



Administering Avaya Mobile Video

Release 3.4
Issue 1.0
December 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:
<http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Hosted Service

“**Hosted Service**” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo), UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “**Software**” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware

products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “**Designated Processor**” means a single stand-alone computing device. “**Server**” means a Designated Processor that hosts a software application to be accessed by multiple users. “**Instance**” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“**VM**”) or similar deployment.

License types

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “**Named User**,” means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “**Named User**” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Heritage Nortel Software

“**Heritage Nortel Software**” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link “**Heritage Nortel Products**,” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“**Third Party Components**” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“**Third Party Components**”), which contain terms regarding the rights to use certain portions of the Software (“**Third Party Terms**”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE [WWW.SIPRO.COM/CONTACT.HTML](http://www.sipro.com/contact.html). THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	8
Purpose	8
Chapter 2: Overview	9
Avaya Mobile Video Application Server Platform.....	9
Audit Logging	9
Chapter 3: Avaya Mobile Video Server Administration Interfaces	11
Avaya Mobile Video Application Server Management Console.....	11
Avaya Mobile Video Gateway Administration Interface	11
Setting Password Constraints	11
Resetting Administrator Credentials.....	13
Chapter 4: Configuring User Credentials	14
LOCAL Authentication.....	14
LDAP Authentication	15
<i>Enabling LDAP Authentication</i>	<i>15</i>
<i>Configuring LDAP Authentication</i>	<i>16</i>
Importing Certificates to the LDAP Truststore.....	18
Chapter 5: Configuring the Avaya Mobile Video Gateway.....	25
Configuring for Voice and Video Calls	25
<i>Defining Banned Codecs</i>	<i>25</i>
<i>Prioritizing Codecs</i>	<i>27</i>
<i>Configuring video resolution</i>	<i>28</i>
<i>Configuring video settings.....</i>	<i>29</i>
<i>Configuring Bitrates.....</i>	<i>30</i>
<i>WebRTC Configuration.....</i>	<i>32</i>
<i>Capturing logs on the Gateway.....</i>	<i>33</i>
To Capture Logs for a Specific Period	34
Configuring Media Brokers.....	35
<i>Setting up the Interface with the Avaya Mobile Video Gateway</i>	<i>35</i>
<i>General Media Broker Configuration</i>	<i>36</i>
<i>Configuring RTP Settings</i>	<i>38</i>
<i>Enabling secure communications between Media Broker and the Web Gateway</i>	<i>38</i>
<i>Call Admission Control.....</i>	<i>39</i>
Call Limit Based Call Admission Control	39
<i>Starting and Stopping Avaya Mobile Video Media Brokers</i>	<i>40</i>
<i>Capturing logs on the Media Broker</i>	<i>40</i>
Configuring the Web Application ID	42
Chapter 6: Configuring Traffic Segregation	43
Internal SIP Traffic.....	44
External Traffic	44
Configuring SIP Network Settings.....	45

Configuring WebRTC Client Settings	46
Example Configuration	49
<i>Avaya Mobile Video Media Broker general settings</i>	50
<i>SIP Network Settings</i>	50
Avaya Mobile Video Media Broker 1	50
Avaya Mobile Video Media Broker 2	51
<i>WebRTC Client Settings</i>	51
Avaya Mobile Video Media Broker 1	51
Avaya Mobile Video Media Broker 2	51
Connection Monitoring	51
<i>Configuring Monitored Connections</i>	53
Chapter 7: Avaya Mobile Video Media Broker Statistics	55
Media Broker Status	55
<i>Media Broker Load</i>	55
<i>Connectivity</i>	55
<i>Statistics</i>	56
Call Log	56
<i>Call Statistics</i>	58
<i>Call Details Log</i>	59
To Change the SIP Call Logging Level	59
Performance Log	60
Chapter 8: Configuring SNMP	61
Configuring the SNMP Agent	61
<i>Configuring SNMP Trap Targets</i>	62
Configuring the SNMP Client	63
Avaya Mobile Video Application Server SNMP Traps	63
<i>Example Scenarios</i>	64
<i>Decoding the Resource ID</i>	64
<i>Traps Raised on MVS Startup</i>	65
Configuring SNMP Trap Security	65
<i>SNMP Security Levels and Users</i>	66
<i>Implementing SNMPv3 Security</i>	66
<i>Configuring the SNMP Client</i>	67
<i>SNMP View Access Control</i>	67
Chapter 9: Resources	72
Documentation	72
Training	72
Support	73
Appendix A: Web Administration interface reference	74
Web Gateway Administration	74
<i>General Administration</i>	74
<i>SIP Global Configuration</i>	74
Outbound SIP Servers	74
Rewrite outbound SIP URIs	74

Server Timeout	75
Ping Interval	75
Dead Link Ping Interval	75
Registration expiry	75
Min SIP session expiry	76
SIP session expiry	76
Web Application IDs	76
WebRTC Configuration	76
Call Log Configuration	77
Performance Log Configuration	78
Resource Management	78
<i>Media Configuration</i>	78
Banned Codecs	78
Audio Codec Prioritization Configuration	78
Video Codec Prioritization Configuration	79
Video Resolution Configuration	79
Video Settings	80
Bitrate Configuration	80
RTP Settings	82
<i>Media Broker Administration</i>	82
General Configuration	82
<i>SIP Network</i>	84
Local Address CIDR	84
Start Port Range	85
Finish Port Range	85
<i>WebRTC Client</i>	85
Source Address CIDR	85
<i>Monitored Connections</i>	87
Group Name	87
Monitored Addresses	87
User Credentials	87
<i>Old password</i>	87
<i>UI username</i>	87
<i>New password</i>	88
<i>Retype new password</i>	88
Appendix B: RFC References	89
Appendix C: Glossary	90

Chapter 1: Introduction

Purpose

This document describes how to administer Avaya Mobile Video.

Chapter 2: Overview

Avaya Mobile Video Server allows users to develop web applications that can make voice and video WebRTC calls directly from Chrome Web Browser, iOS devices, or Android devices to an Avaya one-X[®] Agent.

Mobile Video Server includes components that allow the enterprise to deploy the applications they develop:

- The Avaya Mobile Video Gateway: normalizes the signaling between HTTP clients developed with the Avaya Mobile Video SDK (MVSDK) and Avaya Session Manager so that the two can communicate together seamlessly.
- The Avaya Mobile Video Media Broker converts between browser-originated RTP streams and RTP streams compatible with Avaya one-X[®] Agent endpoints.

Note: This document details the supported configuration, and supported changes that can be made to the product. Any other changes made via the Mobile Video Server administration interface and in configuration files that are not detailed in this documentation are unsupported.

Avaya Mobile Video Application Server Platform

The Mobile Video Server components are built on Avaya Mobile Video Application Server, a high-performance software platform that delivers innovative voice and video services.

The Avaya Mobile Video Application Server is a Java-based execution platform that meets the strict standards and requirements of service providers and the enterprise market. See [RFC References](#) for more information.

Audit Logging

Avaya Mobile Video maintains an audit log of significant events, including the following:

- User login or logout
- MVS start or stop
- Media Broker connections made or lost

The `audit.log` file is saved in the MVS install directory.

Entries are kept for 1 year, and include their category and any specific information, as in the following example:

```
2016-01-28 10:38:30,056 INFO APP_CONN MVS started, user=root,  
address=192.168.8.128
```

```
2016-01-28 10:39:16,905 WARN MB_CONN Gateway 192.168.8.128 has lost  
connection to Media Broker: 192.168.8.129
```

2016-01-28 10:40:00,977 INFO MB_CONN Gateway 192.168.8.128 has made a connection to Media Broker: 192.168.8.129

Chapter 3: Avaya Mobile Video Server Administration Interfaces

You administer the Avaya Mobile Video Server through the interfaces described in this chapter.

Avaya Mobile Video Application Server Management Console

Log on to the Avaya Mobile Video Application Server management Console using the following URL:

```
https://<ip_address>:9990/
```

The credentials to be used were specified during initial installation.

Avaya Mobile Video Gateway Administration Interface

Log on to the Avaya Mobile Video Gateway administration interface using the following URL:

```
https://<ip_address>:8443/web_plugin_framework/webcontroller/admin
```

The user name and password are those supplied during installation.

If the wrong administrative credentials are submitted six consecutive times, then the administrative account is locked for security reasons. To re-enable the administrative account, see [Resetting Administrator Credentials](#).

Setting Password Constraints

By default, the only constraint enforced when setting a password for the web administration interface is that the password must be at least four characters long. You can use the Mobile Video Server Management Console to add a system property which defines a regular expression which any new password must match before it is accepted:

1. Open a web browser and navigate to the Mobile Video Server Management Console:

```
https://<ip_address>:9990
```

where <ip_address> is the Mobile Video Server IP address

- In the left hand menu, under **Server**, select **Server Groups**. The Server Groups page displays:

Host: master-avaygw

Server

Server Configurations

Server Groups

Host Settings

JVM Configurations

Interfaces

Host Properties

Group Configurations

Server Groups

A Server Group does specify a common management policy for a set of servers. Server Groups are associated with profiles.

Available Group Configurations

Add Remove

Group Name	Profile
lb-server-group	lb
main-server-group	ha
mgmt-server-group	management

1-3 of 3

Attributes JVM Configuration System Properties

Add

Key	Value	Boot-Time?	Option
sips.trust.group	default-trust	true	Remove
wpf.gateway.rest.url	\$(rest.scheme):/\${rest.host}:\${rest.port}/ac	true	Remove
wpf.rest.host		true	Remove
wpf.rest.port	8443	true	Remove
wpf.rest.scheme	https	true	Remove

9-13 of 13

- In the *Available Groups Configurations* list, select `main-server-group`.
- To add the new system property, select the **System Properties** tab below, and click **Add**. The **Create System Property** dialog displays:

Create System Property

Name:

Value:

Boot-Time: ☐

Save Cancel

- In the **Name** field enter `appserver.admin.password.validation`
- In the **Value** field, enter an appropriate Java -style regular expression, such as:

Regular Expression	Meaning
<code>.{6,}</code>	At least 6 characters

Regular Expression	Meaning
<code>^[a-zA-Z0-9]{6,}\$</code>	At least 6 alphanumeric characters
<code>^(?=.*[a-z])(?=.*[A-Z])[a-zA-Z]{6,}\$</code>	At least 6 alphabetic characters, with a mix of upper and lower case
<code>^(?=.*\d)(?=.*[a-zA-Z])[a-zA-Z0-9]{6,}\$</code>	At least 6 alphanumeric characters, including both alphabetic and numeric

7. Check the **Boot-Time** checkbox
8. Click **Save**

You should see the new system property in the *System Properties* list for the `main-server-group` on the Server Groups page.

Resetting Administrator Credentials

If you have forgotten the administrator user name or password, you can reset them to the original values set on installation by setting a system property:

1. Edit the `/opt/avaya/awmvs/3.4.x/awmvs/domain/configuration/fas.properties` file, and add the system property:
`appserver.admin.password.reset=true`
2. Restart the AMV Gateway
3. Open a new web browser and navigate to the Web Admin UI
(`https://<ip_address>:8443/web_plugin_framework/webcontroller/admin`)
4. Click **Login**
This will fail; this is expected behavior.
5. Re-edit the `opt/avaya/awmvs/3.4.x/awmvs/domain/configuration/fas.properties` file to remove the `appserver.admin.password.reset` property.
6. Restart the AMV Gateway
7. Login is now re-enabled on the web administration interface and the login credentials have been reset to the default values of:

Username: administrator
Password: administrator
8. Login using the default credentials and change the username and password immediately as the system will be in an insecure state until the defaults are changed.

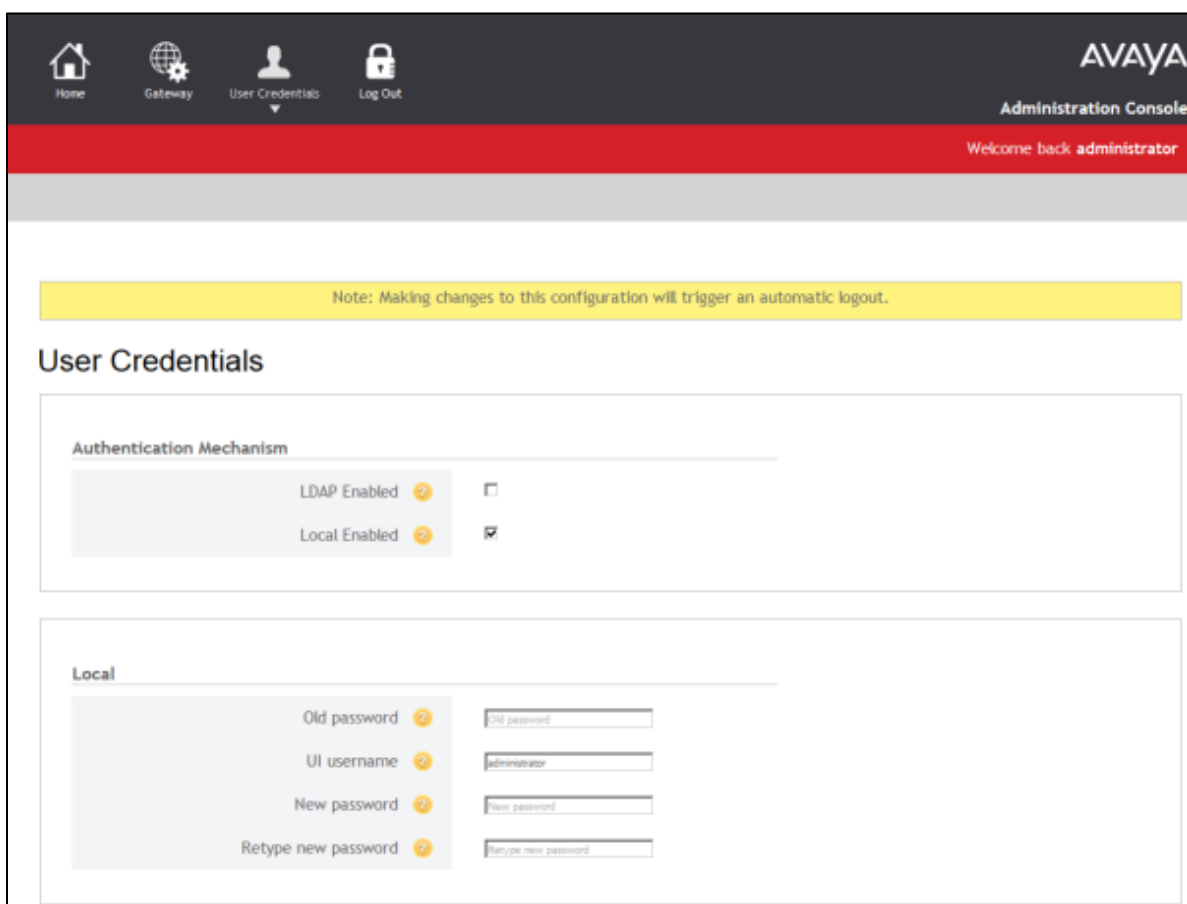
Chapter 4: Configuring User Credentials

Access to the administrative interface is authenticated using a user name and password. The user name and password can be kept locally (see [LOCAL Authentication](#)) or on an LDAP server (see [LDAP Authentication](#)).

LOCAL Authentication

To change the user credentials:

1. Go to the **User Credentials** tab:



The screenshot shows the Avaya Administration Console interface. At the top, there is a navigation bar with icons for Home, Gateway, User Credentials (selected), and Log Out. The Avaya logo and 'Administration Console' text are on the right. Below the navigation bar, a red banner says 'Welcome back administrator'. A yellow warning box states: 'Note: Making changes to this configuration will trigger an automatic logout.' The main section is titled 'User Credentials'. It contains two sections: 'Authentication Mechanism' and 'Local'. In the 'Authentication Mechanism' section, 'LDAP Enabled' is unchecked and 'Local Enabled' is checked. The 'Local' section contains four input fields: 'Old password' (with value 'old password'), 'UI username' (with value 'administrator'), 'New password' (with value 'New password'), and 'Retype new password' (with value 'Retype new password').

2. In the *Authentication Mechanism* section, make sure **Local Enabled** is checked.

3. Enter the information in the *Local* section (all fields are mandatory):

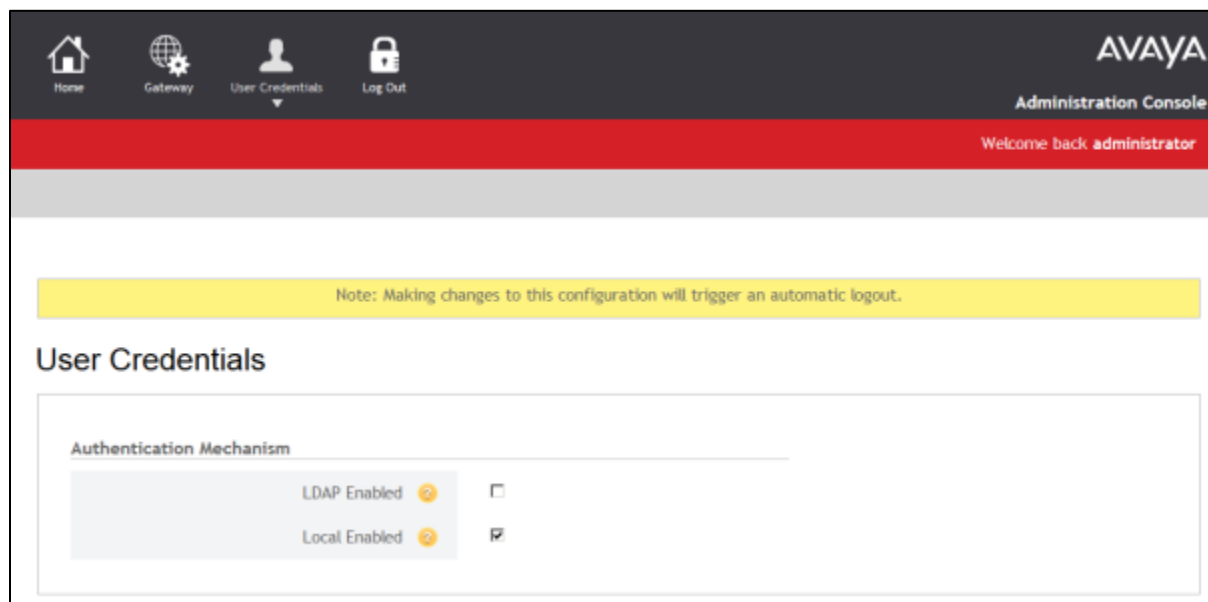
Field	Description
Old password	The current administrative password. Under normal circumstances, this will be the password you have just logged in with.
UI username	The new name of the administrative user. If you are not changing the name of the administrative user, this will be the user name you have just logged in with.
New password	The new password for the administrative user. This is repeated as a check for typing errors - if the two fields do not match, the password will not be reset. Note: It is not a good idea to cut and paste the value from the New password field into the Retype new password field. If you do, and there is a typing mistake, the new password will not be what you think it is.
Retype new password	

4. Click the **Save and Logout** button at the bottom of the page.

Saving the credentials immediately logs you out, and you will have to log in again with the new credentials.

LDAP Authentication

To enable and configure LDAP authentication, click the **User Credentials** tab to go to the User Credentials page:



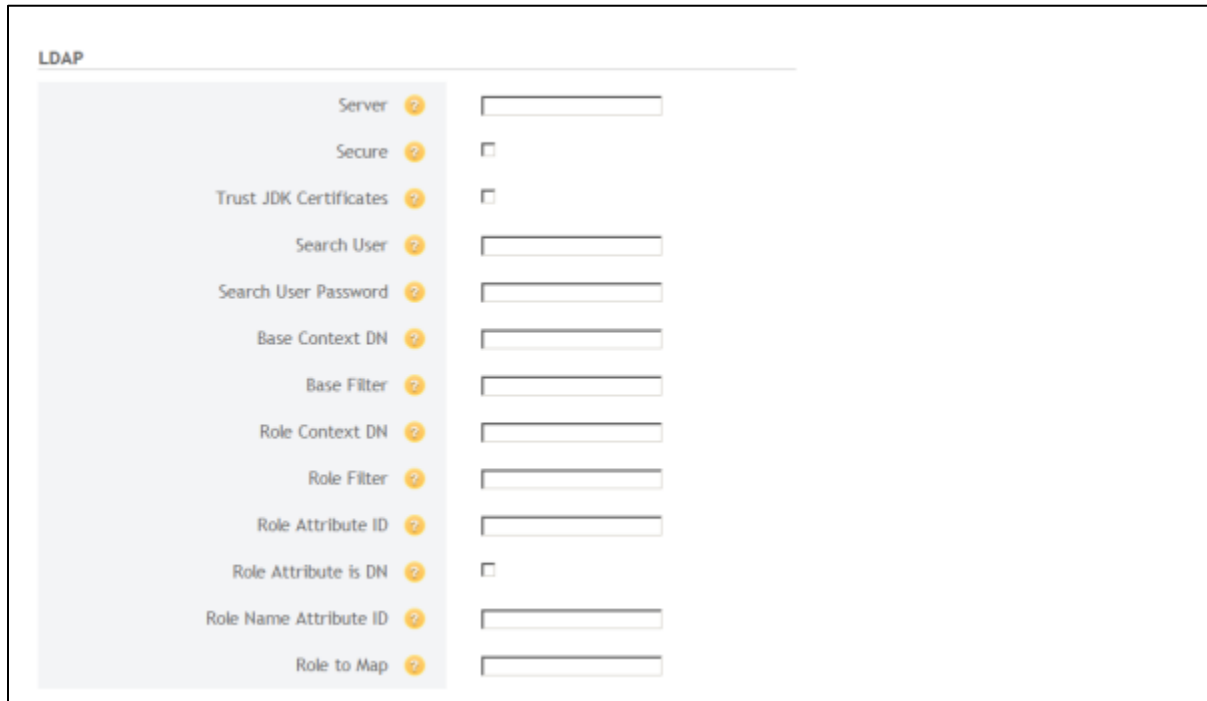
Enabling LDAP Authentication

- Check **LDAP Enabled** to enable LDAP authentication.
- Check **Local Enabled** to enable local password authentication

Note: If both options are enabled, LDAP is done first, and then (if necessary) Local.

Configuring LDAP Authentication

Go to the *LDAP* section on the User Credentials page:



Field	Description
Server	The host of the LDAP server, for example 172.31.20.69
Secure	<p>This checkbox indicates if LDAP authentication should be performed over a secure (HTTPS) connection.</p> <ul style="list-style-type: none">• If <i>checked</i>, a valid LDAP server certificate needs to be imported.• If <i>unchecked</i>, be aware that plain-text credentials are passed across the network.
Trust JDK Certificates	<p>This checkbox indicates if, in addition to the regular LDAP trust store, the Java (JDK) default certificate trust store should be used for LDAP server certificate validation.</p> <ul style="list-style-type: none">• If <i>checked</i>, the JDK trust store is used to validate an LDAP server certificate if validation cannot be performed using the regular LDAP trust store.• If <i>unchecked</i>, only the regular LDAP trust store will be used.
Search User	The full Distinguished Name (DN) of the user that will authenticate against the LDAP server and will be used to perform a search. An

Field	Description
	<p>example is</p> <p>UID=SEARCHUSER, OU=USERS, DC=EXAMPLE, DC=COM</p>
Search User Password	The password for the Search User
Base Context DN	<p>This is the complete DN used to define the authentication parameters</p> <p>An example is</p> <p>OU=USERS, DC=EXAMPLE, DC=COM</p>
Base Filter	<p>The search filter syntax used in the authentication query. The input username will replace any {0} expressions.</p> <p>For example:</p> <p>In this search the filter is the user id.</p> <p>(uid={0})</p> <p>This extra parameter will be attached to the existing query, for example:</p> <p>(UID={0}), OU=USERS, DC=EXAMPLE, DC=VBOX</p>
Role Context DN	<p>The fixed DN of the context to search for user role by LDAP. For example:</p> <p>OU=Users, DC=ldap, DC=company, DC=com</p>
Role Filter	This contains similar properties to the Base Filter but will be used in user role query.
Role Attribute ID	<p>The name of the attribute of the role object that corresponds to the name of the role. For example:</p> <p>employeeType</p>
Role Attribute is DN	<p>This checkbox indicates whether the value of the attribute named by Role Attribute ID contains the fully distinguished name of a role object.</p> <ul style="list-style-type: none"> • If <i>checked</i>, the value of the attribute named by Role Attribute ID represents the DN of a role object, in which case the role name is taken from the value of the Role Name Attribute ID attribute of the corresponding object • If <i>unchecked</i>, the role name is taken from the Role To Map field
Role Name Attribute ID	The name of the attribute of the role object that corresponds to the name of the role. If Role Attribute is DN is <i>checked</i> , this property is used to find the role object's name attribute. Otherwise, it is ignored
Role to Map	<p>The name of a user's role (as defined in LDAP) that authorizes the user to access administrative capabilities. An example is:</p> <p>wpf</p> <p>If left blank, the default role that MVSDK looks for is WEBADMIN.</p>

Important: If a user can log in to the MVS console using their LDAP credentials, and can see the administration pages, but cannot see the administration pages after logging in to MVSDK, then check the Role-related configuration.

- LDAP authentication fails for first time user/user after reset

If a user is set up in Active Directory with the option **User must change password at next logon**, but their first action as an AD user is to attempt to use LDAP authentication, their login fails with the following error:

LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773, v2580]

Workaround:

- Before attempting to use their credentials for LDAP authentication, log the user in using their Active Directory credentials on a system that will prompt to change the password, or
- Do not select the option **User must change password at next logon** when setting up the user.

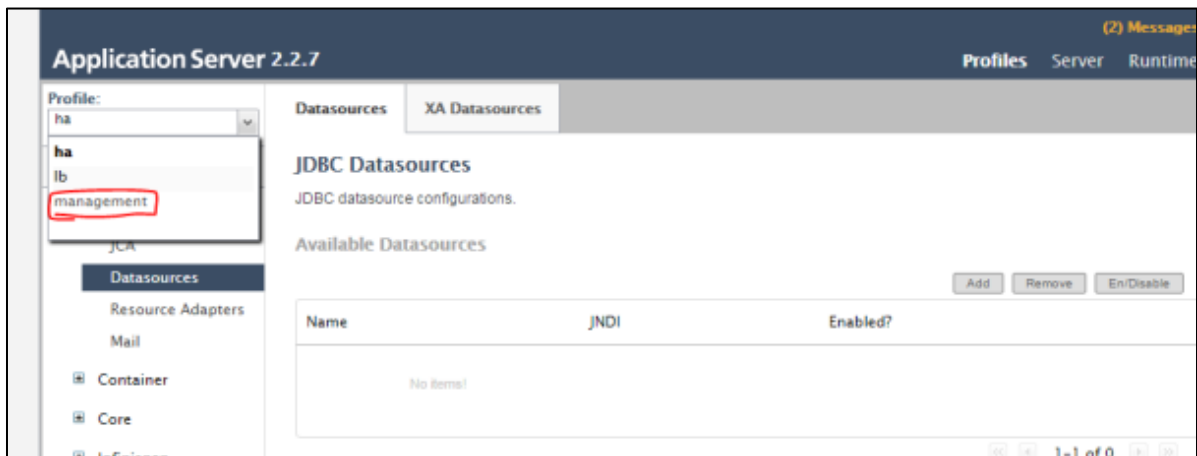
Importing Certificates to the LDAP Truststore

1. Open the MVS admin console at https://<ip_address>:9990
2. Click **Profiles** in the top right menu:

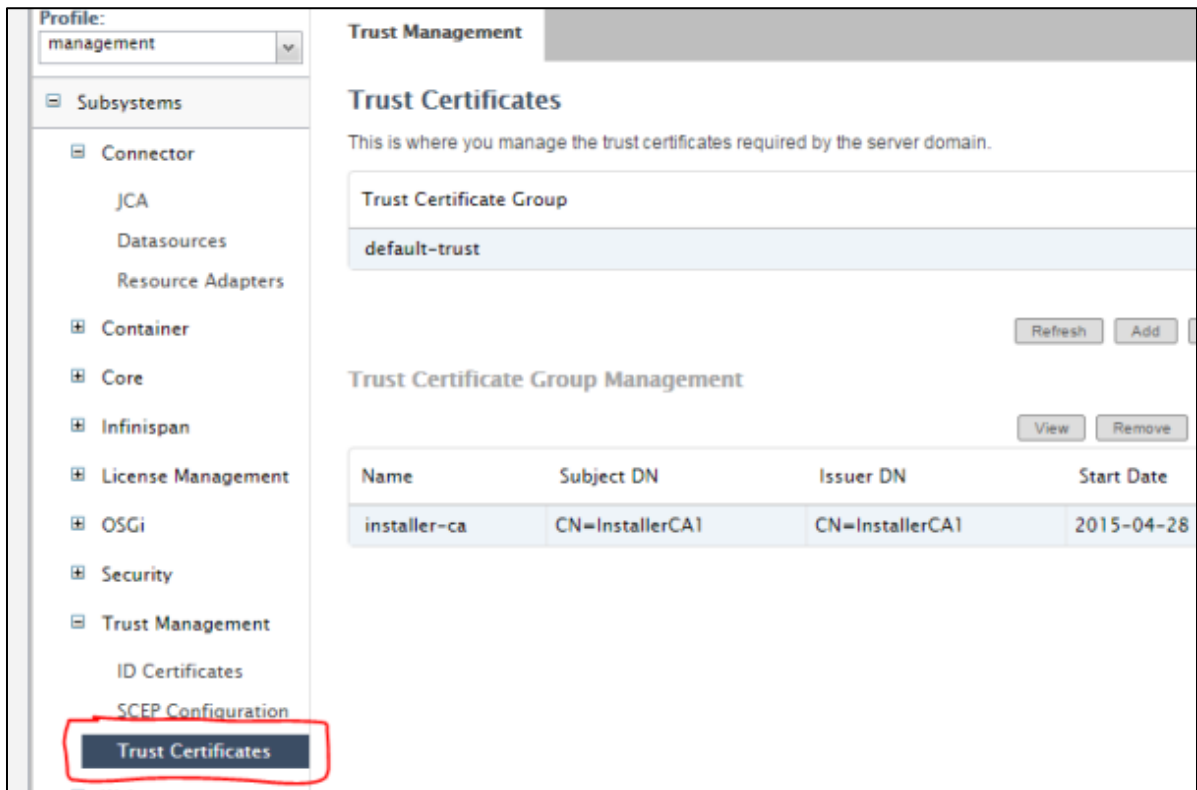
The screenshot shows the Application Server 2.2.7 console. The top navigation bar includes 'Profiles', 'Server', and 'Runtime'. The left sidebar has a tree view with 'Domain' expanded, showing 'Server Instances' and 'Manage Deployments'. Below that, 'Server Status' is expanded, showing 'JVM', 'Databases', 'JPA', 'JNDI View', 'Transactions', 'Web', 'Webservices', 'Runtime Operations', and 'OSGi'. The main content area is titled 'Server Status (Host: master-wlannen-fas)' and includes a 'Stop' button. It contains a table with columns 'Server', 'Server Group', 'Status', and 'Active'. The table lists three server instances: 'appserver-wlannen-fas' (main-server-group), 'loadbalancer-wlannen-fas' (lb-server-group), and 'management' (mgmt-server-group). All are active. Below the table is a 'Status' section with 'Availability' and 'Environment Properties' tabs. At the bottom, it shows 'Server Instance: appserver-wlannen-fas' and 'Server Configuration: appserver-wlannen-fas'.

Server	Server Group	Status	Active
appserver-wlannen-fas	main-server-group		✓
loadbalancer-wlannen-fas	lb-server-group		✓
management	mgmt-server-group		✓

3. From the **Profile** drop-down list on the left, select **management**:

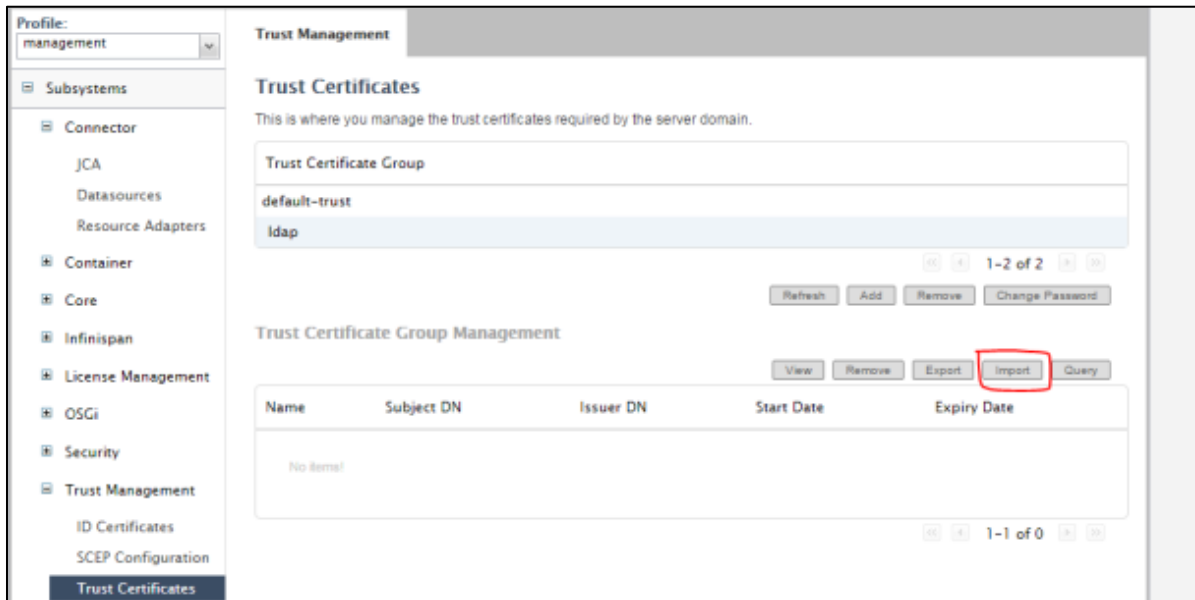


4. In the menu on the right, expand **Trust Management**, then click **Trust Certificates**:

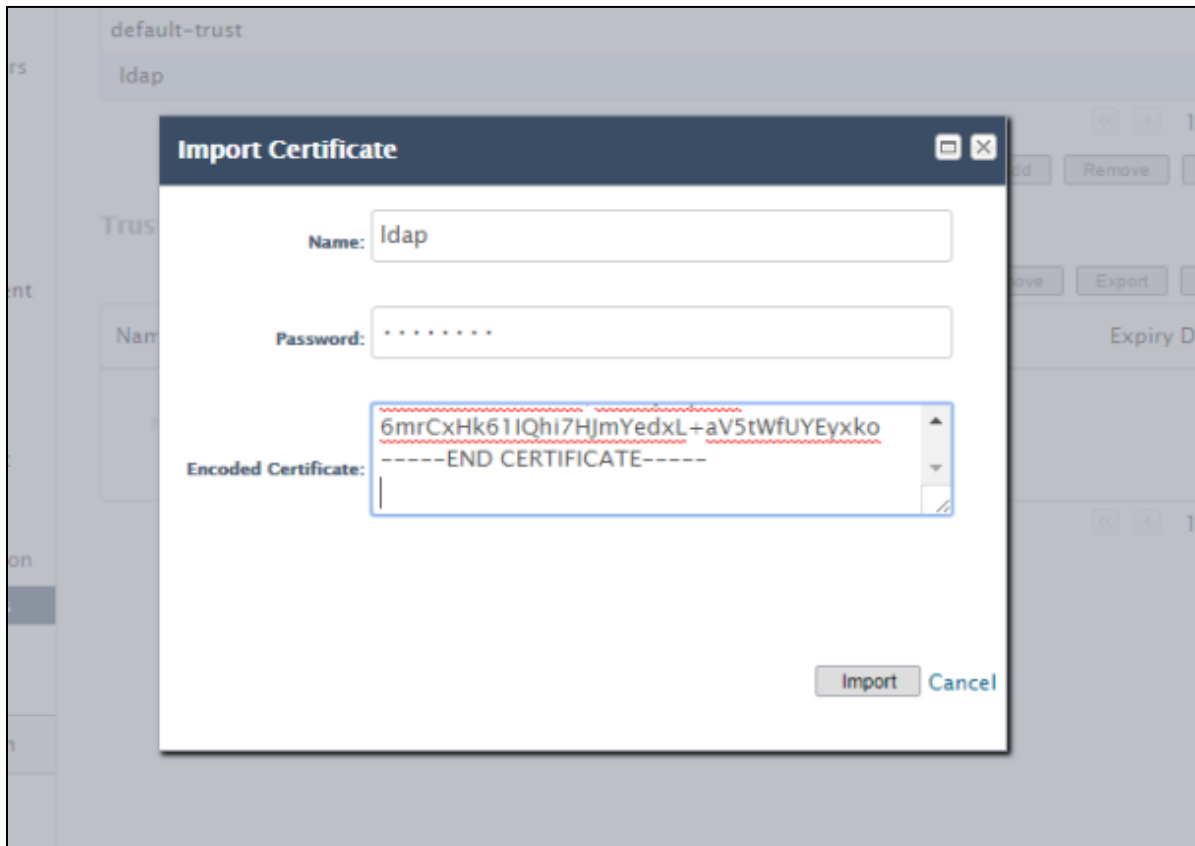


5. On installing MVSDK, a trust store called `ldap` is created, with the password `changeit` (this password will be needed when adding certificates or otherwise changing the trust store).
6. Click the row for `ldap` under *Trust Certificate Group* - there should be no certificates listed in the lower table.

- Click the **Import** button to add the certificate to the newly added Trust Certificate Group.



- Enter a name of your choice for the certificate, the password for the trust store (as chosen in step 5), and in the **Encoded Certificate** box, paste the contents of the LDAP certificate PEM file (including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines).



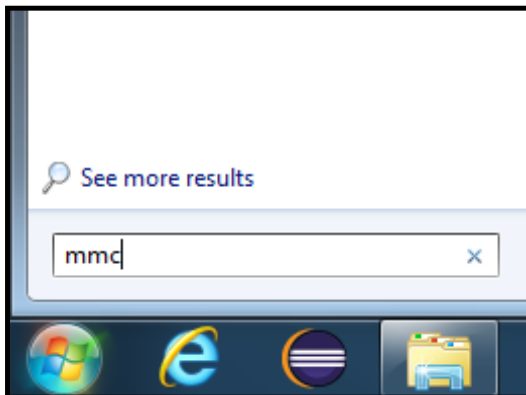
Note: The entire certificate chain for the LDAP server must be fulfilled within the Trust Certificate Group (the main Java truststore is not referenced). In cases where this involves multiple

certificates, it will be necessary to repeat step 7 accordingly. See Exporting and Converting Certificates from the Windows MMC on page 21 for a possible mechanism to obtain the LDAP server certificate in a Windows environment.

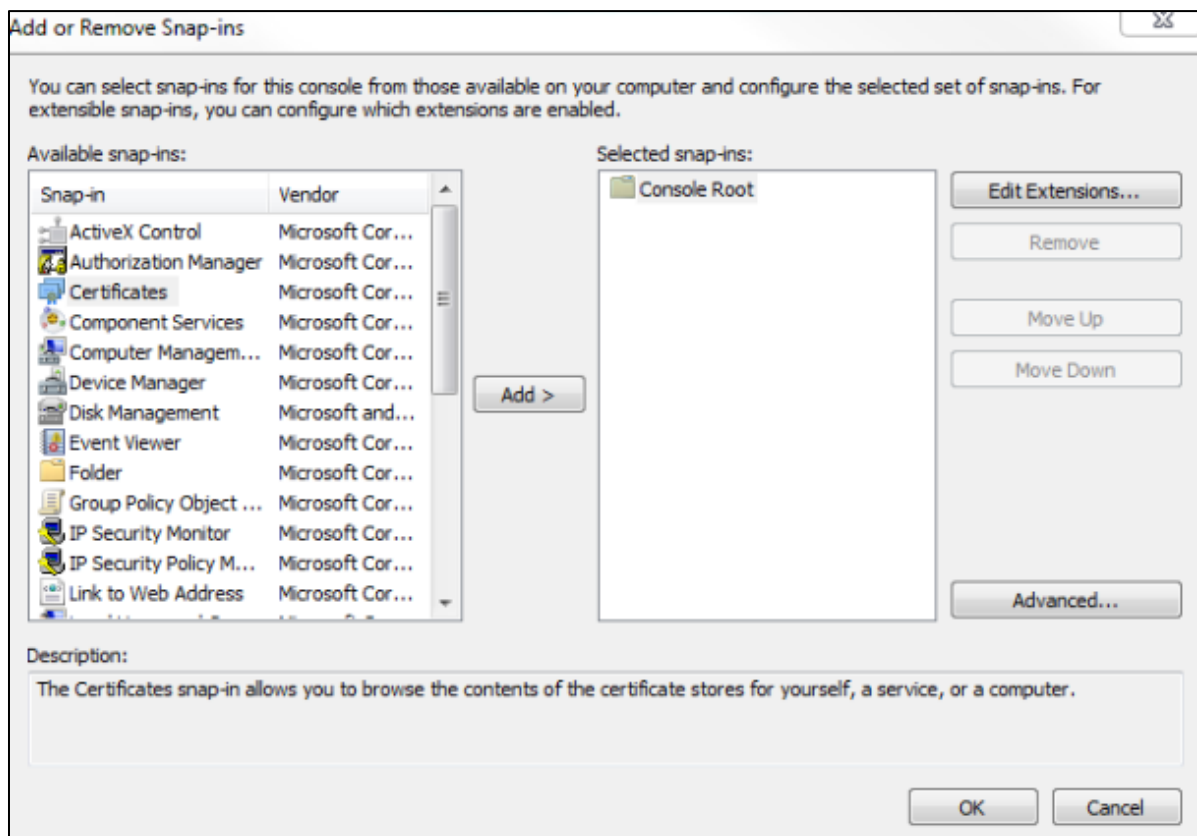
Exporting and Converting Certificates from the Windows MMC

In the case of a Windows environment, the certificate(s) needed to access the LDAP server may be available within the MMC (Microsoft Management Console). For example, if the LDAP server is using a root certificate that is pushed out to users of the same domain, then a user logged into that domain sees this certificate in the MMC.

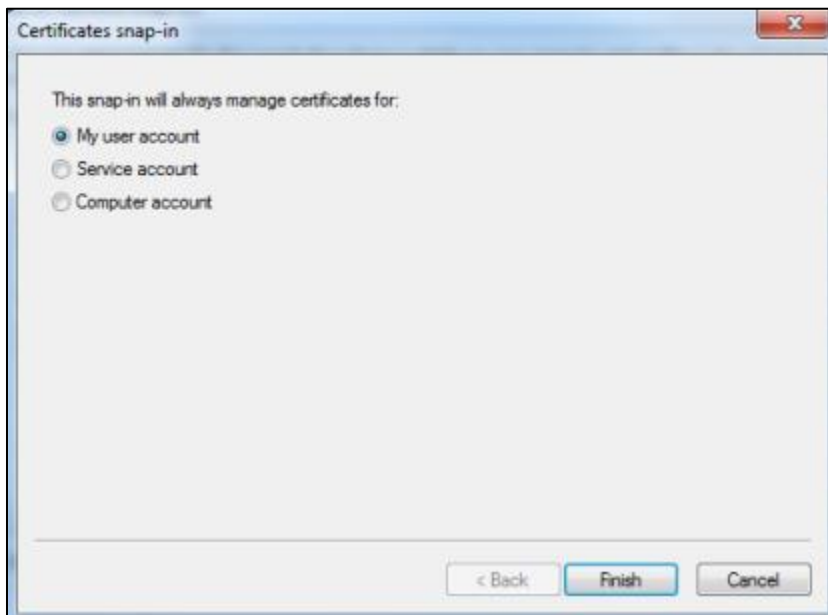
1. Open the MMC in Windows by **Start->Search programs and files**, and type **MMC->ENTER**



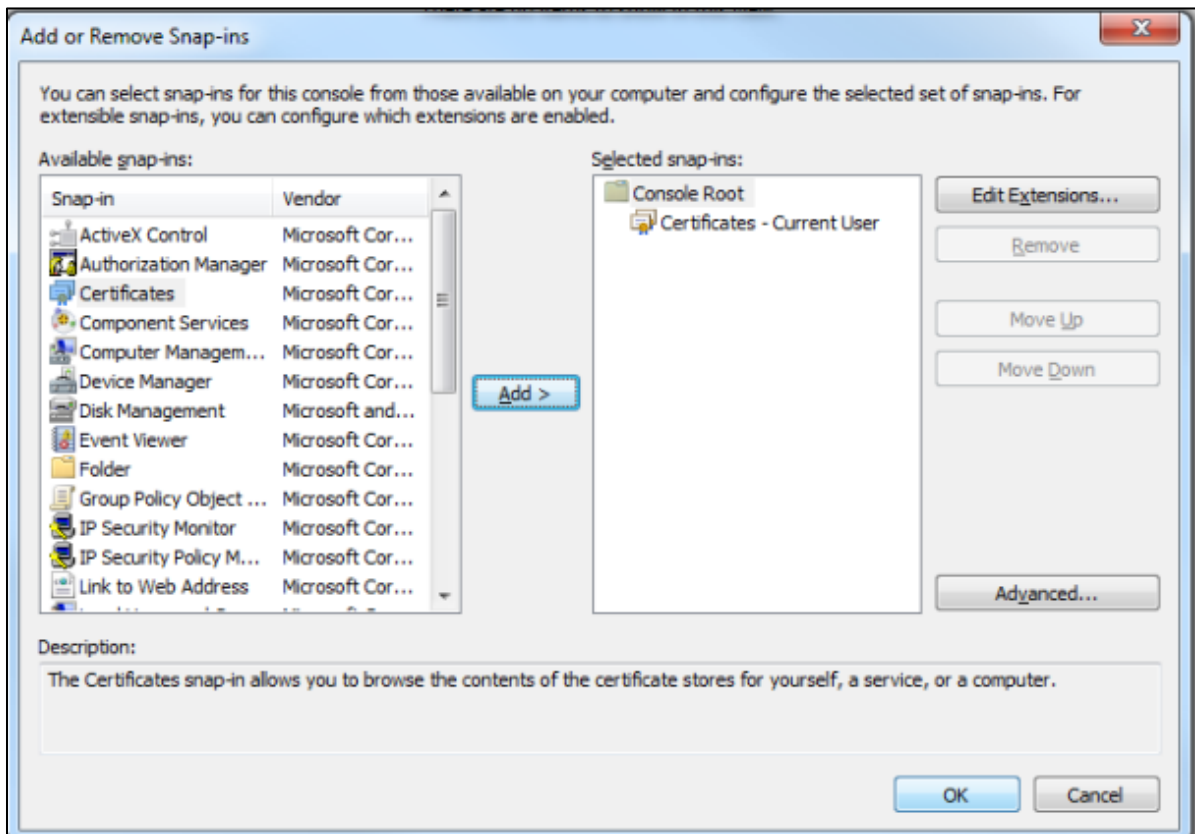
2. Within the MMC, select **File->Add/Remove Snap-in**. Select the Certificates snap-in on the left, then click **Add**.



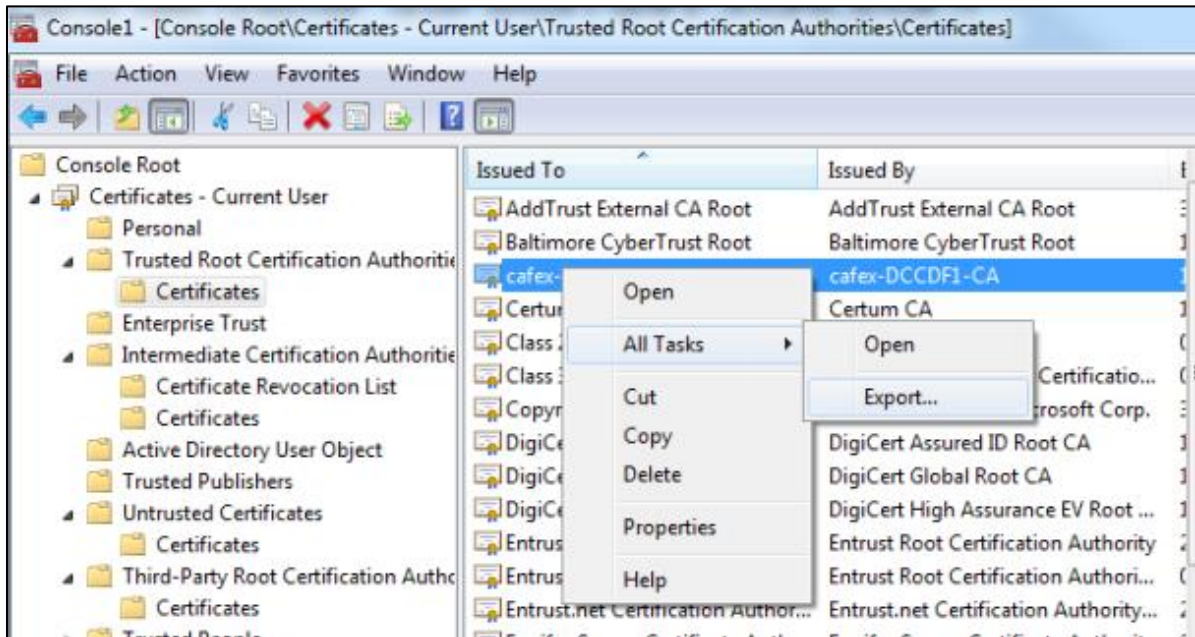
- When prompted, confirm that the snap-in will manage certificates for the user account.



- Click **OK** to add the snap-in



- Expand the tree on the left, locate the required certificate, then click it and select **AllTasks->Export**



- When prompted by the wizard, select **DER** as the format, then save the file to a suitable location.



- The file can then be converted to PEM format using OpenSSL:

```
openssl x509 -inform der -in in_certificate.cer -  
out out_certificate.pem
```

Note: OpenSSL is typically available at the command line of a Linux system; binaries for Windows are also available at <https://www.openssl.org/community/binaries.html>

Chapter 5: Configuring the Avaya Mobile Video Gateway

Avaya Mobile Video includes the Avaya Mobile Video Server, which removes the complexity in the signaling between the clients and Avaya Session Manager so that the two can communicate together seamlessly.

The Avaya Mobile Video Server communicates with the client using the TCP-based WebSockets protocol, providing a standardized way for the server to send content to the client without being solicited, and allowing for messages to be passed back and forth while keeping the connection open.

With the Avaya Mobile Video Gateway, users can make voice and video WebRTC calls to Avaya one-X[®] Agent endpoints.

The primary functions of the Avaya Mobile Video Gateway are to:

- Provide signaling conversion between the client and Avaya Session Manager.
- Only allow clients to create sessions that the Web application has authorized.
- Rely on HTTPS for control channels enabling security through industry standard and existing mechanisms, such as a firewall.

Configuring for Voice and Video Calls

An MVSDK application communicates with the Web Gateway on a WebSocket, using WebRTC to send signaling and media (voice and video) traffic. The Gateway can then transform the signaling to send the same voice and video to a SIP server to be sent to a SIP endpoint (such as a standard video phone). The following pages show how to configure the Gateway for SIP and WebRTC traffic.

Defining Banned Codecs

To ensure that calls are handled correctly, you can define a list of codecs that you do not want to pass to the Media Broker. When the Media Broker receives any of the codecs on this list, it removes them from the SDP that it produces.

To add a codec to the banned codecs list:

1. Log in to the Avaya Mobile Video Web Administration interface and select the **Gateway->Media Configuration** tab.

Home Gateway User Credentials Log Out

General Administration | **Media Configuration** | Media Brokers | Call Log | Performance Log

Media Configuration

Banned Codecs

<input type="checkbox"/>	Codec
<input type="checkbox"/>	G722
<input type="checkbox"/>	ulpfec
<input type="checkbox"/>	red
<input type="checkbox"/>	ilbc
<input type="checkbox"/>	g7221
<input type="checkbox"/>	MP4A-LATM
<input type="checkbox"/>	CN
<input type="checkbox"/>	isac
<input type="checkbox"/>	rtx

View 1 - 9 of 9

Add Delete

2. Click the **Add** button under *Banned Codecs* to display the **Add Record** dialog:

Banned Codecs

Add Record

Codec ?

Submit Cancel

View 1 - 6 of 6

Add Delete

3. Enter the name of the codec in the **Codec** field, for example PCMU

4. Click the **Submit** button. The codec you entered should now be displayed in the *Banned Codecs* list.
5. Repeat the above steps for each codec you want to ban, and click the **Save** button at the bottom of the page.

Prioritizing Codecs

Audio and video codecs can be prioritized in the *Audio Codec Prioritization Configuration* and the *Video Codec Prioritization Configuration* sections of the Media Configuration page:

The screenshot displays two configuration sections within a web interface. The top section, titled "Audio Codec Prioritisation Configuration", features a text input field with a "+" button to its right. Below this, there is a list of two items: "PCMA" and "PCMU", each followed by a small "x" icon in a square, indicating a delete function. The bottom section, titled "Video Codec Prioritisation Configuration", follows a similar layout with a text input field and a "+" button. Below it, a list contains "H264" and "VP8", each with a corresponding "x" delete icon.

Depending on your network's capabilities, and the priority for your organization in terms of bandwidth vs. quality, transcoding to certain codecs can be more preferable than others. Avaya Mobile Video allows you to prioritize the codecs to which media is transcoded, to ensure that the preferred codec is given highest priority.

The prioritized codec lists include the name of the codecs as they appear in the SDP. Any codecs in the prioritized list will be removed from SDP, then re-inserted at the end of the process in the order specified, thereby prioritizing them before all other codecs present in the SDP. It is therefore possible, if desired, to specify the relative priority of all codecs, transcoding or not.

The process of changing the priority of specific codecs is the same for both audio and video codecs:

- Adding a codec
 1. Type the name of the codec into the text box
 2. Click the add (+) button

The codec will be added to the top of the list

- Deleting a codec

Click the delete button (x) by the codec in the list

- Changing the priority of a codec
Drag and drop the codec's label in the list to its new position

Note: All codec names must conform to RFC 1551 (<http://www.ietf.org/rfc/rfc3551.txt>).

Configuring video resolution

You can configure video resolution in the *Video Resolution Configuration* section of the Media Configuration page:

The screenshot shows the 'Video Resolution Configuration' section. It contains four rows of configuration options, each with a label, a yellow question mark icon, and a text input field. The values entered in the fields are 640 for width and 480 for height.

Configuration Option	Value
Default Resolution Width	640
Default Resolution Height	480
Max Resolution Width	640
Max Resolution Height	480

RFC 6236 (<http://www.ietf.org/rfc/rfc6236.txt>) defines the `imageattr` SDP attribute along with the way in which this attribute can be used by endpoints to describe in the SDP, which resolutions they can send and receive.

By configuring the video resolution settings, you can cause the Media Broker to manipulate the values for the `imageattr` attribute in the SDP so that only certain resolutions are permitted. The Media Broker will examine the `imageattr` values in the inbound SDP and set the `imageattr` values in the outbound SDP using those inbound values and applying the following rules:

- The maximum width and height defines the maximum values for the given axis. If either of the values for a given width and height pair exceeds the maximum value then that pair is discarded; thus, if the maximum width and height are 600 and 400 then the outbound `imageattr` value would be as follows for the given inbound `imageattr`

Inbound SDP	Outbound SDP
<pre>send [x=640,y=480] [x=480,y=320] recv [x=480,y=320] [x=640,y=320]</pre>	<pre>send [x=480,y=320] recv [x=480,y=320]</pre>

- The default width and height defines the values to use if the inbound SDP contains no `imageattr` value, or if all the values in the inbound SDP are rejected because they are larger than the maximum width or height. Thus, if the maximum width and height are 600 and 400, and the default width and height are 320 and 240 then the outbound `imageattr` value would be as follows for the given inbound `imageattr`

Inbound SDP	Outbound SDP
-------------	--------------

Inbound SDP	Outbound SDP
None	send [x=320,y=240] recv [x=320,y=240]
send [x=640,y=480] [x=480,y=320] recv [x=640,y=480] [x=640,y=320]	send [x=480,y=320] recv [x=320,y=240]

Note: Not all endpoints implement RFC 6236, and such endpoints may ignore `imageattr` values.

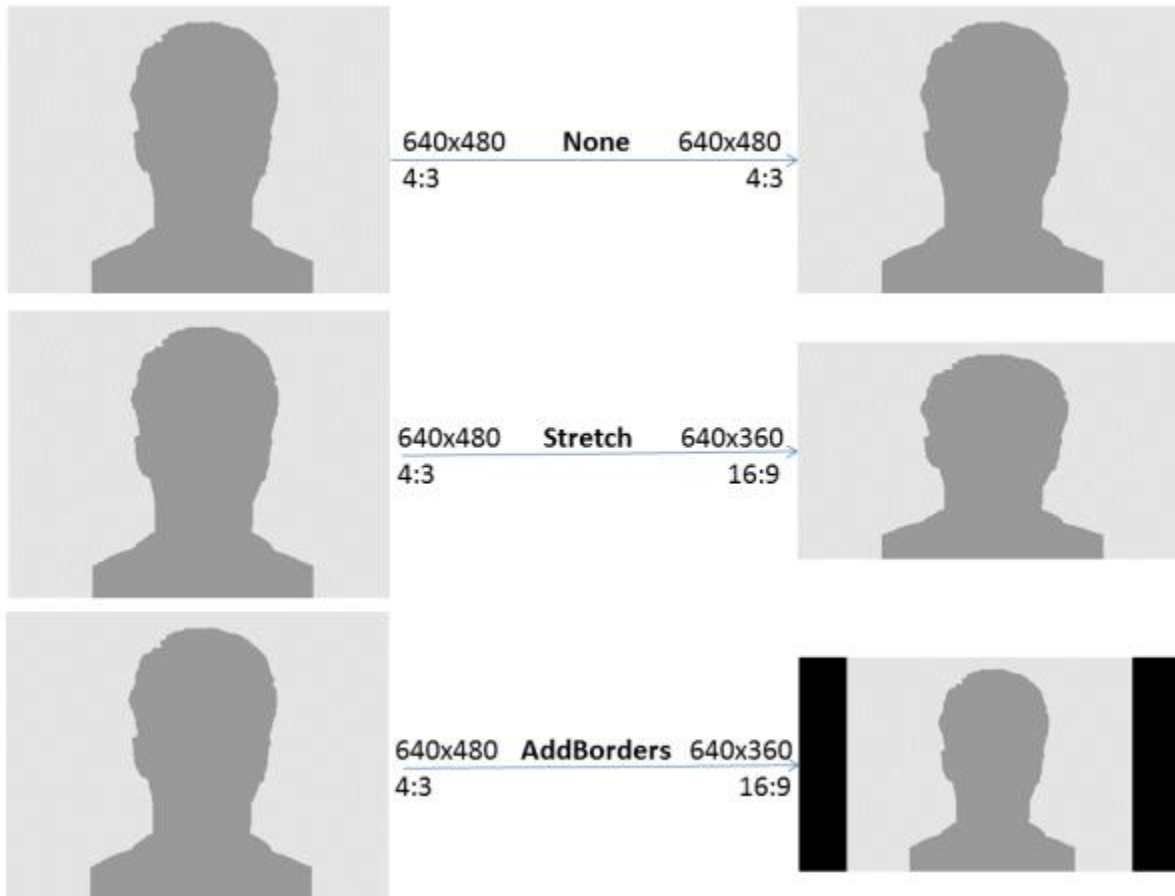
Configuring video settings

The video settings (**Frames per Second** and **Scaling Mode**) affect the behavior of Media Broker when it is transcoding. They are in the *Video Settings* section of the Media Configuration page.

- The **Frames per Second** determines the frame rate that the Media Broker will use when encoding, and thus affects the streams going out from Media Broker to the two endpoints in a call.
- The **Scaling Mode** affects how Media Broker will handle a difference between the resolution received from one endpoint and the resolution it sends to the other. It will always send the maximum (see note below) video resolution that the endpoint included in the `recv imageattr` attribute in the SDP (i.e. the maximum of those resolutions the endpoint has indicated it is happy to accept, or the default if none was present in the SDP). Where there is a difference between the two resolutions the scaling mode acts as follows:
 - **NONE**
No scaling. Media Broker will ignore the `imageattr` values and send the resolution it received. This may mean the aspect ratio of the image received by the endpoint is not what it was expecting, and may result in the endpoint stretching or squashing the image to fit in the available window.
 - **STRETCH**
Media Broker will stretch or squash the inbound image to fill the outbound resolution. If the aspect ratios differ, then the outbound image will appear stretched on one of the two axes. The benefit of this option is that the image will fill all of the target window.
 - **ADD_BORDERS**
Media Broker will shrink or enlarge the inbound image while maintaining the aspect ratio. If the size of the outbound image differs from the inbound one, then Media Broker adds black borders to the edges of the outbound image to maintain the aspect ratio. The benefit of this option is that the image will never be distorted.

Note: The maximum resolution is the one with the largest width. If two or more resolutions share the largest width, then the maximum resolution is the one of them which has the largest height.

The effects of the different scaling modes are as follows:

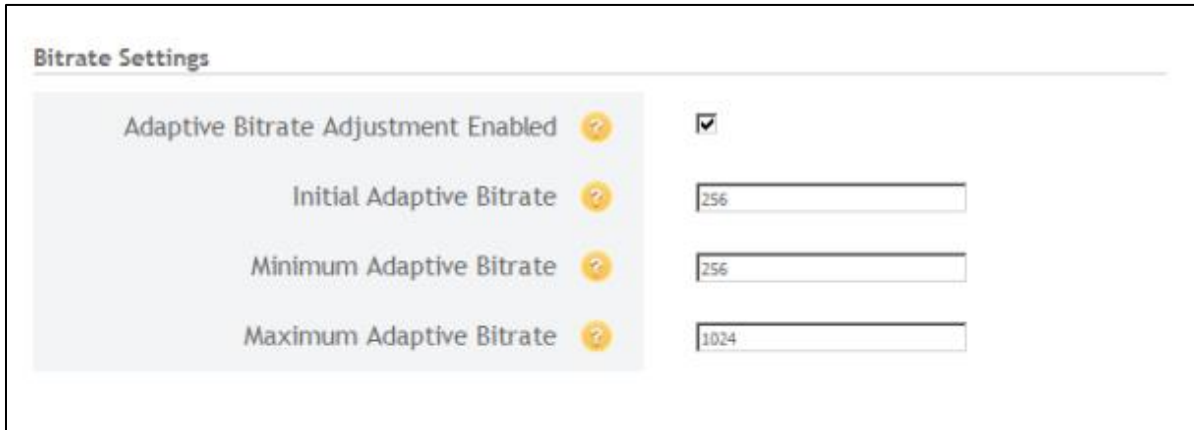


Configuring Bitrates

You can configure video and audio bitrates from the Avaya Mobile Video Web Administration interface. Select the **Gateway -> Media Configuration** tab and scroll down to the *Bitrate Settings* section.

- **Adaptive Bitrate Adjustment Enabled**

If checked, the video bitrate will be dynamically adjusted to maximize the video quality depending on network conditions.



The screenshot shows a configuration window titled "Bitrate Settings". Inside, there is a section with a light blue background. The first item is "Adaptive Bitrate Adjustment Enabled" with a yellow question mark icon and a checked checkbox. Below it are three input fields, each with a yellow question mark icon to its left: "Initial Adaptive Bitrate" with the value 256, "Minimum Adaptive Bitrate" with the value 256, and "Maximum Adaptive Bitrate" with the value 1024.

- **Initial Adaptive Bitrate**

Media Broker is able to estimate the maximum bitrate that network conditions can support for both send and receive video streams in the absence of REMB and TMMBR messages from browser and sip endpoints. This value initializes these algorithms to an expected bitrate from which to start from. A well chosen initial rate may result in the algorithm finding the best quality bitrate more quickly. A poorly chosen initial rate may result in unnecessarily poor initial video (value set too low) or dropped packets / frozen video (value set too high).

The units are kbs (kilobits per second).

- **Minimum Adaptive Bitrate**

Media Broker will receive and act on max bitrate messages from

- a. Browser (RTCP Remb)
- b. SIP endpoint (RTCP TMMBR)
- c. Sender bitrate estimating algorithm
- d. Receiver bitrate estimating algorithms

This value ensures that these max bitrate messages never go below a fixed value (e.g. minimum quality). In these cases this value will be used when setting media broker video encoder bitrates and is used in outbound REMB and TMMBR RTCP messages.

The units are kbs.

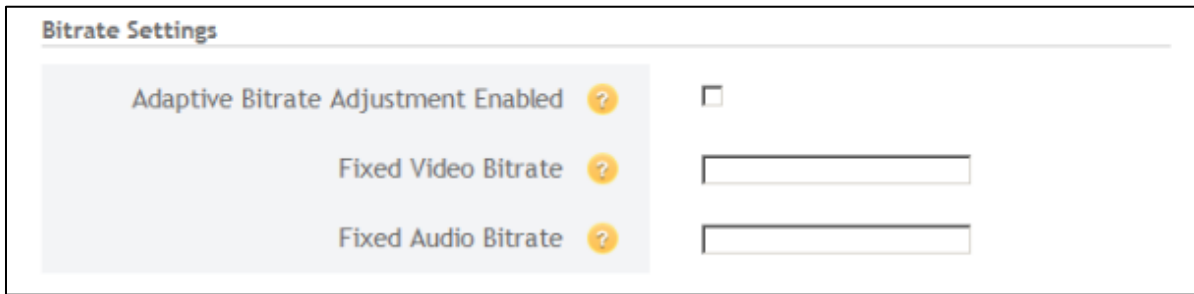
- **Maximum Adaptive Bitrate**

This value ensures that the max bitrate messages never go above a defined value (e.g. maximum quality). In these cases the ceiling will be used when setting *Media Broker* video encoder bitrates and is used in outbound REMB and TMMBR RTCP messages.

The units are kbs

Note: Avaya Communications Manager does not support adaptive bitrate, but the Web Browser side of the call will use the adaptive bitrate settings to get the best possible call quality given the available network resources.

If unchecked, the video and audio bitrates are constant.



- The **Fixed Video** and **Fixed Audio Bitrate** fields are used to negotiate a fixed bitrate for audio and video with browser and SIP endpoints. Using fixed bitrate on poor lines may result in video and audio issues (e.g. video freezing or stuttering audio).

Avaya does not recommend using a fixed bitrate. Adaptive bitrate aims to give the best call quality with the available network resources.

Note: If a bitrate of 384 Kbps or lower is used, Communications Manager will disable sending of video.

WebRTC Configuration

When you create a session on the gateway from your application, you provide a timeout value (see the *Avaya Mobile Video Developers Guide* for more information). This timeout determines the number of minutes that

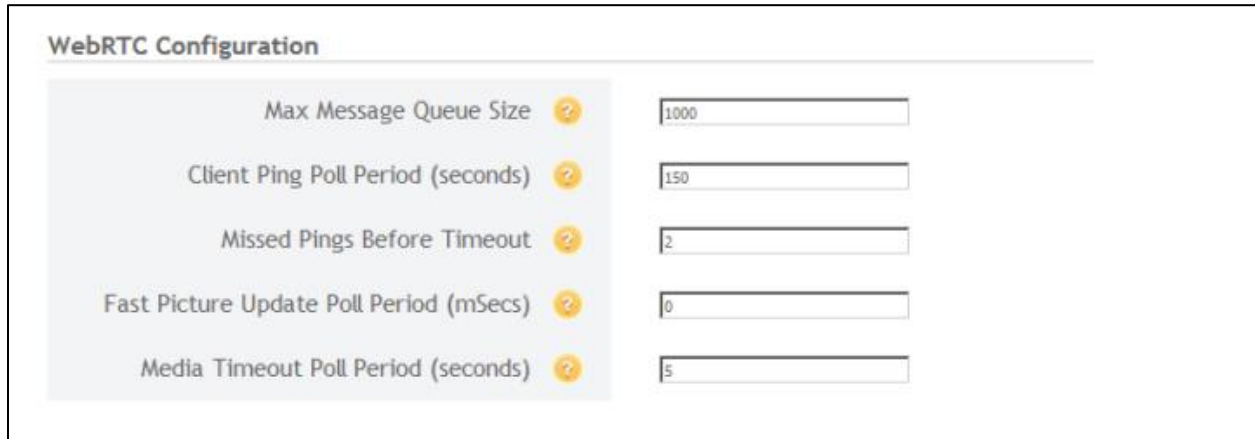
- The session will stay alive if unused
- The session will stay alive once the WebSocket connection to the client is torn down

There is a keep-alive `PING` mechanism to both keep the WebSocket connection open and test that the client is still connected. The Web Gateway will periodically send `PING` requests and expect a `PONG` response. If it receives no `PONG` response to a (configurable) number of consecutive `PING` requests, then it destroys the WebSocket connection and the above timeout kicks in. After this time the call will be ended.

The Gateway also performs regular checks, to determine if media has stopped flowing during a call; if it detects such a situation, it will end the call. The period between each check is configurable.

It will also end the call if the number of messages queued for sending from the Gateway to the client becomes too large; again, this value is configurable.

WebRTC configuration is achieved from the Avaya Mobile Video Web Administration interface. Select the **Gateway->General Administration** tab, and scroll down to the *WebRTC Configuration* section.



WebRTC Configuration	
Max Message Queue Size ?	<input type="text" value="1000"/>
Client Ping Poll Period (seconds) ?	<input type="text" value="150"/>
Missed Pings Before Timeout ?	<input type="text" value="2"/>
Fast Picture Update Poll Period (mSecs) ?	<input type="text" value="0"/>
Media Timeout Poll Period (seconds) ?	<input type="text" value="5"/>

Field	Description
Max Message Queue Size	The maximum number of messages to be queued before tearing down the connection
Client Ping Poll Period	The number of seconds between <code>PING</code> messages
Missed Pings Before Timeout	The number of consecutive <code>PING</code> messages that we send but received no <code>PONG</code> response before ending the WebSocket connection.
Fast Picture Update Poll Period	The number of milliseconds between sending requests for Fast Picture Update info requests - a value of 0 will disable the timer
Media Timeout Poll Period	The number of seconds for the timer to determine if a call has timed-out through lack of media

Capturing logs on the Gateway

To help you identify any issues you may experience, a script is provided that captures call logs and statistics for a specific period. The `logcapture.sh` script is installed in the `<install-dir>/bin` directory and can be used to capture the following information:

- AWMVS configuration
- vmstat output
- Java memory
- Thread dumps
- Network traffic (in a `.pcap` file)

The logging script runs until it is stopped, allowing you to reproduce any problem scenarios during this time. When you stop the logging script, the information you require is captured in a series of log files, which are archived into a `.tar` file:

```
./logcapture.sh -all -tar-file output.tar
```

You can define which information is captured by adding a selection of the following arguments when you run the script:

Argument	Description
-f, --tar-file	The filename of the resulting tar archive (required)
-c, --config	Include configuration files in the archive
-t, --threads	Include thread dumps in the archive
-m, --memory	include heap memory dumps in the archive
-n, --do-not-clean	do not clean the output directory at the end of the run
-p, --capture-pcap	capture network traffic in a pcap file
-v, --vmstat	include vmstat output in the archive
-a, --all	includes all options
-F, --force	Forces memory and stack dumps, even if a process is hung. Only meaningful if -t, -a, or -m are also included
-h, --help	display online help

To Capture Logs for a Specific Period

1. Set the logging levels appropriately.
2. Run the command:
3. Reproduce any scenarios which were causing issues.
4. Press **CTRL+C** to stop the logging script. The output files will be collected in `example.tar`, which (for the `-a` option used above) will have the structure:

```

./vmstat.out
./tcpdump.pcap
./FAS/
./FAS/log/
./FAS/log/alert.log
./FAS/log/host-controller.log
./FAS/configuration/
./FAS/configuration/host-master.xml
./FAS/configuration/mgmt-users.properties
./FAS/configuration/application-roles.properties
./FAS/configuration/fas.properties
./FAS/configuration/host.xml
./FAS/configuration/domain.xml
./FAS/configuration/host-slave.xml
./FAS/configuration/logging.properties
./FAS/configuration/application-users.properties
./FAS/servers/
./FAS/servers/loadbalancer-acb-fas-1/
./FAS/servers/loadbalancer-acb-fas-1/log/
./FAS/servers/loadbalancer-acb-fas-1/log/server.log
./FAS/servers/loadbalancer-acb-fas-1/log/boot.log
./FAS/servers/loadbalancer-acb-fas-1/log/http.log
./FAS/servers/loadbalancer-acb-fas-1/log/calls.log
./FAS/servers/loadbalancer-acb-fas-1/heap.bin
./FAS/servers/loadbalancer-acb-fas-1/thread.dump
./FAS/servers/management/

```

```
./FAS/servers/management/log/  
./FAS/servers/management/log/server.log  
./FAS/servers/management/log/boot.log  
./FAS/servers/management/heap.bin  
./FAS/servers/management/thread.dump  
./FAS/servers/appserver-acb-fas-2/  
./FAS/servers/appserver-acb-fas-2/log/  
./FAS/servers/appserver-acb-fas-2/log/server.log  
./FAS/servers/appserver-acb-fas-2/log/boot.log  
./FAS/servers/appserver-acb-fas-2/log/calls.log  
./FAS/servers/appserver-acb-fas-2/heap.bin  
./FAS/servers/appserver-acb-fas-2/thread.dump  
./FAS/servers/appserver-acb-fas-1/  
./FAS/servers/appserver-acb-fas-1/log/  
./FAS/servers/appserver-acb-fas-1/log/server.log  
./FAS/servers/appserver-acb-fas-1/log/boot.log  
./FAS/servers/appserver-acb-fas-1/log/calls.log  
./FAS/servers/appserver-acb-fas-1/heap.bin  
./FAS/servers/appserver-acb-fas-1/thread.dump
```

Configuring Media Brokers

As with signaling interworking, it is necessary to normalize RTP media streams in order to integrate with SIP environments. With the Media Broker, employees and customers can share secure video calls on a wide variety of devices and join video conferences from almost any endpoint.

Note: The Avaya Mobile Video deployment can contain several Media Brokers. See *Installing Avaya Mobile Video Server and Media Broker* for instructions on how to install Media Brokers.

Setting up the Interface with the Avaya Mobile Video Gateway

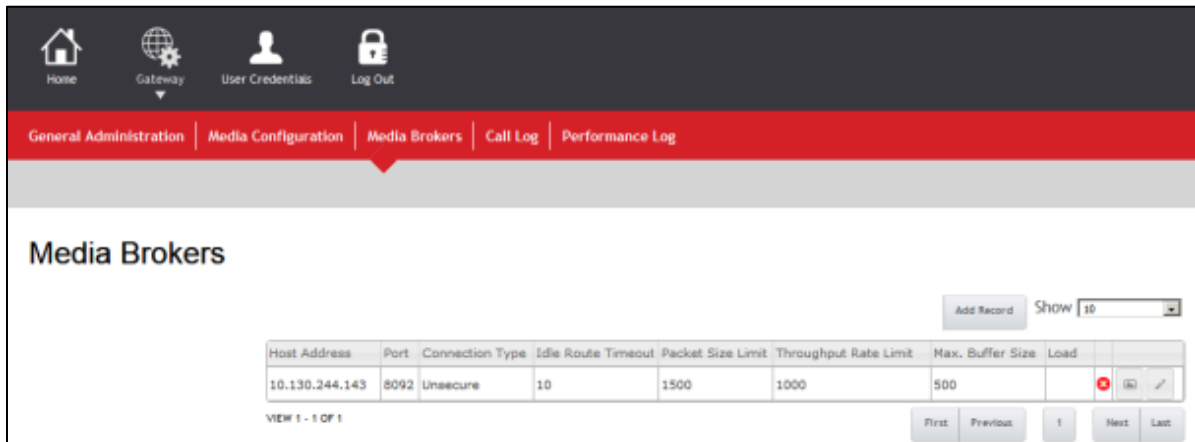
The Web Gateway and Media Broker need to exchange control messages. By default, the Media Broker listens for Web Gateway-to-Media Broker control communication on port 8092, on all available IP addresses. However, if the Media Broker is installed in a DMZ, it is expected that you will want to configure it to listen on a specific control interface.

To configure the IP address for communications with the Web Gateway:


1. On the Media Broker, edit the `<install_directory>/mvsdk/media_broker/proxy.properties` file.
2. The IP address for the control interface is defined by the `broker.rest.addr` setting, which is left blank by default. Enter the IP address you want to set for the control interface here.
3. The port allocated to the control interface is set to 8092 by default. If you want to change this, update the value for `broker.rest.http.port` for non-secure communication, and `broker.rest.https.port` for secure communication. See [Enabling secure communications between Media Broker and the Web Gateway](#).
4. Save your changes
5. Restart the Media Broker to apply the new settings

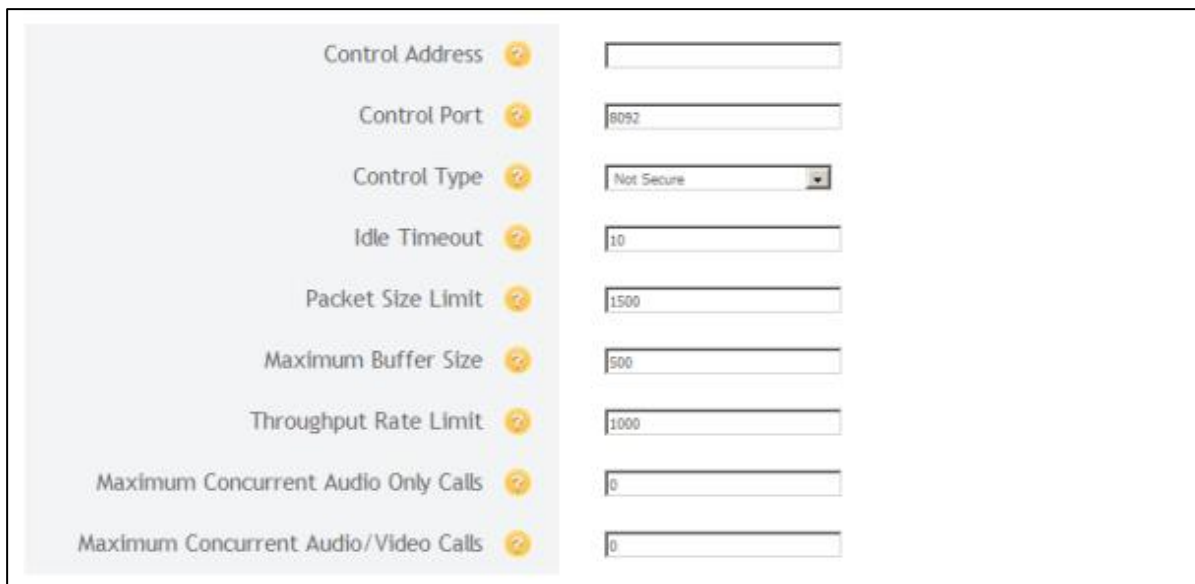
General Media Broker Configuration

1. Log in to the Avaya Mobile Video Web Administration interface and select the **Gateway->Media Brokers** tab. The page shows a list of existing Media Brokers:



Host Address	Port	Connection Type	Idle Route Timeout	Packet Size Limit	Throughput Rate Limit	Max. Buffer Size	Load
10.130.244.143	8092	Unsecure	10	1500	1000	500	0

2. To add a Media Broker, click the **Add Record** button; to edit the settings of an existing Media Broker, click the **Edit** () button next to the record of the Media Broker you want to edit.
3. In either case, you will see a page for a single Media Broker with the *General Configuration* section at the top:



Control Address	<input type="text"/>
Control Port	<input type="text" value="8092"/>
Control Type	<input type="text" value="Not Secure"/>
Idle Timeout	<input type="text" value="10"/>
Packet Size Limit	<input type="text" value="1500"/>
Maximum Buffer Size	<input type="text" value="500"/>
Throughput Rate Limit	<input type="text" value="1000"/>
Maximum Concurrent Audio Only Calls	<input type="text" value="0"/>
Maximum Concurrent Audio/Video Calls	<input type="text" value="0"/>

- **Control Address**

This is the hostname or IPv4 address for the control interface of the Media Broker, for example 192.168.1.2. It is used by the Web Gateway to connect to the Media Broker control port.

If you have configured a specific control interface for the Media Broker (see Setting up the Interface with the Avaya Mobile Video Gateway on page 35), this should match that IP address.

- **Control Port**

This is the port for Web Gateway-to-Media Broker communication. By default, this is set to 8092.

If you have configured a specific control interface for the Media Broker (see Setting up the Interface with the Avaya Mobile Video Gateway on page 35), this should match that port number.

- **Control Type**

Determines if all communication between the Web Gateway and the Media Broker will be secure or not. `Not Secure` is selected by default.

See [Enabling secure communications between Media Broker and the Web Gateway on page 38](#).

- **Idle Timeout**

The maximum period of inactivity (in seconds) on a route before the route is considered invalid and torn down. The default setting is 10.

- **Packet Size Limit**

The maximum RTP packet size that will be accepted. The Media Broker will drop any packet that exceeds this size. The default setting is 1500.

- **Max. Buffer Size**

The maximum number of packets that can be buffered before each call. If users are experiencing video issues at the beginning of calls, this value should be increased. The default setting is 500.

- **Throughput Rate Limit**

The maximum RTP throughput rate (in packets per second) for the Media Broker. The Media Broker will terminate a call where the input rate exceeds this value. The default setting is 1000.

- **Maximum Concurrent Audio Only Calls**

The maximum number of audio only calls that the Media Broker can service. Once this limit is reached (if there are no other calls), the Media Broker will reject new calls. Setting the value to 0 (the default) disables this feature. See [Call Limit Based Call Admission Control](#).

- **Maximum Concurrent Audio/Video Calls**

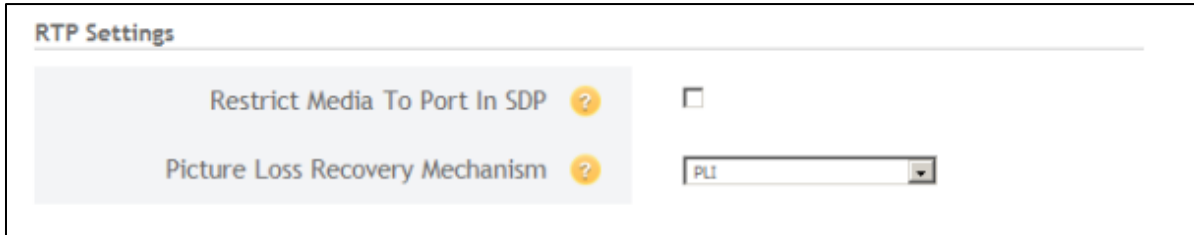
The maximum number of H.264 video calls that the Media Broker can service. Once this limit is reached (if there are no other calls), the Media Broker will reject new calls. Setting the value to 0 (the default) disables this feature. See [Call Limit Based Call Admission Control](#).

4. If you are adding a new Media Broker, configure both the SIP Network (see [Configuring SIP Network Settings](#)) and the WebRTC Client (see [Configuring WebRTC Client Settings](#)). (You cannot save a Media Broker configuration which does not include SIP Network and WebRTC Client configurations.)
5. Click **Save** at the bottom of the page.

Configuring RTP Settings

You can configure RTP settings from the Avaya Mobile Video Web Administration interface:

1. Log in to the Avaya Mobile Video Web Administration interface and select the **Gateway->Media Configuration** tab.
2. Scroll down to the *RTP Settings* section:



The screenshot shows the 'RTP Settings' section. It contains two settings:

- Restrict Media To Port In SDP**: A checkbox that is currently unchecked.
- Picture Loss Recovery Mechanism**: A dropdown menu with 'PLI' selected.

- **Restrict Media To Port In SDP**

When checked, SDP packets are dropped if they are sent from ports other than those negotiated in SDP. This can avoid media bleed-through issues when dealing with SIP endpoints that continue to stream after a call has been transferred or held. It only impacts SIP-side media. The default setting is unchecked.

- **Picture Loss Recovery Mechanism**

When video is lost, this setting determines the mechanism used for picture loss recovery to SIP endpoints. The default setting is `PLI`.

Note: This setting only determines the type of message that Media Broker sends when picture loss is detected on a video stream from a SIP endpoint. SIP endpoints can continue to send any option for recovery regardless of this setting.

3. Click **Save** at the bottom of the page.

Enabling secure communications between Media Broker and the Web Gateway

There is a REST service running on the Media Broker which services requests from the Web Gateway to set up and tear down media routes, send DTMF and also to monitor the health of all Media Brokers. By default, this connection will be unsecured after installation and you will need to configure it for HTTPS if you require this connection to be secure.

When HTTPS is set up, the Media Broker will be authenticated by Mobile Video Server. Hostname verification is done via the Subject Alternative Name (SAN) entries in the server certificate, therefore we recommend you include both an IP address and FQDN.

1. To create the server certificate and keystore, run the following command in the Media Broker install directory:

```
keytool -genkeypair -alias control -keyalg RSA -  
keystore <keystore_name> -keysize 2048 -  
ext san=ip:<ipaddress>,dns:<fqdn> -dname "CN=<common_name>"
```

Where:

- `<keystore_name>` is the name of the keystore file to use. We recommend using the existing `keystore.jks`, rather than creating a new one.
 - `<common_name>` is a common name to use in the certificate
 - `<ipaddress>` and `<fqdn>` are the IP address and fully qualified domain name of the Media Broker server. If an FQDN has not been configured, use only the IP address
2. When prompted for a password for the keystore and certificate, we recommend that you use the same value for both.
 3. To export the public certificate for installation in the Mobile Video Server truststore, run the following command:

```
keytool -export -alias control -file <pem_name> -keystore
<keystore_name> -rfc
```

Where `<pem_name>` is the name of the PEM file to store the certificate in e.g. `mediabroker.pem`.
 4. Update the following settings in `<media_broker_install_dir>/controller.properties`:
 - Set the `broker.rest.https.port` to 8092.
 - Set the `broker.rest.http.port` to 0
 - Set the `keystore.file.path` property to `<keystore_name>` as above.
 - Set the `keystore.file.password` property to the password used above.
 5. Import the PEM file into the Mobile Video Server default trust store (called `default-trust`) - see *Importing the trust certificate in Installing Avaya Mobile Video Server and Media Broker*.
 6. Restart the Media Broker (see [Starting and Stopping Avaya Mobile Video Media Brokers](#)).
 7. Reconfigure the Media Broker by setting the **Control Port** to match that set above, and by setting **Control Type** to `Secure`. See [General Media Broker Configuration](#).

Note: `keytool` commands should be on a single line.

Call Admission Control

Call Admission Control (CAC) is designed to protect a Media Broker against overloading when one is being selected to handle a new call.

When enabled, and a Media Broker is deemed unable to handle another call, the Load Balancer will attempt to select another Media Broker - this, of course, introduces the risk that a new call will be rejected due to no Media Brokers being available.

Note: CAC is not enabled by default, as the relevant properties are not set.

Call Limit Based Call Admission Control

This feature works by setting the maximum allowed number of calls for a given type (audio or video) and then working out the allowed combinations based on these maximum values. For example, setting the **Maximum Concurrent Audio/Video Calls** to 10 and the **Maximum Concurrent Audio Calls** to 100, would allow 5 video calls if there were 50 audio (see [General Media Broker Configuration](#) for details).

Note: Setting either of these values to 0 disables the feature for that call type.

Starting and Stopping Avaya Mobile Video Media Brokers

If you need to start, stop or restart a Avaya Mobile Video Media Broker for any reason, run one of the following commands on the Avaya Mobile Video Media Broker host:

- To start the Media Broker:

```
service media_broker start
```

- To stop the Media Broker:

```
service media_broker stop
```

This command stops the Media Broker immediately. You may prefer to shut down the Media Broker gracefully using the following command:

```
service media_broker request-shutdown
```

This prevents new calls, while allowing existing calls to continue. The Media Broker will shut down as soon as all existing calls have completed.

- To restart the media broker:

```
service media_broker restart
```

Note: Stopping a Media Broker will terminate any calls that are currently being processed by that Media Broker. It is recommended to schedule a maintenance window during times of low traffic to restart Media Brokers. Media Brokers can be restarted one at a time so that some calls can still be processed.

Capturing logs on the Media Broker

To help you identify any issues you may experience, a script is provided with Avaya Mobile Video which captures call logs and statistics. The `logcapture.sh` script is installed in the Media Broker installation directory (`/opt/avaya/awmvs/3.4.x/mv sdk/media_broker`) and can be used to capture the following information:

- Media Broker configuration
- `vmstat` output
- Java memory
- Thread dumps
- Network capture in a `pcap` file

The logging script runs for a period of time which you define, allowing you to reproduce any problem scenarios during this time. When you stop the logging script, the information you require is captured in a series of log files.

You can define which information is captured by adding a selection of the following arguments when you run the script:

Argument	Description
-f	The filename of the resulting tar archive (required)
-c	Include configuration files in the archive
-t	Include thread dumps in the archive
-m	include heap memory dumps in the archive
-n	do not clean the output directory at the end of the run
-p	capture network traffic in a <code>pcap</code> file
-v	include <code>vmstat</code> output in the archive
-a	includes all options
-h	display online help

1. Capture all the information by running:

```
<install dir>/mvsdk/media_broker/logcapture.sh -a -f example.tar
```

(Use other options instead of `-a` if you only want some of the logs.) The console will display the following message:

```
*****
* Capturing files to directory logcapture.temp-LGR *
* Press <CTL>-C when ready to tar up captured files *
*****
```

Note: The final three characters of the directory name (LGR in the above example) will change each time the script is run, as this is a temporary directory.

2. Reproduce any scenarios which are causing the issues
3. Stop logging by pressing **CTRL+C**. The output files will be collected in `example.tar`, which will look something like:

```
./vmstat.out
./tcpdump.pcap
./MB/
./MB/x264_2pass.log
./MB/thread.dump
./MB/heap.bin
./MB/routetable.log
./MB/rest.log
./MB/proxy.log
./MB/log4j.properties
./MB/proxy.properties
```

```
./MB/console.log
./MB/stun.log
./MB/master.console.log
```

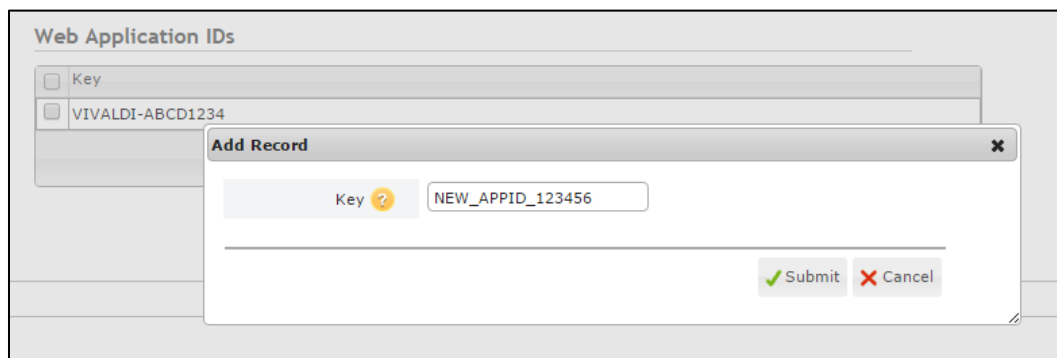
Configuring the Web Application ID

To configure the Web Application ID that is used by the Web Application to create session tokens to be used by clients:

1. Browse to the **General Administration** page on the Avaya Mobile Video Server web administration console:

`https://<GatewayIPAddress>:8443/web_plugin_framework/webcontroller`

2. In the **Web Application IDs** section, click **Add** and enter the 16-character ID of your choice:

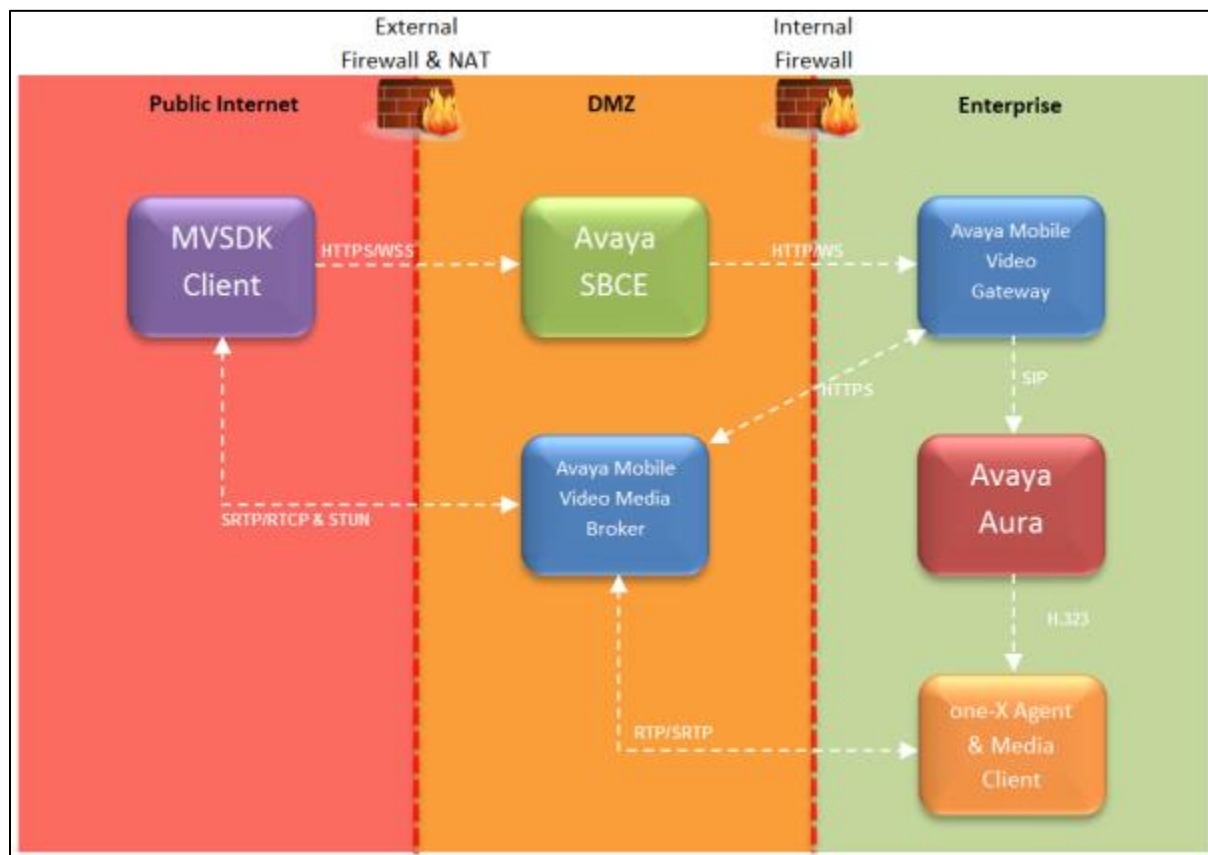


3. Click **Submit** to close the dialog and then click **Save** to save the changes.

Chapter 6: Configuring Traffic Segregation

Avaya Mobile Video Media Broker enables you to configure how the different types of traffic which it handles are allocated to local network interface cards (NICs) on the Avaya Mobile Video Media Broker server, in a flexible way.

The following diagram shows the Avaya Media Broker in the recommended deployment, where the Avaya SBCE and Avaya Mobile Video Media Broker are installed in a DMZ which separates the external network/internet from the internal network.



- The endpoint used is the one-X Agent and Media Client application; this is registered against an Aura Communication Manager in h323 mode.
- The lines between the components show the type of traffic between the components, for example WS (WebSocket traffic).
- As the diagram shows, there are 3 different types of traffic between the Avaya Mobile Video Media Broker and the other components:
 - Management Traffic (shown as Avaya Mobile Video Media Broker to Avaya Mobile Video Gateway link)

- External Traffic (shown as Avaya Mobile Video Media Broker to MVSDK Client link)
- Internal Traffic (shown as Avaya Mobile Video Media Broker to SIP Endpoint link)

Note: The internal firewall is optional in the Avaya Mobile Video Server deployment.

Internal SIP Traffic

The SIP Network settings specify a number of address and port-range records which define the addresses and port ranges of the NICs on the Media Broker that will be available for RTP on the internal SIP network.

Each record contains an address pattern, a lower port number, and an upper port number. The address pattern is in the form of a **Classless Inter-Domain Routing** (CIDR) expression, which can be a wildcard.

Note: CIDRs are used to facilitate the configuration of networks using a cluster of multiple Media Brokers.

All addresses on the Media Broker are matched against the CIDR address pattern to arrive at a set of Media Broker addresses for RTP and RTCP traffic on the internal SIP network. Then each port in the given range (inclusive), on each resolved address, is opened. The Media Broker allocates ports at call time by randomly selecting a consecutive pair of ports (one for data, one for control) from all the opened ports which are not currently in use. One selection is made for audio and, if required, another selection is made for video.

The SIP network port allocation results in the use of two ports for audio-only traffic, and four for audio and video traffic.

External Traffic

The WebRTC Client settings define the addresses and ports through which the Media Broker will receive SRTP/RTP from the client application. During call setup, the Gateway chooses which of these ports to use from those which are not currently in use. Any firewalls in the network must be set up to allow SRTP/RTP on these ports.

The settings specify a list of different client device **source address patterns**. Each pattern should match the address of a node traversed immediately before the Web Gateway; this is represented by the last `X-Forward-For` header entry in the Web Gateway websocket `HttpServletRequest`, so the Gateway will accept any HTTP request whose last `X-Forward-For` header matches one of the patterns.

When a client application is involved in a call, the Gateway will match the source address of the client against the list of CIDR source address patterns. If more than one pattern matches the source address (which can happen if one pattern covers a subset of the addresses covered by another pattern), then it will choose the most specific pattern. If there are no matches, it will reject the call.

The administrator should configure each client application source address pattern with exactly five address and port records. Each record contains a **public address**, a **public port**, a **local address** and a **local port**. These records inform the Gateway which local addresses and ports are available on the Media Brokers, and which corresponding public addresses and ports it should instruct the client to use for SRTP/RTP traffic.

At call time, the Gateway selects among these on a load-balanced basis per media stream, per call - the SDP passed by the Media Broker to the client application will contain the public address and port for the selected media stream, and the Media Broker will listen on the associated local address and port.

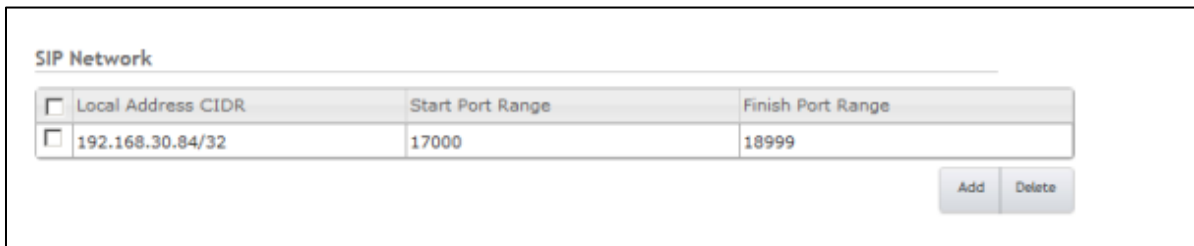
Unlike SIP network traffic, WebRTC Client traffic is multiplexed. An allocated port can handle traffic for the control and data of both audio and video. Selecting an address and port record for a given media stream provides for the control and data for that stream. Because selections are made for each media stream, the number of ports used for a call depends on the configured records and whether the call involves video.

For audio only calls, only one selection is made and only one port is needed. For calls which contain both audio and video, one selection is made for audio and another for video. If there is only one address and port record configured for the chosen source address pattern, then the same port will be selected for both audio and video (resulting in one port for all traffic). If there is more than one record, then because of the load-balanced nature of record selection, the Gateway may select different ports for audio and video (resulting in two ports being used).

Configuring SIP Network Settings

To configure the SIP Network settings, which define how the Media Broker communicates with the internal SIP network:

1. Go to the *SIP Network* section of the Media Broker Configuration page, and click **Add**:

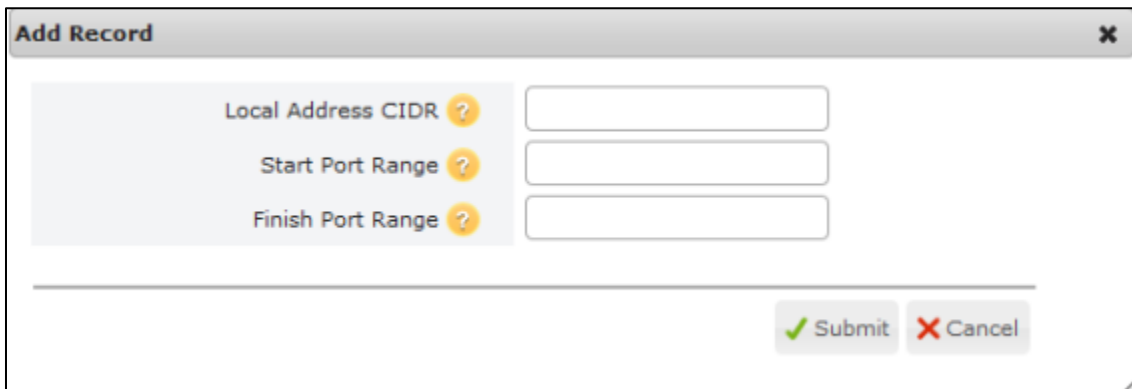


The screenshot shows a table titled "SIP Network" with three columns: "Local Address CIDR", "Start Port Range", and "Finish Port Range". There is one row with the values "192.168.30.84/32", "17000", and "18999". Below the table are "Add" and "Delete" buttons.

Local Address CIDR	Start Port Range	Finish Port Range
192.168.30.84/32	17000	18999

Add Delete

2. The **Add Record** dialog displays:



The screenshot shows the "Add Record" dialog box. It has three input fields: "Local Address CIDR", "Start Port Range", and "Finish Port Range". Each field has a yellow question mark icon to its right. At the bottom right are "Submit" and "Cancel" buttons.

Local Address CIDR ?

Start Port Range ?

Finish Port Range ?

Submit Cancel

Enter the following information:

- **Local Address CIDR**

A block of addresses on the Media Broker for RTP and RTCP traffic on the internal SIP network. This setting is a range of IP addresses signified by a CIDR notation: for example 192.0.2.0/24.

In the above example, the Media Broker sends and receives RTP and RTCP on any of its NICs having an address like 192.0.2.x. You can set the **Local Address CIDR** to `all` to allow all the available IPs on the Media Broker to send and receive RTP and RTCP.

- **Start Port Range**

The lower limit of the range of ports used for RTP and RTCP.

- **Finish Port Range**

The upper limit of the range of ports used for RTP and RTCP.

Note: At runtime, RTP and RTCP ports are assigned in pairs from the pool, so the **Start Port Range** value should be an even number, and the **Finish Port Range** value should be an odd number.

3. Click the **Submit** button.

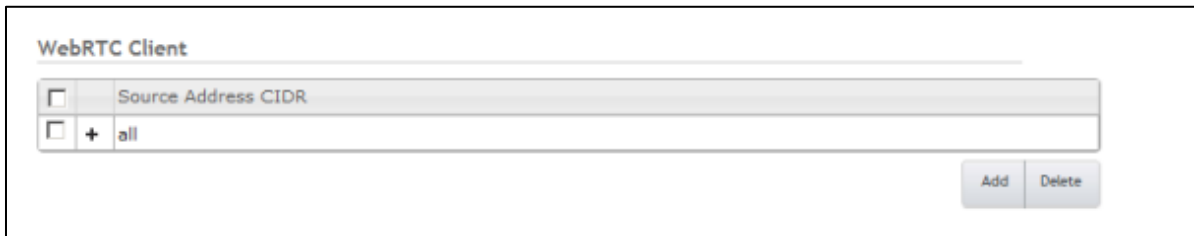
The range you entered now displays in the SIP Network list. Repeat the process to add any other ranges. Alternatively, to delete a range you have created, select the range by checking the checkbox next to it, and click **Delete**.

4. Click the **Save** button at the bottom of the page.

Configuring WebRTC Client Settings

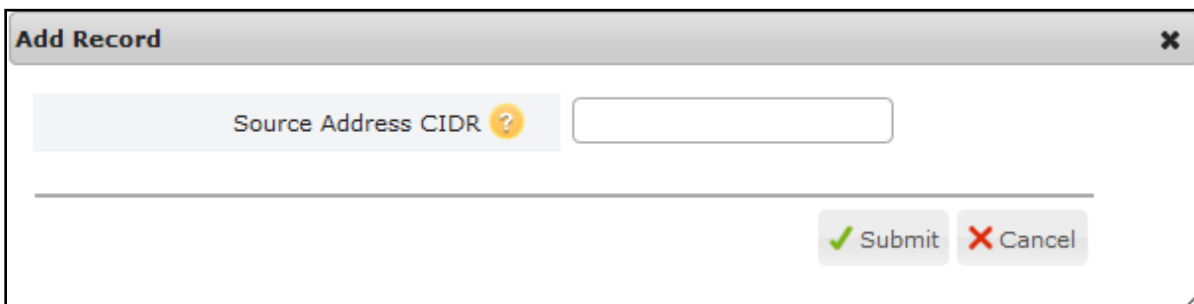
To configure the WebRTC Client settings, which define the addresses that clients use to communicate with the Media Broker:

1. Go to the *WebRTC Client* section of the Media Broker Configuration page, and click **Add**.



The screenshot shows the 'WebRTC Client' configuration section. It contains a table with two rows. The first row has a checkbox and the text 'Source Address CIDR'. The second row has a checkbox, a plus sign, and the text 'all'. To the right of the table are 'Add' and 'Delete' buttons.

2. The **Add Record** dialog displays:



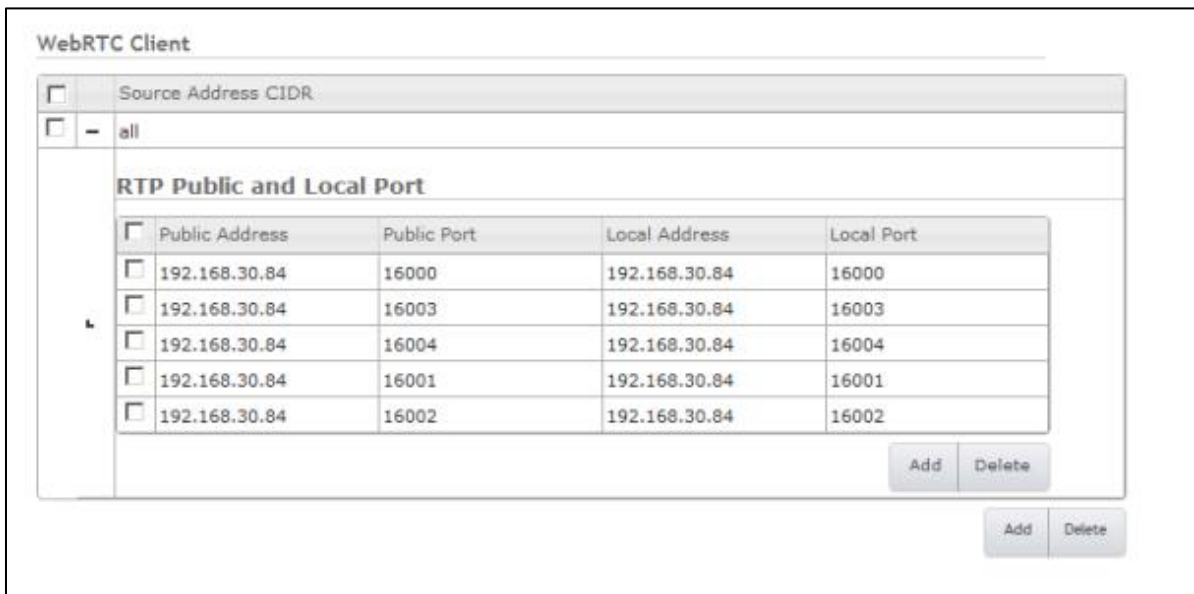
The screenshot shows the 'Add Record' dialog box. It has a title bar with the text 'Add Record' and a close button. The main area contains a label 'Source Address CIDR' followed by a question mark icon and an empty text input field. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Enter the **Source Address CIDR**, which defines a block of IP addresses of client endpoints; for example, 198.51.100.0/24.

Each **Source Address CIDR** has an associated block of addresses. Clients whose IP addresses are in the block defined by the **Source Address CIDR** communicate with the Media Broker using one of the addresses in the block. In the above example, the block of addresses will be associated with clients having IP addresses which match 198.51.100.x.

You can set the **Source Address CIDR** to match all IP addresses by setting the value to `all`.

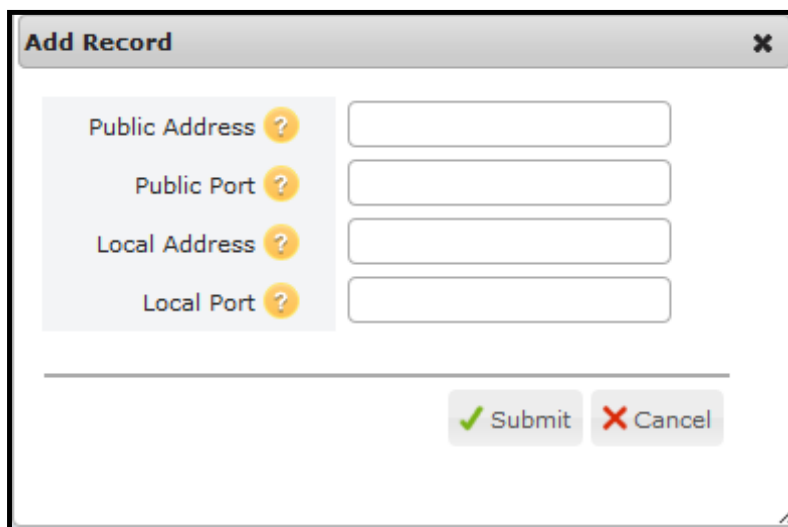
3. Click the **Submit** button. The **Source Address CIDR** you entered will appear in the WebRTC Client list.
4. Click the **+** next to the **Source Address CIDR** to expand the entry and show the public and local addresses and ports:



The screenshot shows the 'WebRTC Client' interface. At the top, there is a 'Source Address CIDR' section with a dropdown menu currently set to 'all'. Below this, the 'RTP Public and Local Port' section is expanded, displaying a table with five rows of public and local addresses and ports. Each row has a checkbox to its left. At the bottom right of the table, there are 'Add' and 'Delete' buttons. Below the table, there are additional 'Add' and 'Delete' buttons.

	Public Address	Public Port	Local Address	Local Port
<input type="checkbox"/>	192.168.30.84	16000	192.168.30.84	16000
<input type="checkbox"/>	192.168.30.84	16003	192.168.30.84	16003
<input type="checkbox"/>	192.168.30.84	16004	192.168.30.84	16004
<input type="checkbox"/>	192.168.30.84	16001	192.168.30.84	16001
<input type="checkbox"/>	192.168.30.84	16002	192.168.30.84	16002

5. Click **Add** to add a new set of public and local addresses and ports. The **Add Record** dialog displays:



The screenshot shows the 'Add Record' dialog box. It has a title bar with a close button. Inside, there are four input fields with labels: 'Public Address', 'Public Port', 'Local Address', and 'Local Port'. Each label has a yellow question mark icon to its right. Below the input fields, there are 'Submit' and 'Cancel' buttons. The 'Submit' button has a green checkmark icon, and the 'Cancel' button has a red X icon.

6. Enter the public and local addresses and ports:

- **Public Address**

The RTP IP address exposed on a firewall. It is used by the Media Broker when generating SDP to inform clients which address to send RTP traffic to. For example, 84.1.6.1.

If a firewall is not being used (for instance, in a testing installation), this can be the same as the **Local Address**, though unlike the **Local Address**, it must *not* be `all`.

- **Public Port**

The RTP port exposed on the **Public Address**. Used by clients for RTP traffic and used by the Media Broker when generating SDP. For example, 16000.

- **Local Address**

This is the Local RTP IP address on Media Broker, which the firewall should be set up to map from the **Public Address**. For example, 203.0.113.0.

You can set the **Local Address** to `all` to expose all available IPs on the Media Broker. Do not use `all` if you are configuring traffic segregation.

- **Local Port**

This is the RTP port on the Media Broker which the firewall should be set up to map from the **Public Port**. For example, 16000.

7. Click the **Submit** button. The public and local addresses will display in a line in the RTP Public and Local Port table.

Repeat steps 5, 6, and 7 five times in total to enter all five of the Media Broker's public address and port combinations. There should be one entry for each `rtp-proxy` process which the Media Broker starts.

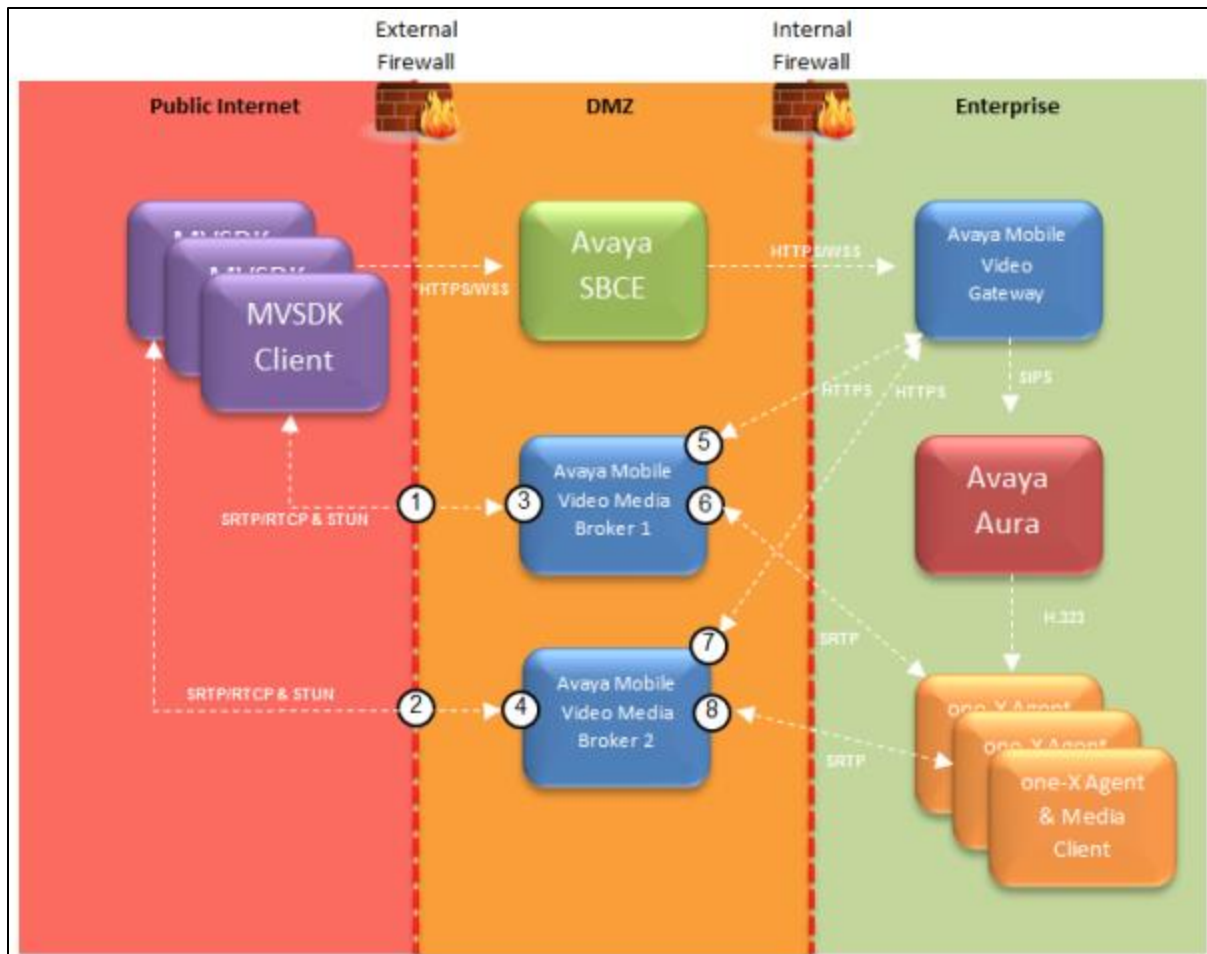
Note: You can edit existing entries in the *RTP Public and Local Port* table by clicking on them and editing in place.

Incoming RTP from a client will be assigned to the **Source Address CIDR** that the client's IP address matches most closely; one of the associated block of addresses will be chosen on a round-robin basis.

8. Repeat as many times as necessary, then click the **Save** button at the bottom of the page.

Example Configuration

The following diagram shows a more detailed view of the addresses and ports on a recommended configuration with two Avaya Mobile Video Media Brokers:



- Callout 1 and 2 represent the external IP addresses and ports configured on the External Firewall:
 - Callout 1 has an IP address configured on the external firewall as 81.144.171.73, which has 5 ports opened: 19000 -> 19004. The firewall is configured to send RTP traffic on these ports to Media Broker 1.
 - Callout 2 has an IP address configured on the external firewall as 81.144.171.73, which has 5 ports opened: 19005 -> 19009. The firewall is configured to send RTP traffic on these ports to Media Broker 2.

The address configured on the external firewall appears as the Public Address in the WebRTC Client settings for each Media Broker, together with the ports associated with that Media Broker.

- On the Avaya Mobile Video Media Broker:
 - Callouts 3 and 4 represent the first network interface card in each Avaya Mobile Video Media Broker that is used to communicate with the Client via the external firewall.
 - Callout 3 has an IP address configured as 173.31.252.122

- Callout 4 has an IP address configured as 172.31.252.123

These addresses appear as the Local Address in the WebRTC Client settings for each Media Broker.

- Callouts 5 and 7 represent the second network interface card, used for control traffic between the Avaya Mobile Video Media Broker and the Avaya Mobile Video Gateway via the internal firewall.
 - Callout 5 has an IP address configured as 192.168.0.122
 - Callout 7 has an IP address configured as 192.168.0.123

These addresses appear as the Media Broker addresses in the Media Brokers page.

- Callouts 6 and 8 represent the third network interface card that is used to communicate with the Avaya one-X[®] Agent/Media Clients via the internal firewall
 - Callout 6 has an IP address configured as 10.254.254.122
 - Callout 8 has an IP address configured as 10.254.254.123

These addresses appear as the Local Address CIDR of the SIP Network configuration.

- The Media Brokers also have network interface cards configured for communication with external RTP devices:
 - 173.31.253.122 on Media Broker 1
 - 173.31.253.123 on Media Broker 2

These addresses appear as a Local Address CIDR in the SIP Network configuration.

The above configuration is represented in the following tables:

Note: All values are example values only.

Avaya Mobile Video Media Broker general settings

Host Address	Port	Connection Type	Idle Route Timeout	Packet Size Limit	Throughput Rate Limit	Max. Buffer Size	Load			
192.168.0.122	8092	Secure	10	1500	1000	500	Min	✓	🔍	✎
192.168.0.123	8092	Secure	10	1500	1000	500	Min	✓	🔍	✎

SIP Network Settings

Avaya Mobile Video Media Broker 1

SIP Network		
<input type="checkbox"/>	Local Address CIDR	Start Port Range
<input type="checkbox"/>	10.254.254.0/24	17000
<input type="checkbox"/>	172.31.253.0/24	17000

Avaya Mobile Video Media Broker 2

SIP Network			
<input type="checkbox"/>	Local Address CIDR	Start Port Range	Finish Port Range
<input type="checkbox"/>	10.254.254.0/24	17000	17299
<input type="checkbox"/>	172.31.253.0/24	17000	17299

WebRTC Client Settings

Avaya Mobile Video Media Broker 1

WebRTC Client				
<input type="checkbox"/>	Source Address CIDR			
<input type="checkbox"/>	all			
<input type="checkbox"/>	RTP Public and Local Port			
	Public Address	Public Port	Local Address	Local Port
	81.144.171.73	19000	172.31.252.122	19000
	81.144.171.73	19001	172.31.252.122	19001
	81.144.171.73	19002	172.31.252.122	19002
	81.144.171.73	19003	172.31.252.122	19003
	81.144.171.73	19004	172.31.252.122	19004

Avaya Mobile Video Media Broker 2

WebRTC Client				
<input type="checkbox"/>	Source Address CIDR			
<input type="checkbox"/>	all			
<input type="checkbox"/>	RTP Public and Local Port			
	Public Address	Public Port	Local Address	Local Port
	81.144.171.73	19005	172.31.252.123	19005
	81.144.171.73	19006	172.31.252.123	19006
	81.144.171.73	19007	172.31.252.123	19007
	81.144.171.73	19008	172.31.252.123	19008
	81.144.171.73	19009	172.31.252.123	19009

Connection Monitoring

In a production environment, you will typically configure a Media Broker with multiple network interfaces, in which case the management REST interface is bound to a different network than at least one of the media-carrying interfaces (internal or external). If one of the network interfaces

fails, it is possible for the Media Broker to be able to process calls (via the management REST interface), but be unable to send or receive media for those calls.

To ensure that the Media Broker only accepts calls over the management interface when it is fully connected to the internal and external networks, you can configure connection monitoring.

How it works

Each Media Broker can be configured with one or more groups of addresses. A Media Broker will consider itself connected, and therefore able to service calls, if it can reach at least one of the addresses in each group (thus the logical operations are **ORs** within each group and **ANDs** between each group). The Media Broker will attempt to establish the **reachability** of an address by:

- ping (ICMP echo requests)
- If that receives no response then attempt to establish a TCP connection to port 7 at that address

A success with either mechanism will mark that address as reachable.

If there are no groups configured, then the Media Broker is considered to be connected.

Example

A typical network setup for Media Broker has 3 network interfaces:

- Management – The REST interface used by the Web Gateway is bound to this addresses
- External – external media; by default, uses SRTP.
- Internal – internal media; by default, uses RTP.

In this case there is no need to monitor connectivity on the management interface, as the gateway will only use the Media Broker if it can reach it over this interface. Therefore it is sensible to monitor the external and internal interfaces.

An example configuration is shown in the following diagram:

The screenshot shows the 'Monitored Connections' configuration page. It contains two group configurations. The first group, 'External Group', has two monitored addresses: '10.10.10.1' and '10.10.10.99'. The second group, 'Internal Group', has one monitored address: '192.168.17.1'. At the bottom, there is a '+ New Group' button.

Configuring Monitored Connections

1. Go to the *Monitored Connections* section of the Media Broker Configuration page:

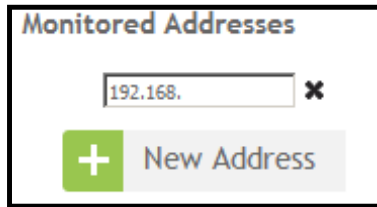
The screenshot shows the 'Monitored Connections' section with a '+ New Group' button.

2. Click the **New Group** button:

The screenshot shows the 'Monitored Connections' section with a '+ New Group' button. The 'Group Name' field is empty, and the 'Monitored Addresses' section is also empty.

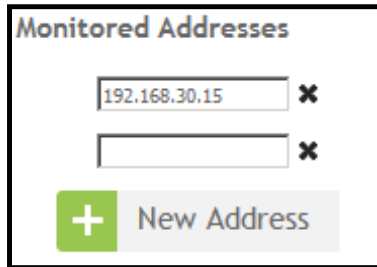
3. Enter a name in the **Group Name** field (this simply serves to identify the group).

4. Enter one of the Media Broker's IP addresses in the **Monitored Address** field.



The screenshot shows a box titled "Monitored Addresses". Inside, there is a text input field containing "192.168." followed by a small 'x' icon to its right. Below the input field is a green button with a white plus sign and a grey button labeled "New Address".

5. To add another address, click the **New Address** button and add the address in the new **Monitored Address** field which appears:



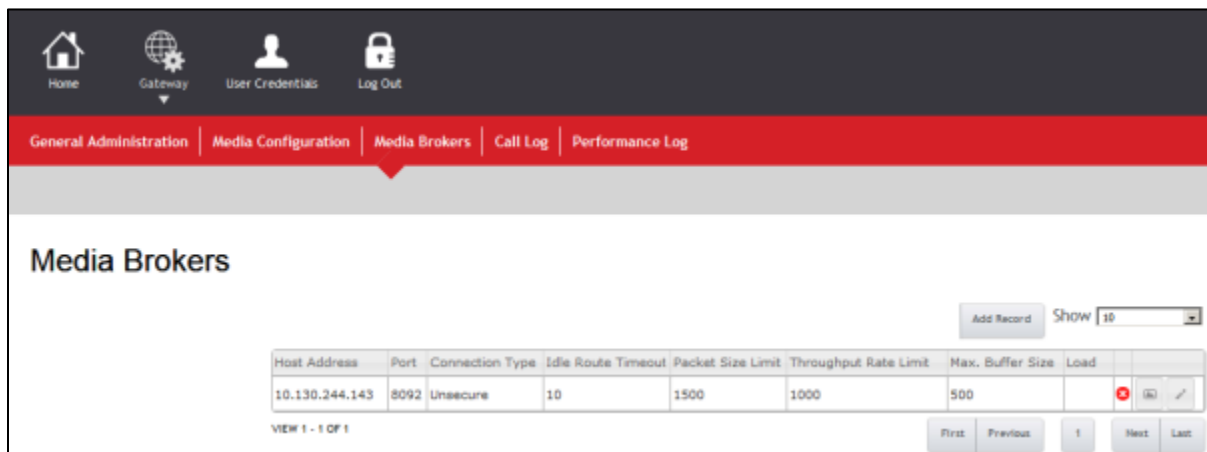
The screenshot shows the "Monitored Addresses" box with two input fields. The first field contains "192.168.30.15" and the second field is empty. Each field has a small 'x' icon to its right. The "New Address" button is still visible at the bottom.


6. When you have created all the groups you need, click the **Save** button.

Chapter 7: Avaya Mobile Video Media Broker Statistics

Media Broker Status

As well as its basic settings, the Media Broker page displays status information about each Media Broker:



Host Address	Port	Connection Type	Idle Route Timeout	Packet Size Limit	Throughput Rate Limit	Max. Buffer Size	Load
10.130.244.143	8092	Unsecure	10	1500	1000	500	

Media Broker Load

The **Load** column indicates the current load of the media broker, and is an indication of the load on each machine e.g. the CPU load.

The column contains a textual representation of the load, and can contain one of the following values (sorted in severity):

- Min
- Low
- Med
- High
- Max

Connectivity


The **Connectivity** column (located to the right of the **Load** column) indicates the connection status of the cluster Gateways to each Media Broker.

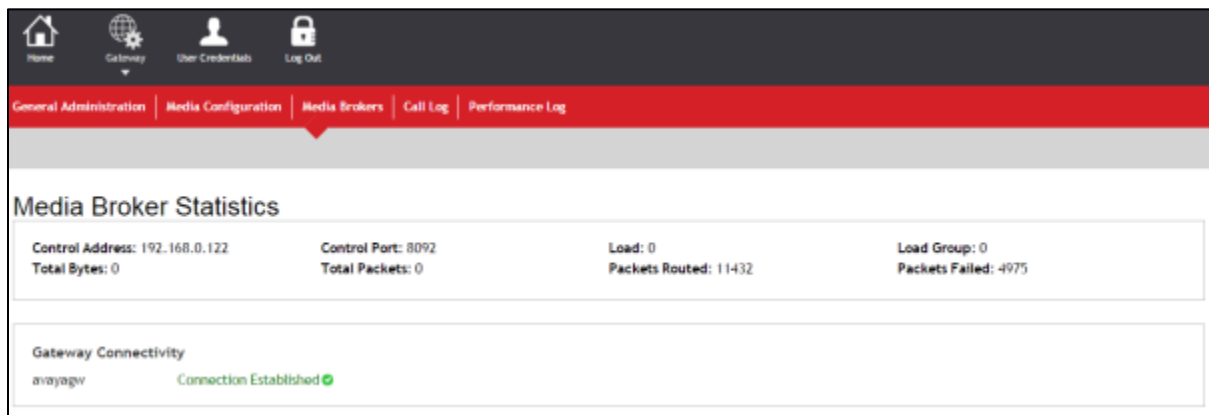
The column contains a visual representation of the connectivity status, and can contain one of the following images (hover over the image to reveal the textual representation of the status):

- A green tick (✓) indicates that the gateway is connected to the media broker
- A red cross (✗) indicates that the gateway cannot connect

Note: Initially the page can take a short period of time before it displays a true reflection of the connectivity status while it polls all machines involved

Statistics

To reveal detailed statistics for a particular media broker, click on the graph image () in the column to the right of the **Connectivity** column.



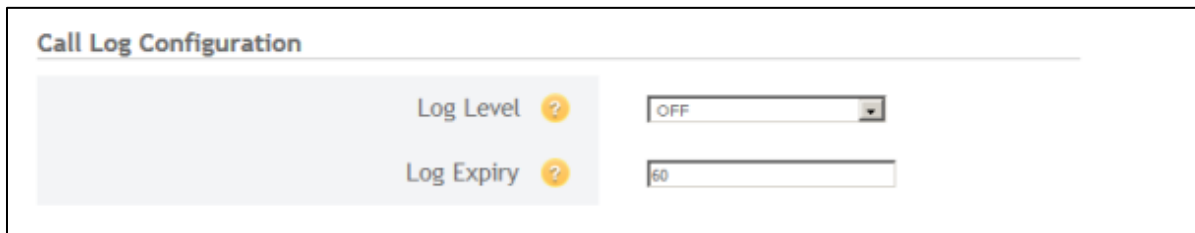
The **Load** value, is the actual load reported by the media broker, whilst the **Load Group** value is the **band** that the load value fits into, with 0 being the lowest loaded group band - this group is then used in the load balancers' media broker selection strategy.

The *Connectivity* section lists the gateway node, and its connection status to this particular media broker.

Call Log

To enable call log statistics:

1. On the **Gateway->General Administration** tab, scroll down to the *Call Log Configuration* section:



Call Log Configuration

Log Level ? OFF

Log Expiry ? 60

2. Set the **Log Level** to ON.

3. Set the **Log Expiry** to a value greater than 0 and less than 35000 (the expiry time is in minutes, so 35000 represents over 20 days).

Note: The call detail statistics could potentially cause problems if the logs are allowed to get too large. We recommend that you keep to a limit of 4,000 log entries, and go no higher than 10,000 entries. We enforce a maximum of 20,000 log entries, and every minute we remove all except the most recent 20,000 entries.


4. Click the **Save** button at the bottom of the page

To display the call logs, navigate to **Gateway->Call Log**


Call ID	From	To	Direction	Start	End
7fb7f6ab-d8a5-455f-b294-sip:fgahd@collaboratory	sip:2102@collaboratory.av	Outbound	2015-05-14 05:05	2015-05-14 05:06	
7fb7f6ab-d8a5-455f-b294-sip:fgahd@collaboratory	sip:2102@collaboratory.av	Outbound	2015-05-14 05:03	2015-05-14 05:04	
435a662e-d17a-440f-b939-sip:fgahd@collaboratory	sip:2102@collaboratory.av	Outbound	2015-05-14 04:51	2015-05-14 04:51	
435a662e-d17a-440f-b939-sip:fgahd@collaboratory	sip:2202@collaboratory.av	Outbound	2015-05-14 04:49	2015-05-14 04:49	

The **Direction** column indicates:

- **Inbound**
The media broker is handling the SDP for the callee
- **Outbound**
The media broker is handling the SDP for the caller

Click on the graph () button at the end of a column to display detailed statistics for that call (see [Call Statistics](#)).

Call Statistics

Click on the graph () button at the end of a column of a particular Call Log entry, to display detailed statistics for that call:

Call Details

Call ID: 7fb7f6ab-dda5-455f-b29d-0b8c46ae84fd:2:gateway_gateway\$BG-a4b76650-e47e-4723-85fd-3710d1a76e96

Media Broker: 10.130.244.143:8092 (Not Secure)

From: sip:fgshdfjs@collaboratory.avaya.com

Start: 2015-05-14 05:03:54

To: sip:2102@collaboratory.avaya.com;calluuiid=4d444961-eb08-4f4d-8f39-e8f13cced5a6-0

End: 2015-05-14 05:04:39

Call Direction: Outbound

Termination Reason: SIP Hangup

Call Statistics

Packets Received: 9638

Packets Sent: 7567

Client Call Quality

Inbound

Medium	Started	SSRC	Codec	Clock (Hz)	Channels	Payload Type	Skew (ms/ s)	Jitter (ms)	Packets			
									Total	Lost	Late	Dropped
Audio	05:04:00	2335077388	PCMU	8000	1	0	0.00	6.00	1930	0	0	0
Video	05:04:00	2759458896	VP8	90000	1	100	0.00	8.44	2236	0	0	0

Outbound

Medium	Started	SSRC	Codec	Clock (Hz)	Channels	Payload Type	Jitter (ms)	Packets	
								Total	Lost
Audio	05:04:00	1976110740	PCMU	8000	1	0	4.25	1929	0
Video	05:04:00	657617921	VP8	90000	1	100	9.02	3002	0

SIP Call Quality

Inbound

Medium	Started	SSRC	Codec	Clock (Hz)	Channels	Payload Type	Skew (ms/ s)	Jitter (ms)	Packets			
									Total	Lost	Late	Dropped
Audio	05:04:00	328813509	PCMU	8000	1	0	0.00	3.00	1929	0	0	0
Video	05:04:04	1940726191	H264	90000	1	100	0.00	1.01	3149	0	0	0

Outbound

Medium	Started	SSRC	Codec	Clock (Hz)	Channels	Payload Type	Jitter (ms)	Packets	
								Total	Lost
Audio	05:04:00	2162165054	PCMU	8000	1	0	-	212	0
Audio	05:04:05	1859381259	PCMU	8000	1	0	-	1688	0
Video	05:04:06	2590836308	H264	90000	1	100	-	592	0
Video	05:04:01	4051849818	H264	90000	1	100	-	69	0

The *Call Details* section shows information about the call itself - the underlined party indicates which party this call is being handled for.

The *Call Statistics* section shows the packets received and sent at the top, and below that is displayed detailed information relating to the call quality.

- *Client Call Quality*: Shows statistics between the Media Broker and the MVSDK endpoint
 - *Inbound*: Shows statistics **from** the Media Broker to the MVSDK endpoint
 - *Outbound*: Shows statistics **from** the MVSDK endpoint to the Media Broker
- *SIP Call Quality*: Shows statistics between the Media Broker and the SIP endpoint
 - *Inbound*: Shows statistics **from** the Media Broker to the SIP endpoint

- *Outbound*: Shows the statistics **from** the SIP endpoint to the Media Broker

Call Details Log

The MVSDK also puts in place a call details logger, which logs a subset of the Call Log information into a log file; it also includes information about the WebRTC endpoints involved in the call.

This log is enabled at install time and rotates daily. By default, the period for which old logs are stored is set to 7 days. The log file can be found alongside the MVS server logs at

`/opt/avaya/awmvs/x.x.x/awmvs/domain/servers/appserver-avayagw.log`.

To Change the SIP Call Logging Level

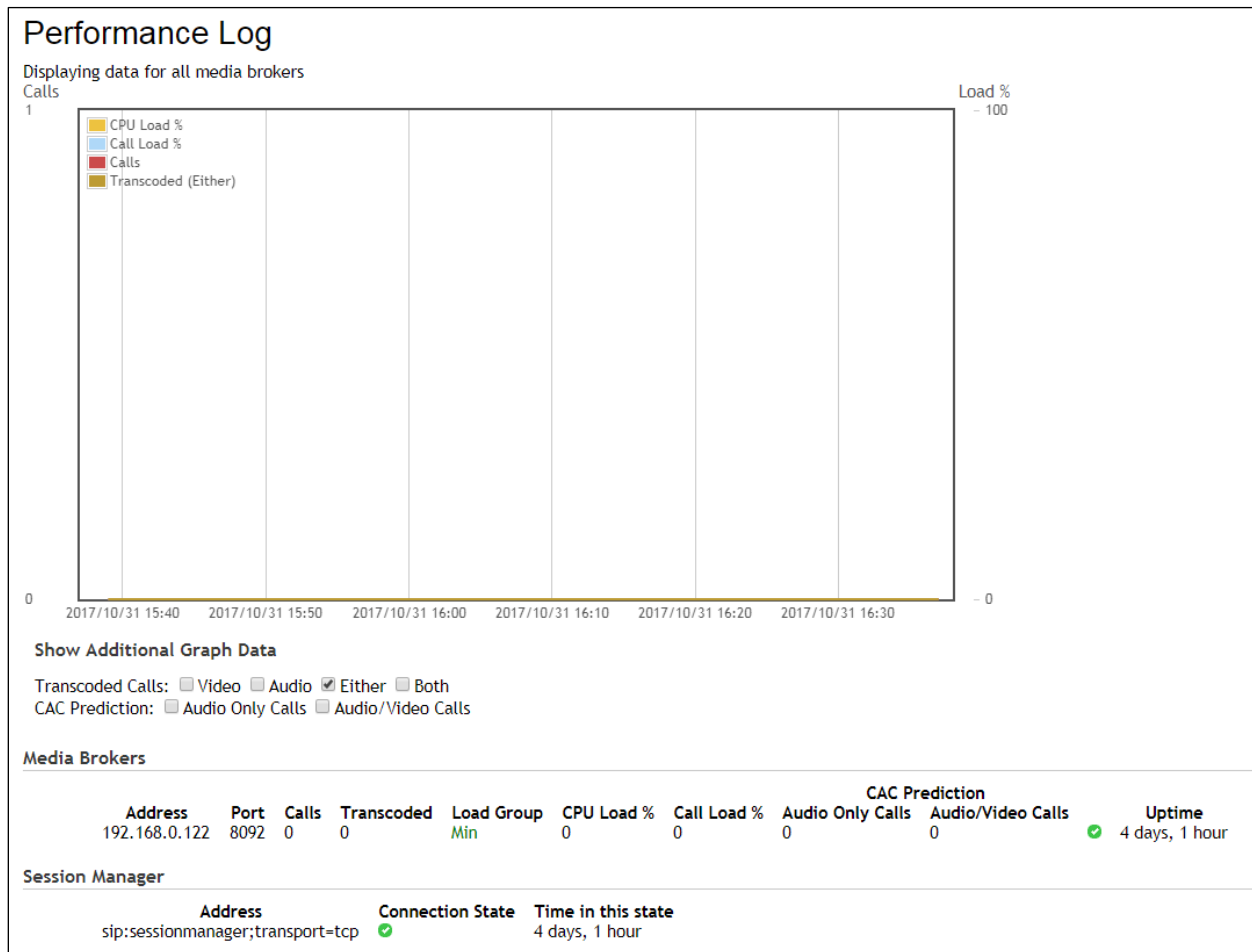
1. In the **Management Console**, from the top right menu, select **Profiles**
2. Select the `ha` profile from the top left menu
3. From the menu on the left, expand **Core** and select **Logging**
4. Select the **Log Categories** navigation tab
5. Select the `call.details` category
6. Click **Edit**
7. Change the **Log Level** entry by selecting from the drop down list.

Useful log levels to choose are `OFF` (to switch logging off), `DEBUG` (to give more information), and `INFO` (the default).

8. Click **Save**

Performance Log

The Media Broker publishes performance related statistics on the **Performance Log** page.



If there is more than one media broker, statistics are displayed separately for each. Information includes:

- How many calls are running.
- How many of these are being transcoded. If they are not transcoded then they are passthrough.
- The **call load**: the amount of current calls as a percentage of configured call load limits (according to CAC prediction status). This is a total value for both passthrough and transcodable calls.
- A graph showing the following data by default (extra data can be added via the check-boxes beneath the graph):
 - CPU load
 - Call Load
 - Total number of calls,
 - Which calls are transcoded (either audio or video)

Chapter 8: Configuring SNMP

Avaya applications that run on Avaya Mobile Video can generate SNMP event data (**traps**). This data can provide valuable usage and diagnostic information to administrators and network operations personnel.

For example, an application that monitors changes to a critical resource might raise an asymmetric trap when the resource changes. Similarly, you might have an application that monitors the availability of specific resources (such as the memory, or some other limited resource). When that resource runs low the application might set a warning state and a **Set** trap is sent. Once that resource goes back to acceptable levels a **Clear** trap is sent.

For details of the architecture of the SNMP subsystem, see the *Avaya Mobile Video Overview and Specification*.

If you need to change the configuration details for the SNMP agent after installing MVS, you can do so by modifying the attributes defined in the `snmp_subsystem` within the management profile using the JBoss CLI, and then restarting the SNMP service.

You can optionally configure the SNMP agent to send notifications to multiple SNMP trap receivers, each with its own SNMP protocol version, IP address, and port. The installer can only configure a single receiver, but you can add extra receivers to the configuration after installation by adding trap-target entries for the `snmp_subsystem` using the JBoss CLI, and then restarting the SNMP service (see [Configuring SNMP Trap Targets](#)).

The Avaya Mobile Video platform itself can also raise SNMP notifications. These are detailed in [Avaya Mobile Video Application Server SNMP Traps](#).

Configuring the SNMP Agent

An SNMP agent runs as part of the Host Controller process on each MVS node. The SNMP agent sends the event data to an SNMP client of your choice. An SNMP client is not supplied with Avaya Mobile Video: you must install your own client and supply the IP address of the server on which the client is running when you install the MVS and SNMP agent.

If you need to change the configuration details for the SNMP agent, such as the location of the SNMP client or the transport protocol used, or if you need to add additional SNMP trap receivers, you can do so using the JBoss CLI.

You can change some properties at the SNMP subsystem level, and other properties can be set for a specific SNMP trap target:

```
/profile=management/subsystem=snmp_subsystem/:write-attribute(name=<attribute-name>,value=<new-value>)
```

The attributes you can change are:

Attribute	Details
port	The default port is 8161, but can be changed to any valid port number.
protocol	The protocol used for sending the traps. Can be <code>udp</code> or <code>tcp</code> . If the protocol is not

Attribute	Details
	specified, udp is used.
poll-period	The polling period in seconds which the SNMP Agent uses to check for changes to JMX attributes. When it detects a change, it sends a symmetric trap.

For example, to change the port used to 1061, you would use the following command:

```
/profile=management/subsystem=snmp_subsystem/:write-attribute(name=port,value=1061)
```

If you make any changes to the SNMP options, you must restart the SNMP service:

```
/profile=management/subsystem=snmp_subsystem/:restart-snmp
```

You can also change the security options for SNMP – see [Configuring SNMP Trap Security](#).

Configuring SNMP Trap Targets

To add an address for receiving traps, you add an SNMP trap target:

```
/profile=management/subsystem=snmp_subsystem/trap-target=<target name>/:add(protocol=snmp protocol>,ip=<target ip>,port=<target port>)
```

where:

- <target name> is the ID of the trap target (a name for identification purposes)
- <snmp protocol> is the SNMP protocol to use for this target. This must be one of
 - SNMPv1
 - SNMPv2c
 - SNMPv3

If the protocol is omitted, it defaults to SNMPv2c.

- <target ip> is the IP address of the trap target
- <target port> is the port number which the trap target is listening on

For example, to add a target with an ID of local, you might use a command like:

```
/profile=management/subsystem=snmp_subsystem/trap-target=local/:add(protocol=SNMPv2c,ip=127.0.0.1,port=1062)
```

The properties for each trap target can be changed using a command that specifies the target-name:

```
/profile=management/subsystem=snmp_subsystem/trap-target=local/:write-attribute(name=port,value=1063)
```

If any changes are made to the SNMP trap target options, the SNMP service must be restarted:

```
/profile=management/subsystem=snmp_subsystem/:restart-snmp
```

Configuring the SNMP Client

We recommend that you use an SNMP client that implements the `ALARM-MIB` file. You can download the file from a site such as <http://www.simpleweb.org/ietf/mibs/>. You must then import this file, along with any MIB files supplied with applications that you will deploy and which will raise traps, into your SNMP client tool.

For the Avaya Mobile Video traps, you must import the following MIB files into your SNMP client:

- `AS-PLATFORM.MIB`
- `AS-LICENSING.MIB`

These files can be found in the `<install-dir>/docs/mibs` directory.

Avaya Mobile Video Application Server SNMP Traps

There are a number of SNMP traps that might be raised when significant events occur within the MVS cluster. Each of the following SNMP traps for MVS are symmetric; this means that each trap contains `Set` when an issue is detected, or `Clear` when the issue is resolved:

Set Trap Name	Description
<code>platformSetSlaveDomainConnectionDown</code>	A slave AS could not connect to the Domain Host Controller, suggesting that the Domain Host Controller is not running. Applies to multi-box deployments only.
<code>platformSetServerGroupDown</code>	The Server Group has no active server processes
<code>platformSetServerConnection</code>	The SNMP agent failed to connect to a server process. This could be an AS, LB, or Management Server; as identified by the <code>resourceId</code> in the notification. (See Decoding the Resource ID)
<code>platformSetServerState</code>	Set for any server process state change for an AS, Management Server or LB. Server has either stopped or a restart is required.
<code>platformSetNodesNotRegisteredWithLoadbalancer</code>	An LB has no ASs registered with it. This trap is fired only when an LB is restarted at a time when there are no ASs running.

The `Clear` traps are called `platformClearSlaveDomainConnectionDown`, etc.

When the issue is resolved, the associated `Clear` trap is raised, for example, if the `platformSetServerGroupDown` trap is raised and at least one server in the server group is started, the `platformClearServerGroupDown` trap is raised, signifying that the issue is resolved.

There is also an asymmetric trap, `platformAbnormalServerShutdown`. This trap is raised every time an AS or LB shuts down unexpectedly. By default, when an unexpected shutdown is detected the Host Controller will restart that server. This trap ensures that administrators are alerted to multiple restarts that might affect service, so that they can investigate the issue.

There are also two symmetric traps related to licensing, whose meaning is slightly different to those above:

Trap Name	Description
asLicensingSetState	A license has changed state to something other than <code>ACTIVE</code> . The new state may be one of: <ul style="list-style-type: none">• <code>NOT_STARTED</code>• <code>EXPIRED</code>• <code>EXPIRING_SOON</code>
asLicensingClearState	The state of the license has changed to <code>ACTIVE</code> .

The content of these traps includes the `Resource ID` and the `State`. The `Resource ID` encodes information about the product whose license has changed state: the server process (which is always `management`), the product ID, and the license ID.

Example Scenarios

- If all of the ASs in a Server Group go down, no traffic can be processed for that Server Group, MVS raises the `platformSetServerGroupDown` trap.
- If the management server process on the Domain Host Controller goes down, the licensing subsystem becomes unavailable, so MVS raises the `platformSetServerConnection` trap. It might also raise the `platformSetServerState`, as the server state changes from the running state.
- If a slave Host Controller loses connection to the Domain Host Controller, the configuration on that might become stale, so MVS raises the `platformSetSlaveDomainConnectionDown` trap.
- If a slave Host Controller reinstates a connection to the Domain Host Controller, MVS raises the `platformSetServerState` trap (restart required state).

Decoding the Resource ID

The resource ID identifies a MVS resource. It consists of a prefix which identifies MVS itself, followed by a single digit which identifies either the Host Controller itself, or one of two tables; if it is a table, it is followed by an index identifying the member of that table.

All the table and scalar OIDs for the MVS trap resources start with `1.3.6.1.4.1.7377.100`:

Resource ID	Resource
<code>1.3.6.1.4.1.7377.100.0</code>	Host Controller
<code>1.3.6.1.4.1.7377.100.1</code>	Server Process table
<code>1.3.6.1.4.1.7377.100.2</code>	Server Group

Resource ID	Resource
	table

For the tables, the indexes are keys consisting of an encoded string (containing the server process name for the server process table, or the server group name for the server group table). The encoded string that makes up the index has a number representing the number of characters in the string, followed by the ASCII character numbers that make up the string.

For example, for a server process named `Hello`, the resource ID would be:

```
1.3.6.1.4.1.7377.100.1.5.72.101.108.108.111
```

where `1.3.6.1.4.1.7377.100.1` indicates the server process table, `5` is the length of the string (**H**ello), followed by `72` (ASCII **H**), `101` (**e**), `108` (**l**), `108` (**l**), and `111` (**o**).

Traps Raised on MVS Startup

When a MVS cluster is first started, a number of traps are raised. This is because the system has no history of traps raised, so the status of each node is tested. If the status is fine, a `Clear` trap will be raised, regardless of any previous state. Therefore, on start-up, MVS will raise at least the `platformClearNodesNotRegisteredWithLoadbalancer` and `platformClearServerGroupDown` traps.

As the nodes in a MVS cluster are started in an undefined order, it is likely that it will raise some `Set` traps, closely followed by the associated `Clear` traps.

Configuring SNMP Trap Security

By default, where applications raise SNMP traps, SNMPv2 traps are generated. You can optionally change this to SNMPv3 traps on installation, as these traps can be secured. By default, however, they are insecure. This section describes how SNMPv3 traps can be secured.

You can also restrict access to SNMP managed objects for any SNMP protocol version. This is done using the View Access Control Model (VACM). This is described in [SNMP View Access Control](#).

SNMP security levels and users are defined as properties of the `snmp_subsystem`, and can be configured using the CLI. To get a list of all the properties in the SNMP subsystem, use:

```
/profile=management/subsystem=snmp_subsystem/:read-
resource(recursive=true)
```

All of the values starting `snmp4j.agent.config` are related to SNMPv3 security, but because there are a great many of them, only some of these options are discussed in this section.

You can configure them using a command like:

```
/profile=management/subsystem=snmp_subsystem/property=<property
name>/:write-attribute(name=value,value=<property value>)
```

After any change to the SNMP subsystem or properties, the SNMP service must be restarted:

```
/profile=management/subsystem=snmp_subsystem/:restart-snmp
```

SNMP Security Levels and Users

SNMPv3 User-based Security Model (USM) security can be implemented at one of three levels; there are three users specified by default, each one corresponding to one of the three levels, using specific authentication and encryption algorithms:

User	Maximum Security Level	Description
SHADES	authPriv	Authorization (SHA) and encryption (DES)
SHA	authNoPriv	Authorization (SHA) without encryption
unsec	noAuthNoPriv	Neither authorization nor encryption

These users are defined by the SNMP properties

`snmp4j.agent.cfg.oid.1.3.6.1.6.3.15.1.2.2.1`,
`snmp4j.agent.cfg.index.1.3.6.1.6.3.15.1.2.2.1.0` (SHADES),
`snmp4j.agent.cfg.index.1.3.6.1.6.3.15.1.2.2.1.1` (SHA), and
`snmp4j.agent.cfg.index.1.3.6.1.6.3.15.1.2.2.1.2` (unsec), together with their associated properties (`snmp4j.agent.cfg.value.1.3.6.1.6.3.15.1.2.2.1.0.0`,
`snmp4j.agent.cfg.value.1.3.6.1.6.3.15.1.2.2.1.0.1`, etc. - note that the `1.3.6.1.6.3.15.1.2.2.1` part is constant across the user definitions). The only values in the user definitions which should be changed are the passwords (`SHADESAuthPassword`, `SHADESPrivPassword`, and `SHAAuthPassword`).

Other values in the SNMP subsystem may be changed. For instance, to change the SNMPv1 read access to unrestricted, use:

```
/profile=management/subsystem=snmp_subsystem/property=snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.1/:write-attribute(name=value,value={s}unrestrictedReadOnly)
```

Implementing SNMPv3 Security

The following properties control which security level and user the SNMPv3 messages use:

- `snmp4j.agent.cfg.value.1.3.6.1.6.3.12.1.3.1.2.2`
- `snmp4j.agent.cfg.value.1.3.6.1.6.3.12.1.3.1.2.3`

To set the user the SNMPv3 messages will use:

```
/profile=management/subsystem=snmp_subsystem/property=snmp4j.agent.cfg.value.1.3.6.1.6.3.12.1.3.1.2.2/:write-attribute(name=value,value=<user>)
```

where `<user>` is one of SHADES, SHA, or unsec.

To set the security level, use:

```
/profile=management/subsystem=snmp_subsystem/property=snmp4j.agent.cfg.value.1.3.6.1.6.3.12.1.3.1.2.3/:write-attribute(name=value,value=<level>)
```

where <level> is one of:

Value	Level	Description
1	noAuthNoPriv	Can be specified for any of SHADES, SHA, or unsec
2	authNoPriv	Can be specified only for SHADES or SHA
3	authPriv	Can be specified only for SHADES

After making changes to the SNMP subsystem properties, the SNMP service should be restarted – see [Configuring SNMP Trap Security](#).

Configuring the SNMP Client

For every SNMP agent that a NMS SNMP management client will be receiving traps from, the management client will need to perform an SNMP GET on the `snmpFrameworkMib.snmpFrameworkMIBObjects.snmpEngine.snmpEngineID` (.1.3.6.1.6.3.10.2.1.1.0) for that SNMP agent. This engineID will be used to set up the USM user for the management client.

For every SNMP agent, the management client will need a USM entry containing the following:

```
EngineID,USER[,SHA,auth passphrase][,DES, priv passphrase]
```

The details of this configuration will depend on the SNMP client being used. The following configuration has been tested with `net-snmp`, using the `snmptrapd` tool (set up your own client with the equivalent settings in the way that your client expects).

For `snmptrapd`, put these settings in the `usr/etc/snmp/snmptrapd.conf` file:

```
authCommunity log,execute,net public

createUser -e <engineID> SHADES SHA <SHADESAuthPassword> DES
<SHADESPrivPassword>

createUser -e <engineID> SHA SHA <SHAAuthPassword>

createUser -e <engineID> unsec

authUser log,execute,net SHADES
authUser log,execute,net SHA
authUser log,execute,net unsec noauth
```

where <SHADESAuthPassword>, <SHAAuthPassword>, and <SHADESPrivPassword> should be replaced by the real passwords set in the SNMP subsystem configuration, and <engineID> is the value returned by the SNMP GET described above..

SNMP View Access Control

You can restrict access to SNMP managed objects for any SNMP protocol version. This is done using the View Access Control Model (VACM).

The `vacmSecurityToGroupTable` (at property `snmp4j.agent.cfg.oid.1.3.6.1.6.3.16.1.2.1`) defines the default SNMP Agent. It contains indexes at properties `snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.2.1.0`,

snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.2.1.1, and so on. These indexes map a combination of security model and security name to a group (at the properties snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.2.1.0.0, snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.2.1.1.0, etc.). The group is used to define an access control policy.

The index is made up of the integer representing the security model, the length of the string representing the security name, and the security name itself, for example:

3.5.'unsec'

for a security model of 3 and the five character security name unsec.

The security model may be:

- 0 - Reserved for any
- 1 - SNMPv1
- 2 - SNMPv2
- 3 - User Based Security Model (USM) used by SNMPv3

The security name is the **community string** for SNMPv1 or SNMPv2, or the USM user name for SNMPv3 (i.e. SHADES, SHA, or unsec - (see [SNMP Security Levels and Users](#))).

For instance, these entries map the SHADES user (using the USM security model) to the v3group:

```
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.2.1.1" => {"value" =>
{o}3.6.'SHADES'"}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.2.1.1.0" => {"value" =>
{s}v3group"}:
```

...

By default, the groups are:

- v1v2cgroup
- v3group

The default access rights for groups are defined by another table (at snmp4j.agent.cfg.oid.1.3.6.1.6.3.16.1.4.1). The indexes into this table (at snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.0, etc.) contain a group name, a context prefix, a security model, and a security level. For example:

7.'v3group'.0.3.1

means a 7 character group name (which is v3group), a zero length context string (context strings are not currently used, so all are 0), the security model is 3 (USM), and the security level is 1 (noAuthNoPriv).

In the default configuration the following index entries are defined:

- 10.'v1v2cgroup'.0.2.1 - SNMPv2, noAuthNoPriv (SNMPv2 'public')
- 10.'v1v2cgroup'.0.1.1 - SNMPv1, noAuthNoPriv (SNMPv1 'public')
- 7.'v3group'.0.3.3 - USM, authPriv (SNMPv3 'SHADES')
- 7.'v3group'.0.3.2 - USM, authNoPriv (SNMPv3 'SHA')

- 7.'v3group'.0.3.1 - USM, authPriv (SNMPv3 'unsec')

Three of the values associated with each index contain the access levels for read, write, and notify access for each group:

- .1={s}unrestrictedReadOnlyView
- .2={s}unrestrictedWriteView
- .3={s}unrestrictedNotifyView

These entries can either be set to the value above, or left blank to prevent that particular access to the managed object.

Thus the entries:

```
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.1" => {"value" =>
{o}7.'v3group'.0.3.3"}:
```

...

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.1" => {"value" =>
{s}unrestrictedReadOnlyView"}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.2" => {"value" =>
{s}unrestrictedWriteView"}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.3" => {"value" =>
{s}unrestrictedNotifyView"}:
```

...

define the v3group as having unrestricted access for read, write, and notify, while:

```
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.1" => {"value" =>
{o}10.'v1v2cgroup'.0.2.1"}:
```

...

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.1" => {"value" => {s}}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.2" => {"value" =>
{s}unrestrictedWriteView"}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.3" => {"value" => {s}}:
```

...

defines the v1v2cgroup as having unrestricted write access, but no access for read or notify.

For each entry in the access table the appropriate read, write, and notify views should be set. For example, if you wanted to allow all groups to be able to raise notifications, but only v3group with USM, authPrivsecurity, to allow reads and writes, the following configuration would achieve that:

```
"snmp4j.agent.cfg.oid.1.3.6.1.6.3.16.1.4.1" => {"value" => 6:6"}:
```

```
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.0={o}10.'v1v2cgroup'.0.2.1":
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.0" => {"value" => {i}1"}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.1" => {"value" => {s}}:
```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.2" => {"value" => {s}}:
```

```

"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.3" => {"value" =>
{s}unrestrictedNotifyView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.4" => {"value" => {i}4}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.0.5" => {"value" => {i}1}:
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.1" => {"value" =>
{o}7.'v3group'.0.3.3"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.0" => {"value" => {i}1}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.1" => {"value" =>
{s}unrestrictedReadView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.2" => {"value" =>
{s}unrestrictedWriteView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.3" => {"value" =>
{s}unrestrictedNotifyView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.4" => {"value" => {i}4}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.1.5" => {"value" => {i}1}:
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.2" => {"value" =>
{o}10.'v1v2cgroup'.0.1.1"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.2.0" => {"value" => {i}1}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.2.1" => {"value" => {s}}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.2.2" => {"value" => {s}}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.2.3" => {"value" =>
{s}unrestrictedNotifyView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.2.4" => {"value" => {i}4}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.2.5" => {"value" => {i}1}:
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.3" => {"value" =>
{o}7.'v3group'.0.3.2"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.3.0" => {"value" => {i}1}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.3.1" => {"value" => {s}}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.3.2" => {"value" => {s}}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.3.3" => {"value" =>
{s}unrestrictedNotifyView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.3.4" => {"value" => {i}4}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.3.5" => {"value" => {i}1}:
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.4" => {"value" =>
{o}7.'v3group'.0.3.1"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.4.0" => {"value" => {i}1}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.4.1" => {"value" => {s}}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.4.2" => {"value" => {s}}:

```

```
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.4.3" => {"value" =>
{s}unrestrictedNotifyView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.4.4" => {"value" => {i}4}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.4.5" => {"value" => {i}1}:
"snmp4j.agent.cfg.index.1.3.6.1.6.3.16.1.4.1.5" => {"value" =>
{o}7.'v3group'.0.4.1}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.5.0" => {"value" => {i}1}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.5.1" => {"value" => {s}":
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.5.2" => {"value" => {s}":
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.5.3" => {"value" =>
{s}unrestrictedNotifyView"}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.5.4" => {"value" => {i}4}:
"snmp4j.agent.cfg.value.1.3.6.1.6.3.16.1.4.1.5.5" => {"value" => {i}1}:
```

Chapter 9: Resources

Documentation

The following table lists the related documents for Avaya Mobile Video Server. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description
Avaya Mobile Video Overview and Specification	Describes the features and specifications for Avaya Mobile Video.
Avaya Mobile Video Release Notes	Describes any late-changing information about the release and known issues for the product.
Avaya Mobile Video Planning and Security Reference	Describes the components, deployment, and security options for Avaya Mobile Video.
Installing Avaya Mobile Video Server and Media Broker	Describes how to install Avaya Mobile Video.
Installing Avaya Media Client	Describes how to install Avaya Media Client.
Using Avaya Media Client	Describes how to use the features of Avaya Media Client.
Administering Avaya Mobile Video	Describes how to administer Avaya Mobile Video.
Avaya Mobile Video Server Software Development Guide	Describes how to develop Mobile Video applications.
Avaya Mobile Video Port Matrix	Describes the ports used for Avaya Mobile Video

Training

Course code	Course title
Avaya Oceana™ Solution Training	
3420W	Avaya Oceana™ Solutions Design Fundamentals
3470T	Avaya Oceana™ Solutions Design Fundamentals APDS Online Test
2402W	Avaya Oceana™ Workspaces Agent Desktop Training
2404W	Avaya Oceana™ Workspaces Supervisor Desktop Training

Support

Visit the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Web Administration interface reference

Using the Web Administration interface you can configure Mobile Video Web interactively.

The Avaya Mobile Video Server administration page allows you to configure:

- Avaya Mobile Video Gateway Administration
- Avaya Mobile Video Media Brokers

Web Gateway Administration

The following sections give information about the individual pages and sections of the configuration Web UI.

General Administration

The General Administration page contains the main Gateway Administration settings.

SIP Global Configuration

Outbound SIP Servers

Description	This value specifies the Outbound SIP proxy to be used by the Gateway. This value should always point to <code>sip:sessionmanager</code> ; and should not be changed. Only the transport can be changed between <code>tcp</code> or <code>tls</code> .
Mandatory	Yes
Values	A SIP URI, in the format of <code>sip:<URI></code> .
Default	None

Rewrite outbound SIP URIs

Description	If this is set to <code>true</code> , the Gateway will update the host part of the Request URI of all outbound requests to match the host part of the outbound SIP server address. If this is set to <code>false</code> , requests are sent on to the outbound sip server(s) without change. See Outbound SIP Servers
--------------------	--

Mandatory	Yes
Values	true or false
Default	false

Server Timeout

Description	The time, in milliseconds, which the Gateway allows for a server to respond to a request before it considers it to be down and tries another server. See Outbound SIP Servers
Mandatory	Yes
Values	A period of time in milliseconds between 500 and 3600000
Default	3000

Ping Interval

Description	The interval between successive OPTIONS messages being sent to an outbound SIP server when that server is considered up . See Outbound SIP Servers
Mandatory	Yes
Values	A period of time in milliseconds between 0 and 1800000
Default	30000

Dead Link Ping Interval

Description	The interval between successive OPTIONS messages being sent to an outbound SIP server when that server is considered down . See Outbound SIP Servers
Mandatory	Yes
Values	A period of time in milliseconds between 0 and 1800000
Default	5000

Registration expiry

Description	The time period in between REGISTER messages. Used by the Web Gateway to set how often REGISTER messages are sent to the SIP Registrar. It is set in the REGISTER Expires header. See Section 10.2 of RFC 3261 for more details. This value is used for voice and video in registrations sent to the internal or external Registrar.
Mandatory	Yes
Values	A period of time in seconds between 120 and 86400

Default	1800
----------------	------

Min SIP session expiry

Description	The minimum allowable SIP session expiration period
Mandatory	Yes
Values	A period of time in seconds between 90 and 86400
Default	400

SIP session expiry

Description	SIP session expiry period
Mandatory	Yes
Values	A period of time in seconds between 90 and 86400 Note: This value should be greater than the Min SIP session expiry , and less than half the Registration expiry
Default	

Web Application IDs

Description	List of keys for web applications to use to allow the service to verify them. Used by the Web Gateway to validate calls from the associated web application.
Mandatory	Yes
Values	A text string, for example <code>webappid-0123456789</code> . The web application key must be a minimum of 16 characters in length.
Default	None

WebRTC Configuration

Max Message Queue Size

Description	The maximum number of messages to be queued before tearing down the connection
Mandatory	Yes
Values	Number of messages
Default	

Client Ping Poll Period

Description	The number of seconds between PING messages
Mandatory	Yes

Values	A time period in seconds
Default	

Missed Pings Before Timeout

Description	The number of consecutive <code>PING</code> messages that we send but received no <code>PONG</code> response before ending the WebSocket connection.
Mandatory	Yes
Values	Number of <code>PING</code> messages
Default	

Fast Picture Update Poll Period

Description	The time between sending requests for Fast Picture Update info requests. Set to 0 to disable.
Mandatory	Yes
Values	Number of milliseconds
Default	

Media Timeout Poll Period

Description	The time without media after which a call will time out
Mandatory	Yes
Values	A time period in seconds
Default	

Call Log Configuration

Log Level

Description	The level of detail in the call log.
Mandatory	Yes
Values	<ul style="list-style-type: none"> • ON • OFF
Default	OFF

Log Expiry

Description	The time to keep call logs
Mandatory	Yes
Values	Time in minutes
Default	60

Performance Log Configuration

Log Enabled

Description	Whether or not the performance should be logged
Mandatory	Yes
Values	true or false
Default	true

Log Expiry

Description	Length of time to keep performance logs
Mandatory	Yes
Values	Time in minutes
Default	60

Sample Period

Description	Time between samples of the performance data
Mandatory	Yes
Values	Time in seconds
Default	60

Resource Management

Max Concurrent Sessions Per Node

Description	The maximum number of concurrent user session allowed per gateway
Mandatory	Yes
Values	Number of users
Default	5000

Media Configuration

Banned Codecs

Description	A list containing codecs <i>not</i> to be allowed to pass through the Media Broker. Used by the Media Broker to produce SDP; codecs on the banned list will be removed from the SDP as it passes through the Media Broker.
Mandatory	No
Values	A text string
Default	None

Audio Codec Prioritization Configuration

Description	A list of audio codec names indicating the priority in which they should be
--------------------	---

	used for transcoding.
Mandatory	No
Values	A list of codec names, sorted from top to bottom in the priority in which they should be used.
Default	None

Video Codec Prioritization Configuration

Description	A list of video codec names indicating the priority in which they should be used for transcoding.
Mandatory	No
Values	A list of codec names, sorted from top to bottom in the priority in which they should be used.
Default	None

Video Resolution Configuration

Default Resolution Height

Description	The default height, in pixels, of the video stream passed through the Media Broker
Mandatory	Yes
Values	A number of pixels greater than or equal to 1
Default	288

Default Resolution Width

Description	The default width, in pixels, of the video stream passed through the Media Broker
Mandatory	Yes
Values	A number of pixels greater than or equal to 1
Default	352

Max Resolution Height

Description	The maximum height allowable, in pixels, of the video stream passed through the Media Broker
Mandatory	Yes
Values	A number of pixels greater than, or equal to, 1. Must be greater than or equal to Default Resolution Height .
Default	288

Max Resolution Width

Description	The maximum width, in pixels, of the video stream passed through the Media Broker
Mandatory	Yes

Values	A number of pixels greater than, or equal to, 1. Must be greater than, or equal to, Default Resolution Width .
Default	352

Video Settings

Frames per Second

Description	Frame rate for the video display
Mandatory	Yes
Values	number in frames per second
Default	30

Video Scaling Mode

Description	How to scale video if the video window is not the same size as the signal.
Mandatory	Yes
Values	NONE, STRETCH, or ADD_BORDERS
Default	STRETCH

Bitrate Configuration

Adaptive Bitrate Adjustment Enabled

Description	Indicates whether adaptive bitrate mechanisms should be used to dynamically adjust video bitrates. If this is checked, then other adaptive bitrate properties (see Initial , Minimum , and Maximum Adaptive Bitrate below) will appear and should also be set. If this is not checked, the fixed bitrate settings (see Fixed Video and Audio Bitrate below) should be set.
Mandatory	Yes
Values	true or false
Default	true

Initial Adaptive Bitrate

Description	This value is only considered if Adaptive Bitrate Adjustment Enabled is true. Media broker is able to estimate the maximum bitrate that network conditions can support for both send and receive video streams in the absence of REMB and TMMBR messages from browser and sip endpoints. The Initial Adaptive Bitrate value is used to initialize these algorithms to an expected bitrate from which to start from. A well chosen initial rate may result in the algorithm finding the best quality bitrate more quickly. A poorly chosen initial rate may result in unnecessarily poor initial video (value set too low) or
--------------------	---

	dropped packets / frozen video (value set too high).
Mandatory	Yes
Values	0 – MAX INT (2 ³¹) in kbs (kilobytes per second)
Default	512

Minimum Adaptive Bitrate

Description	<p>This value is only considered if Adaptive Bitrate Adjustment Enabled is <code>true</code>.</p> <p>The media broker will receive and act on max bitrate messages from 1) browser (RTCP Remb), 2) SIP endpoint (RTCP TMMBR), 3) sender bitrate estimating algorithm and 4) receiver bitrate estimating algorithms.</p> <p>The Minimum Adaptive Bitrate value ensures that these max bitrate messages never go below a fixed value (e.g. minimum quality). In these cases this value will be used when setting media broker video encoder bitrates and is used in outbound REMB and TMMBR RTCP messages.</p>
Mandatory	Yes
Values	0 – MAX INT (2 ³¹) in kbs
Default	128

Maximum Adaptive Bitrate

Description	<p>This value is only considered if Adaptive Bitrate Adjustment Enabled is <code>true</code>.</p> <p>The media broker will receive and act on max bitrate messages from 1) browser (RTCP Remb), 2) SIP endpoint (RTCP TMMBR), 3) sender bitrate estimating algorithm and 4) receiver bitrate estimating algorithms. The Maximum Adaptive Bitrate ensures that these max bitrate messages never go above a defined value (e.g. maximum quality). In these cases this value will be used when setting media broker video encoder bitrates and is used in outbound REMB and TMMBR RTCP messages.</p>
Mandatory	Yes
Values	0 – MAX INT (2 ³¹) in kbs
Default	1024

Fixed Video Bitrate

Description	<p>This value is only considered if Adaptive Bitrate Adjustment Enabled is <code>false</code>.</p> <p>This is used to negotiate (in SDP) a fixed video bitrate with browser and sip endpoints. Using a fixed video bitrate on poor lines may result in video issues (e.g. video freezing).</p>
Mandatory	Yes
Values	0 – MAX INT (2 ³¹) in kbs
Default	Disabled by default

Fixed Audio Bitrate

Description	This value is only considered if Adaptive Bitrate Adjustment Enabled is <code>false</code> . This is used to negotiate (in SDP) a fixed audio bitrate with browser and sip endpoints. Using a fixed audio bitrate on poor lines may result in audio issues (e.g. stuttering audio).
Mandatory	Yes
Values	0 - MAX_INT (2^31) in kbs
Default	Disabled by default

RTP Settings

Restrict Media To Port in SDP

Description	Whether to drop packets which are being sent from ports other than those negotiated in SDP. See Configuring RTP Settings .
Mandatory	Yes
Values	<code>true</code> or <code>false</code>
Default	<code>false</code>

Picture Loss Recovery Mechanism

Description	Mechanism used for picture loss recovery to SIP endpoints See Configuring RTP Settings
Mandatory	Yes
Values	PLI, RFC 2032 FIR, RFC 5168 FPU, or RFC 5168 FPU AND PLI
Default	PLI

Media Broker Administration

This describes the values available when editing the configuration of a Media Broker.

General Configuration

Control Address

Description	Hostname or IPv4 address for control interface of Media Broker. Used by the Web Gateway to connect to the Media Broker control port. For example, 192.168.1.2.
Mandatory	Yes

Values	Host name of IPv4 address
Default	None

Control Port

Description	Port for Web Gateway-to-Proxy communication (over REST API). Changing the port here doesn't change the port that the Media Broker will bind to, just the connection the Web Gateway will use for that proxy. To change the port used you must also change the configuration file on the Media Broker itself. For example, 8092.
Mandatory	Yes
Values	Port number
Default	8092

Control Type

Description	Select if all communication between the Web Gateway and the Media Broker will be secure or not.
Mandatory	Yes
Values	Secure or Not Secure
Default	Not Secure

Idle Timeout

Description	The maximum duration of inactivity (no RTP on either leg) on a call before it is torn down For example, 10.
Mandatory	Yes
Values	A time period in seconds
Default	10

Packet Size Limit

Description	The maximum RTP packet size that the Media Broker will accept. The Media Broker will drop any packet that exceeds this size.
Mandatory	Yes
Values	Number of bytes
Default	1500

Maximum Buffer Size

Description	The maximum number of packets that can be buffered before each call. If you are experiencing video issues at the beginning of calls, this value
--------------------	--

	should be increased.
Mandatory	Yes
Values	Number of packets
Default	500

Throughput Rate Limit

Description	The maximum RTP throughput rate that the Media Broker will perform. The Media Broker will terminate a call where the input rate exceeds this value. For example, 1000.
Mandatory	Yes
Values	Number of packets per second
Default	1000

Maximum Concurrent Audio Only Calls

Description	The maximum number of concurrent audio only calls which the media broker will accept. See Call Limit Based Call Admission Control .
Mandatory	Yes
Values	Number of calls
Default	0, meaning that the limit is disabled

Maximum Concurrent Audio/Video Calls

Description	The maximum number of concurrent video calls which the media broker will accept. See Call Limit Based Call Admission Control .
Mandatory	Yes
Values	Number of calls
Default	0, meaning that the limit is disabled

SIP Network

Multiple SIP Network range definitions can be defined for each Media Broker. All of the ports in each range will be exposed to the SIP network.

Note: At least one range is required.

Local Address CIDR

Description	A block of addresses that will be exposed to the internal SIP network for
--------------------	---

	RTP; a subset of which will match those of local network interface cards (NICs) on the Media Broker server.
Mandatory	Yes
Values	A range of IP addresses in Classless Inter-Domain Routing notation (e.g. 192.0.2.0/24) or <code>all</code> , which exposes all NICs on the media broker server
Default	<code>all</code>

Start Port Range

Description	The lower limit of a range of ports that will be exposed to the internal SIP network for RTP on the corresponding matching NICs.
Mandatory	Yes
Values	A port number
Default	17000

Finish Port Range

Description	The upper limit of a range of ports that will be exposed to the internal SIP network for RTP on the corresponding matching NICs.
Mandatory	Yes
Values	A port number
Default	17099

Note: At runtime, RTP and RTCP ports are assigned in pairs from the pool, so the **Start Port Range** value should be an even number, and the **Finish Port Range** value should be an odd number.

WebRTC Client

These are the addresses that browsers from a range of IP addresses (signified in a *Classless Inter-Domain Routing* (CIDR) notation) will use to communicate with the Media Broker. Multiple addresses can be defined for each range of browser IP addresses.

Note: At least one set of addresses is required; a range of addresses configured for all browsers has been added by default.

Source Address CIDR

Description	A block of addresses of browser endpoints. Each Source Address CIDR has an associated block of addresses and ports, which defines which public and local ports that block of browser endpoints will communicate on.
Mandatory	Yes
Values	A range of IP addresses in CIDR notation (e.g. 192.0.2.0/24) or <code>all</code> , which exposes all NICs on the media broker server
Default	None

Public Address

Description	<p>RTP IP address exposed on firewall (e.g. 84.1.2.3).</p> <p>Used by browsers for RTP traffic. Used by the Media Broker to generate SDP.</p> <p>You can configure IPv6 addresses, but they require extra components and are not supported for production use. See <i>Developing with Mobile Video SDK > Creating an iOS application > Testing IPv6</i>.</p> <p>Note: If there is no firewall, or no network address translation (NAT) is taking place, this will be the IP address of the Media Broker.</p>
Mandatory	Yes
Values	An IPv4 address
Default	None

Public Port

Description	<p>RTP port exposed on firewall (e.g. 16000).</p> <p>Used by browsers for RTP traffic. Used by the Media Broker to generate SDP.</p>
Mandatory	Yes
Values	A port number
Default	None

Local Address

Description	<p>Local RTP IP address on Media Broker (e.g. 203.0.113.0).</p> <p>Mapped by firewall from the Public Address.</p>
Mandatory	Yes
Values	An IP address, or <code>all</code> , which exposes all NICs on the media broker.
Default	None

Local Port

Description	<p>Local RTP port on Media Broker (e.g. 16000).</p> <p>Mapped by firewall from the Public Port. Note: SRTP is used by default on the Local Port.</p>
Mandatory	Yes
Values	A port number
Default	None

Monitored Connections

Optionally configure one or more groups of monitored connections. See [Connection Monitoring](#) for more details on this feature.

Group Name

Description	The name of the group
Mandatory	Yes
Values	A string value to act as a label
Default	None

Monitored Addresses

Description	Address to monitor
Mandatory	At least one is mandatory
Values	IP address or host name
Default	None

User Credentials

This section allows you to change the administrative user's credentials. Note that if there are other administrative sessions open, through the web administrative interface or the CLI, then those users will need to log out and log back in again with the updated credentials in order to continue administering the system.

Old password

Description	The current administrative account password. If this is incorrectly submitted six consecutive times, then the administrative account will be locked for security reasons. To re-enable the administrative account follow the instructions in Resetting Administrator Credentials .
Mandatory	Yes
Values	The existing password
Default	None

UI username

Description	The username of the administrative account you are setting the password for.
--------------------	--

Mandatory	Yes
Values	The username
Default	The current username

New password

Description	The new password for the administrative account
Mandatory	Yes
Values	The new password
Default	None

Retype new password

Description	The new administrative account password. This is a confirmation of the New password field to protect against typing mistakes.
Mandatory	Yes
Values	The new password
Default	None

Appendix B: RFC References

The following RFC specifications are referred to throughout this document.

- **RFC3551**
RTP Profile for Audio and Video Conferences with Minimal Control
<http://www.ietf.org/rfc/rfc3551.txt>
- **RFC 6236**
Negotiation of Generic Image Attributes in the Session Description Protocol (SDP)
<http://www.ietf.org/rfc/rfc3551.txt>
- **RFC 2032**
RTP Payload Format for H.261 Video Streams
<http://www.ietf.org/rfc/rfc3551.txt>
- **RFC3261**
SIP: Session Initiation Protocol
<http://www.ietf.org/rfc/rfc3551.txt>

Appendix C: Glossary

Item	Description
Avaya Aura® Communication Manager	The Avaya telecommunications system used for unified communications and collaboration.
Avaya one-X® Agent	A desktop application for contact center agents and supervisors.
Avaya SBCE	Avaya Session Border Control for Enterprise—a reverse proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as though they originated from the SBCE itself.
AMVS	<p>Avaya Mobile Video Server—platform for delivering web applications to make voice and video calls directly from a Web browser, iOS device, or Android device, to an Avaya one-X Agent.</p> <p>The AMVS Web Administration interface is used to configure the services facilitating this communication.</p>
CAC	Call Admission Control
CIDR	Classless Inter-Domain Routing. CIDR notation is a compact representation of an IP address and its associated routing prefix. The notation is constructed from an IP address, a slash (/) character, and a decimal number representing the network mask, for example: 192.0.2.0/24
CODEC	“Coder-decoder” encodes a data stream or signal for transmission and decodes it for playback in voice over IP and video conferencing applications.
DMZ	A demilitarized zone (also referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to the Internet.
FQDN	A fully qualified domain name—the complete domain name for a specific computer, or host, on the Internet, for example examplehost.example.com
G.711	PCMU/A 8-bit audio codec used for base telephony applications.
G.729a	Low bit rate audio codec for VoIP applications.

Item	Description
H.264	Video codec. H.264 is the dominant video compression technology, or codec, in industry that was developed by the International Telecommunications Union (as H.264 and MPEG-4 Part 10, Advanced Video Coding, or AVC).
Media Broker	Intercepts SDP messages, performs transcoding where required, and can remove any banned codes. Multiple Media Brokers can be installed on the same network, for load balancing and scaling.
MVSDK	Mobile Video SDKs. Includes three distinct SDKs for iOS, Android and web/JavaScript developers.
MVSDK Client	A web/JavaScript, iOS, or Android client with which a connection is established using the MVSDK.
Opus	Low bit rate, high definition audio codec for VoIP applications. See RFC 6716.
Ping	Query (ICMP echo request) made to another computer on a network to determine whether there is a connection to it.
PLI	A feedback mechanism of the Real-time Transport Control Protocol (RTCP) which enables the sender to resend keyframe packets to re-establish a full video picture when communicating over the Internet or poor network conditions.
Pong	A response made to a Ping request, confirming that a connection exists.
REMB	Receiver Estimated Maximum Bitrate
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol. SIP is a VoIP call setup protocol that operates at the application layer. It sets up calls that then use RTP to actually send the voice data between phones.
TIMMBR	Temporary Maximum Media-Stream Bit Rate Request
UC	Unified Communications
VP8	Video codec. VP8 is a video compression format owned by Google. VP8 is roughly equivalent in processor usage, bandwidth and quality to H.264.

Item	Description
Web Gateway	Permits users to make calls to one-X agent endpoints.
WebRTC	Web Real Time Communications for communications without plug-ins.
WebSockets	A protocol providing full-duplex communication channels over a single TCP connection, standardized by the IETF as RFC 6455.