:

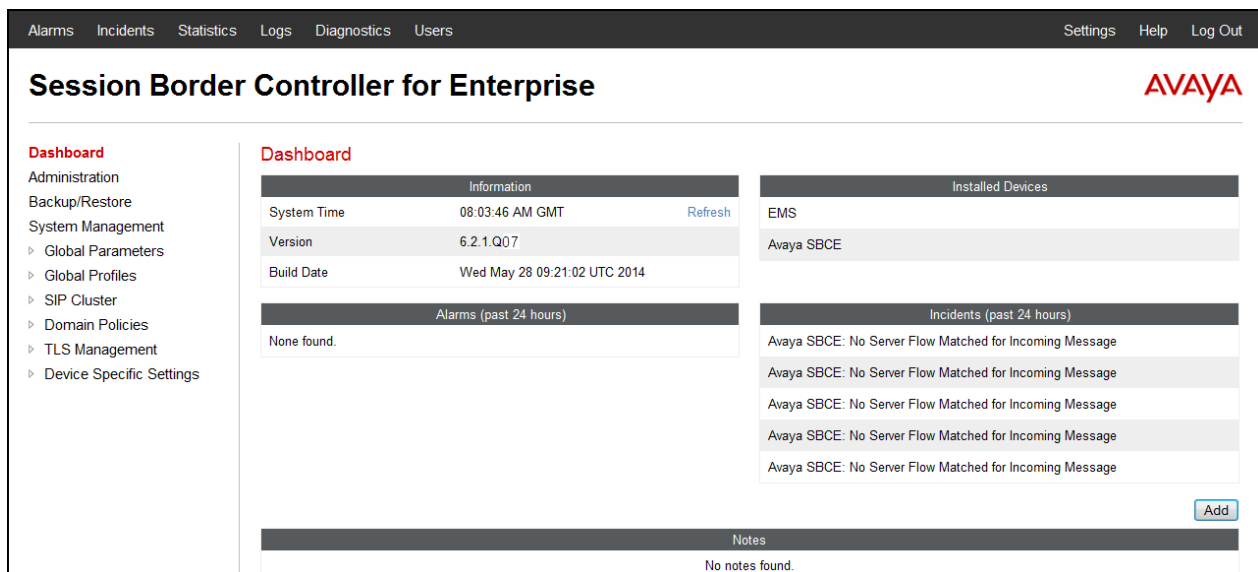
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

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

© 2011 - 2013 Avaya Inc. All rights reserved.

The **Dashboard** main page will appear as shown below.



The image shows the Avaya SBCE Dashboard. At the top is a navigation bar with links for "Alarms", "Incidents", "Statistics", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". Below the navigation bar is the "Session Border Controller for Enterprise" header with the Avaya logo. The dashboard is divided into several sections: "Administration" (Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, Device Specific Settings), "Information" (System Time: 08:03:46 AM GMT, Version: 6.2.1.Q07, Build Date: Wed May 28 09:21:02 UTC 2014), "Installed Devices" (EMS, Avaya SBCE), "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (Avaya SBCE: No Server Flow Matched for Incoming Message), and "Notes" (No notes found). There is an "Add" button next to the "Incidents" section.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Information

System Time	08:03:46 AM GMT	Refresh
Version	6.2.1.Q07	
Build Date	Wed May 28 09:21:02 UTC 2014	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message

Notes

No notes found.

To view the system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.

Session Border Controller for Enterprise AVAYA

System Management

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status
Avaya SBCE (PC531030132)	172.16.x.x	6.2.1.Q07	Commissioned

Reboot Shutdown Restart Application **View** Edit Delete

The **System Information** window is displayed as shown below.

The **System Information** screen shows **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

The **A1** and **B1** interfaces and IP addresses shown below are part of a prior configuration that was added to support SIP Trunks only and are **not** relevant to the configuration required by Remote Workers. The configuration required to support Remote Workers is illustrated on sections that follow. The management IP was blurred out for security reasons.

The screenshot shows a window titled "System Information: Avaya SBCE" with a close button (X) in the top right corner. The window is divided into several sections:

- General Configuration:** A table with three rows: "Appliance Name" (Avaya SBCE), "Box Type" (SIP), and "Deployment Mode" (Proxy).
- Device Configuration:** A table with two rows: "HA Mode" (No) and "Two Bypass Mode" (No).
- Network Configuration:** A table with five columns: "IP", "Public IP", "Netmask", "Gateway", and "Interface". It contains two rows of data:

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
192.168.157.186	192.168.157.186	255.255.255.192	192.168.157.129	B1
- DNS Configuration:** A table with four rows: "Primary DNS" (172.16.5.102), "Secondary DNS" (blank), "DNS Location" (DMZ), and "DNS Client IP" (172.16.5.71).
- Management IP(s):** A table with one row: "IP" (blurred out).

7.2.1. Create Backup

It's always a good idea to backup the configuration prior to making changes to the Avaya SBCE.

Under **Backup/Restore** → **Snapshots** tab:

- Click on **Create Snapshot**, give a description and Click **Create**.
- Save the backup to the desktop by clicking **Download** and save the file to the PC.
- After finishing the configuration it is recommended to take another snapshot and to save the file to the PC.

The screenshot shows the 'Backup / Restore' section of the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Backup/Restore' highlighted. The main content area has three tabs: 'Snapshots', 'Snapshot Servers', and 'Automatic Snapshot Configuration'. The 'Snapshots' tab is active, displaying a table of snapshots. Above the table are buttons for 'Local', 'Refresh', 'Hide incompatible snapshots', 'Remove Selected Snapshots', 'Restore by File', and 'Create Snapshot'. A warning message states: 'To minimize the risk of data loss, create a Snapshot before restoring from another Snapshot.'

	Date	Build	Description	
<input type="checkbox"/>	02/09/2014 14:50:09 GMT	6.2.1.Q07	SaskTel with IPO Restore Point	Download Restore Delete
<input type="checkbox"/>	02/05/2014 05:34:42 GMT	6.2.1.Q07	SaskTel with CM Restore Point	Download Restore Delete
<input type="checkbox"/>	02/03/2014 07:08:25 GMT	6.2.1.Q07	SaskTel Restore Point	Download Restore Delete
<input type="checkbox"/>	01/22/2014 12:43:50 GMT	6.2.1.Q07	Restore Point	Download Restore Delete
<input type="checkbox"/>	01/21/2014 07:03:00 GMT	6.2.1.Q07	Remote Worker Restore Point	Download Restore Delete

The 'Create Snapshot' dialog box contains a warning message: 'A snapshot can only be restored to the same version of the same EMS it was created on with the same management IP when it was created.' Below the warning is a text input field for the 'Description' with the value 'Restore Point'. At the bottom is a 'Create' button.

7.3. Network Management

The following screen shows the Network Configuration of the Avaya SBCE. In the reference configuration shown, the Avaya SBCE was configured with three “public” IP addresses assigned to physical interface B1, and two “private” IP addresses assigned to physical interface A1.

Note: For Remote Worker configuration, only two “public” IP addresses and one “private” IP address are required (enclosed in a red bracket). The other IP addresses shown (not enclosed in red bracket) were previously configured and are used for SIP Trunking only; they are not relevant to the functionality of Remote Workers. The Avaya SBCE used in the reference configuration was provisioned to support SIP Trunking and Remote Worker functionalities, IP addresses used for SIP Trunking are listed here simply for clarification.

Following are the IP addresses and associated interfaces used in the reference configuration:

- **172.16.5.71** is the Avaya SBCE “private” address previously provisioned for SIP Trunks. This address is **not** relevant to Remote Workers functionality and is not discussed in this document.
- **172.16.5.72** is the new Avaya SBCE “private” address added for Remote Workers access to the enterprise private network (e.g., Session Manager). Note that this address is also used to access the HTTPS file server residing inside of the enterprise (private network side) containing the 46xxsettings.txt configuration and phone firmware files (see **Section 7.8.4**).
- **192.168.157.186** is the Avaya SBCE “public” address previously provisioned for SIP Trunks to the Service Providers. This address is **not** relevant to Remote Workers functionality and is not discussed in this document.
- **192.168.157.180** is one of the two new Avaya SBCE “public” addresses added for Remote Worker access to Session Manager via the Avaya SBCE. Remote Worker SIP endpoints will use this “public” address to establish connection to Session Manager through the Avaya SBCE, for registration, telephony functions and PPM data download.
- **192.168.157.181** is one of the two new Avaya SBCE “public” addresses added for Remote Worker access to the HTTPS file server residing inside of the enterprise (private network side) containing the 46xxsettings.txt configuration file and Deskphone firmware. This address is also referred to as the “Relay Services” address.

Under **Device Specific Settings** → **Network Management** → **Network Configuration** tab, select **Add** to create a new interface entry. Use IP address values specific to the enterprise. Values shown below were used in the reference configuration. Select **Save** when done (not shown). Repeat the steps for each entry.

AlarmsIncidentsStatisticsLogsDiagnosticsUsers

SettingsHelpLog Out

Session Border Controller for Enterprise

AVAYA

DashboardAdministrationBackup/RestoreSystem ManagementGlobal ParametersGlobal ProfilesSIP ClusterDomain PoliciesTLS ManagementDevice Specific SettingsNetwork ManagementMedia InterfaceSignaling InterfaceSignaling ForkingEnd Point FlowsSession FlowsRelay ServicesSNMPSyslog ManagementAdvanced OptionsTroubleshooting

Network Management: Sipera

DevicesSipera

Network ConfigurationInterface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management

A1 Netmask 255.255.255.0A2 NetmaskB1 Netmask 255.255.255.192B2 Netmask

AddSaveClear

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
192.168.157.186		192.168.157.129	B1	Delete
192.168.157.180		192.168.157.129	B1	Delete
192.168.157.181		192.168.157.129	B1	Delete
172.16.5.72		172.16.5.254	A1	Delete

On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

AlarmsIncidentsStatisticsLogsDiagnosticsUsers

SettingsHelpLog Out

Session Border Controller for Enterprise

AVAYA

DashboardAdministrationBackup/RestoreSystem ManagementGlobal ParametersGlobal ProfilesSIP ClusterDomain PoliciesTLS ManagementDevice Specific SettingsNetwork ManagementMedia InterfaceSignaling InterfaceSignaling ForkingEnd Point FlowsSession FlowsRelay ServicesSNMPSyslog ManagementAdvanced OptionsTroubleshooting

Network Management: Sipera

DevicesSipera

Network ConfigurationInterface Configuration

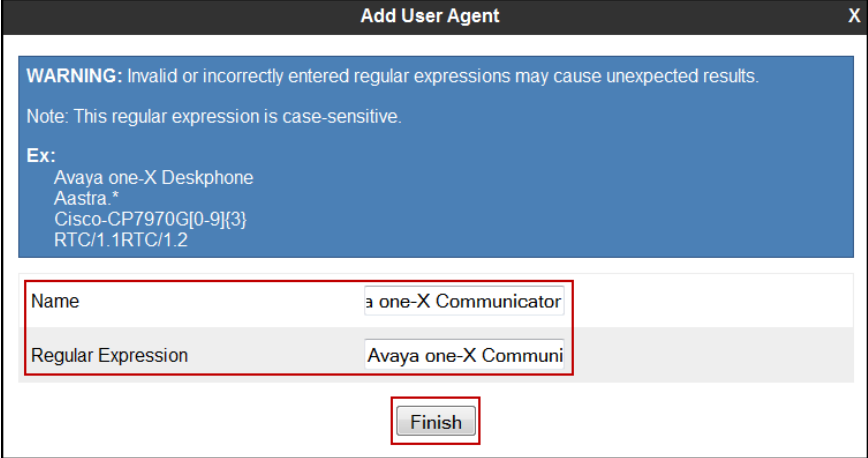
Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.4. User Agents

User Agents were created for each type of endpoint tested. This allows for different policies to be applied based on the type of device being used.

Under **Global Parameters** → **User Agents**, select **Add** (not shown), use values specific to the enterprise. The following values were used in the reference configuration:

- Under **Name** enter *Avaya one-X Communicator*
- Under **Regular Expression** enter *Avaya one-x Communicator.**
- Click **Finish**.



Add User Agent X

WARNING: Invalid or incorrectly entered regular expressions may cause unexpected results.
Note: This regular expression is case-sensitive.
Ex:
Avaya one-X Deskphone
Aastra.*
Cisco-CP7970G[0-9]{3}
RTC/1.1RTC/1.2

Name: Avaya one-X Communicator

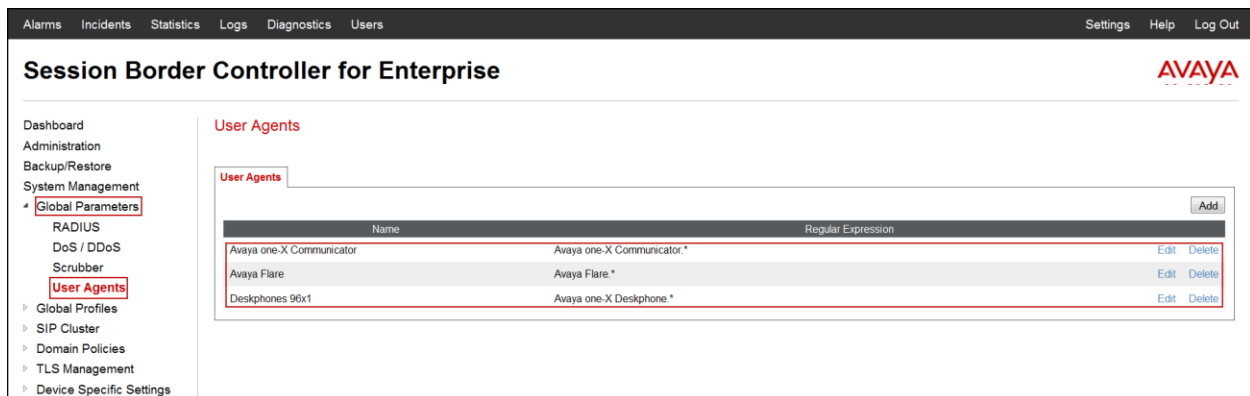
Regular Expression: Avaya one-X Communi

Finish

Repeat the above steps adding two additional User Agents with the following values:

- **Name:** *Avaya Flare*
- **Regular Expression:** *Avaya Flare.**
- **Name:** *Deskphone 96x1*
- **Regular Expression:** *Avaya one-X Deskphone.**

The following screenshot shows the User Agents after they were added.



The following abridged output of traceSM shows the details of an Invite message from an Avaya one-X Deskphone. The **User-Agent** shown in this trace will match User Agent with **Regular Expression** of “Avaya one-X Deskphone.*”. In this example, the expression “.*” will match any software version listed after the user agent name.

```

-----
172.16.5.72:15137 --TLS-> 172.16.5.32:5061
-----
INVITE sips:50150@172.16.5.32:avaya-cm-fnu=off-hook SIP/2.0
From: <sips:50150@172.16.5.32>;tag=27a305d8538dcabf-58e46800_F501510.10.10.13
To: <sips:50150@172.16.5.32:avaya-cm-fnu=off-hook>
CSeq: 10 INVITE
Call-ID: a_538dcabf6c62b81e-58e46a80_I@10.10.10.13
Contact: <sips:50150@172.16.5.72:5061;transport=tls;subid_ipcs=972640342>;+avaya-cm-line=1
Record-Route: <sip:172.16.5.72:5061;ipcs-line=76;lr;transport=tls;subid_ipcs=972640342>
Allow: INVITE,ACK,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PRACK,PUBLISH,UPDATE
Supported: 100rel,eventlist,feature-ref,replaces,tdialog
User-Agent: Avaya one-X Deskphone 6.3.1.22 (22)
Max-Forwards: 69
Via: SIP/2.0/TLS 172.16.5.72:5061;branch=z9hG4bK-s1632-002066383241-1--s1632-
Expires: 30
Accept-Language: en
Content-Length: 0

```

7.5. Global Profiles

The Global Profiles menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

7.5.1. Server Interworking Profile

Under **Global Profiles → Server Interworking**, select the existing Server Interworking profile that was previously created for Session Manager, if one exist (see note below). In the reference configuration the Server Interworking profile by the name of **Avaya-SM** was previously created for SIP Trunking.

The following screenshots show the Server Interworking profile **Avaya-SM** that was previously created for SIP Trunking; no changes were made for Remote Workers. It's shown here since it will later be used in **Section 7.5.3**.

Note: The Avaya SBCE used in the reference configuration was provisioned to support SIP Trunking and Remote Worker functionalities. If there is no existing Server Interworking Profile for SIP Trunking, the default **avaya-ru** profile can be cloned to create a new Server Interworking Profile. The new profile can then be modified to meet the specific requirements for the enterprise. Directly modifying an existing default profile is not recommended.

The following screenshot shows the **General** tab of the existing **Avaya-SM** Server Interworking profile.

Editing Profile: Avaya-SM X

General

Hold Support ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group None ▼

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

T.38 Support ☐

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261 ☐ RFC2543

Next

The following screenshot shows the **Advanced** tab of the existing **Avaya-SM** Server Interworking profile.

The screenshot displays a window titled "Editing Profile: Avaya-SM" with a close button (X) in the top right corner. The window contains a list of configuration options for the Avaya-SM Server Interworking profile, each with a checkbox or radio button. The "Record Routes" option is expanded, showing three radio button options: "None" (selected), "Single Side", and "Both Sides".

Configuration Option	Value / State
Record Routes	None (selected), Single Side, Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input checked="" type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

At the bottom of the window, there is a "Finish" button.

7.5.2. Routing Profile

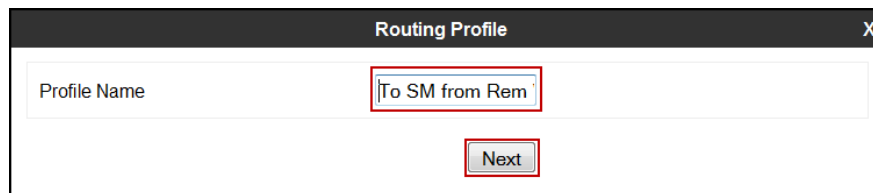
Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Note: **172.16.5.32** is the IP address of Session Manager Security module in the reference configuration (this address can be found in the screenshots shown in **Section 6.3** under **Security Module**).

The Routing Profile **To SM from Rem W** was created for Remote Workers access to Session Manager.

Under **Global Profiles → Routing**, select **Add** on top, left (not shown), use values specific to the enterprise. The following values were used in the reference configuration:

- Under **Profile Name** enter *To SM from Rem W* and click on **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "To SM from Rem". A red rectangular box highlights the input field. Below the input field, there is a "Next" button, also highlighted with a red rectangular box.

Under **Routing Profile** enter the following:

- Under **Next Hop Server 1** field enter the IP address of Session Manager (e.g., **172.16.5.32**).
- Verify the **Routing Priority based on Next Hop Server** box is checked.
- Select **TLS** for the **Outgoing Transport**.
- Use defaults for all remaining parameters.
- Click on **Finish**.

Routing Profile

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group *

Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port 172.16.5.32

Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port

Routing Priority based on
Next Hop Server ☒

Use Next Hop
for In Dialog Messages ☐

Ignore Route Header
for Messages Outside Dialog ☐

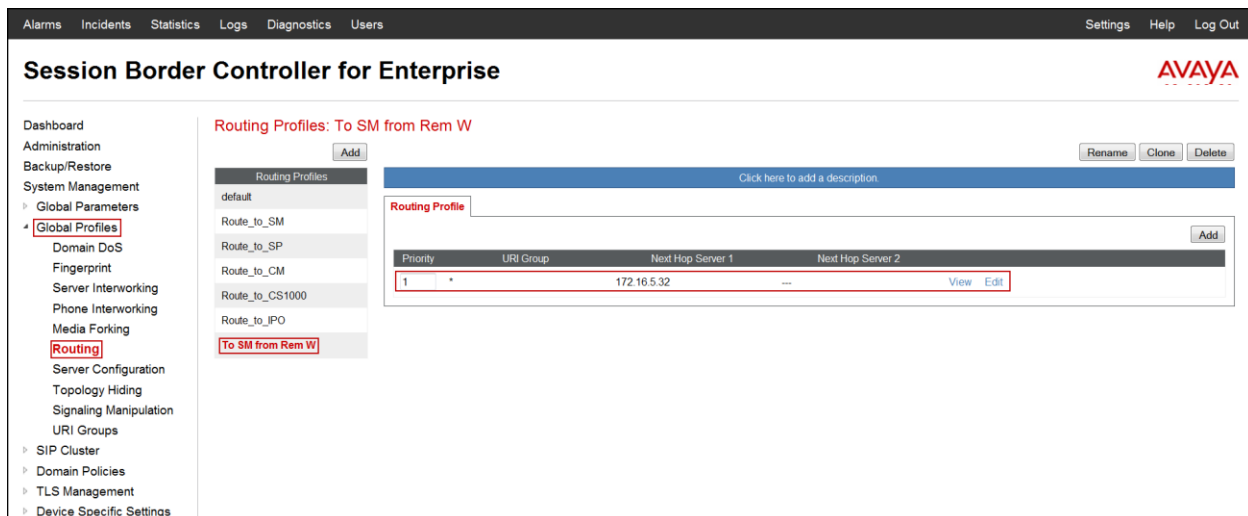
NAPTR ☐

SRV ☐

Outgoing Transport ☒ TLS ☐ TCP ☐ UDP

Back Finish

The following screenshot shows the newly created **To SM from Rem W** routing profile.



7.5.3. Server Configuration

Server Profiles should be created for the Avaya SBCE's peers. In the reference configuration, the server configuration by the name of **Session Manager** was previously created for SIP Trunking. The configuration shown was previously configured with TCP transport and port 5060. TLS transport and port 5061 were added for Remote Workers.

To edit an existing Server Configuration profile, under **Global Profiles → Server Configuration**, select the existing Server Configuration toward Session Manager and select **Edit** under the **General** tab (not shown). The following values were used in the reference configuration:

- Under **Supported Transports** select **TLS**.
- Under **TLS Port** enter **5061**.
- Keep all other values as default.
- Click on **Finish**.

Note: 172.16.5.32 is the IP address of Session Manager in the reference configuration. The Avaya SBCE used in the reference configuration was provisioned to support SIP Trunking and Remote Worker functionalities. If there is no existing configuration for SIP Trunking, and if the Server Configuration will only be used for Remote Workers, add a new Server Configuration profile with **TLS** transport and port **5061**.

The following screenshot shows the parameters under the **General** tab that were changed in the existing **Session Manager** Server Configuration profile, previously created for SIP Trunks.

Edit Server Configuration Profile - General X

This profile is in use by a SIP Cluster or is associated with a Turing Test Use Case in Media Rules and the Server Type cannot be changed.

Server Type: Call Server

IP Addresses / Supported FQDNs
Separate entries with commas: 172.16.5.32

Supported Transports:
☒ TCP
☐ UDP
☒ TLS

TCP Port: 5060

UDP Port:

TLS Port: 5061

Finish

On the existing **Session Manager** Server configuration profile, under the **Advanced** tab, select **Edit**, or if adding a new profile, continue selecting **Next** until the **Advanced** tab is reached. The following values were used in the reference configuration:

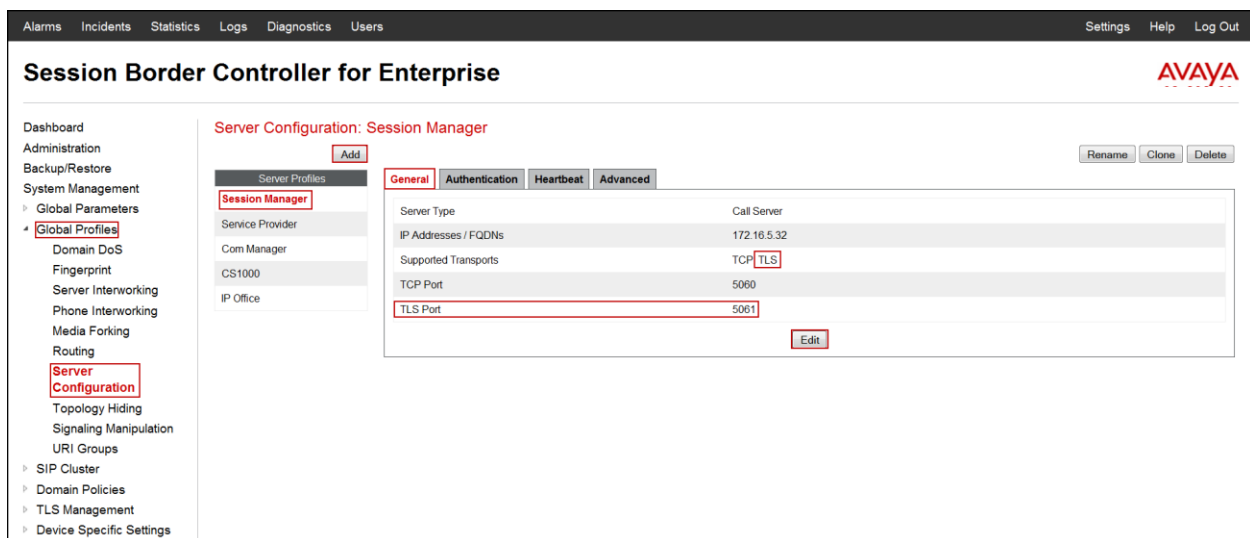
- Check **Enable Grooming**, if not already checked.
- Under Interworking Profile, **Avaya-SM** was previously created and was selected for SIP Trunking. If a new Server Configuration is being added, and if a **Server Interworking** profile was not previously created for SIP Trunks, select the interworking profile created in **Section 7.5.1**.
- Under **TLS Client Profile** select **AvayaSBCClient**.
- Keep all other values as default.
- Click on **Finish**.

Edit Server Configuration Profile - Advanced

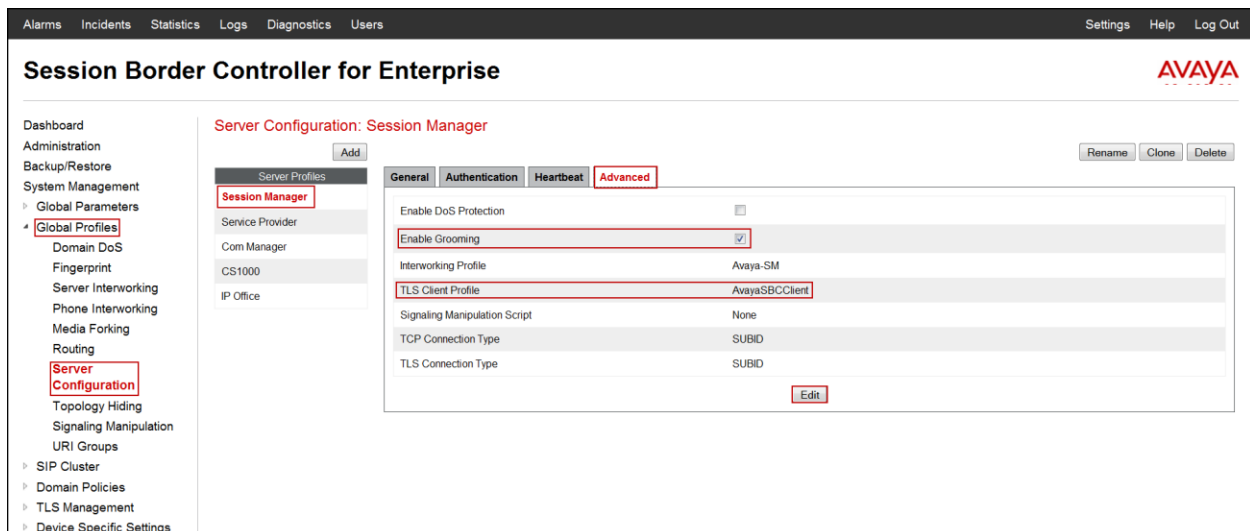
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
TLS Client Profile	AvayaSBCClient
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
TLS Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish

The following screenshot shows the **General** tab of the existing **Session Manager** Server Configuration profile after changes were made.



The following screenshot shows the **Advanced** tab of the existing **Session Manager** Server Configuration profile after changes were made.



7.6. SIP Cluster Proxy

A SIP Cluster Proxy is defined for Personal Profile Manager (PPM) data and Presence services between the Remote Worker endpoints and Session Manager. The following screen shows the cluster proxy named **Remote_Workers** created in the reference configuration. The SIP Cluster Proxy enables the remote Avaya SIP endpoints to send and receive PPM data to and from Session Manager via the Avaya SBCE.

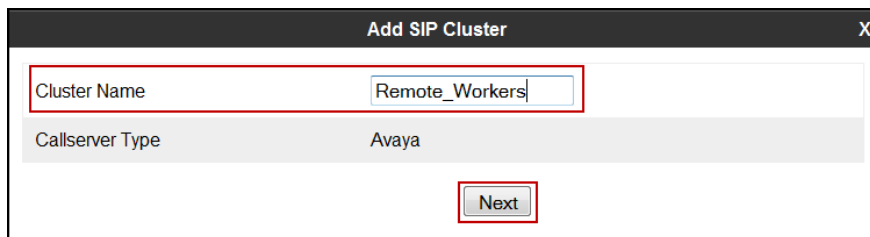
Note: A Presence Services server was not part of the reference configuration. Therefore, configuration of the Cluster Proxy for use with Presence is not shown.

The Cluster Proxy may be configured to use HTTPS between the Remote Worker phones and the Avaya SBCE, as well as between the Avaya SBCE and Session Manager. Alternatively, HTTP may be defined between the Avaya SBCE and Session Manager. In the reference configuration HTTPS was used between the Remote Worker phones and the Avaya SBCE and HTTP was used between the Avaya SBCE and Session Manager.

In this configuration HTTPS (port 443) is used between the Remote Workers and the Avaya SBCE, and HTTP (port 80) is used between the Avaya SBCE and Session Manager.

Under **SIP Cluster → Cluster Proxy**, select **Add** (not shown), use values specific to the enterprise. The following values were used in the reference configuration:

- Under **Cluster Name** enter **Remote_Workers** and click **Next**. Note that the **CallServer Type** field will default to **Avaya**.



The screenshot shows a dialog box titled "Add SIP Cluster" with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first field is labeled "Cluster Name" and contains the text "Remote_Workers". The second field is labeled "Callserver Type" and contains the text "Avaya". Below these fields is a button labeled "Next".

- Check **Secure Mode**, leave **SDP Capability Negotiation for SRTP** unchecked
- Under **Domain Name** field enter the enterprise domain name, *avaya.lab.com* was used.
- Under **Configuration Update Interval** field enter **15** (minutes). Note: This field is not used anymore but an entry is required.
- Click **Next**. The **Primary Device** window will open.

Add SIP Cluster

Security Information

Secure Mode ☒ Enabled

SDP Capability Negotiation for SRTP ☐ Enabled

Miscellaneous Information

Domain Name avaya.lab.com

Configuration Update Interval 15 minutes

Back Next

In the **Primary Device** section, PPM traffic received on **Device IP 192.168.157.180** (public IP) will be routed to the **Configuration Server Client Address 172.16.5.72** (private IP). Enter the following values (for IP address assignment refer to **Section 7.3**):

- Under **Device Name** the default is *Avaya SBCE* since it was previously defined.
- Under **Device IP** field enter *192.168.157.180* (public IP not used for relay services).
- Under **Configuration Server Client Address** field enter *172.16.5.72* (private IP).
- Click **Next** to open the **Configuration Server** window (note that “Finish” is shown in the screenshot below since this entry was previously created and **Edit** was used instead).

Edit Device

To change the device associated with this cluster device you will need to remove this cluster proxy and re-add it.

Device Configuration

Device Name Avaya SBCE

Device IP 192.168.157.180

Configuration Server Client Address 172.16.5.72

Finish

Under **Add Configuration Server** section enter the following values:

- Under **Server Type** select **HTTPS** from the drop down menu.
- Under **Real Server Type** select **HTTP** from the drop down menu.
- Under **Port** enter **443**.
- Under **Real Server IP** enter any IP address (e.g., **1.1.1.1**). This address entry is not used.
- Under **Real Server Port** enter **80**.
- Under **Server TLS Profile** the default value of **AvayaSBCServer** will be displayed.
- Click **Next**.

Add Configuration Server

Server Type: HTTPS

Real Server Type: HTTP

Options: ☐ Relay, ☐ Rewrite URL

Port: 443

Real Server IP: 1.1.1.1

Real Server Port: 80

Server TLS Profile: AvayaSBCServer

Back Next

Under **Add Signaling Server** section enter the following values:

- Under **Server Configuration Profile** field select **Session Manager** from the drop down menu.
- Under **End Point Signaling Interface** field select **RW_Public_sig** from the drop down menu. Note: **Signaling Interface** entries needs to be created first (refer to **Section 7.8.2**).
- Under **Session Policy Group** field use the **default** value.
- Click on **Finish**.

Edit Signaling Server

Server Configuration Profile: Session Manager

End Point Signaling Interface: RW_Public_sig

Session Policy Group: default

Finish

The following screenshot shows the **General** tab of the newly created **Remote_Workers** SIP Cluster Proxy.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows a navigation menu with 'SIP Cluster' and 'Cluster Proxy' highlighted. The main content area is titled 'Cluster Proxy: Remote_Workers' and features tabs for 'General', 'Primary', 'Secondary', and 'Tertiary'. The 'General' tab is active, showing the following configuration details:

Cluster Information	
Call Server Type	Avaya

Security Information	
Secure Mode	Enabled
SDP Capability Negotiation for SRTP	Disabled

Miscellaneous Information	
Domain Name	avaya.lab.com
Configuration Update Interval	15 minute(s)

An 'Edit' button is located at the bottom right of the configuration area.

The following screenshot shows the **Primary** tab of the newly created **Remote_Workers** SIP Cluster Proxy.

The screenshot displays the 'Session Border Controller for Enterprise' web interface, showing the 'Primary' tab of the 'Remote_Workers' SIP Cluster Proxy configuration. The left sidebar shows 'SIP Cluster' and 'Cluster Proxy' highlighted. The main content area is titled 'Cluster Proxy: Remote_Workers' and features tabs for 'General', 'Primary', 'Secondary', and 'Tertiary'. The 'Primary' tab is active, showing the following configuration details:

Device Information	
Device Name	Avaya SBCE
Device IP	192.168.157.180
Configuration Server Client Address	172.16.5.72

An 'Edit' button is located at the bottom right of the Device Information section.

Configuration Servers							
Type	Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TLS Profile
HTTPS	HTTP	443	1.1.1.1	80	--	--	AvayaSBCServer

An 'Add' button is located at the top right of the Configuration Servers section.

Signaling Servers		
Server Configuration Profile	End Point Signaling Interface	Session Policy Group
Session Manager	RW_Public_sig	default

An 'Add' button is located at the top right of the Signaling Servers section, and an 'Edit' button is located at the bottom right of the table.

7.7. Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

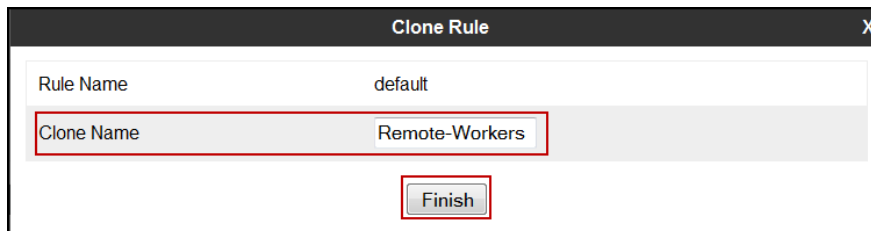
7.7.1. Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the Avaya SBCE will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules defines the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Note: The **Maximum Concurrent Sessions** and the **Maximum Sessions Per Endpoint** for Audio and Video should be set per the customer licenses purchased for the specific enterprise site. The values shown below are just an example; they represent the values used in the reference configuration.

From the navigation menu on the left-hand side, select **Domain Policies → Application Rules** (not shown).

- Select **default** in the **Application Rules** list (not shown).
- Click the **Clone** button on top right of the screen (not shown).
- Name: enter the name of the profile (e.g., **Remote-Workers**).
- Click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	Remote-Workers
<div>Finish</div>	

- Select the newly created Application Rule and Click **Edit** (not shown).
- For **Audio** set the **Maximum Concurrent Sessions to 2000**.
- For **Audio** set the **Maximum Sessions Per Endpoint to 10**.
- For **Video** set the **Maximum Concurrent Sessions to 100**.
- For **Video** set the **Maximum Sessions Per Endpoint to 10**.
- Click **Finish**.

Editing Rule: Remote-Workers

X

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	10
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	10
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support

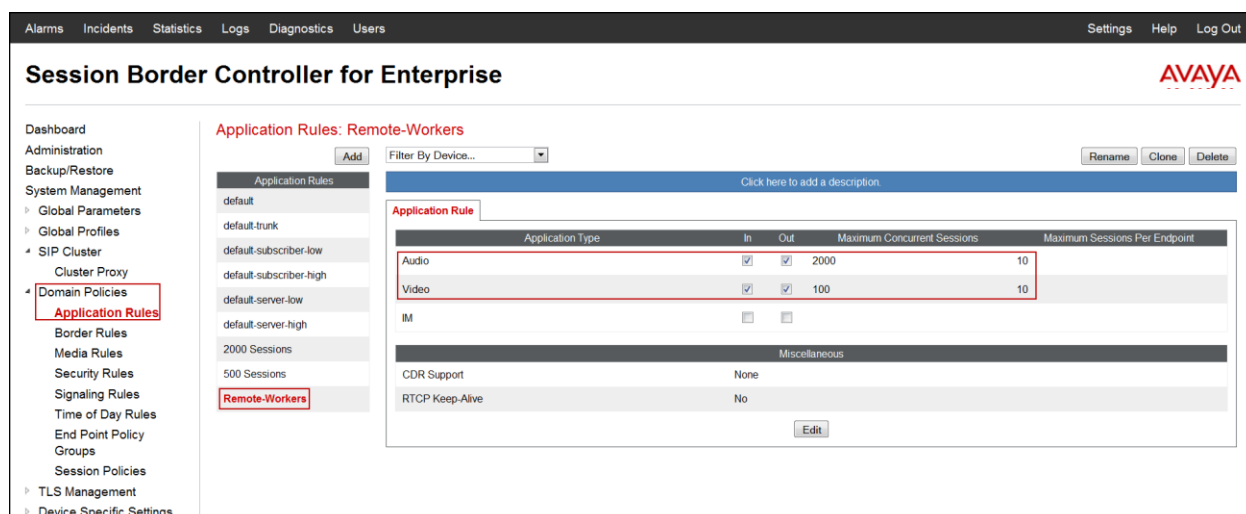
☒ None
☐ CDR w/ RTP
☐ CDR w/o RTP

RTCP Keep-Alive

☐

Finish

The following screen capture shows the newly created **Remote-Workers** application rule.

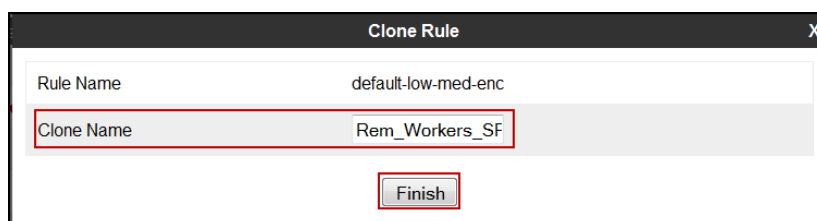


7.7.2. Media Rules

The following section shows the new Media Rule **Rem_Workers_SRTP** added for Remote Worker (cloned from the **default-low-med-enc** rule).

From the navigation menu on the left-hand side, select **Domain Policies** → **Media Rules** (not shown)

- Select **default-low-med-enc** in the **Media Rules** list (not shown).
- Click the **Clone** button on top right of the screen (not shown).
- Name: enter the name of the profile (e.g., **Rem_Workers_SRTP**).
- Click **Finish**.



For the newly created **Rem_Workers_SRTP** Media Rule, select the **Media Encryption** tab; click **Edit** (not shown):

Under **Audio Encryption** section, select the following values:

- From the drop down menu, set **Preferred Formats** to ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Uncheck **Encrypted RTCP**.
- Verify that **Interworking** is checked.

Under **Video Encryption** section, select the following values:

- From the drop down menu, set **Preferred Formats** to ***SRTP_AES_CM_128_HMAC_SHA1_80***.
- Verify **Encrypted RTCP** is unchecked.
- Verify that **Interworking** is checked.

Under the **Miscellaneous** section, select the following values

- Check **Capability Negotiation**.
- Click **Finish**.

Media Encryption

X

Audio Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Miscellaneous

Capability Negotiation

☒

Finish

For the newly created **Rem_Workers_SRTP** Media Rule, select the **Media QoS** tab; click **Edit** (not shown):

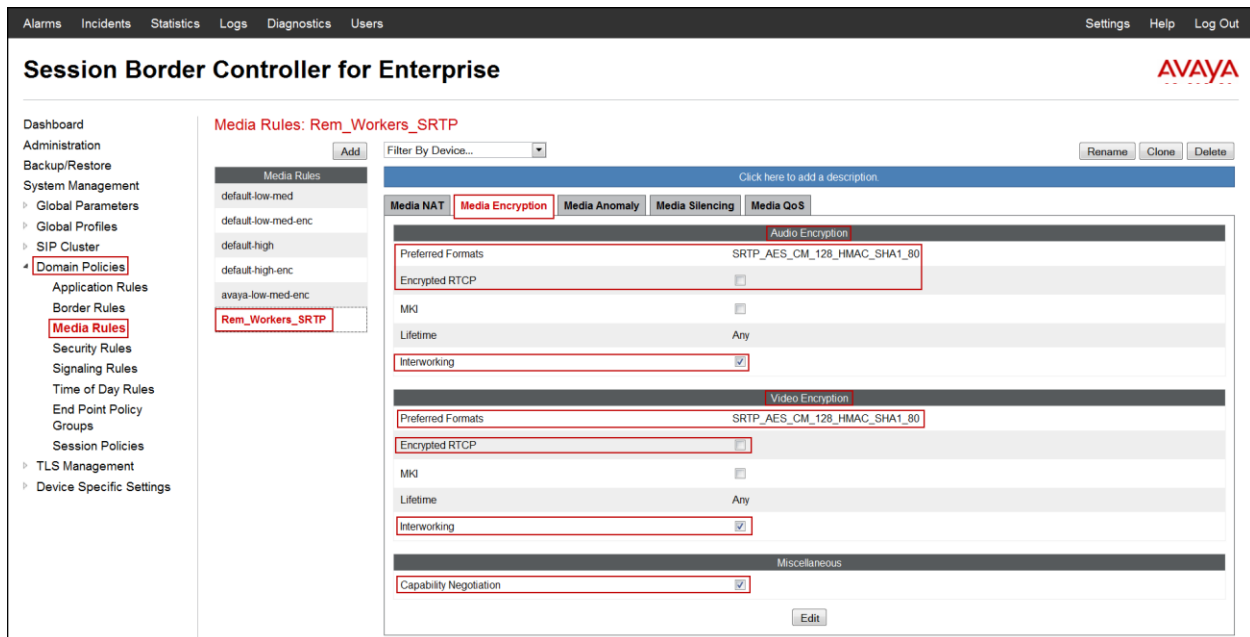
- Under **Media QoS Marking** check **Enabled**.
- Check **DSCP**.
- **DSCP** for Audio and Video will default to **EF**.
- Click **Finish**.

Media QoS Reporting		
RTCP Enabled	<input type="checkbox"/>	

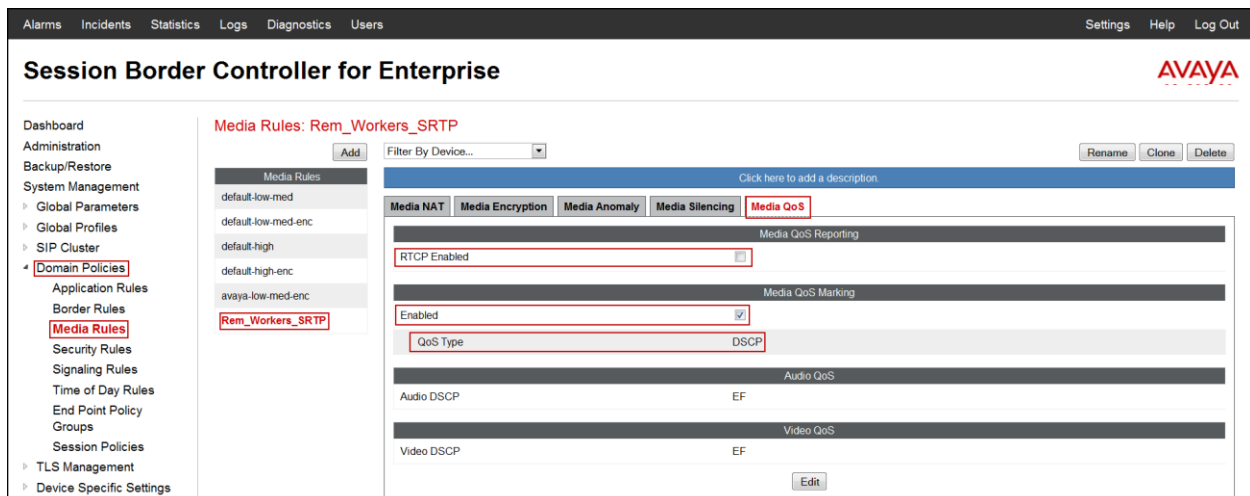
Media QoS Marking		
Enabled <input checked="" type="checkbox"/>		
<input type="radio"/> ToS		
Audio Precedence	Routine	000
Audio ToS	Minimize Delay	1000
Video Precedence	Routine	000
Video ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP		
Audio	EF	101110
Video	EF	101110
Finish		

Note: The Media **QoS** settings shown above are the recommended values (default). **QoS** values for audio and video should be set according to specific enterprise requirements and should match values agreed on, otherwise the Avaya SBCE will override the **QoS** values with the settings shown above.

The following screenshot shows the **Media Encryption** tab of the newly created **Rem_Workers_SRTP** Media Rule.



The following screenshot shows the **Media QoS** tab of the newly created **Rem_Workers_SRTP** Media Rule.



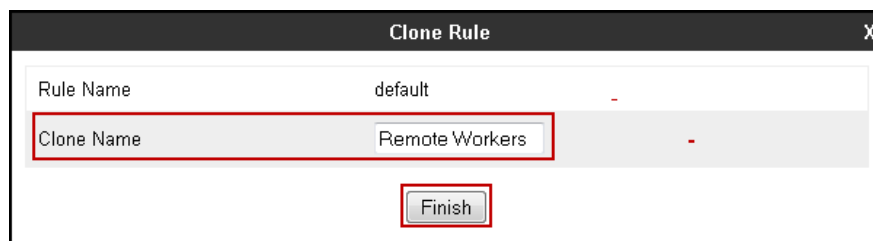
7.7.3. Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

The following section describes the new Signaling Rule **Remote Workers**, cloned from the **default** signaling rule.

From the navigation menu on the left-hand side, select **Domain Policies** → **Signaling Rules** (not shown).

- Select **default** in the **Signaling Rules** list (not shown).
- Click the **Clone** button on top right of the screen (not shown).
- Name: enter the name of the profile (e.g., **Remote Workers**).
- Click **Finish**.



For the newly created **Remote Workers** Signaling Rule, select the **Signaling QoS** tab; click **Edit** (not shown):

Under the **Signaling QoS** tab, enter the following values:

- Select **DSCP** (the **Value** field will default to **AF41**).
- Click **Finish**.



Note: The Media **QoS** settings shown above are the recommended values (default). **QoS** values for audio and video should be set according to specific enterprise requirements and should match values agreed on, otherwise the Avaya SBCE will override the **QoS** values with the settings shown above.

7.7.4. End Point Policy Groups

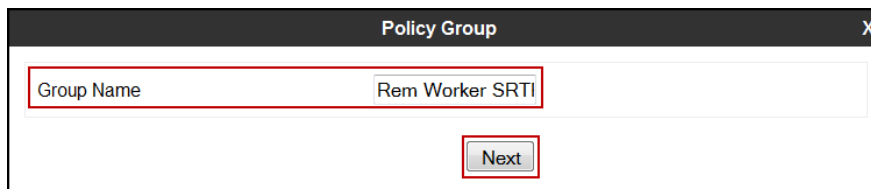
End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

Two new End Point Policy Groups were created for Remote Workers, **Rem Workers SRTP**, and **Rem Workers RTP**.

To create the new **Rem Workers SRTP** group, do the following:

Under **Domain Policies** → **End Point Policy Groups**, select **Add** (not shown), use values specific to the enterprise. The following values were used in the reference configuration:

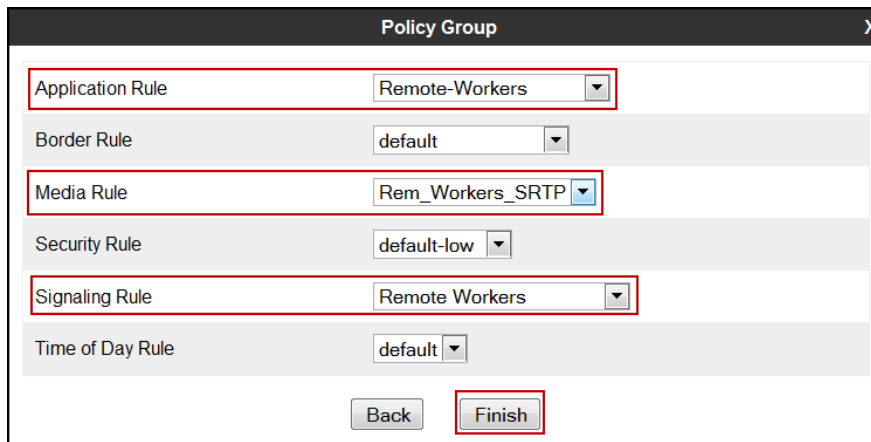
- Under **Group Name** enter *Rem Worker SRTP*.
- Click **Next**.



The screenshot shows a window titled "Policy Group" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Group Name" containing the text "Rem Worker SRTI". Below this field is a button labeled "Next". Both the input field and the button are highlighted with red rectangular boxes.

The **Policy Group** window will open. Enter the following:

- Under **Application Rule** select *Remote-Workers* from the drop down menu.
- Under **Media Rule** select *Remote_Workers_SRTP* from the drop down menu.
- Under **Signaling Rule** select *Remote Workers* from the drop down menu.
- Remaining fields should left with default values.
- Click **Finish**.



The screenshot shows the "Policy Group" window with several configuration options. Each option consists of a label and a dropdown menu. The dropdown menus are highlighted with red rectangular boxes. The options are: "Application Rule" set to "Remote-Workers", "Border Rule" set to "default", "Media Rule" set to "Rem_Workers_SRTP", "Security Rule" set to "default-low", "Signaling Rule" set to "Remote Workers", and "Time of Day Rule" set to "default". At the bottom of the window, there are two buttons: "Back" and "Finish". The "Finish" button is highlighted with a red rectangular box.

To create the new **Rem Workers RTP** End Point Policy Group, follow the above steps, use the following values:

- Under **Group Name** enter **Rem Worker RTP** (not shown).
- Under **Application Rule** select **Remote-Workers** from the drop down menu.
- Under **Media Rule** use the default value of **default-low-med**.
- Under **Signaling Rule** select **Remote Workers** from the drop down menu.
- Remaining fields should with default values.
- Click on **Finish**.

The following screenshot shows the newly created **Rem Workers SRTP** End Point Policy Group.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	Remote-Workers	default	Rem_Workers_SRTP	default-low	Remote Workers	default	Edit Clone

The following screenshot shows the newly created **Rem Workers RTP** End Point Policy Group.

Alarms

Incidents

Statistics

Logs

Diagnostics

Users

Settings

Help

Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

SIP Cluster

Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Time of Day Rules

End Point Policy Groups

Session Policies

TLS Management

Device Specific Settings

Policy Groups: Rem Workers RTP

Add

Filter By Device...

Rename

Clone

Delete

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

OCS-default-high

avaya-def-low-enc

avaya-def-high-subscriber

avaya-def-high-server

Enterprise

Service Provider

Rem Workers Inside

Rem Workers SRTP

Rem Workers RTP

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Add

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	Remote-Workers	default	default-low-med	default-low	Remote Workers	default	<div>EditClone</div>

7.8. Device Specific Settings

The Device Specific Settings allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

7.8.1. Media Interfaces

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

Under **Device Specific Settings** → **Media Interface**, select **Add** to create a new Media Interface (not shown). Use values specific to the enterprise, the following values were used in the reference configuration:

- Under **Name** enter *RW_Private_med*.
- Under **IP Address** pull down menu select *172.16.5.72*. This is the “private” IP address for interface A1 used for Remote Workers.
- Under **Port Range** leave the default port range of *35000-40000*.
- Click **Finish**.

The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "RW_Private_med", "IP Address" with a dropdown menu showing "172.16.5.72", and "Port Range" with the value "35000 - 40000". A "Finish" button is located at the bottom right of the dialog. A red rectangle highlights the input fields, and another red rectangle highlights the "Finish" button.

Repeat the above procedure for the “public” interfaces using the following values:

- Under **Name** enter ***RW_Public_med***.
- Under **IP Address** pull down menu select ***192.168.157.180***. This is one of the two “public” IP addresses for interface B1 used for Remote Worker (public IP not used for relay services).
- Under **Port Range** leave the default port range of ***35000-40000***.
- Click **Finish**.

The following screenshot shows the newly created **RW_Private_med** and **RW_Public_med** Media Interfaces.

Media Interface: Sipera

Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.71	35000 - 40000	Edit	Delete
Public_med	192.168.157.186	35000 - 40000	Edit	Delete
RW_Private_med	172.16.5.72	35000 - 40000	Edit	Delete
RW_Public_med	192.168.157.180	35000 - 40000	Edit	Delete

7.8.2. Signaling Interfaces

Under **Device Specific Settings** → **Signaling Interface**, select **Add** to create a new Signaling Interface (not shown). Use values specific to the enterprise, the following values were used in the sample configuration:

- Under **Name** enter ***RW_Private_sig***.
- Under **IP Address** pull down menu select ***172.16.5.72***. This is the private IP address for interface A1 used for Remote Workers.
- Under **TLS Port** enter ***5061***. TLS is the preferred transport towards Session Manager, port 5061 is used for TLS.
- Under **TLS Profile** the default ***AvayaSBCServer*** profile will be displayed.
- Click **Finish**.

Edit Signaling Interface X

Name	RW_Private_sig
IP Address	172.16.5.72
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
Enable Stun	<input type="checkbox"/>
TLS Port Leave blank to disable	5061
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Repeat the above procedure for the “public” interface using the following values:

- Under **Name** enter ***RW_Public_sig***.
- Under **IP Address** pull down menu select ***192.168.157.180***. This is one of the two “public” IP addresses for interface B1 used for Remote Worker (public IP not used for relay services).
- Under **TLS Port** enter ***5061***. TLS is the preferred transport towards the Remote Workers, port 5061 is used for TLS.
- Under **TLS Profile** the default ***AvayaSBCServer*** profile will be displayed.
- Click **Finish**.

Edit Signaling Interface X

Name	RW_Public_sig
IP Address	192.168.157.180 ▼
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
Enable Stun	<input type="checkbox"/>
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	AvayaSBCServer ▼
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

The following screenshot shows the newly created **RW_Private_sig** and **RW_Public_sig** Signaling Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Device Specific Settings' and 'Signaling Interface' highlighted. The main content area is titled 'Signaling Interface: Sipera' and contains a table of configured signaling interfaces. The table has columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. Two new interfaces, RW_Private_sig and RW_Public_sig, are listed and highlighted with a red box. Each interface entry includes 'Edit' and 'Delete' links. An 'Add' button is located at the top right of the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.71	5060	5060	---	None	Edit Delete
Public_sig	192.168.157.186	---	5060	---	None	Edit Delete
RW_Private_sig	172.16.5.72	---	---	5061	AvayaSBCServer	Edit Delete
RW_Public_sig	192.168.157.180	---	---	5061	AvayaSBCServer	Edit Delete

7.8.3. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

The End-Point Flows define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

7.8.3.1 Subscriber Flow

Three Subscriber Flows were defined for Remote Workers. One for each User Agent previously created, as follows: **Deskphones 96x1** (for Avaya 96x1 Deskphones), **Avaya Flare** (for Avaya Flare[®] Experience for Windows softphone) and **Avaya one-X Communicator** (for one-X[®] Communicator softphone).

The following screen shows the details of the Subscriber Flow **Deskphones 96x1** used in the reference configuration.

Under Device **Specific Setting** → **End Point Flows** → **Subscriber Flows** tab, click on **Add** (not shown). The following values were used in the reference configuration:

- Under **Flow Name** enter ***Rem Worker 96x1 TLS-SRTP***.
- Under **User Agent** select ***Deskphone 96x1*** from the pull down menu (created in **Section 7.4**).
- Under **Signaling Interface** select ***RW_Public_sig*** from the pull down menu (created in **Section 7.8.2**).
- Leave remaining fields with default values.
- Click **Next**.

The screenshot shows a dialog box titled "Add Flow" with a close button (X) in the top right corner. The dialog contains a "Criteria" section with the following fields:

- Flow Name:** A text input field containing "Rem Worker 96x1 TLS-SRTP".
- URI Group:** A dropdown menu with a single visible option, indicated by an asterisk (*).
- User Agent:** A dropdown menu with "Deskphones 96x1" selected.
- Source Subnet:** A text input field with an asterisk (*) and example text "Ex: 192.168.0.1/24".
- Via Host:** A text input field with an asterisk (*) and example text "Ex: domain.com, 192.168.0.1/24".
- Contact Host:** A text input field with an asterisk (*) and example text "Ex: domain.com, 192.168.0.1/24".
- Signaling Interface:** A dropdown menu with "RW_Public_sig" selected.

At the bottom of the dialog is a "Next" button.

The **Profile** and **Optional Settings** window will open. Enter the following values:

- Under **Media Interface** select ***RW_Public_med*** from the pull down menu (created in **Section 7.8.1**).
- Under **End Point Policy Group** select ***Rem Workers SRTP*** from the pull down menu (created in **Section 7.7.4**).
- Under **Routing Profile** select ***To SM from Rem W*** from the pull down menu (created in **Section 7.5.2**).
- Under **Phone Interworking Profile** select ***Avaya-RU*** from the pull down menu (existing default profile).
- Under **TLS Client Profile** select ***AvayaSBCClient*** from the pull down menu (existing profile).
- Leave remaining fields with default values.
- Click **Finish**.

Add Flow X

Certain End Point Policy Groups are not available because there are no RADIUS servers configured. To use End Point Policy Groups containing Security Rules configured for authentication please add a RADIUS server.

Profile

Source: ☒ Subscriber ☐ Click To Call

Methods Allowed Before REGISTER: INFO, MESSAGE, NOTIFY, OPTIONS

Media Interface: RW_Public_med

End Point Policy Group: Rem Workers SRTP

SIP Cluster Flow: ☐

Routing Profile: To SM from Rem W

Optional Settings

Topology Hiding Profile: None

Phone Interworking Profile: Avaya-Ru

TLS Client Profile: AvayaSBCClient

File Transfer Profile: None

Signaling Manipulation Script: None

Back Finish

Repeat the above steps to create Subscriber Flows for **Avaya Flare** (used with Avaya Flare[®] Experience for Windows softphone), as follows:

To create the **Avaya Flare** Subscriber Flow, click on **Add** (not shown). The following values were used in the reference configuration:

- Under **Flow Name** enter ***Rem Worker Flare TLS-SRTP***.
- Under **User Agent** select ***Avaya Flare*** from the pull down menu (created in **Section 7.4**).
- Under **Signaling Interface** select ***RW_Public_sig*** from the pull down menu (created in **Section 7.8.2**).
- Leave remaining fields with default values.
- Click **Next**.

Criteria

Flow Name	Rem Worker Flare TLS-SRTP
URI Group	*
User Agent	Avaya Flare
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	RW_Public_sig

Next

The **Profile** and **Optional Settings** window will open. The following values were used in the reference configuration:

- Under **Media Interface** select *RW_Public_med* from the pull down menu (created in **Section 7.8.1**).
- Under **End Point Policy Group** select *Rem Workers SRTP* from the pull down menu (created in **Section 7.7.4**) (see note below).
- Under **Routing Profile** select *To SM from Rem W* from the pull down menu (created in **Section 7.5.2**).
- Under **Phone Interworking Profile** select *Avaya-RU* from the pull down menu (existing default profile).
- Under **TLS Client Profile** select *AvayaSBCClient* from the pull down menu (existing profile).
- Leave remaining fields with default values.
- Click **Finish**.

Edit Flow: Rem Worker Flare TLS-SRTP

Certain End Point Policy Groups are not available because there are no RADIUS servers configured. To use End Point Policy Groups containing Security Rules configured for authentication please add a RADIUS server.

Profile

Source: ☒ Subscriber ☐ Click To Call

Methods Allowed Before REGISTER: INFO MESSAGE NOTIFY OPTIONS

Media Interface: RW_Public_med

End Point Policy Group: Rem Workers SRTP

SIP Cluster Flow: ☐

Routing Profile: To SM from Rem W

Optional Settings

Topology Hiding Profile: None

Phone Interworking Profile: Avaya-Ru

TLS Client Profile: AvayaSBCClient

File Transfer Profile: None

Signaling Manipulation Script: None

Back Finish

Note: The current release of Avaya Flare[®] Experience for Windows softphone (Rel. 1.1.4.23) doesn't support SRTP video encryption; testing was done with video disabled on the Avaya Flare[®] Experience for Windows PC client application (under **Settings → Video**). With the Avaya Flare[®] Experience for Windows End Point Policy Group setting shown above (**Rem Worker SRTP**), audio is encrypted across the public internet. With this setting; video has to be disabled on the Avaya Flare[®] Experience for Windows PC client application, as mentioned. If video is enabled with this setting, calls origination attempts from the PC client application will fail with busy tone to the user. If video is required for Remote Workers using Avaya Flare[®] Experience for Windows and audio/video encryption is not crucial to the enterprise across the public internet, the End Point Policy Group setting for the Avaya Flare[®] Experience for Windows shown above can be set to the value of **Rem Workers RTP** instead (selected from the pull down menu). With this setting, video can be enabled on the PC client application. Please keep in mind that with this setting media encryption of audio and video will not be done across the public internet. If privacy is crucial to the enterprise, **Rem Workers RTP** should not be used for audio. This restriction only applies to Remote Workers using Avaya Flare[®] Experience for Windows. The current release of one-X[®] Communicator softphone (Rel. 6.2.2.07-SP2) supports SRTP audio and video encryption.

Repeat the above steps to create a subscriber flow for **Avaya one-X Communicator** (used with Avaya one-X[®] Communicator softphone), as follows:

To create the **Avaya one-X Communicator** Subscriber Flow, click on **Add** (not shown). The following values were used in the reference configuration:

- Under **Flow Name** enter *Rem Worker one-XC TLS-SRTP*.
- Under **User Agent** select *Avaya one-X Communicator* from the pull down menu (created in **Section 7.4**).
- Under **Signaling Interface** select *RW_Public_sig* from the pull down menu (created in **Section 7.8.2**).
- Leave remaining fields with default values.
- Click **Next**.

The screenshot shows a web-based configuration interface titled "Edit Flow: Rem Worker one-XC TLS-RTP". It features a "Criteria" section with the following fields and values:

Field	Value
Flow Name	Rem Worker one-XC TLS-RTP
URI Group	*
User Agent	Avaya one-X Communicator
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	RW_Public_sig

A "Next" button is located at the bottom right of the form.

The **Profile** and **optional settings** window will open. The following values were used in the reference configuration:

- Under **Media Interface** select *RW_Public_med* from the pull down menu (created in **Section 7.8.1**).
- Under **End Point Policy Group** select *Rem Workers SRTP* from the pull down menu (created in **Section 7.7.4**).
- Under **Routing Profile** select *To SM from Rem W* from the pull down menu (created in **Section 7.5.2**).
- Under **Phone Interworking Profile** select *Avaya-Ru* from the pull down menu (existing default profile).
- Under **TLS Client Profile** select *AvayaSBCClient* from the pull down menu (existing profile).
- Leave remaining fields with default values.
- Click **Finish**.

Edit Flow: Rem Worker one-XC TLS-RTP

Certain End Point Policy Groups are not available because there are no RADIUS servers configured. To use End Point Policy Groups containing Security Rules configured for authentication please add a RADIUS server.

Profile

Source: ☒ Subscriber ☐ Click To Call

Methods Allowed Before REGISTER: INFO MESSAGE NOTIFY OPTIONS

Media Interface: RW_Public_med

End Point Policy Group: Rem Workers SRTP

SIP Cluster Flow: ☐

Routing Profile: To SM from Rem W

Optional Settings

Topology Hiding Profile: None

Phone Interworking Profile: Avaya-Ru

TLS Client Profile: AvayaSBCClient

File Transfer Profile: None

Signaling Manipulation Script: None

Back Finish

The following screenshot shows the newly created Subscriber Flows.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo.

On the left sidebar, the "Device Specific Settings" menu is expanded, showing options like Network Management, Media Interface, Signaling Interface, Signaling Forking, End Point Flows (highlighted), Session Flows, Relay Services, SNMP, Syslog Management, Advanced Options, and Troubleshooting.

The main content area is titled "End Point Flows: Sipera". It features two tabs: "Subscriber Flows" (active) and "Server Flows". Below the tabs, there is an "Update" button and an "Add" button. A table lists the configured flows:

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group	View	Clone	Edit	Delete
1	Rem Worker 96x1 TLS-SRTP	*	*	Desktopphones 96x1	Rem Workers SRTP	View	Clone	Edit	Delete
2	Rem Worker Flare TLS-SRTP	*	*	Avaya Flare	Rem Workers SRTP	View	Clone	Edit	Delete
3	Rem Worker one-XC TLS-RTP	*	*	Avaya one-X Communicator	Rem Workers SRTP	View	Clone	Edit	Delete

7.8.3.2 Remote Worker Server Flow

The following screens show the new Server Flow settings for Remote Worker access to Session Manager.

To create a new Server Flow for Remote Workers access to Session Manager, do the following:

Under **Device Specific Setting** → **End Point Flows** → **Server Flows** tab, click on **Add** (not shown). The following values were used in the reference configuration:

- Under **Flow Name** enter *SM from Rem Workers*.
- Under **Server Configuration** select *Session Manager* from the pull down menu (created in **Section 7.5.3**).
- Under **Received Interface** select *RW_Public_Sig* from the pull down menu (created in **Section 7.8.2**).
- Under **Signaling Interface** select *RW_Private_Sig* from the pull down menu (created in **Section 7.8.2**).
- Under **Media Interface** select *RW_Private_med* from the pull down menu (created in **Section 7.8.1**).
- Under **End Point Policy Group** select *Rem Workers RTP* from the pull down menu (created in **Section 7.7.4**) (see note below).
- Under **Topology Hiding Profile** select *default* from the pull down menu.
- Leave remaining fields with default values.
- Click **Finish**.

The screenshot shows the 'Add Flow' configuration window with the following settings:

Field	Value
Flow Name	SM from Rem Workers
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	RW_Public_sig
Signaling Interface	RW_Private_sig
Media Interface	RW_Private_med
End Point Policy Group	Rem Workers RTP
Routing Profile	default
Topology Hiding Profile	default
File Transfer Profile	None

The 'Finish' button is located at the bottom right of the window.

The following screenshot shows the newly created **SM from Rem Workers** Server Flow. The other Server Flows shown in the screenshot (not enclosed in red bracket) were previously added and are used for SIP Trunking only; they are not relevant to Remote Worker functionality.

Session Border Controller for Enterprise

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management **Device Specific Settings** Network Management Media Interface Signaling Interface Signaling Forking **End Point Flows** Session Flows Relay Services SNMP Syslog Management Advanced Options Troubleshooting

End Point Flows: Sipera

Devices **Sipera**

Subscriber Flows **Server Flows**

Hover over a row to see its description.

Server Configuration: Service Provider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP_Trunk_Flow	*	Private_sig	Public_sig	Service Provider	Route_to_SM	View Clone Edit Delete

Server Configuration: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM from Rem Workers	*	RW_Public_sig	RW_Private_sig	Rem Workers RTP	default	View Clone Edit Delete
2	Session_Manager_Flow	*	Public_sig	Private_sig	Enterprise	Route_to_SP	View Clone Edit Delete

Note: With the End Point Policy Group setting of **Rem Workers RTP** assigned to the Server Flow shown above, RTP, or non-media encryption, will be used inside of the enterprise (private network side), this is the recommended value inside of the enterprise (private network side). Keep in mind that Server Flow settings only impact how signaling and media will be treated inside of the enterprise (private network side), while Subscriber Flow settings impact how signaling and media will be treated outside of the enterprise (public network side).

7.8.4. Relay Services

Relay Services are used to define how file transfers (e.g., for phone firmware upgrades and configuration), are routed to the Remote Worker endpoints. Both HTTP and HTTPS protocols are supported.

In the reference configuration, both protocols (HTTP and HTTPS) were configured and used for accessing the file server located at the enterprise, HTTPS is the preferred method. To create a new Relay Service for Remote Workers, do the following:

7.8.4.1 For accessing the file server using HTTP protocol:

Under **Device Specific Setting** → **Relay Services**, click on **Add** (not shown).

The following values were used in the reference configuration:

Under the **Remote Configuration** section:

- Set **Remote Domain** to the enterprise domain name (e.g., *avaya.lab.com*) (match the enterprise domain name used in Session Manager).
- Under **Remote IP** enter the IP address of the enterprise HTTP file server (e.g., *172.16.5.250*) used to provide the firmware file updates and configuration files to Remote Worker endpoints.
- Under **Remote Port** enter *80* (HTTP).
- Under **Remote Transport** select *TCP*.

Under the **Device Configuration** section:

- Set the **Remote Domain** to the enterprise domain name (e.g., *avaya.lab.com*) (match the enterprise domain name used in Session Manager).
- Under **Listen IP** select the IP address of the Avaya SBCE's public IP address designated for file transfers/relay services (*192.168.157.181*).
- Under **Listen Port** enter *80* (HTTP).
- Under **Connected IP** select the internal or private IP address of the Avaya SBCE used for Remote Worker (*172.16.5.72*).
- Under **Listen Transport** select *TCP*.
- Click on **Finish**.

Add Application RelayX

Remote Configuration

Remote Domain

avaya.lab.com

Remote IP

172.16.5.250

Remote Port

80

Remote Transport

TCP

Device Configuration

Published Domain

avaya.lab.com

Listen IP

192.168.157.181

Listen Port

80

Connect IP

172.16.5.72

Listen Transport

TCP

General Configuration

Whitelist Flows

☐

Use Relay Actors

☐

Options

Use Ctrl+Click to select or deselect multiple items.

RTCP Monitoring

End-to-End Rewrite

Hop-by-Hop Traceroute

Bridging

Finish

7.8.4.2 For accessing the file server using HTTPS protocol:

Under **Device Specific Setting** → **Relay Services**, click on **Add** (not shown). The following values were used in the reference configuration:

Under the **Remote Configuration** section:

- Set **Remote Domain** to the enterprise domain name (e.g., *avaya.lab.com*) (match the enterprise domain name used in Session Manager).
- Under **Remote IP** enter the IP address of the enterprise file server (e.g., *172.16.5.250*) used to provide the firmware updates and configuration data to Remote Worker endpoints.
- Under **Remote Port** enter *443* (HTTPS).
- Under **Remote Transport** select *TCP*.

Under the **Device Configuration** section:

- Set the **Remote Domain** to the enterprise domain name (e.g., *avaya.lab.com*) (match the enterprise domain name used in Session Manager).
- Under **Listen IP** select the IP address of the Avaya SBCE's public IP address designated for file transfers/relay services (*192.168.157.181*).
- Under **Listen Port** enter *443* (HTTPS).
- Under **Connected IP** select the internal or private IP address of the Avaya SBCE used for Remote Worker (*172.16.5.72*).
- Under **Listen Transport** select *TCP*.
- Click on **Finish**.

Add Application RelayX

Remote Configuration

Remote Domain

avaya.lab.com

Remote IP

172.16.5.250

Remote Port

443

Remote Transport

TCP

Device Configuration

Published Domain

avaya.lab.com

Listen IP

192.168.157.181

Listen Port

443

Connect IP

172.16.5.72

Listen Transport

TCP

General Configuration

Whitelist Flows

☐

Use Relay Actors

☐

Options

Use Ctrl+Click to select or deselect multiple items.

RTCP Monitoring

End-to-End Rewrite

Hop-by-Hop Traceroute

Bridging

Finish

The following screenshot shows the newly created Relay Services.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Relay Services" highlighted under "Device Specific Settings". The main content area is titled "Relay Services: Avaya SBCE" and features two tabs: "Application Relay" (selected) and "File Transfer". Below the tabs is a table listing configured relay services. The table has columns for Remote Domain, Remote IP:Port, Remote Transport, Published Domain, Listen IP:Port, Listen Transport, and Connect IP. Two entries are shown, both for the domain "avaya.lab.com". Each entry includes "View", "Edit", and "Delete" links. An "Add" button is located in the top right corner of the table area.

Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP	
avaya.lab.com	172.16.5.250:80	TCP	avaya.lab.com	192.168.157.181:80	TCP	172.16.5.72	View Edit Delete
avaya.lab.com	172.16.5.250:443	TCP	avaya.lab.com	192.168.157.181:443	TCP	172.16.5.72	View Edit Delete

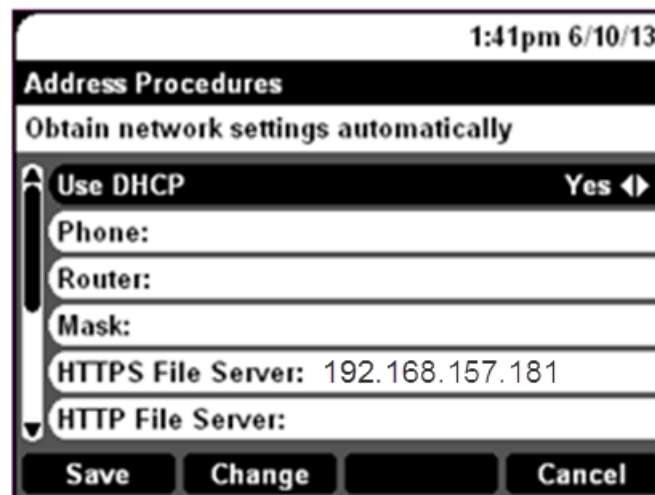
8. Remote Worker IP Deskphones (96x1 SIP) Configuration

The following screens illustrate the administration settings for a Remote Worker 96x1 SIP Deskphone used in the reference configuration.

8.1. ADDR Screen

In the reference configuration, both protocols (HTTP and HTTPS) were used for accessing the file server located at the enterprise. HTTPS is the preferred method, shown below.

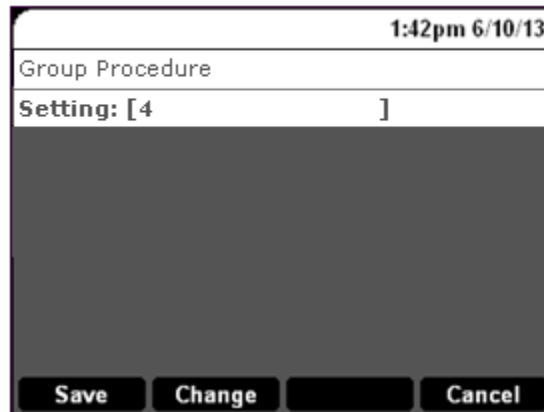
In the reference configuration, the 96x1 SIP Deskphones used DHCP to receive IP address assignments, therefore the **Use DHCP** field was set to **Yes** (a router was used as the DHCP server as well as the firewall and default gateway, see **Section 3**). Since HTTPS is the preferred method for file transfer, an HTTPS file server was configured at the enterprise. The Avaya SBCE IP address defined for Remote Worker file transfers/relay services, **192.168.157.181**, was specified in the **HTTPS File Server** field.



The screenshot displays the 'ADDR' screen of a device. At the top right, the time and date '1:41pm 6/10/13' are shown. The title 'Address Procedures' is centered. Below it, the option 'Obtain network settings automatically' is selected. A scrollable list contains the following items: 'Use DHCP' (set to 'Yes'), 'Phone:', 'Router:', 'Mask:', 'HTTPS File Server: 192.168.157.181', and 'HTTP File Server:'. At the bottom, there are four buttons: 'Save', 'Change', and 'Cancel'.

8.2. Set Group Number Screen

In the reference configuration, the Remote Worker 96x1 Deskphones was set to use group **4**. The configuration parameters used specifically for Remote Worker endpoints are specified in the 46xxsettings.txt file under this group number, refer to **Section 8.3** below. Non-Remote Worker endpoints used **GROUP_0** (not shown under the 46xxsettings.txt file).



Note: In the reference configuration, the setting parameters: **Use DHCP** set to *Yes* is the default value for new phones. **HTTPS File Server** and **GROUP** specified above were the only settings that were configured manually on the Remote Worker 96x1 SIP Deskphones, remaining configuration parameters were downloaded automatically from the **46xxsettings.txt** file once the connection to the HTTPS file server was established. The DHCP server can also be used to automatically assign values, such as the HTTPS File Server address, this is accomplished with the use of DHCP options, not shown here.

8.3. Avaya IP Deskphones (96x1 SIP) 46xxsettings Configuration File

The **46xxsettings.txt** file contains configuration parameters used by Avaya IP endpoints. This file resides in the HTTPS file server used in the reference configuration. Whenever an Avaya IP endpoint is rebooted, it will attempt to download the **46xxsettings** file from the designated file server.

In the **46xxsettings** file, **GROUP_4** specifies parameters specifically used by Remote Worker endpoints, non-Remote Worker endpoints use **GROUP_0** (not shown)

```
##### For Remote Workers #####
IF $GROUP SEQ 4 GOTO GROUP_4
##
# GROUP_4
##### Add SET Statements for GROUP 4 below #####
SET SIG 2
SET SIPDOMAIN avaya.lab.com
SET SIP_CONTROLLER_LIST 192.168.157.180:5061;transport=tls
SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 0
SET CONFIG_SERVER 192.168.157.180
SET CONFIG_SERVER_SECURE_MODE 2
SET DIALPLAN 3xxx|5xxx|91xxxxxxxxxx|9[2-9]xxxxxxxx
SET GMTOFFSET "-5:00"
SET WAIT_FOR_REGISTRATION_TIMER 40
SET SECURECALL 1
SET MEDIAENCRYPTION 1

##### END OF GROUP 4 SETTINGS #####
GOTO END
```

9. Personal Computer (PC) Configuration

This section describes the Personal Computer (PC) settings required when running Avaya Flare® Experience for Windows or Avaya one-X® Communicator on a PC used for Remote Workers.

In the reference configuration, the Network Adapter on the PC was configured to ***obtain an IP address automatically***.

9.1. Remote Worker Avaya Flare® Experience for Windows Configuration

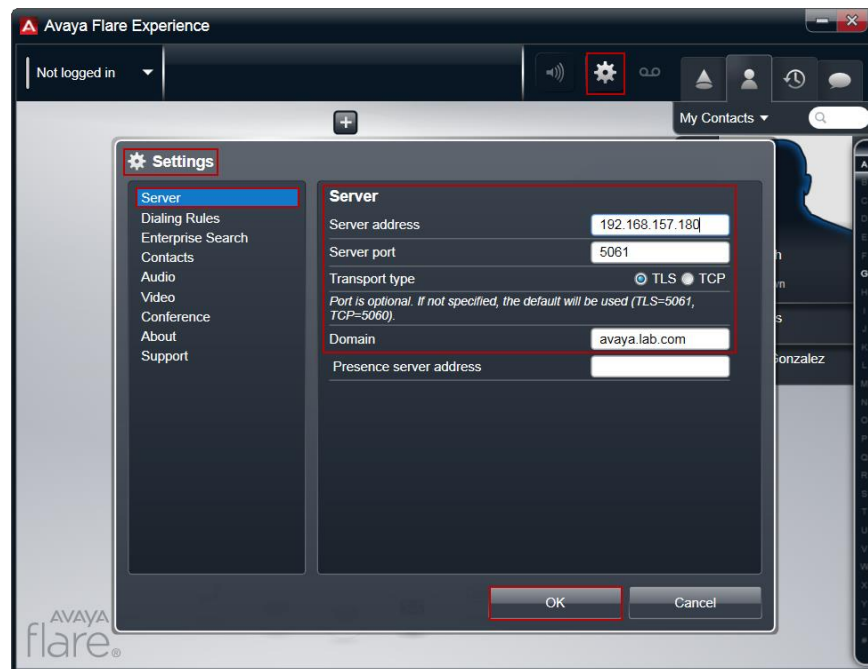
The following screens illustrate the Avaya Flare® Experience for Windows administration settings for the Remote Worker used in the reference configuration.

To configure Avaya Flare® Experience for Windows, do the following:

On the Avaya Flare® Experience for Windows application running on the PC, click on the **Settings** icon on the top right to display the **Settings** window.

Click on **Server**, the following values were used in the reference configuration:

- Under **Server address** enter **192.168.157.180** (This is one of the two “public” IP addresses for interface B1 on the Avaya SBCE used for Remote Worker access to Session Manager (public IP not used for relay services).
- Under **Transport type** select **TLS**.
- **Server port** will default to **5061** if TLS was selected above.
- Under **Domain** enter the enterprise domain name, **avaya.lab.com** in the reference configuration (match the enterprise domain name used in Session Manager).
- Click **OK**.



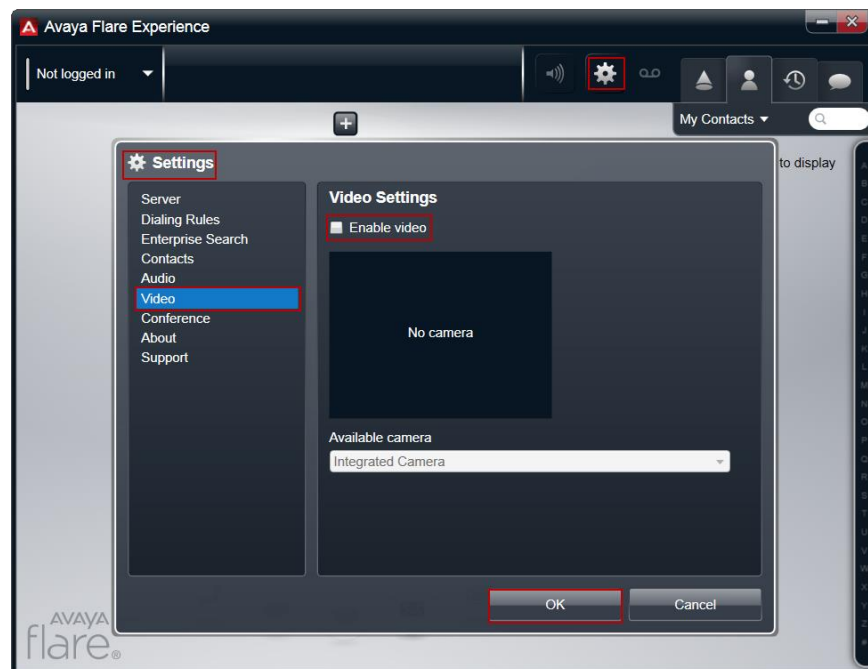
As mentioned previously, currently SRTP video encryption is not supported on Avaya Flare® Experience for Windows (Release 1.1.4.23), thus if SRTP encryption for audio is enabled under the Avaya SBCE Subscriber Flows, ensure video is disabled as shown below. If video is enabled the user will get a busy signal when attempting to make call; refer to **Section 7.8.3.1**.

To verify that video is disabled do the following:

Click on the **Settings** icon on the top right to display the Settings window.

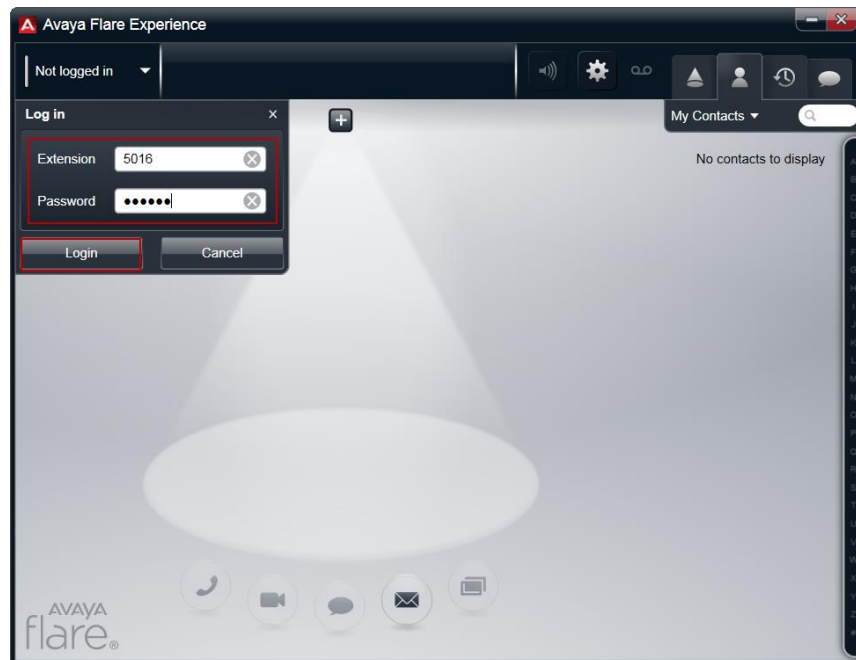
Click on **Video**, the following value was used in the reference configuration:

- Verify that **Enable video** is **not** checked.
- Click **OK**.

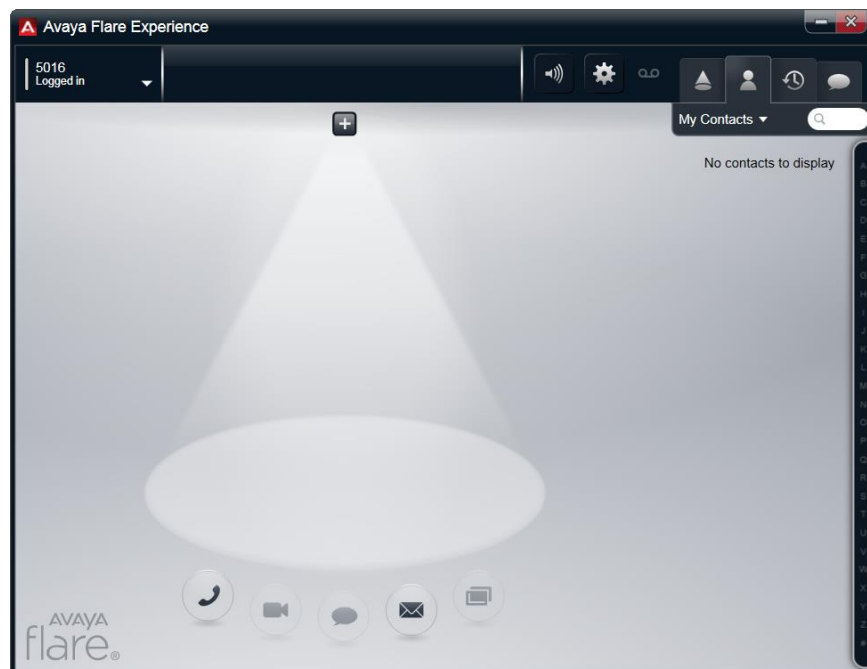


To login into Avaya Flare® Experience for Windows:

- Enter the **Extension** number provided for the Remote Worker user.
- Enter the **Password** provided for the Remote Worker user.
- Click **Login**.



The following screen will appear after the login process is completed, the Remote Worker user is now ready to make and receive audio calls.



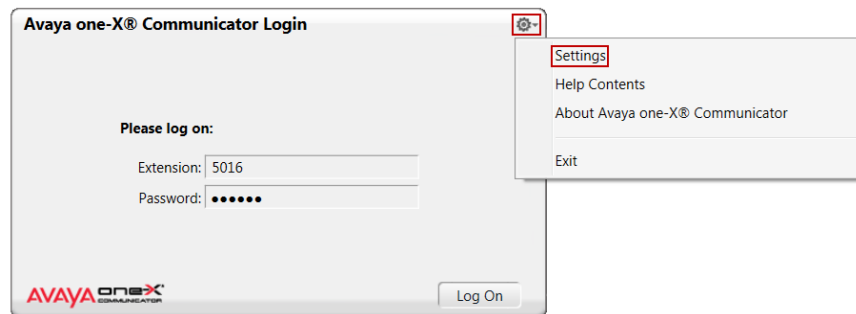
9.2. Remote Worker Avaya one-X® Communicator Configuration

The following screens illustrate Avaya one-X® Communicator administration settings for the Remote Worker used in the reference configuration.

To configure Avaya one-X® Communicator, do the following:

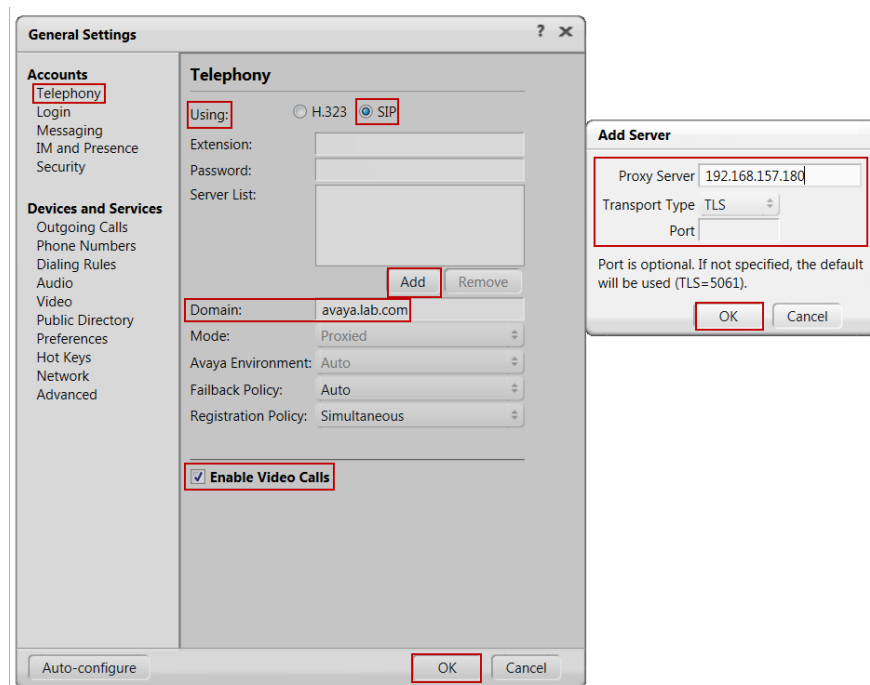
On the Avaya one-X® Communicator application running on the PC, click on the **Settings** icon on the top right to display the Settings window.

- Click on **Settings**.



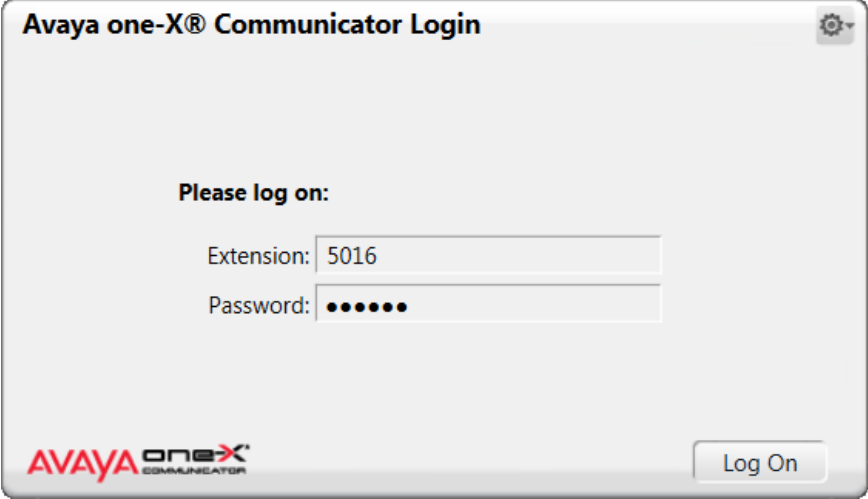
Click on **Telephony**, the **General Settings** window will appear. The following values were used in the reference configuration:

- Under **Using:** select **SIP** (SIP must be selected; H.323 is not supported for Remote Workers).
- Under **Server List**, click **Add** (the **Add Server** window to the right will appear).
- Under **Proxy Server** enter **192.168.157.180** (This is one of the two “public” IP addresses for interface B1 on the Avaya SBCE used for Remote Worker access to Session Manager (public IP not used for relay services).
- Under **Transport** select **TLS**.
- **Server port** will default to **5061** if TLS was selected above.
- Click **OK** on the **Add Server** window.
- Under **Domain** enter the enterprise domain name, **avaya.lab.com** in the reference configuration.
- **Enable Video Calls** can be checked if the Remote Worker user wishes to use video (SRTP audio and video encryption is supported on Avaya one-X® Communicator).
- Click **OK** under the **General Settings** window.



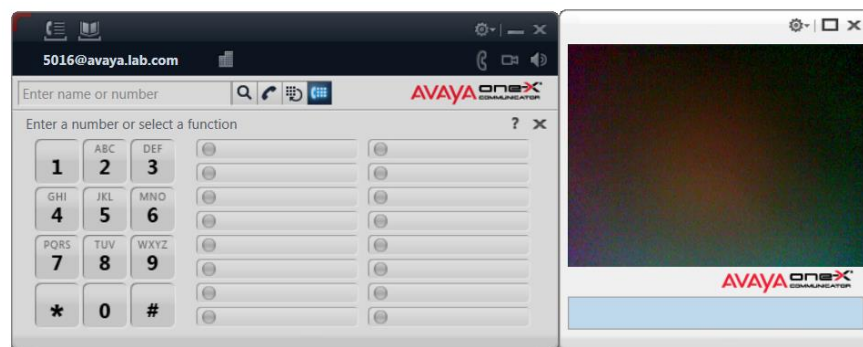
To login into Avaya one-X® Communicator:

- Enter the **Extension** number provided for the Remote Worker user.
- Enter the **Password** provided for the Remote Worker user.
- Click **Log On**.



The image shows a login window titled "Avaya one-X® Communicator Login". It contains a "Please log on:" section with two input fields: "Extension:" with the value "5016" and "Password:" with masked characters "••••••". At the bottom right is a "Log On" button. The Avaya one-X Communicator logo is at the bottom left.

The following screen will appear after the login process is completed. Note that **Enable Video Calls** was selected above, a separate video window will appear to the right. The Remote Worker user is ready to make and receive audio calls with video.



10. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya Aura® Communication Manager, including the following, is available at: <http://support.avaya.com/>

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, June 2014, Document Number 03-300509.

Product documentation for Avaya Aura® System Manager, including the following, is available at: <http://support.avaya.com/>

- [2] *Administering Avaya Aura® System Manager for Release 6.3.8*, Issue 4, Issue 4, June 2014.

Product documentation for Avaya Aura® Session Manager, including the following, is available at: <http://support.avaya.com/>

- [3] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 4, June 2014.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: <http://support.avaya.com/>

- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014.
- [5] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2013.
- [6] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 4, June 2014.

Product documentation for the Avaya 96x1 IP Deskphones, Avaya one-X® Communicator and Avaya Flare® Experience for Windows, including the following, is available at: <http://support.avaya.com/>

- [7] *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*, Release 6.3.1, Issue 3, January 2014
- [8] *Administering Avaya one-X® Communicator*, July 2013.
- [9] *Using Avaya one-X® Communicator*, Release 6.2, December 2013
- [10] *Administering Avaya Flare® Experience for Windows*, Release 1.1, Document Number: 18-604156, Issue 4, September 2013.
- [11] *Implementing Avaya Flare® Experience for Windows*, Release 1.1, Document Number: 18-604153, Issue 2, February 2013.
- [12] *How to Add SIP users in Avaya Aura Session Manager*, Documents ID: VIDEO100959, Version 1.0, July 17, 2014.

©2014 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.