AudioCodes WebRTC Solutions for Enterprises

# WebRTC Client Installation on HTTP Server

Version 2.6.0



**C**audiocodes

# Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: January-02-2024

## **Customer Support**

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

## **Documentation Feedback**

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

## Stay in the Loop with AudioCodes



## **Related Documentation**

**Document Name** 

https://www.audiocodes.com/solutions-products/solutions/enterprise-voice/webrtcconnectivity

WebRTC Softphone Client Quick Guide

WebRTC Softphone User's Manual

WebRTC Click-to-Call Widget Installation and Configuration Guide

WebRTC Android Client SDK API Reference Guide

**Document Name** 

WebRTC iOS Client SDK API Reference Guide

WebRTC Web Browser Client SDK API Reference Guide

# **Document Revision Record**

LTRT	Description
14120	Initial document release (Ver. 1.1).
14121	NGINX file settings and reload file commands.
14122	Typo (in footer).
14123	Update for Version 1.2; HTTP basic authentication for NGINX and Apache.
14124	Updated Sections: Solution Overview; Advanced Options Configuration File; Added Sections: Client Logo Customization; Deploying AudioCodes WDE Extension.
14125	Update for Version 1.5; Oauth configuration.
14126	IIS HTTP server configuration and installation.
14127	Update for Version 2.2; additional advancedOptions customization options, and deploying AudioCodes WDE Extension using an installation wizard.
14128	sipServerAddress configuration.
14129	Upgrade instructions for WebRTC.
14150	Updated for Version 2.4; configuration on auto-play, additional OAuth configurations and customer-info; browser auto-play policy configuration.
14151	Configuration on SDK patch modes.
14152	Configuration for VDI integration, media device selection, and ACD Client Configuration Not-Ready state values.
14153	Configure Citrix Remote Desktop for Integration with

LTRT	LTRT Description	
	the WebRTC Client.	
14154	Troubleshooting client connections; configuration for Agent Assist, codec filtering, and additions to media device selection; customizing sound files.	
14155	Updated for Version 2.4.6; localVideofilter configuration; Virtual Background Images.	
14156	Updated for Version 2.4.7; storageConfig and forceLoginPromptOnEmptyCache.	
14157	forceLoginPromptOnEmptyCache. Updated for Version 2.4.8. Updated Advanced Options Configuration File section, Advanced Options Con- figuration File section. Added Language and Text Cus- tomization section.	
14158	Added the Upgrading Web Client to a New Release sec- tion. Updated Upgrading WebRTC Client on NGINX Server, Upgrading WebRTC Client on Apache Server and Upgrading WebRTC Client on IIS sections.	
14159	Updated for Version 2.5.3. Added the <i>isAllowedToResumeLocalHoldByRemoteReInvite</i> attribute to Advanced Options Configuration File.	
14160	-	
	It is no longer mandatory to deploy the client specifically at a directory named webrtc_client.	
	In the Configuring the HTTPS Site section, references to the deprecated Web Platform Installer were removed.	
	In the Advanced Options Configuration File section, the disableEditing property under defaultServerConfig was added.	
	In the Advanced Options Configuration File section, the <i>autoplayNotificationOptions</i> property has been deprecated and has been replaced with the <i>notificationOptions</i> property.	
	The Maintaining Web Client Activity When Browser Tab is in the Background section was added.	

LTRT	Description
	The Troubleshooting Client Connections section was updated.
14161	Updated for Version 2.5.5. Added support for Dual registration.
14162	<ul> <li>Updated for Version 2.5.6.</li> <li>Added support for No-answer Timeout configuration.</li> </ul>
14163	<ul> <li>Updated for Version 2.6.0.</li> <li>Modified the Customizing WebRTC Client section:         <ul> <li>Deprecated and removed defaultOAuthConfig</li> <li>Deprecated and removed supportedAuthenticationSchemes</li> <li>Added the Configure Authentication Providers for User Sign-In sub-section, for supporting multiple authentication providers</li> <li>Added the Configure Integrations with Contact Center Platforms sub-section, for</li> </ul> </li> </ul>
	<ul> <li>Supporting multiple Contact Center integrations including Genesys PureCloud</li> <li>Added the Migrating Authentication Providers and Contact Center Configuration from Previous Versions section</li> <li>Added the Configuring SBC WebRTC section</li> </ul>

## **Table of Contents**

1	Introduction	1
2	Solution Overview	2
	Benefits	2
	Components	
	High-level Call Flow	
3	Installing WebRTC Client on HTTP Server	4
	Installing on NGINX HTTP Server	4
	Prerequisites	4
	Configuring NGINX	4
	Deploying WebRTC Client on NGINX Server	6
	Restricting Access with HTTP Basic Authentication	7
	Upgrading WebRTC Client on NGINX Server	7
	Installing on Apache HTTP Server	7
	Prerequisites	8
	Deploying WebRTC Client on Apache Server	8
	HTTP Basic Authentication	8
	Upgrading WebRTC Client on Apache Server	9
	Installing Internet Information Services (IIS) on Windows HTTP Server	9
	Prerequisites	9
	Installing the IIS Server	9
	Installing the SSL Certificate	16
	Using IIS Manager	16
	Using Open Source	16
	Creating the HTTPS Site	19
	Configuring the HTTPS Site	20
	Installing URL Rewriter 2.1	21
	Creating HTTP to HTTPS Request Redirection	21
	Configuring Compression of Responses	25
	Enable Special Signs in Filenames	26
	Configuring Windows Server to Only Use TLS 1.2	28
	Deploying WebRTC Client on IIS	32
	Upgrading WebRTC Client on IIS	32
	Customizing WebRTC Client	32
	Advanced Options Configuration File	32
	Configure Integrations with Contact Center Platforms	38
	Configure Authentication Providers for User Sign-In	40
	Migrating Authentication Providers and Contact Center Configuration from Previous Versior	าร42
	Contact Center Integration – Genesys Pure Engage	42
	Authentication Provider Configuration	42
	Client Resource Customization – Images, Sounds and Text	44
	Logo	44
	Sound Files	44

	Virtual Background Images	44
	Language and Text Customization	45
	Browser Auto-Play Control for Tone Playback	46
	Maintaining Web Client Activity When Browser Tab is in Background	46
	NGINX and Apache Server Web Access Examples	48
	Upgrading the Web Client to a New Release	49
4	Deploying AudioCodes WDE Extension	50
5	Configuring Genesys WebRTC DN Object Endpoint	52
6	Configuring Citrix Remote Desktop for Integration with WebRTC Client	
7	Configuring SBC WebRTC	59
7	Configuring SBC WebRTC Creating an IP-to-IP Message Route	
7		
7	Creating an IP-to-IP Message Route	
7	Creating an IP-to-IP Message Route Creating a Call (Voice Only) Route	
7	Creating an IP-to-IP Message Route Creating a Call (Voice Only) Route Creating an IP-to-IP Route for Video Calls	
8	Creating an IP-to-IP Message Route Creating a Call (Voice Only) Route Creating an IP-to-IP Route for Video Calls Configuring Call Setup Rules	
	Creating an IP-to-IP Message Route Creating a Call (Voice Only) Route Creating an IP-to-IP Route for Video Calls Configuring Call Setup Rules Configuring IP Groups	

# **1** Introduction

This document provides an overview of AudioCodes' WebRTC client solution and describes how to deploy and configure the WebRTC client on an HTTP-based server (NGINX or Apache).

# 2 Solution Overview

AudioCodes offers a WebRTC-based softphone client that can be used by agents in the Genesys PureEngage and PureConnect environment. This WebRTC softphone is used by agents, in conjunction with Genesys agent desktop applications - Workspace Desktop Edition (WDE), Workspace Web Edition (WWE) and Interaction desktop - as their telephony device that enables them to make and receive calls and perform other telephony functions.

This WebRTC-based phone is intended primarily for work-at-home agents and can also be used by agents located on the customer's premises.

As part of the solution, the Customer is required to embed a Web page within an existing Web server (it can be the Customer's main server, or a Web server dedicated to the WebRTC setup). This Web page will be used by agents to browse their Softphone page. Specific guidance on how to embed this page is described in Chapter 4.

In addition, the Customer is required to adjust the Genesys PureEngage DN object configuration, as described in this document.

The agent can refer to the WebRTC Web Softphone User's Manual for a description on using this WebRTC softphone.

## **Benefits**

AudioCodes WebRTC client provides the following benefits:

- Ease of maintenance as there is no need to install and maintain softphone applications
- Enhanced voice quality using Opus codecs
- Removes requirement for VPN:
  - WebRTC uses ICE that can traverse NAT and firewalls
  - Secure and encrypted calls, using HTTPS, DTLS and SRTP
- Allows video calls (next phase)

#### Components

The following high-level diagram illustrates the components of this solution, which are also described in detail below.



Figure 2-1: Solution Components

- The following components are located at the Customer's data center:
  - Genesys PureEngage / PureConnect servers
  - WebRTC gateway used to convert WebRTC traffic from the agents to plain SIP and RTP traffic towards Genesys SIP server
  - Web server used for browsing to the page that displays the client softphone and downloads the WebRTC-based client JavaScript
- The following components are located on the agent's desktop:
  - Genesys agent desktop applications (WDE or WWE or Interaction desktop)
  - Google/Firefox-based client used for the WebRTC softphone application

## **High-level Call Flow**

The call flow of this WebRTC client solution is as follows:

- 1. The agent browses to the Web server.
- 2. The browser downloads the client JavaScript that points to the SBC IP address.
- 3. The agent enters the agent's DN number, and associated credentials.
- 4. The client registers to the Genesys SIP server using the SIP protocol.
- 5. The SIP server authenticates the client using SIP digest authentication.
- 6. The SIP server pairs the client with the agent.
- **7.** The agent can originate and receive calls, perform call transfers, conference calls, and hold and retrieve calls. In this first phase, all telephony actions control is performed from the agent's desktop application (third-party call control).

# 3 Installing WebRTC Client on HTTP Server

The WebRTC client needs to be installed on an HTTP-based server. This server can either be a dedicated HTTP server or one of your existing servers used for other applications (for example, your Web-hosting server).

This document describes the installation on the following popular HTTP servers:

- NGINX HTTP server (see Installing on NGINX HTTP Server below)
- Apache HTTP server (see Installing on Apache HTTP Server on page 7)
- Internet Information Services (IIS) for Windows (see Installing Internet Information Services (IIS) on Windows HTTP Server on page 9)

## Installing on NGINX HTTP Server

The following describes how to deploy the WebRTC client on an NGINX HTTP server.

#### **Prerequisites**

Make sure you have fulfilled the following prerequisites:

- Operating system installed (tested with CentOS 7)
- NGINX installed
- DNS domain name for the server
- SSL certificates installed
- Redirect HTTP to HTTPS is configured

#### **Configuring NGINX**

The following describes the special configuration for NGINX. The configuration file is located in the /etc/nginx/nginx.conf directory.



- TLSv1.2 and TLSv1.3 have been set as the supported protocols.
- The cache needs to be controlled.
- This configuration uses gzip compression.
- This configuration supports IPv6 and the HTTP2 protocol.

#### ➤ To configure NGINX:

1. Copy and paste the below configuration to the nginx.conf file. This contains all the basic settings required for AudioCodes WebRTC softphone client.

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;
include /usr/share/nginx/modules/*.conf;
events {
  worker_connections 1024;
}
http {
  log_format main '$remote_addr - $remote_user [$time_local] "$request" '
           '$status $body_bytes_sent "$http_referer" '
           "$http_user_agent" "$http_x_forwarded_for";
  access_log /var/log/nginx/access.log main;
  sendfile
                on;
  tcp_nopush
                   on;
  tcp_nodelay
                   on;
  keepalive_timeout 65;
  types_hash_max_size 2048;
  include
                /etc/nginx/mime.types;
                  application/octet-stream;
  default_type
  include /etc/nginx/conf.d/*.conf;
  server {
              80;
    listen
    server_name YOUR_SITE_NAME;
              301 https://$host$request_uri;
    return
  }
  server {
             443 ssl http2 default_server;
    listen
             [::]:443 ssl http2 default server;
    listen
    server_name YOUR_SITE_NAME;
    ssl on;
    ssl certificate
                      /etc/pki/tls/certs/site_certificate.crt;
    ssl_certificate_key /etc/pki/tls/private/private.key;
```

root /var/html;

gzip on; gzip\_vary on; gzip\_min\_length 1024; gzip\_proxied any; gzip\_types text/plain text/css application/javascript application/json text/xml application/xml text/javascript;

```
add_header Cache-Control no-cache;
expires 24h;
ssl_session_timeout 10m;
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
```

include /etc/nginx/default.d/\*.conf;

```
location / {
   try_files $uri $uri/ =404;
}
```

2. Reload the NGINX server, using the following commands:

sudo nginx -t sudo systemctl reload nginx sudo systemctl status nginx

#### **Deploying WebRTC Client on NGINX Server**

The following describes how to deploy the WebRTC client on an NGINX HTTP server:

```
> To deploy on NGINX server:
```

}

- 1. Unzip the file webrtc-web-client-vx.x.zip, using the 7-Zip utility.
- 2. Copy the unzipped content to the */var/html/webrtc\_client/* directory.

/var/html/ is not the default directory for NGINX.

3. Verify owners and permissions:

```
-rw-rw-r-- 1 centos 1819 Mar 23 17:46 asset-manifest.json
-rw-rw-r-- 1 centos 22382 Mar 23 17:46 favicon.ico
-rw-rw-r-- 1 centos 2529 Mar 23 17:46 index.html
-rw-rw-r-- 1 centos 8581 Mar 23 17:46 logo192.png
-rw-rw-r-- 1 centos centos 22920 Mar 23 17:46 logo512.png
-rw-rw-r-- 1 centos centos 722 Mar 23 17:46 logo-audiocodes.ico
-rw-rw-r-- 1 centos centos 492 Mar 23 17:46 precache-manifest.f4a95be0ec7e7fa979e757e1c258814f.js
-rw-rw-r-- 1 centos centos 57 Mar 23 17:46 robots.txt
-rw-rw-r-- 1 centos centos 1209 Mar 23 17:46 service-worker.js
drwxrwxr-x 5 centos centos 37 Mar 24 07:57 static
```

#### **Restricting Access with HTTP Basic Authentication**

To restrict access to the WebRTC client, you can configure basic authentication on the NGINX server for the client page, which obligates users to enter a preconfigured username and password when accessing the page.

- To configure basic authentication on NGINX server:
- Follow the instructions in https://docs.nginx.com/nginx/admin-guide/securitycontrols/configuring-http-basic-authentication/.
- Edit the NGINX configuration file, and set restricted access to the client installation path ("/webrtc\_client" in our example):

location /webrtc\_client {
 auth\_basic "Restricted Content";
 auth\_basic\_user\_file /etc/nginx/.htpasswd;
 try\_files \$uri \$uri/ =404;
}

#### Upgrading WebRTC Client on NGINX Server

#### To upgrade WebRTC Client on NGINX Server:

To upgrade the WebRTC Client on the NGINX server, see Upgrading the Web Client to a New Release.

## Installing on Apache HTTP Server

The following describes how to deploy the WebRTC client on an Apache server.

#### **Prerequisites**

Make sure you have fulfilled the following prerequisites:

- Operating system installed (validated with CentOS 7)
- Apache installed
- DNS domain name for the server
- SSL certificates installed
- Redirect HTTP to HTTPS is configured

#### **Deploying WebRTC Client on Apache Server**

The following describes how to deploy the WebRTC client on an Apache server:

#### > To deploy on Apache server:

- 1. Unzip the file webrtc-web-client-vx.x.zip, using the 7-Zip utility.
- 2. Copy the unzipped content to the /var/www/html/webrtc\_client/ directory (CentOS 7).
- 3. Verify owners and permissions:

-rw-rw-r-- 1 centos 1819 Mar 23 17:46 asset-manifest.json
-rw-rw-r-- 1 centos centos 22382 Mar 23 17:46 favicon.ico
-rw-rw-r-- 1 centos centos 2529 Mar 23 17:46 index.html
-rw-rw-r-- 1 centos centos 22920 Mar 23 17:46 logo192.png
-rw-rw-r-- 1 centos centos 22920 Mar 23 17:46 logo512.png
-rw-rw-r-- 1 centos centos 722 Mar 23 17:46 logo-audiocodes.ico
-rw-rw-r-- 1 centos centos 492 Mar 23 17:46 manifest.json
-rw-rw-r-- 1 centos centos 1365 Mar 23 17:46 precache-manifest.f4a95be0ec7e7fa979e757e1c258814f.js
-rw-rw-r-- 1 centos centos 57 Mar 23 17:46 service-worker.js
drwxrwxr-x 5 centos centos 37 Mar 24 07:57 static

#### **HTTP Basic Authentication**

To restrict access to the WebRTC client, you can configure basic authentication on the Apache server for the client page. This obligates users to enter a preconfigured username and password when accessing the page:

> To configure basic authentication for Apache server:

Edit /var/www/html/.htaccess, and then set restricted access to the client installation path ("/webrtc\_client" in our example): SetEnvIf Request\_URI ^/webrtc\_client require\_auth=true Order Deny,Allow Deny from all Satisfy any Require valid-user Allow from env=!require\_auth AuthType Basic AuthName "Restricted Content" AuthUserFile /etc/httpd/.htpasswd Require valid-user

#### Upgrading WebRTC Client on Apache Server

#### **To Upgrade WebRTC Client on Apache Server:**

To upgrade the WebRTC Client on the Apache Server, see Upgrading the Web Client to a New Release.

# Installing Internet Information Services (IIS) on Windows HTTP Server

The procedures below describe how to install the WebRTC client on an IIS server. All actions are performed from the Administrator account.

#### **Prerequisites**

Make sure you have fulfilled the following prerequisites:

- Windows server has been installed (validated with Amazon Web Services cloud with Microsoft Windows Server 2019 Base)
- Cloud firewall (if the server is installed on the cloud) was configured for HTTP and HTTPS
- Public static IP address has been assigned to the Windows server
- Created a Fully Qualified Domain Name (FQDN) (DNS domain name) for the IP
- Configured a remote desktop connection for communication and file exchange with the server

#### Installing the IIS Server

The procedure below describes how to install the IIS server.

#### ➤ To install the IIS server:

1. From the Windows Start menu, click Control Panel.



- 2. Click Programs, and then click Turn Windows features on or off.
- 3. On the Before you Begin page, click **Next**; the Installation Type page appears.

Add Roles and Features Wizard			-		×
Before you begin				IATION SER MAZ-JKGCF	
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, roi features to install based on the comp hosting a website. To remove roles, role services, or feat Start the Remove Roles and Features Before you continue, verify that the fi • The Administrator account has a str • Network settings, such as static IP a • The most current security updates fi If you must verify that any of the pre- complete the steps, and then run the To continue, click Next.	uting needs of your organization, s ures: <u>Wizard</u> ollowing tasks have been complete rong password addresses, are configured from Windows Update are installed ceding prerequisites have been cor	such as sharing doo	cuments,	
		< Previous Next >	Install	Cance	el

4. Select the Role based or feature-based installation option, and then click Next.



5. On the Select Destination Server page, select the server, and then click Next.

Add Roles and Features Wizard						×
Add Roles and Features Wizard				_		~
Select destination	server				ATION SER MAZ-JKGCF	
Before You Begin	Select a server or a virtual	hard disk on which	to install roles and features.			
Installation Type	Select a server from th	a canvar pool				
21	<ul> <li>Select a server from th</li> <li>Select a virtual hard discussion</li> </ul>					
Server Selection Server Roles	0	24				
	Server Pool					
Features	Filter:					
Confirmation						
Results	Name	IP Address	Operating System			
	EC2AMAZ-JKGCRHQ	172.31.31.248	Microsoft Windows Server 20	19 Datacente	r	
	1 Computer(s) found					
	and that have been added	by using the Add S	lows Server 2012 or a newer rele ervers command in Server Mana on is still incomplete are not sho	ager. Offline s		
	newly-budeu servers from	which data collectic	an is suit incomplete are not sho			
		< Pre	vious Next >	Install	Cance	el

6. On the Select Server Roles page, select the 'Web Server IIS' check box.



7. On the Add features that are required for Web server page, select the 'Include management tools' check box, and then click Add Features.

La Add Roles and Features Wizard	×
Add features that are required for Web Server (IIS)?	
The following tools are required to manage this feature, but do not have to be installed on the same server.	
<ul> <li>Web Server (IIS)</li> <li>Management Tools [Tools] IIS Management Console</li> </ul>	
Include management tools (if applicable)  Add Features Cancel	

8. On the Select Features page, click Next.

Before You Begin       Installation Type         Installation Type       Server Selection         Server Roles       • • .NET Framework 3.5 Features       Oescription         Features       • • .NET Framework 4.7 Features (2 of 7 installed)       • • .NET Framework 4.7 features (2 of 7 installed)         Web Server Role (IIS)       BitLocker Drive Encryption       FinanchCache       omprehensive and consistent         Confirmation       BitLocker Network Unlock       BitLocker Orive Encryption       patienchCache         Data Center Bridging       Direct Play       Enhanced Storage       Server Clustering         Group Policy Management       Host Guardian Hyper-V Support       UO Quality of Service       Visit Management (IPAM) Server         IIS Hostable Web Core       IIS Hostable Web Core       IIS Hostable Web Core       Visit Management (IPAM) Server	Select features			DESTINATION SERVER ECZAMAZ-JKGCRHQ	
Features <ul> <li>Background meingent marger service (Bris)</li> <li>BitLocker Network Unlock</li> <li>BitLocker Network Unlock</li> <li>BranchCache</li> <li>Client for NFS</li> <li>Containers</li> <li>Data Center Bridging</li> <li>Direct Play</li> <li>Enhanced Storage</li> <li>Failover Clustering</li> <li>Group Policy Management</li> <li>Host Guardian Hyper-V Support</li> <li>I/O Quality of Service</li> <li>IIS Hostable Web Core</li> <li>Internet Printing Client</li> <li>IP Address Management (IPAM) Server</li> </ul>	Installation Type Server Selection	Features           Image: Image shows the second state stat	^	.NET Framework 4.7 provides a comprehensive and consistent	
	Web Server Role (IIS) Role Services Confirmation	BitLocker Drive Encryption     BitLocker Network Unlock     BranchCache     Client for NFS     Containers     Data Center Bridging     Direct Play     Enhanced Storage     Failover Clustering     Group Policy Management     Host Guardian Hyper-V Support     I/O Quality of Service     IIS Hostable Web Core     Intermet Printing Client     IP Address Management (IPAM) Server	•	easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public	id

9. On the Web Server Role (IIS) page, click Next.

Add Roles and Features Wiz	ird	_		×
Veb Server Rol	e (IIS)		IATION SER	
Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Web servers are computers that let you share information over extranets. The Web Server role includes Internet Information Se diagnostic and administration, a unified Web platform that inter Communication Foundation. • The default installation for the Web Server (IIS) role includes t enable you to serve static content, make minor customization errors), monitor and log server activity, and configure static of	rvices (IIS) 10.0 with enhan- grates IIS 10.0, ASP.NET, an the installation of role servi rs (such as default docume	ced securi d Window ces that	ty, vs
	More information about Web Server IIS	> Install	Cance	2

**10.** On the Select Role Services page, select 'HTTP Redirection' and 'Basic Authentication', and then click **Next**.

ouver manager	<u></u>	
ե Add Roles and Features Wizard		- 0 X
Add Roles and Features Wizard Select role service Before You Begin Installation Type Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	S Select the role services to install for Web Server (IIS) Role services Image: Provide the services         Image: Provide the service the service the service the services         Image: Provide the service the servic	– C × DESTINATION SERVER ECZAMAZ-JKGCRHQ Description Basic authentication offers strong browser compatibility. Appropriate for small internal networks, this authentication method is rarely used on the public Internet. Its major disadvantage is that it transmits passwords across the network using an easily decrypted algorithm. If intercepted, these passwords are simple to decipher. Use SSL with Basic authentication.
	Client Certificate Mapping Authentication	
	< Previous Next	t > Install Cancel
	< Frevious INex	instail Calicei

- **11.** On the Confirm Installation Selections page, select the 'Restart the destination server automatically if required' check box; a message appears regarding automatic restarts.
- **12.** If a restart is required, click **Yes**.

Confirm installa	tion selections	DESTINATION SERVER EC2AMAZ-JKGCRHQ
Before You Begin	To install the following roles, role services, or features on selected server, click	Install.
Installation Type	<ul> <li>Restart the destination server automatically if required</li> </ul>	
Server Selection	Optional features (such as administration tools) might be displayed on this page	
Server Roles Add	Roles and Features Wizard × tional feature	es, click Previous to clear
Features		
Web Server Role (II:	If a restart is required, this server restarts automatically, without	^
Role Services	additional notifications. Do you want to allow automatic restarts?	
Confirmation		
Results	Yes No	
	onceres y or only g	
	HTTP Errors HTTP Redirection	
	Security Request Filtering	
	Dasis Authoritisation	~
	Export configuration settings Specify an alternate source path	

**13.** Click **Install**; the Installation Progress page appears.

Add Roles and Features Wiza	-	- 0	)
Confirm installat	ion selections	DESTINATION EC2AMAZ-JK	
Before You Begin	To install the following roles, role services, or features on selected se	erver, click Install.	
Installation Type	<ul> <li>Restart the destination server automatically if required</li> </ul>		
Server Selection	Optional features (such as administration tools) might be displayed		
Server Roles	been selected automatically. If you do not want to install these opti- their check boxes.	onal features, click Previous t	o clear
Features			
Web Server Role (IIS)	Web Server (IIS)		-
Role Services	Web Server Common HTTP Features		
Confirmation	Static Content		
Results	Default Document		
	Directory Browsing		
	HTTP Errors		
	HTTP Redirection		
	Security		
	Request Filtering		
	Darie Authentication		~
	Export configuration settings Specify an alternate source path		
	< Previous Next >	Install	ancel

**14.** When the installation has completed, click **Close**.

		DECTIN	ATION SER	N AT T
Installation prog	ress		ATON SER	
	View installation progress			
	Feature installation			
	Installation succeeded on EC2AMAZ-JKGCRHQ.			
	Web Server (IIS)			
	Web Server			
	Common HTTP Features			
	Static Content Default Document			
Results	Directory Browsing			
	HTTP Errors			ł
	HTTP Redirection			
	Security			
	Request Filtering			
	Basic Authentication			

- **15.** Close the Control Panel.
- **16.** Using Windows Search, enter "IIS Manager".

- **17.** Open the file location and create a desktop link to IIS Manager.
- **18.** Open IIS Manager; ensure that your IIS HTTP server has started in the right pane (Manage Server).
- **19.** On a different computer, try to open http://<your\_site\_fqdn> in the browser; the following page appears.

u		Nindov	vs Server								Í
	Int	ern	et Infor	'ma'	tion S	ervic	es				
l Micr	Welco	ome		Bienv	enue Ter	vetuloa					
		ようこそ	Benvenuto	歡迎 了了了	Bienvenic	lo Hoşgi	eldiniz	ברוכים הבאים			Welko
		Bem-\	vindo	Vítejte	Καλώς ορίσατε	Välko	mmen	환영합니다	Добро пожаловать	Üdvözöljük	
									欢迎		•

For more information, see the official Microsoft IIS site at https://docs.microsoft.com/en-us/iis.

#### Installing the SSL Certificate

There are two ways to order a security certificate:

- IIS Manager
- Open Source

#### **Using IIS Manager**

The Certificate Signed Request (CSR) can be created with the IIS Manager. This is the standard way and is described in many places. For example, go to https://www.ibm.com/support/pages/how-generate-csr-certificate-signing-request-using-iis.

Send the created CSR to the certificate authority, and then install the received signed certificates. For more information, go to https://www.ibm.com/support/pages/how-install-ssl-certificate-iis7.

#### **Using Open Source**

You can use the openssl open source utility, in the same way as it is used for other HTTP servers, such as Apache and Nginx. For more information, go to

#### https://en.wikipedia.org/wiki/OpenSSL.

- 1. Send the CSR to the certificate authority and receive a signed certificate.
- 2. From the command prompt, convert the following files with the openssl utility
  - private.key
  - certificate.crt
  - ca\_bundle.crt

to pfx file format using openssl.

openssl pkcs12 -export -out certificate.pfx -inkey private.key -in certificate.crt - certfile ca\_bundle.crt

3. Enter and confirm the Export password.

👞 Administr	ator: Command	d Prompt			-		×
undle.crt		>openssl p	kcs12 ·	-export -out certificate.pfx -inkey private.key -in certificate.cu	rt -ce	rtfile	ca_
Enter Expor Verifying -	t Password: Enter Expo	ort Password	d:				
	ministrator drive C has						
	ial Number		7B				
Directory	of C:\Users	\Administr	ator				
11/04/2020	11:26 AM	<dir></dir>					
	11:26 AM	<dir></dir>					
11/04/2020		<dir></dir>		3D Objects			
	11:17 AM			ca_bundle.crt			
	11:17 AM			certificate.crt			
	12:16 PM			certificate.pfx			
1/04/2020		<dir></dir>		Contacts			
	12:06 PM	<dir></dir>		Desktop			
	11:29 AM	<dir></dir>		Documents			
	11:20 AM	<dir></dir>		Downloads			
1/04/2020		<dir></dir>		Favorites			
1/04/2020	09:45 AM	<dir></dir>		Links			
1/04/2020	09:45 AM	<dir></dir>		Music			
	09:56 AM	<dir></dir>		Pictures			
	11:17 AM		1,702	private.key			
1/04/2020	09:45 AM	<dir></dir>		Saved Games			
	09:45 AM	<dir></dir>		Searches			
11/04/2020	09:45 AM	<dir></dir>		Videos			

- **4.** Create the pfx file.
- 5. Copy the created certificate to the Windows server using Remote Desktop Connection.
- 6. Open IIS Manager and from the left Connections pane, select the local host entry, below Start Page.



In the above example, the local host is EC2AMAZ-HFH46B9(EC2AMAZ-HFH46B9\Administrator. If you hover the mouse pointer on this entry, the following tooltip is shown - http://localhost.

- **7.** Click the **Server Certificates** icon, and then from the right Actions pane, click **Import**; the Import Certificate page appears.
- 8. In the 'Certificate Enter' field, enter the pfx file path.
- 9. In the 'Password' field, enter the Export password.
- 10. From the 'Select Certificate Store' drop-down list, select Web Hosting, and then click OK.

1 Internet Information Serv	ices (IIS) Manager			- 🗆 X
← → €C2AM	AZ-JKGCRHQ			📴 🖂 🏠 I 🔞 •
File View Help				
Connections	Use this feature to re configured for SSL.	Certificates Import Certificate ? × Certificate file (.pfx):	sites	Actions Import Create Certificate Request Complete Certificate Request
- 🧐 Application Poo > - 🗑 Sites	Filter:	C:\Users\Administrator\certificate.pfx Password:		Create Domain Certificate Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate
		Select Certificate Store: Web Hosting ~ Allow this certificate to be exported OK Cancel		😧 Help
< >> Ready	<     Features View	Content View	>	

The certificate.pfx file has been installed on the IIS Manager.

## **Creating the HTTPS Site**

The procedure below describes how to create an HTTPS site.

#### > To create an HTTPS site:

- 1. Open the IIS Manager.
- 2. On the left Connections pane, select the local host entry under Start Page.
- 3. Expand Sites.

😫 Internet Information Servi	ces (IIS) Manager					- 🗆 X
← →	AZ-JKGCRHQ • Sites	•				📅 🐼 🚯 🕑 -
File View Help						*
Connections	Citor					Actions
Q- 🔒 🖄 😣	Sites					💕 Add Website
Start Page	Filter:	- 🛒 Go	- Show A	II Group by: No Grouping +		Set Website Defaults
- Application Poo	Name	ID	Status	Binding	Path	Help
> - Sites	Default Web Site	1	Started (ht	*:80 (http)	%Syste	
	<				>	
< >	📧 Features View 💦 C	Content View				
Ready						• <u>.</u>

4. On the right Actions pane, click Add Website; the following page appears:

ite name:		Application po	nak		
nttps		https		Select	
Content Directory					
Physical path:					
C:\inetpub\www	root				
Pass-through aut	hentication				
Connect as	Test Settings				
Binding					
Туре:	IP address:		Port:		
https	<ul> <li>All Unassigne</li> </ul>	ed	~ 443		
Host name:					
ac.l5.ca					
Require Server     Disable HTTP/     Disable OCSP:	2				
SSL certificate:			✓ Select	View	
SSL certificate: ac.I5.ca					
	mediately				

- In the 'Site name' field, enter "https". In the 'Physical path' field, enter "C:\inetpub\wwwroot" (default IIS path).
- 6. From the 'Binding type' drop-down list, select https.
- 7. In the 'Host name' field, enter your site FQDN.
- 8. Select the 'Require Server Name Indication' check box.

The 'Require Server Name Indication' check box must be selected when you create multiple HTTPS sites in IIS Manager and use many FQDNs. For a single HTTPS site, this is optional.

- From the SSL certificate drop-down list, select the SSL certificate you created in Using Open Source on page 16.
- **10.** Click **OK**.
- **11.** Check the created site by opening a browser at https://<your\_site\_fqdn>. You should see the default IIS start page.

#### **Configuring the HTTPS Site**

To configure the HTTPS site, do the following:

Install URL Rewriter 2.1 Component

- Create HTTP to HTTPS Request Redirection
- Configure Compression of Responses
- Enable Special Signs in Filenames

∕₽

Previously, the Web Platform Installer was used to install URL Rewriter. It's no longer supported as described in https://blogs.iis.net/iisteam/web-platform-installer-end-of-support-feed. Now we download the *url- rewrite module* from https://www.iis.net/downloads/microsoft/url-rewrite.

#### **Installing URL Rewriter 2.1**

The procedure below describes how to install URL Rewriter Version 2.1.

- **To install URL Rewriter 2.1:**
- **1.** Download the installer by clicking here.
- 2. Select Download URL Rewrite Module 2.1 x64 installer.
- 3. Download and open the *rewrite\_amd64\_en-US.msi* file.

#### **Creating HTTP to HTTPS Request Redirection**

The procedure below describes how to create HTTP to HTTPS request redirection.

#### **To create HTTP to HTTPS request redirection:**

- **1.** Start IIS Manager.
- 2. On the left Connections pane, select the local host entry under Start Page.

File View Help		
Connections	EC2AMAZ-JKGCRHQ Home	Actions
Start Page	Filter: • 🐨 Go - 🦕 Show All Group by: Area • 📰 •	Manage Server Restart Start
		Stop
	Authentic Compression Default Directory Error Pages Handler	View Application Pools View Sites
	Document Browsing Mappings	<ul> <li>Get New Web Platform Components</li> </ul>
	HTTP HTTP Logging MIME Types Modules Output Redirect Respon	😧 Help
	Request Server URL Rewrite Worker	
	Filtering Certificates Provides URL and content rewriting capabilities based on rules.	
	Management	
	Configurat Feature Shared Web Editor Delegation Configurat Platfor	
< >	🔟 Features View 💦 Content View	
Ready		¶1.:

- 3. Click the URL Rewrite icon; the URL Write page appears:
- 4. On the right Actions pane, click Add Rule(s); the Add Rule(s) page opens.

onnections	Actions	
- 🖬 🖄 😣	Add Rule(s) ? ×	(s)
Start Page EC2AMAZ-JKG	Select a rule template:	erver Variables er Variables
> - i Sites	Inbound rules          Blank rule       Rule with rewrite map         Request blocking       Inbound and Outbound Rules         Weser-friendly URL       Inbound Rules	Providers rite Maps iders les
	Outbound rules         Blank rule         Search Engine Optimization (SEO)         Image: Search Engine Optimization (SEO)	iom Tags
	Select this template to create a new inbound rule without any preset values. This template opens the "Edit Rule" page that you can use to define a new rewrite rule for changing the requested URL address.	

5. Select Blank Rule, and then click **OK**; the Edit Inbound Rule page appears:

Connections	Edit	t Inbound Rule			Actions				
• 🖬 🖄 😽		Inbound Rule		0	Apply				
- 🥞 Start Page - 🛀 EC2AMAZ-JKGCRH0	Match URL			^	Cancel				
Application Poo		RL:		Using:	Back to Rules				
> -🗃 Sites	Matches the		~	Regular Expressions	😧 Help				
	Pattern:								
	(.*)			Test patte					
	✓ Ignore cas Conditions	ie							
		Logical grouping:							
	Match All								
	Input	Туре	Pattern	Add					
				Edit					
				Remove					
				Move Up					
				Move Dow					
				Move Dow					

- 6. From the 'Requested URL' drop-down list, select Matches the Pattern.
- 7. From the 'Using' drop-down list, select **Regular Expressions**.
- 8. In the 'Pattern' field, enter "(.\*)".



(.\*) is entered in the 'Pattern' field.

- 9. Select the Ignore case check box.
- **10.** From the Logical Grouping drop-down list, select **Match all**, and then click **Add**; the Add Condition page appears.

File View Help						
Connections		haved Dula				Actions
S. 🗐 🖄 😽	Edit In	bound Rule			^	Apply
Start Page	Match URL				~	Cancel
- Application Poo	Requested URL:		Using:			P Back to Rules
> - 🚺 Sites	Matches the Patt	tern ~	Regular Express	sions		😢 Help
	Pattern:	Add Condition		? ×		
	(.*)	Condition input:			est pat	
		{HTTPS}				
	Ignore case	Check if input string:				
		Matches the Pattern	~			
	Conditions	Pattern:				
	Logical grouping:	^OFFS	Tes	st pattern		
	Match All					
	Input	✓ Ignore case			Add	
			ОК	Cancel	Edit	
			OK	Cancel	L. GTUTT	
					Remove	
					_	
					Move U <sub>l</sub>	
				N	love Dou	
	L					
	Track capture	groups across conditions				
	<	· ·			>	

11. In the 'Condition input' field, enter "{HTTPS}".

{HTTPS} is entered in the 'Condition input' field.

- **12.** From the 'Check if input string' drop-down list, select **Matched the Pattern**.
- 13. In the 'Pattern' field, enter "^OFF\$".



^OFF\$ is entered in the 'Pattern' field.

- **14.** Select the 'Ignore case' check box.
- **15.** Click **OK**; the Edit Inbound Rule page with Action settings appears:

(← → SEC2AM	AZ-JKGCRHQ				😝 🖂 🔐 -
File View Help					
Connections	Gill Edit I	nbound Rule			Actions
🔍 • 🔒 🖄 😽 👘	Euit II	Matches the Pattern	"UTTS		Apply
Start Page	(	There are a sector	0	Edit ^	🖹 Cancel
EC2AMAZ-JKGCRHC     Application Poo				Remove	🗢 Back to Rules
> - iii Sites				NUTION.	😢 Help
				Mariall	
				Move U	
				Move Dov	
	Track captur				
	-				
	Server Variables				
	Action				
	Action type:				
	Redirect				
	Action Proper	ties			
	Redirect URL:				
		HTTP_HOST   {REQUEST_U	JRI}		
			JRI}		
	https://()	uery string	JRI}		
	https://() Append qu Redirect type:	uery string	JRI )		
	https://()	uery string	JRI }		

- **16.** From the 'Action type' drop-down list, select **Redirect**.
- **17.** In the 'Redirect URL' field, enter "https://{HTTP\_HOST}{REQUEST\_URI}".
- **18.** Clear the 'Append query string' check box.
- 19. In the 'Redirect type' field, enter "Permanent (301)".
- **20.** In the right pane, click **Apply**.
- 21. Open your browser and confirm that it has been redirected to http://<your\_site\_fqdn>.

#### **Configuring Compression of Responses**

The procedure below describes how to configure the settings compression of responses.

#### > To use compression:

- 1. Start IIS Manager.
- 2. On the left Connections pane, select the local host entry under Start Page.

File View Help		
Connections	EC2AMAZ-JKGCRHQ Home	Actions
💐 - 🔚 🖄 😽		Manage Server
Start Page	Filter:     • 🐨 Go - 🕞 Show All     Group by:     Area     • 📰 •       IIS     IIS     IIS     IIS     IIS     IIS       Authentic     Compression     Default     Directory     Error Pages     Handler       INTP     HTTP     HTTP     Logging     MIME Types     Modules     Output	<ul> <li>Restart</li> <li>Start</li> <li>Stop</li> <li>View Application Pools View Sites</li> <li>Get New Web Platform Components</li> <li>Help</li> </ul>
S	Image: Server Filtering Certificates     URL Rewrite       Management     Image: Server Filtering       Image: Configurat     Feature Shared Web Editor Delegation Configurat	
ge 33 of 54 5342 words [) දි		BP

3. Click the **Compression** icon; the Compression page appears:

File View Help		
Connections	Compression	Alerts Use of dynamic compression
Start Page EC2AMAZ-JKGCRHC	Use this feature to configure settings for compression of responses. This can improve the perceived performance of a website greatly and reduce bandwidth-related charges.	may increase processor utilization and reduce the overall performance of the server.
	<ul> <li>Enable dynamic content compression</li> <li>Enable static content compression</li> </ul>	The dynamic content compression module is not installed.
	Static Compression	Actions
	Only compress files larger than (in bytes):  2700	Apply Cancel
	Z/00 Cache directory:	1 Help
	%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files	
	Per application pool disk space limit (in MB):	

4. Ensure that Static Compression is enabled.

## **Enable Special Signs in Filenames**

The procedure below describes how to enable special signs, (e.g.,+) in filenames.

- > To enable special signs:
- 1. Start IIS Manager.

2. On the left Connections pane, select the local host entry under Start Page.

File View Help		
Connections	EC2AMAZ-JKGCRHQ Home	Actions
Start Page       EC2AMAZ-JKGCRH(       Application Poo       Sites	Filter: • @ Go - E Show All Group by: Area • E +	Manage Server Restart Start Stop
	Authentic Compression Default Directory Error Pages Handler HTTP HTTP Document Browsing	View Application Pools View Sites Get New Web Platform Components
	Logging MIME Types Modules Output Caching Filter Use this feature to configure filtering rules es	😧 Help
	Configurat Feature Shared Web Editor Delegation Configurat Platfor	

3. Click the **Request filtering** icon; the Request Filtering page appears:

Connections	Reque	est Filt	ering	Alerts
CZ2MAZ-JKGCRH(     CZ2MAZ-JKGCRH(     Application Poo     Sites	Use this feature to	configur	Edit Request Filtering Settings ? X General	appear in the list and ha Allowed set to False are blocked. No other file na extensions are blocked. Actions
			Allow unlisted file name extensions         Allow unlisted verbs         Allow high-bit characters         Allow double escaping         Request Limits         Maximum allowed content length (Bytes):         3000000         Maximum URL length (Bytes):         4096         Maximum query string (Bytes):         2048	Allow File Name Extensio Deny File Name Extensio Edit Feature Settings Help

4. On the right pane, click Edit Feature Settings; the Edit Request Filtering Settings page appears.

it Request Filtering Settings	?	$\times$
General		
Allow unlisted file name extensions		
Allow unlisted verbs		
Allow high-bit characters		
Allow double escaping		
Request Limits		
Maximum allowed content length (Bytes):		
3000000		
Maximum URL length (Bytes):		
4096		
Maximum query string (Bytes):		
2048		
OK	Cancel	

- 5. Enable the allow double escaping check box.
- 6. Click OK.

## **Configuring Windows Server to Only Use TLS 1.2**

The procedure below describes how to configure the Windows server to only use TLS 1.2.



This procedure is not necessary for Windows Server 2022.

- > To configure the Windows server to only use TLS 1.2:
- Check the server security grade by service. Go to https://www.ssllabs.com/ssltest/index.html; the following page appears:

Qualys. SSL Labs	5		I	Home	Projects	Qualys Free Trial	Contact
You are here: <u>Home</u> > <u>Projects</u> > SSL Server Test							
SSL Server Test							
This free online service performs a deep a information you submit here is used on will.		· · ·					
Hostnar		to not show the results on the boards			Submit		
Recently Seen		Recent Best			Recent Worst		
www.b2b.preops.nm.eurocontro		osmproservices.com	A+	-	api-sandbox-dev.	nwm.io	F
agora365.vinci-autoroutes.co		<u>dga-ag.de</u>	А	1	taejai.opendream	.in.th	т
ssitest.mywayorelse.net		g <u>enerali-uat.webssup.com</u>	Α	1	digitalbank.iciciba	ink.com	F
ap.maxval-soft.com		www.nespresso.com	Α	4	statics.boyner.com	<u>m.tr</u>	F
www.ggtern.com E	Err	meals4moms.org	Α	1	barracuda.bit-stu	dio.at	т
erobab.com		<u>ral.dk</u>	в		cesc24.com		т
www.magyarhitelkozpont.hu		thinksharp.com	в		n-organic.jp		F
locadmin.nl		appliedroots.com	в		hn1504.biz		F
<u>utilitys.nl</u>		cmss.emunicipis.ddgi.cat	в		aaes-av.assaablo	<u>y.com</u>	т
www.podium.tv		equiposer.sytes.net	В	1	tools.jthanoi.com		т
SSL Report v2.1.8							

2. Enter the hostname, and then click **Submit**; a summary report is displayed with the following message: This server supports TLS 1.0 and TLS 1.1. Grade capped to B.

Summary							
	<b>Overall Rating</b>				1		
		Certificate					
		Protocol Support					
		Key Exchange					
		Cipher Strength					
			0	20	40	60	
	Visit our <u>documentation</u>	page for more information, configuration guide	es, and b	ooks. Kn	own issue	s are docur	me
		his server supports TLS 1.0 and TLS 1.1. Grad					
		This site works only in browsers wi	ith SNI su	upport.			

Certificate #1: RSA 2048 bits (SHA384withRSA)

- **3.** Disable TLS 1.0 and TLS 1.1 in the Windows server (refer to https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings).
- 4. From the Windows start menu, open the Registry Editor. Run as the administrator.
Open Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols



In Windows Server 2019, there are no "TLS 1.0" and "TLS 1.1" keys; there is only a Default value.

- 6. Add the TLS 1.0 sub-tree, by right-clicking the Protocols entry.
- 7. Select "New" "Key", and then create the TLS 1.0 key.
- 8. Right-click the TLS 1.0 entry, and then select "New" "Key".
- 9. Create the Server key.

PnP     Power     Print     PriorityControl     ProductOptions     RadioManagement	^	Name (Default) DisabledByDefa	Type REG_SZ	Data (value not set)
<ul> <li>SafeBoot</li> <li>SAM</li> <li>ScEvents</li> <li>SCMConfig</li> <li>ScsiPort</li> <li>SecureBoot</li> <li>SecurePipeServers</li> <li>SecurityProviders</li> <li>SasIProfiles</li> <li>SCHANNEL</li> <li>CipherS</li> <li>CipherSuites</li> <li>Hashes</li> <li>KeyExchangeAlgorithms</li> <li>Protocols</li> <li>Server</li> <li>WDigest</li> <li>ServiceAggregatedEvents</li> </ul>		22 Enabled	REG_DWORD REG_DWORD	0x0000000 ((

- **10.** Right-click the Server entry, select "New" "DWORD (32-bit) Value" and then create the DisabledByDefault value.
- Right-click the Server entry, select "New" "DWORD (32-bit) Value", and then create the Enabled value.

Both DisabledByDefault and Enabled should be set to 0.

- **12.** Add the TLS 1.1 sub-tree in the same way as you did for the TLS 1.0 sub-tree. See Step Add the TLS 1.0 sub-tree, by right-clicking the Protocols entry. on the previous page.
- 13. Right-click the 'Protocols' entry, select "New" "Key", and then create the TLS 1.1 key.
- 14. Right-click the TLS 1.1 entry, select "New" "Key", and then create the Server key.
- **15.** Right click the Server entry, select "New" "DWORD (32-bit) Value", and then create the DisabledByDefault value.
- **16.** Right-click the Server entry, select "New" "DWORD (32-bit) Value" and then create the Enabled value.

Both DisabledByDefault and Enabled should be set to 0.

- 17. Reload Windows Server 2019.
- **18.** Re-check the security grade, by opening https://www.ssllabs.com/ssltest, and then clicking the **Clear cache** button; the result will now be Grade A.

Summary					
Overall Rating					
	Certificate				
	Protocol Support				
	Key Exchange				
	Cipher Strength				
		0 20	40	60	8
Visit our documentation	n page for more information, configuration guide	s, and books. Ki	nown issues	s are docur	mente
	This site works only in browsers wi	th SNI support.			

Certificate #1: RSA 2048 bits (SHA384withRSA)

# **Deploying WebRTC Client on IIS**

#### > To deploy on IIS server:

- **1.** Unzip the file webrtc-web-client-vx.x.zip.
- 2. Copy the unzipped content to the *C*:\*inetpub*\*wwwroot*\*webrtc\_client* directory.

## **Upgrading WebRTC Client on IIS**

#### To upgrade the WebRTC client on IIS:

To upgrade the WebRTC client on IIS, see Upgrading the Web Client to a New Release.

# **Customizing WebRTC Client**

The procedures below describe how to customize the WebRTC client.

## **Advanced Options Configuration File**

The advancedOptions.js file allows you to edit several attributes. Most of the configuration is self-explanatory and should remain as default configuration. Below is a list of the most important parameters:

**defaultServerConfig:** Defines the default SIP server configuration.

• **sipDomain:** Defines the domain name (for example, audiocodes.com) used by the WebRTC client in the SIP messages (INVITE/REGISTER) sent to the WebRTC gateway.

- sipServerAddress: Defines an array of the default SBC addresses list, shown on the client server field (for example, wss://s-bcGENLab1.customers.audiocodesaas.com:10081). If a server's URL in the list is not responding, another one in the list will be attempted. The 'prioritize' value below determines how the next URL is chosen.
- prioritize: If 'true', then the SBC URLs list is sorted by priority, so that if connecting to a
  URL fails, the next one in the list is attempted. If 'false', then the next attempt is
  selected randomly.
- **sipIceServers:** Recommended to leave empty but if required may be edited to contain list of ice servers as shown below.
- backupSipServerAddress: Defines an array of the backup SBC addresses list (same structure as sipServerAddress). If the address is set, the dual registration feature is enabled.

Default: empty list, dual registration feature is disabled.

- **guiEnabled:** Defines whether to allow showing server configuration settings in the client GUI. Default: true.
- **disableEditing**: Defines whether modifying server configuration by the user through the Settings UI is disabled, so that server configuration settings are always determined by the values from the configuration file. Default: false (the user is allowed to edit).
- **storageConfig:** Configure the client storage and caching behavior.
  - location: Defines the web storage mechanism the client uses to cache user data, including authentication states. Possible values:
    - localStorage: Uses the browser's persistent local storage.
    - sessionStorage: Uses only the session cache (e.g., tab lifetime).
- defaultOAuthConfig: DEPRECATED, see "Migrating Authentication Providers and Contact Center Configuration from Previous Versions".
- **ACDClientConfig:** Configuration for contact-center agent ACD support.
  - enabled: Defines whether Automatic Call Distribution is enabled.
  - notReadyDefaultReasonCode: Defines the value that is used by default, when the client automatically goes to a "not-ready" state. It can be one of the list in notReadyReasonCodeMapping, or a totally different one.
  - notReadyReasonCodeMapping: Defines the list of codes and corresponding text values that are presented to the user as selectable not-ready reason codes.
  - notReadyStatusValue: DEPRECATED. Use notReadyDefaultReasonCode and notReadyReasonCodeMapping instead.
- **sipAccountGUIConfig:** Configures the GUI display and control of SIP account details.
  - sipDisplayNameHidden: Determines whether to hide SIP display-name from GUI altogether. Default: false.

- **sipDisplayNameDisabled:** Determines whether to disable SIP display-name configuration in Settings. Default: false.
- notificationOptions: Optional configuration for displaying a warning when auto-play is disabled by the browser. By default, the warning will not be displayed.
  - focusWindowOnClick (true / false): Determines whether to bring the browser tab into focus when clicking on browser notifications from the client. Default: true.
  - autoplay:
    - showAutoplayDisabledAlert (true / false): Upon page load, displays an alert to the user on the page itself. Default: true.
    - showAutoplayDisabledNotification (true / false): Upon page load, attempts to display a browser notification. This is only supported for now with Chrome, Edge and Safari. Default: true.
- **autoplayNotificationOptions: DEPRECATED**. Use **notificationOptions** > **autoplay** instead.
- customerInfoContextDisplayMapping: Optional key-value json object: When an incoming call INVITE message arrives with the "X-Customer-Info" header for displaying customer information, this object can map keywords from the customer information into user-readable text to display. For example: customerInfoContextDisplayMapping = {advice: "Getting expert advice for the product"}
- **isVideoEnabled:** Determines whether the client has video support.
- **enableAddVideo:** Enables adding video to audio calls.
- isScreenSharingEnabled: Enables / Disables the screen sharing feature.
- isCrossScreenSharingAllowed: When incoming screen sharing occurs during a call, the client should also allow outgoing screen sharing. Default: False.
- **isAllowedToResumeLocalHoldByRemoteReInvite:** This value indicates whether or not the client is supposed to release the local hold, when receiving a reINVITE with the sendrecv media direction. Default value: false.
- registerExpires: Defines the SIP registration expiry time (seconds)
- **voiceQualityMonitorEnabled:** Enables / Disables voice quality monitoring.
- restoreCallQualityMaxDelay: Defines the maximum interval to store the last call quality score.
- **restoreCall:** Determines whether call restoration functionality is enabled.
  - True upon refresh the client restores the previous call.
  - False call won't restore upon refresh.
- restoreCallMaxDelay: Defines the maximum interval to restore a call after page reload (in seconds).
- reconnectIntervalMin: Defines the minimum interval between WebSocket reconnection attempts (in seconds).

- reconnectIntervalMax: Defines the maximum interval between WebSocket reconnection attempts (in seconds).
- **dtmfUseWebRTC:** Determines which DTMF type to use: RFC 2833 or SIP info.
- dtmfDuration: Defines the duration of the DTMF tone (in milliseconds). The default value is 100.
- dtmfInterToneGap: Defines the interval between two DTMF tones (in milliseconds). The default value is 500.
- **useSessionTimer:** Enables Session Timers (as per RFC 4028). Default: False.
- noAnswerTimeout: Defines the interval in seconds, from when an incoming call is received, until it automatically terminates due to no answering. Default: 60 seconds.
- avoidTwoWayHold: If the call is in remote Hold, disable the local Hold button to avoid 2 way holds.
- **disableOutgoingCalls:** If set to "true", it does not allow outgoing calls.
- **autoAnswerOptions:** Defines the options for behavior with auto-answering a call:
  - **answerDelayedOfferWithVideo:** When an incoming offer with no SDP arrives with an auto-answer trigger, answer with video media. Default: False.
  - autoAnswerDefaultDelaySeconds: Defines the delay in seconds before an incoming call is auto-answered, given that the call is eligible for auto answer. Default is 0 (no delay).
- **callHistoryConfig:** Defines call history configuration.
  - maxEntries: Defines the maximum number of call history entries per user. Default: 100
  - guiEnabled: Defines whether to allow the call history GUI. Default: true.
- maxSizeForCallHistory: Defines the maximum size for the client's call history database.DEPRECATED. Use callHistoryConfig > maxEntries instead.
- **IayoutConfig:** This section contains several color theme configurations.
  - alwaysShowFullCallsList: Defines whether or not to allow the GUI calls list to expand or collapse.
    - If false (default), allow the calls list GUI to collapse and show only the currently focused call.
    - If true, the calls list will not collapse and will always show all existing calls.
- supportedAuthenticationSchemes: DEPRECATED, see "Migrating Authentication Providers and Contact Center Configuration from Previous Versions".

Auto-login from within a CTI software (e.g., Genesys WDE): When embedding the client in a program such as Genesys Workspace Desktop Edition, auto-login works if "user-password" is the only available scheme.



Debug mode is used for debugging purposes only and should not be set on customer deployments.

**modes:** Adds miscellaneous patches to the SDK for various features:

- cache\_register\_auth\_mode: reuse SIP Authorization header for REGISTER refresh requests, so that the user agent will not have to be challenged for every REGISTER refresh. Default value: true.
- ice\_timeout\_fix: timeout interval in milliseconds for ICE candidate gathering. Default value: 2000 ms.
- VDIIntegrationConfig: Defines configuration for integrating with VDI (Virtual Desktop Infrastructure) solutions:
  - vdiSolutionType: The VDI solution to be used. Supported values:
    - "none" for no VDI integration (default value)
    - "citrix" for Citrix Workspace VDI

To work with the Citrix VDI, the Citrix remote machine must be configured to enable proper client functionality. See Configuring Citrix Remote Desktop for Integration with WebRTC Client on page 58 for details.

**mediaDeviceSettings:** Configuration for media device selection.

- deviceCategories: List of allowed media device categories. Defaults to ["microphone", "voiceoutput", "ringeroutput", "camera"]. Possible values:
  - **microphone:** WebRTC voice input device
  - voiceoutput: WebRTC voice and audio playback output device
  - ringeroutput: Secondary output for ringing sound of incoming call to play simultaneously with voiceoutput
  - camera: WebRTC video input device
- allowMediaDeviceSelection: If set to "true", it allows the user to select the media input / output devices to use for WebRTC voice in calls. Default value: false.
- devicesMustBeSelectedByUser: When media device selection is allowed, and the user has not selected audio input / output devices; If "false", the default media input / output devices are automatically selected. If "true", the user is prompted to select media devices explicitly. Default value: false.

For the Citrix VDI solution (vdiSolutionType = "citrix"), both values are overridden and considered to be "true".

codecFilter: Control codec behavior: Filter and set priority for WebRTC SDP codec generation.

- **audio:** Control audio SDP codec generation.
  - remove: Array of codec names to remove (e.g., [isac, 'pcma',]).
  - priority: Array of codec names prioritized in descending order, so that SDP creation will arrange them such (e.g., ['opus', 'pcma', 'pcmu']).
- video:
  - remove: Same as "audio", but for video codecs.
  - priority: Same as "audio", but for video codecs.
- IocalVideoFilter: Client configuration for camera-capture video filters such as virtual background.
  - **supported: DEPRECATED**. Use *virualBackgroundSupported* instead.
  - virualBackgroundSupported: If set to "true", the client includes settings for the user to apply virtual background effects. If set to "false", these settings are not available to the user
  - maxSizeForLocalBGImages: Defines the maximum additional amount of possible virtual background images that the user can choose in Virtual Background Settings.
- IocalizationConfig: Configures the client usage of its text resource file. See the Language and Text Customization section for text customization.
  - defaultLanguageResrouceURL: Sets an alternative location for the text resource. See the Language and Text Customization section.
  - waitForDefaultResourceFetch: Defines whether to hide the GUI until the text resource is downloaded. See the Language and Text Customization section.
- customGeneralSIPHeaders: Defines optional custom SIP headers that are to be added to outgoing SIP requests and responses. Defined as an array in the following format: ["headerName1: headerValue1", "headerName2: headerValue2", ...]
  - Currently the custom SIP headers are only added to: REGISTER, INVITE, re-INVITE to add video, INFO except DTMF, call answer and call reject.
- **isAgentAssistEnabled:** Whether or not to enable Agent Assist (Default = False).
  - Show/Hide the Agent Assist chatbot UI during a call
  - Show/Hide the Agent Assist settings
  - Show/Hide Agent Assist chat history for recent calls.

- agentAssistDefaultBotName: The default bot name that the client requests to activate for Agent Assist.
- agentAssistDefaultServiceUrI: The default URL for the machine running the Agent Assist service (typically part of the Voice-AI Connect server), to which Agent Assist requests are sent.
- agentAssistDefaultServicePath: A socket-io service path, used as a URL suffix for the service URL.



- agentAssistMaxHistoryEntries: The number of recent agent assist chat sessions that can be stored (Default = 50).
- agentAssistDefaultConversationConfig: Configuration related to conversation parameters defined here.
  - defaultRoles: Default participant names of the conversation, to distinguish which party is speaking when a call-transcript message arrives:
    - caller: Default participant name of the caller. Typically, "participant".
    - callee: Default participant name of the callee. Typically, "participant-2".

Depending on deployment platform, this file is located in:

- **Apache server:** /var/www/html/webrtc\_client/static/js/advancedOptions.js
- NGINX server: /var/html/webrtc\_client/static/js/advancedOptions.js

```
var defaultServerConfig = {
    sipDomain: "audiocodes.com",
    sipServerAddress: ["wss://sbcGENLab1.customers.audiocodesaas.com:10081"],
    sipIceServers: ["74.125.140.127:19302", "74.125.143.127:19302"]
};
```

# **Configure Integrations with Contact Center Platforms**

The advancedOptions.js file allows you to set the contactCenterConfig object, which defines integration with Contact Center platforms, such as Genesys Pure Engage / PureCloud, so that the web client functionality can be seamlessly integrated into these systems.

For example:

```
var contactCenterConfig = {
  integrations: [
    {
      enabled: true,
      contactCenterPlatform: "genesys pure engage",
      serviceName: "Genesys Pure Engage",
      customSipHeaderNames: {
        contactCenterCallUuidHeader: "x-genesys-calluuid",
      },
    },
    {
      enabled: true,
      contactCenterPlatform: "genesys cloud",
      serviceName: "Genesys Cloud US-West-2",
      environment: "usw2.pure.cloud",
      clientId: "8612e5af-3c70-4178-ba3e-4333dcee0b32",
      redirectUri: "", // Empty for current, or for specific URL
      customSipHeaderNames: {
        contactCenterCallUuidHeader: "x-inin-cnv",
      },
    },
  ],
  defaultSipHeaderNames: {
    contactCenterCallUuidHeader: "call-id",
    contactCenterCallUserInfoHeader: "x-customer-info",
  },
}
```

- defaultSipHeaderNames: Defines default SIP header names of various features integrated with contact center platforms. See customSipHeaderNames: Defines custom SIP headers that, if included in SIP messages, have a particular significance. below
- Integrations: The object structure is an array of contact center integration objects. Each object can include the following properties:
  - **contactCenterPlatform:** Defines the platform-type-name of this integration object. Possible values: "genesys\_cloud", "genesys\_pure\_engage".
  - serviceName: Defines a unique name identifying the contact center integration service.
  - enabled: Defines whether this integration is available in the client or not. Default: false.
  - customSipHeaderNames: Defines custom SIP headers that, if included in SIP messages, have a particular significance.
    - contactCenterCallUuidHeader: Defines the SIP header name to be used, to denote the call UUID for that platform integration.
    - contactCenterCallUserInfoHeader: Defines the SIP header name to be used, to contain a customer-info JSON value.
- Other platform-specific attributes: For example, clientId / redirectUri / environment that are specific to allow Genesys Cloud sign-in. These require proper knowledge of the interoperability of a web client application with the contact center platform

## **Configure Authentication Providers for User Sign-In**

The advancedOptions.js file allows you to set the authProvidersConfig object, which configures parameters of all the available authentication providers for the user to sign into. These authentication providers typically feature OpenID Connect / OAuth 2.0 sign-in, to allow the web client to obtain SIP credentials and other protected resources for the client functionality.

For example:

```
var authProvidersConfig =
  mandatoryProviderLoginName: "Genesys Cloud US-West-2",
  providers: [
    {
      providerLoginName: "Azure Active Directory",
      providerType: "AAD",
      authority: "https://login.microsoftonline.com/1911c65c-89....
      endpointUrl: "https://graph.microsoft.com/v1.0",
      realm: "",
      clientId: "e8a69733-d978-47b9-a938-cc8b260636a4",
      redirectUri: undefined,
      knownAuthorities: [],
      requestScopes: [],
      authRefreshRetriesForSipError: 5,
      forceLoginPromptOnEmptyCache: false,
      userInfoUrlRelativePath: "/me",
      tokenRevocationRelativePath: "",
      cacheLocation: "",
      sipAttributes: {
        SIP_DN_Attribute_name: "voip identity username",
        SIP_Password_Attribute_name: "voip identity password",
      },
    },
    ł
      providerLoginName: "Keycloak",
      providerType: "Keycloak",
      authority: "https://keycloak.webrtc.audiocodes.com:8443",
      realm: "demo",
      clientId: "WebRTCDemo",
    },
  ]
}
```

mandatoryProviderLoginName: Defines the providerLoginName attribute of the login provider which is mandatory. That is, the client, upon launch, always verifies that the user is logged in to it. Otherwise, it prompts a login to that specific provider without allowing you to continue. This can also be the serviceName property of a contact center integration that also serves as an authentication provider, e.g., Genesys Cloud.

- Providers: Defines the authentication providers that the user is allowed to sign into from the client GUI. They are represented as an array of elements, each corresponds to a single authentication provider:
  - providerLoginName: Defines the name of the authentication provider, as displayed as an entry in the client Account Settings. This name must be unique.

- providerType: Denotes the identity provider type and the mode of operation. Possible values:
  - AAD (default): Defines an Azure Active Directory endpoint
  - Keycloak: Defines a specific for the Keycloak identity platform
  - OIDC: Defines a general purpose provider that is Open Id Connect-compliant
- endpointUrl: Defines the identity-provider API endpoint URL. This is used for API calls to access resources protected by the OAuth token, such as a user identity profile. Default: https://graph.microsoft.com/v1.0 for "AAD" protocol mode, and the value for "authority" for OIDC mode. (Optional)
- Authority: Defines the endpoint from which tokens are obtained. For the AAD providerType, it should be https://login.microsoftonline.com/<tenant-id>, and for multi-tenant applications the tenant-id can be "common".
- Realm: Defines the optional authentication realm value. Mandatory for the 'Keycloak' providerType.
- clientId: Defines the identifier of the client application, as registered with the identity provider.
- knownAuthorities: Defines a list of optional known authorities. Required for providerType "AAD" if the "authority" value is not a commonly trusted authority such as https://login.microsoftonline.com.
- redirectUri: Typically and if not specified, this would be the client's site URL. It must be listed in the app registration for the "Single-page application" platform configuration. It can be left undefined.
- requestScopes: Defines the custom request scopes for obtaining access tokens.
   "User.Read" is automatically added for "AAD" protocol mode, and "openid" is added for other modes.
- authRefreshRetriesForSipError: Defines the number of times the client attempts to refresh the access token after an authentication error response from SIP registration. Default: 5.
- forceLoginPromptOnEmptyCache: When no cached OAuth account exists, for example when using session-storage:
  - false (default): Allows re-use of active session cookies if available, to save the user the need to enter credentials again.
  - true: Forces redirection to login page even though an active session cookie exists, to allow the user to log in to a different account if possible.
- userInfoUrlRelativePath: (Optional) The suffix is added to the endpoint URL for requesting the logged-in user info.
  - Default: '/me' for the 'AAD' providerType, and 'openid-connect/userinfo' for other providerType values.

- tokenRevocationRelativePath: Optional, the suffix added to the authority URL for revoking the user session on sign-out. No default value.
  - If this value is set to a non-empty path, then the client attempts to use it to invoke token revocation, so that all other login sessions with the same token are invalidated.
- cacheLocation: (Optional) Sets the preferred browser storage location. Default is the value under "storageConfig". Possible values:
  - localStorage: Best user experience, less secure. This allows the login session to persist across multiple browser sessions.
  - sessionStorage: Medium user-experience, more secure. On a new browser session, the login session does not exist, unless secure cookies are enabled and forceLoginPromptOnEmptyCache is false.
  - memoryStorage: Most secure, not using browser storage. Login session persists based on secure cookies, if enabled.
- **sipAttributes:** Defines the attribute names of SIP credential attributes that are assigned to the user profile once logged-in.

The following two attributes must be unique in the user profile and are searched recursively throughout all the user's attribute hierarchy.

- SIP\_DN\_Attribute\_name: (Optional) Defines the name of the id-token claim or user profile attribute, which defines the directory number / SIP username.
- SIP\_Password\_Attribute\_name: (Optional) Defines the name of the id-token claim or user profile attribute, which defines the SIP password. If not defined, then the authentication flow uses the "Bearer <oauth-id-token>" as the SIP authorization header.

# Migrating Authentication Providers and Contact Center Configuration from Previous Versions

#### **Contact Center Integration – Genesys Pure Engage**

To keep full support of the Genesys Pure Engage integration similarl to previous versions, especially when embedding the client within the Genesys Workspace Desktop Edition application, the **contactCenterConfig** object must contain the Genesys Pure Engage entry, exactly as it is in the example under Configure Integrations with Contact Center Platforms.

#### **Authentication Provider Configuration**

**Backward Compatibility:** The client is backward compatible with the previous authentication configuration, which uses the deprecated **defaultOAuthConfig** and **supportedAuthenticationSchemes** objects. However, this support is not guaranteed to last. We highly recommend to migrate to the new configuration structure using the **authProvidersConfig** object, as described below.

#### Migrating to the new configuration

#### SupportedAuthenticationSchemes:

This configuration is deprecated and should be removed altogether. The included authentication scheme values are to be incorporated as follows:

- "user-password": To support the user-password SIP registration authentication scheme, make sure that the attribute value authProvidersConfig.mandatoryProviderLoginName is an empty string or not set - i.e., there must not be a mandatory provider.
- "oauth"/ "user-password\_from\_oauth": This value is determined according to the authentication provider being used at runtime and whether its configuration includes the sipAttributes properties.
  - If supportedAuthenticationSchemes includes only a single scheme which is not user-password, then the authentication provider represented by defaultOAuthConfig should be set to be the value of authProvidersConfig.mandatoryProviderLoginName. (See below)

defaultOAuthConfig: This object represents a single authentication provider, where Version 2.6.0 and later supports multiple providers.

- The object authProvidersConfig should be created and include the following properties:
  - providers: This is an array of a single element which represents the provider from defaultOAuthConfig as follows:
  - providerType: If defaultOAuthConfig.mechanismType is "keycloak", set the value to "Keycloak". Otherwise, set the value to be the value of defaultOAuthConfig.protocolMode.
  - Authority: Set to be defaultOAuthConfig.msal.authority for msal mechanismType, or defaultOAuthConfig.keycloak.oAuthUrl for keycloak mechanismType.
  - realm: Set to be defaultOAuthConfig.keycloak.realm if keycloak is used, otherwise it is empty.
  - authRefreshRetriesForSipError: Same as defaultOAuthConfig.accessTokenRefreshRetries.
  - forceLoginPromptOnEmptyCache: Same as defaultOAuthConfig.forceLoginPromptOnEmptyCache.
  - sipAttributes: Should contain the SIP\_DN\_Attribute\_name and SIP\_Password\_ Attribute\_name properties and values from defaultOAuthConfig.msal.

- redirectUri: (Optional) Recommended to be left empty so that the client uses its current location URL. Alternatively, this can be set to be the same as defaultOAuthConfig.msal.redirectUri.
- All other properties, e.g., clientId, endpointUrl, etc., can either be set similarly as in defaultOAuthConfig, or according to the guidelines under Configure Authentication Providers for User Sign-In on page 40.

#### **Client Resource Customization – Images, Sounds and Text**

The following describes the client resource customization.

#### Logo

Client logos may be modified to reflect the customer company logo. The images may be found in the "images" folder. Customers should use the currently provided images as reference:

- The svg logo pixel dimensions is 241 X 34, and the logo-small image is 54 X 32 pixels. For logo-small this is optional, the logo-small can be of any size that's not larger than the svg logo in either width or height.\*
- The svg file can be easily generated from a bitmap image of the size 241 X 34 using standard image conversion tools. The svg in this case, should contain the viewBox attribute <0 0 241 43>, which is auto-generated during the creation of the image.\*

#### **Sound Files**

Client sound files for call-related rings, such as incoming call / outgoing call progress / call ended etc., can be modified by overriding the corresponding files under webrtc\_ client/sounds.

#### Virtual Background Images

- The client includes several pre-packaged image files, that serve as default available virtual background images. These images are presented to the user in the Virtual Background settings, so they can select one of them to apply as a virtual background image effect.
- These images are contained in "images/virtual-backgrounds/", as image01.jpg, image02.jpg and so on.
- These images can be modified by the customer if they wish to use other default images as available virtual backgrounds.



The images must be replaced using the same filenames.

The client does not support adding more images than currently exist.

#### Language and Text Customization

The client GUI text can be modified or translated to a different language. To do so, the client uses a text resource JSON file, which by default is located at *webrtc\_client/static/localization/strings-default.json*.

#### **Text JSON Format and Behavior**

- The text file format is a JSON object containing key-value entries of the following type: "KEY\_NAME": "Corresponding text value".
- Each key can be assigned a different text value, which modifies the client text on screen.
- Each key with an empty value will prompt the client to use its own English default value.
- The client also has default English textual data, in case the text resource file is not in use or missing.



The text customization file only allows you to replace existing text data with modified values. It does NOT cause any GUI orientation or layout changes according to the language.

#### **Setting Client Lozalization**

In the text JSON file, the "LANGUAGE\_RESOURCE\_LOCALE" entry denotes the localization that this text resource represents, which defaults to "en-US". This localization information notifies the client how to format language and region-related text data, such as date and time. The value to this key must be a valid IETF BCP 47 language-tag.

#### **Setting a Different Language Resource**

The client can be configured to fetch its text resource file from a different location URL. In order to do so, modify the **defaultLanguageResrouceURL in advancedOptions.js** property.

#### **Resource Fetch Behavior**

Each time the client page loads, it performs the following:

- Load custom string resource from cache, if exists
- Fetch custom string resource from defaultLanguageResrouceURL or from the default location
- Override the previous cache with the fetched custom string resource

#### **Configure GUI Behavior with Regards to Text Resource Fetch**

To prevent the client from showing its default English text GUI when waiting to download the text resource, the client can be configured to hide its GUI until it successfully loads a language resource from cache or by fetching it from the network.

Use the **waitForDefaultResourceFetchconfiguration** property in **advancedOptions.js** to determine whether the client GUI should be hidden until it has a language resource.

## **Browser Auto-Play Control for Tone Playback**

Most browsers block media auto-play by default. This means that without user interaction on the page, no tone playback will be available, e.g., ringtones for incoming calls.

To support scenarios in which the client can play tones without user interactions, e.g., when the client page was just reloaded by the user and an incoming call arrives, the browser must allow auto-play for the client's website.

To enable auto-play for the browsers we officially support, you can either configure the browser settings or alternatively, configure the browser enterprise policies on Windows:

#### ➤ Google Chrome:

- Browser Settings: Navigate to chrome://settings/content/sound, and add the web client URL to the "Allowed To Play Sound" list.
- Enterprise Policy Configuration: See https://chromeenterprise.google/policies/#AutoplayAllowlist

#### ➤ Microsoft Edge:

- Browser Settings: Navigate to edge://settings/content/mediaAutoplay, and then add the web client URL to the "Allow" list.
- Enterprise Policy Configuration: See https://docs.microsoft.com/enus/deployedge/microsoft-edge-policies#autoplayallowlist

#### ➤ Firefox:

 Browser Settings: Navigate to the web client page, press Ctrl + I to show the page information, go to the Permissions tab and modify the "Auto-play" settings for that site to "Allow Audio and Video".

#### ➤ Safari:

 Browser Settings: Navigate to the web client page. Go to the Safari menu, and then click Settings for This Website. In the displayed panel, under "Auto-Play", select Allow All Auto-Play.

## Maintaining Web Client Activity When Browser Tab is in Background

Modern browsers introduce new performance features that save resources, by automatically discarding tabs or putting them to sleep after being hidden for a certain period of time. Specifically, the introduction of new memory-saving features in both Chrome Memory Saver and Edge Sleeping Tabs, can negatively impact the client's ability to maintain active connections and receive incoming calls.

The client attempts to mitigate this by implementing approaches to keep the tab active. However, such endeavors are not reliable enough, because the browsers can still decide to proactively discard the tab without notifying the client or the user.

Currently, the best way to keep the tab active when hidden and avoid it from going to sleep or being discarded, is to disable memory-saving features for the client website as follows:

#### > To disable memory-saving features in Google Chrome:

1. Navigate to chrome://settings/performance; the following appears:

Performance	Ŀ
Memory Saver When on, Chrome frees up memory from inactive tabs. This gives active tabs and other ap computer resources and keeps Chrome fast. Your inactive tabs automatically become act when you go back to them. <u>Learn more</u>	
Always keep these sites active	Add
No sites added	

- 2. In the 'Always keep theses sites active' field, click Add.
- **3.** In the dialog that opens, type the WebRTC web client full URL (including the schema), and then click **Add**.



#### > To disable memory-saving features in Microsoft Edge:

- 1. Navigate to edge://settings/system.
- 2. In the 'Never put these sites to sleep' field, click Add.

Efficiency mode 🕜	Are you satisfied with efficiency mode?	ථ	8	•
Helps minimize power usage by saving computer resources. Ber While the efficiency mode in Microsoft Edge may be turned off, resources on your device, as indicated in the Task Manager.				
Improve your PC gaming experience with efficiency mode	Are you satisfied with efficiency mode for PC gaming?	3	8	
When you're playing a PC game, Microsoft Edge reduces its cor	mputer resource (CPU) usage to create a better gaming experie	ence.		
Save resources with sleeping tabs	Are you satisfied with sleeping tabs?	3	8	
When this is on, inactive tabs will go to sleep after a specified ti	ime to save system resources. Learn more			
Fade sleeping tabs				
Fade sleeping tabs Tabs will appear faded when saving memory and CPU to improv	ve performance.			
		Ir of inad	ctivity	<b>•</b>
Tabs will appear faded when saving memory and CPU to improv <b>Put inactive tabs to sleep after the specified amount</b> When efficiency mode is on, inactive tabs will be put to sleep af	of time: 1 hou			·
Tabs will appear faded when saving memory and CPU to improv <b>Put inactive tabs to sleep after the specified amount</b> When efficiency mode is on, inactive tabs will be put to sleep af activities that prevent a site from sleeping (e.g. playing audio).	of time: 1 hou			·
Tabs will appear faded when saving memory and CPU to improv	of time: 1 hou fter 5 minutes or less. Actual time may vary depending on reso			, I

**3.** In the dialog box, in the 'Site' field, enter the WebRTC web client full URL (including the schema), and then click **Add**.

Add a site	/			
Site				
https://demo.webrtc.audiocodes.com/webrtc_client/				
Add Cancel				

# **NGINX and Apache Server Web Access Examples**

Based on the configuration shown in this document, the WebRTC client can be accessed through a Web browser using the following URL examples:

- NGINX server: https://webrtcdemo.audiocodes.com/webrtc\_client
- Apache server: https://ik.I5.ca/webrtc\_client

The URLs above are AudioCodes demo sites and may not always be accessible.

# Upgrading the Web Client to a New Release

When performing an upgrade, do the following to ensure that current modifications to configurations and resources are not lost.

- 1. Maintain a list of all changes made to resources or configurations in the current release, that you wish to preserve when upgrading.
- 2. Backup the contents of the webrtc\_client folder into webrtc\_client\_old.
- Delete the entire contents of webrtc\_client, and then copy into it the contents of the new build folder.
- 4. Preserve modified resources from the previous build by doing the following:
  - a. Copy all files in *webrtc\_client\_old/images* that are listed in Step #1, and then paste and override them into *webrtc\_client/images*.
  - **b.** Copy all files in *webrtc\_client\_old/sounds* that are listed in Step #1, and then paste and override them into *webrtc\_client/sounds*.
  - c. Edit the file at webrtc\_client/static/localization/strings-default.json, and then override all entries listed in Step #1 with their corresponding values from webrtc\_client\_ old/static/localization/strings-default.json.
- 5. Preserve the client configuration by doing the following:
  - a. For every configuration property in *webrtc\_client/statis/js/advancedOptions.js*, that is listed in step #1, perform the following:
    - i. If the configuration property is not marked as @deprecated, then modify its value to be the same as *webrtc\_client\_old/statis/js/advancedOptions.js*.
    - ii. If the configuration property is marked as @deprecated, then use the documented recommendation next to it, to assign the modification to the alternative corresponding property.
- 6. Delete the *webrtc\_client\_old* folder.

# 4 Deploying AudioCodes WDE Extension

AudioCodes provides the WebRTC client as a WDE extension which is embedded in in the Genesys WDE. This client extension allows the WDE user (agent) to handle all the agent tasks in one application including the calls.

#### **To deploy the WDE extension:**

- 1. Locate the WDE installation folder, e.g., C:\Program Files (x86)\GCTI\Workspace Desktop Edition\.
- 2. Unzip the file "ac\_webrtc\_wde.zip" to a temporary folder.
- **3.** Run the installation wizard AudioCodes-WDE-WebRTC-Module-Setup.msi, and then follow the installation instructions (see figure below).
  - a. To produce the installation log, use the command line to run the installer and configure the log file output, for example: msiexec /i AudioCodes-WDE-WebRTC-Module-Setup.msi /l\*v myLog.txt.
  - b. Web Client Host Configuration:
    - Web Client Website URL (mandatory): The URL of the WebRTC client.
    - Basic Authentication Username (optional): If the HTTP requires basic authentication to enter the page this value is for username.
    - Basic Authentication Password (optional): If the HTTP requires basic authentication to enter the page this value is for password.

HaudioCodes WDE WebRTC Module Setup -	
Module Configuration	
You can configure the module installation below:	
Path to your copy of Workspace Desktop Edition:	
C:\Program Files (x86)\GCTI\Workspace Desktop Edition\	
Change	
Web Client Host Configuration:	
Web Client Website URL:	
https://webrtcdemo.audiocodes.com/webrtc_dient/	
Basic Authentication Username:	
AudioCodes	
Basic Authentication Password:	
qzXWecVR	
,	
Back Next	Cancel

# 5 Configuring Genesys WebRTC DN Object Endpoint

You can configure Genesys WebRTC DN (Directory Number) objects using various options, as shown in the following example:

## contact = \*

dual-dialog-enabled = false enable-agentlogin-presence = false enable-agentlogin-subscribe = true make-call-rfc3725-flow = 1 refer-enabled = false rfc-2976-dtmf = true session-refresh-interval = 90 sip-cti-control = talk,hold,dtmf transfer-complete-by-refer = false use-register-for-service-state = true

The following table describes the DN objects options:

Option	Values	Description	Comment
authenticate- requests	register, invite	Specifies whether incoming SIP requests are treated with an authentication procedure under the following conditions: The name of the incoming SIP message exists in the list of the	Defined on the DN object, not on the agent ID object
		authenticate- requests	
		<ul> <li>parameter.</li> <li>The option password is configured on the same DN object.</li> </ul>	

#### Table 5-1: DN Objects Descriptions

Option	Values	Description	Comment
contact	<ul> <li>No default</li> <li>SIP URI</li> <li>*</li> </ul>	The contact URI that the SIP Server uses for communication with the endpoint.	If it is defined as "*", the SIP Server uses the contact URI it receives when considering self- registering a WebRTC endpoint.
dual-dialog- enabled	<ul><li>true (default)</li><li>false</li></ul>	Provides the functionality to make consultation calls for endpoints that can only accept one active SIP dialog. Set the value to "false" for endpoints that accept only one active SIP dialog.	Must be set to "false" for the WebRTC client endpoint.
enable- agentlogin- subscribe	<ul> <li>false (default)</li> <li>true</li> </ul>	Enables SIP Server control over the state of an agent based on SIP messages that are received from the agent endpoint. The SIP server can log in or log out an agent, in response to SIP SUBSCRIBE requests. It can also change the availability state for an agent in response to NOTIFY requests. To enable this functionality, set this option to "true". To disable the functionality, set the option to	This must be set to "false" when considering the Genesys Business Continuity feature. Genesys Business Continuity is not supported in the initial release of the Genesys WebRTC client

Option	Values	Description	Comment
		"false".	
make-call- rfc3725-flow	1, 2	Controls which SIP call flow to choose when a call is initiated by a RequestMakeCall. The specified value is equal to the Call Flow number as described in RFC 3725. Only Flow 1 and Flow 2 from RFC 3725 are currently supported. Note: This option is enabled only when the option refer- enabled is set to "false" for that DN. See refer-enabled for more information on this option.	Both flow definitions work with WebRTC client endpoint.
Password	String	Specifies the password for SIP endpoint registration with the local registrar. If it is present, registration attempts are challenged, and the password is verified. If it is not present, the registration is not challenged. The realm for password authentication is configured globally; there is one realm per SIP Server.	Defined on the DN object, not on the agent ID object

Option	Values	Description	Comment
refer-enabled	<ul><li>true (default)</li><li>false</li></ul>	Set this option to "false" for the SIP Server to use a re- INVITE request method when contacting the softswitch.	This must be set to "false" for the WebRTC client endpoint.
rfc-2976-dtmf	<ul> <li>false (default)</li> <li>true</li> </ul>	When this option is set to "true" in a particular DN configuration, the SIP server sends DTMF tones in RFC 2976 format, to that device using the INFO request method when an agent issues a TSendDTMF request.	For the WebRTCclient configured to 'true'
session-refresh- interval	<ul> <li>1800 (default)</li> <li>0, 90-86400</li> </ul>	Specifies (in seconds) how often active calls are checked to see if they are still active. A 0 (zero) value disables this feature (the session refresh mechanism is turned off). Values between 1 and 89 (inclusive) are treated as value 90. This option is used to remove stuck calls that must accumulate, if endpoints terminate calls without sending the appropriate SIP	As needed. The default value is 1800.

Option	Values	Description	Comment
		message.	
sip-cti-control	<ul> <li>No default</li> <li>talk, hold, dtmf</li> </ul>	Specifies the behavior of the DN which represents a SIP endpoint which supports the BroadSoft SIP Extension Event Package. When set to "talk", the TAnswerCall request is issued against the DN, which means that the call is answered remotely by a T-Library client. Otherwise, the TAnswerCall request is not supported. When set to "hold", the endpoint is put on hold by a NOTIFY hold message. Note: "talk, hold, dtmf" could be used simultaneously as a list of comma- separated values.	For 3pcc, depending on actions, consider setting "talk, hold, dtmf".
transfer- complete-by- refer	<ul> <li>false (default)</li> <li>true</li> </ul>	If set to "true", this option enables the SIP server to complete a two-step transfer by sending a REFER message to the party in the primary call. The SIP server uses the same content as in the REFER message that is sent for a single-step transfer.	This must be set to "false" for the WebRTC client endpoint.

Option	Values	Description	Comment
		For this option to work, you must configure refer- enabled on the Trunk DN to "true".	

# 6

# Configuring Citrix Remote Desktop for Integration with WebRTC Client

To enable Citrix remote desktop deployment, the remote Citrix machine must be configured as follows:

- **1.** The following registry modifications must be applied:
  - a. Enable Citrix redirection:
    - Key Path: HKCU\Software\Citrix\HDXMediaStream
    - Key Name: MSTeamsRedirSupport
    - Key Type: DWORD
    - Key Value: 1
  - **b.** Add the Chrome program to the allow list:
    - Key Path: HKLM\Software\WOW6432Node\Citrix\WebSocketService
    - Key Name: ProcessWhitelist
    - Key Type: MULTISZ
    - Key Value: chrome.exe
  - c. (Optional) Configure Citrix logging:
    - Key Path: Computer\HKEY\_CURRENT\_USER\Software\Citrix\HDXMediaStream
    - Key Name: WebrpcLogLevel
    - Key Type: DWORD
    - Key Value: 0

The log files are created in the local machine, not at the remote Citrix machine. For each RTP session, a log directory is created with a timestamp. You can find log files for RTP sessions at the path: %temp%\HdxRTCEngine\<session-timestamp>\

2. Configure Microphone Privacy Settings: In Citrix Desktop Windows, open Microphone Privacy Settings, and then enable microphone usage.

# 7 Configuring SBC WebRTC

The procedures below describe how to configure SBC WebRTC.

# **Creating an IP-to-IP Message Route**

The following describes how to create an IP-to-IP message route.

#### **To create an IP-to-IP Message Route:**

- Open the Message Conditions table (Setup menu > Message Manipulation folder > Message Conditions).
- 2. Click New; the following appears:

Message Conditions		- I ×
GENERAL		
Index	0	
Name	USER MESSAGE	
Condition	Header.Request-URI.MethodType == '13'	Editor
	[₂	
	Cancel APPLY	

- 3. In the 'Name' field, enter "USER MESSAGE".
- **4.** In the 'Condition' field, enter the condition, and then click **APPLY**; the message condition has been created.

Message Conditions (1)		
+ New Edit 💼	Page 1 of 1 → > Show 10 V records per page	
INDEX 🗢	NAME	CONDITION
0	USER MESSAGE	Header.Request-URI.MethodType == '13'
#0[USER MESSAGE]		Edit
GENERAL		_

5. Open the IP-to-IP routing page (Setup menu > SBC folder > Routing > IP-to-IP Routing) and then click New; the following appears:

#0[message ok]					Edit
GENERAL			ACTION		
Name	• message ok		Destination Type	<ul> <li>Internal</li> </ul>	
Alternative Route Options	Route Row		Destination IP Group		View
			Destination SIP Interface	**	View
MATCH			Destination Address		
Source IP Group	Genesys-WebSocket	View	Destination Port	0	
Request Type	All		Destination Transport Type		
Source Username Pattern	*		IP Group Set		View
Source Host	*		Call Setup Rules Set ID	-1	
Source Tag			Group Policy	Sequential	
Destination Username Patt	*		Cost Group		View
Destination Host	*		Routing Tag Name	default	
Destination Tag			Internal Action	<ul> <li>Reply(Response='200')</li> </ul>	
Message Condition	USER MESSAGE	View	Modified Destination User		
Call Trigger	Any				
ReRoute IP Group	• Any	View			

6. From the 'Message Condition' drop-down list, select USER MESSAGE, and then click View; the following appears:

USER MESSAGE	Header.Request-URI.MethodType
USER MESSAGE	
Header.Request-URI.MethodType == '13'	
	• USER MESSAGE

7. In the 'Condition' field, enter the condition, and then click Save.

# Creating a Call (Voice Only) Route

Condition • Header.Request-URI.MethodType == '13'

The following describes how to create a Call (Voice Only) Route.

- > To create a Call route for voice calls with a Message Condition:
- Open the Message Conditions table (Setup menu > Message Manipulation folder > Message Conditions).
- 2. Click New; the following appears:

Messag	ge Conditions		– x
	GENERAL		
	Index	1	
	Name	Genesys with no VideoByPass route	
	Condition	Header.X-AC-Media-Link-Route!exists	ditor
		Cancel APPLY	

- 3. In the 'Name' field, enter "Genesys with no VideoByPass route".
- 4. In the 'Condition' field, enter the condition, and then click **APPLY**; the message condition has been created.
- 5. Open the IP-to-IP routing page (Setup menu > SBC folder > Routing > IP-to-IP Routing) and then click New; the following appears:

[Genesys-WebSocket F	Register]				Edit
GENERAL			ACTION		
Name	Genesys-WebSocket Register		Destination Type	IP Group	
Alternative Route Options	Route Row		Destination IP Group	<ul> <li>Genesys-PBX</li> </ul>	View
			Destination SIP Interface		View
МАТСН			Destination Address		
Source IP Group	Genesys-WebSocket	View	Destination Port	0	
Request Type	All		Destination Transport Type		
Source Username Pattern	*		IP Group Set		View
Source Host	*		Call Setup Rules Set ID	-1	
Source Tag			Group Policy	Sequential	
Destination Username Patt	*		Cost Group		View
Destination Host	*		Routing Tag Name	default	
Destination Tag			Internal Action		
Message Condition	<ul> <li>Genesys with no VideoByPass route</li> </ul>	View	Modified Destination User		
Call Trigger	Any				
ReRoute IP Group	• Any	View			

- 6. In the 'Name' field, enter "Genesys-WebSocket-Register".
- 7. In the 'Alternative Route Options' field, enter "Route Row".
- 8. From the 'Message Condition' drop-down list, select Genesys with no VideoByPass route.
- 9. From the 'Destination Group' drop-down list, select IP Group.

- 10. In the 'Destination IP Group' drop-down list, select Genesys-PBX.
- 11. Click Apply.

# **Creating an IP-to-IP Route for Video Calls**

The following describes how to create an IP-to-IP Route for video calls.

#### To create an IP-to-IP Route for Video Calls:

- 1. Open the IP-to-IP table (Setup menu > SBC folder > Routing > IP-to-IP Routing).
- 2. Click New; the following appears:

Routing						
		Routing Policy	#0 [De	fault_SBCRoutingPolicy]		
GENERAL				ACTION		
Index	28			Destination Type	IP Group	v
Name				Destination IP Group	-	✓ View
Alternative Route Options	Route Row		~	Destination SIP Interface	-	▼ View
				Destination Address		
MATCH				Destination Port	0	
Source IP Group	Any	•	View	Destination Transport Type		v
Request Type	All		~	IP Group Set	-	✓ View
Source Username Pattern	•			Call Setup Rules Set ID	-1	
Source Host	*			Group Policy	Sequential	~
Source Tag				Cost Group	-	✓ View
Destination Username Pattern	•			Routing Tag Name	default	
Destination Host	•			Internal Action		Edit
Destination Tag				Modified Destination User Name		
Message Condition	-	•	View			
Call Trigger	Any		~			
ReRoute IP Group	Any	•	View			

- 3. In the 'Name' field, enter "Genesys-Websocket with Video".
- 4. From the 'Alternative Route Options' drop-down list, select **Route Row**.
- 5. From the 'Source IP Group' drop-down list, select Genesys-WebSocket.
- 6. From the 'Destination Type' drop-down list, select IP Group.
- 7. From the 'Destination IP Group' drop-down list, select Genesys-WebSocket.
- 8. Click Apply.

# **Configuring Call Setup Rules**

The following describes how to configure Call Setup rules.

#### **To configure Call Setup Rules:**

- 1. Open the Call Setup Rules table (Setup menu > SIP Definitions folder > Call Setup Rules).
- 2. Click New; the following appears:

o Rules						
GENERAL			ACTION			
Index	0		Action Subject		Editor	
Name			Action Type	Add	~	
Rules Set ID	0		Action Value		Editor	
Request Type	None	~				
Request Target						
Request Key		Editor				
Attributes To Get						
Row Role	Use Current Condition	~				
Condition		Editor				
		Cancel	APPLY			
	GENERAL Index Name RadueS set ID Request Type Request Type Request Type Astributes To Get Sow Role	GENERAL Index  0 Name   Raukes RiD  Reguest Type  Request Type  Request Type  Request Arget  Request To Get  Sow Rols  Use Current Condition	GENERAL  Index  Index  Index  Index  Index  Index Inde	GENERAL     ACTON       index     0     Action Subject       Name     Action Type       Raukes Rip     0     Action Value       Reguest Type     None     Action Value       Request Ranger     Intervention     Action Value       Request To Get     Intervention     Intervention       Bow Role     Use Current Candition     Intervention	GENERAL     ACTON       Index     0       Name     Index       Rades Set ID     0       Request Type     Acid Confugee       Request Taget     Index       Request Taget     Index       Request Taget     Index       Request Taget     Index       Condoin     Index	GENERAL     ACTION       Index     0       Name     Action Subject       Rades Set ID     0       Bequest Type     Action Yabe       Request Target     -       Request Target     -       Bequest Target     -       Bon Role     Use Current Condition       Condition     Editor

- **3.** Create Setup Rule #0 with the following:
  - a. In the 'Name' field, enter "Check Route Set".
  - **b.** In the 'Rules Set ID' field, enter "5".
  - c. In the 'Row Role' field, enter "Use Current Condition".
  - d. In the 'Condition' field, enter "Header.X-AC-Media-Link-Set!exists, and then click Save.
  - e. In the 'Action Type' field, enter "Run Rules Set".
  - f. In the 'Action Value' field, enter "6".
  - g. Click APPLY.

con octop	- Marco				- ×
	GENERAL		ACTION		
	Index	0	Action Subject		Editor
	Name	Check Route Set	Action Type	Run Rules Set	~
	Rules Set ID	5	Action Value	6	Editor
	Request Type	None	~		
	Request Target				
	Request Key		Editor		
	Attributes To Get				
	Row Role	Use Current Condition	~		
	Condition	Header.X-AC-Media-Link-Setlexists	Editor		
			Cancel APPLY		

The following appears:

Call S	etup Rules (1)										
+ New	Edit Insert 🛧 🕴	â	ter ke	Page 1 of 1   >>	▶ Show <sup>10</sup> ♥ records pe	r page					Q
INDEX	RULES SET ID	NAME	REQUEST TARGET	REQUEST KEY	ATTRIBUTES TO GET	ROW ROLE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	
0	5	Check Route Set				Use Current Condition	Header.X-AC-Media-Link		Run Rules Set	6	

- 4. Create Setup Rule #1 with the following.
  - a. In the 'Name' field, enter "X-Header\_DB\_Set".
  - **b.** In the 'Rules Set ID' field, enter "5".
  - c. In the 'Request Type' field, enter "HTTP GET".
  - d. In the 'Request Target' field, enter "X-Header\_DB\_SET".

- e. In the 'Request Key' field, enter " Header.X-AC-Media-Link-Set+'/'+Header.From.URL+'/ex/3600'".
- f. In the 'Row Role' field, enter "Use Current Condition".
- g. In the 'Action Subject' field, enter " Header.temp".
- h. In the 'Condition' field, enter "Header.X-AC-Media-Link-Set!exists".
- i. In the 'Action Type' field, enter "Add".
- j. In the 'Action Value' field, enter "HTTP.Response.Body".
- k. Click APPLY.
- 5. Create Setup Rule #2 with the following.
  - a. In the 'Name' field, enter "check route".
  - b. In the 'Rules Set ID' field, enter "5".
  - c. In the 'Row Role' field, enter "Use Current Condition".
  - d. In the 'Condition' field, enter " Header.X-AC-Media-Link-Route !exists".
  - e. In the 'Action Type' field, enter "Add".
  - f. In the 'Action Value' field, enter "HTTP.Response.Body".
  - g. In the 'Action Type' field, enter "Exit".
  - h. In the 'Action Value' field, enter "true".
  - i. Click APPLY.
- 6. Create Setup Rule #3 with the following.
  - a. In the 'Name' field, enter "X-AC-Media-Link-Route".
  - b. In the 'Rules Set ID' field, enter "6".
  - c. In the 'Request Type' field, enter "HTTP GET".
  - d. In the 'Request Target' field, enter "X-Header\_DB\_GET".
  - e. In the 'Request Key' field, enter "Header.X-AC-Media-Link-Route".
  - f. In the 'Row Role' field, enter "Use Current Condition".
  - g. In the 'Condition' field, enter "HTTP.Response.Body regex (.\*)(sip:)(.\*)(.@)(.\*)(").\*".
  - h. In the 'Action Subject' field, enter "param.call.dst.User".
  - i. In the 'Action Type' field, enter "Modify".
  - j. In the 'Action Value' field, enter "\$3".
  - **k.** Click **APPLY**.
- 7. Create Setup Rule #4 with the following.
  - a. In the 'Name' field, enter "X-AC-Media-Link-Route".

- b. In the 'Rules Set ID' field, enter "6".
- c. In the 'Row Role' field, enter "Use Previous Condition".
- d. In the 'Action Subject' field, enter "param.call.dst.host".
- e. In the 'Action Type' field, enter "Modify".
- f. In the 'Action Value' field, enter "\$5".
- g. Click APPLY.

# **Configuring IP Groups**

The following describes how to configure IP groups.

#### **To configure IP Groups:**

- Open the IP Groups page for Genesys-WebSocket (Setup menu > Core Entities folder > IP Groups).
- 2. In the 'Call Setup Rules ID', enter "5", and then click APPLY.

Edit #4[Genesys-WebSocket] DefaultSRD GENERAL QUALITY OF EXPERIENCE Name Genesys-WebSocket QoE Profile Topology Location Down Bandwidth Profile Туре • User User Voice Quality Report Disabl Proxy Set IP Profile WebRTC DM MESSAGE MANIPULATION Media Realm DefaultRealmWAN View Inbound Message Manipul... • 1 Internal Media Realm Outbound Message Manip... Contact User Message Manipulation Use... SIP Group Name Message Manipulation Use... Created By Routing Server No Proxy Keep-Alive using IP ... Disabl Used By Routing Server Not Used Proxy Set Connectivity NA SBC REGISTRATION AND AUTHENTICATION Max. Number of Registere... SBC GENERAL Registration Mode User Initiates Registration Classify By Proxy Set Enable User Stickiness Disable Validate Source IP Disable User UDP Port Assignment Disable SBC Operation Mode Not Configured Authentication Mode User Authenticates SBC Client Forking Mode Sequential Authentication Method List CAC Profile SBC Server Authentication ... According to Global Parameter

View

SIP Source Host Name			OAuth HTTP Service		
			Username As Client		
ADVANCED			Password As Client		
Local Host Name			Username As Server		
UUI Format	Disable		Password As Server		
Always Use Src Address	No				
			GW GROUP STATUS		
SBC ADVANCED			GW Group Registered IP A		
Source URI Input			GW Group Registered Status	Not Registered	
Destination URI Input					
SIP Connect	No				
SBC PSAP Mode	Disable				
Route Using Request URI P	Disable				
Media TLS Context	WebRTC	View			
Keep Original Call-ID	No				
Dial Plan		View			
Call Setup Rules Set ID	• 5				
Tags					
SBC Alternative Routing Re		View			
Teams Local Media Optimiz	None				
Teams Local Media Optimiz	DirectMedia				
Teams Local Media Optimiz					
Teams Direct Routing Mode	Disable				

# 8 Troubleshooting Client Connections

The following sections describes troubleshooting client connections.

# **Client Communication with the SBC**

- The first step for troubleshooting SBC connections or registration issues, is to prevent the browser from automatically freezing or discarding the web client to save resources. See Maintaining Web Client Activity When Browser Tab is in Background on page 46.
- It's highly recommended to use a certificate issued by a public CA for the SBC.
- If the certificate is provided internally, the following pre-requisites must be fulfilled:
  - The certificate must contain a FQDN (may also be resolved by internal DNS name) for the SBC
  - FQDN in the Certificate must include SAN (Subject Alternative Name)
  - The browser's trusted root certificates store must contain a certificate in the same trusted certificate chain, as the internally generated certificate

# **Client HTTP Secure Connectivity**

The WebRTC web client may connect to various services via HTTPS. Typically, the browser might reject these service connections if they do not meet proper security requirements.

To resolve HTTPS certificate issues:

Use a valid certificate issued by a public CA.

or

For self-signed certificate, or one issued by the organization's internal CA:

The browser might deem the certificate as invalid, in which case it must be configured to accept it for the specific HTTPS request domain. See below for a detailed example.

- **Example:**
- **1.** The client might show the following connection error when the Agent-Assist service is being used:



- 2. To diagnose and verify the underlying error, open the browser console by opening the webinspector (right-click and then choose **inspect**).
- 3. Select the "console" tab; an error message such as the following might appear:

🕞 🚹   Elements Console Sources Application Performance » 💿 1 🔺 9 📮 1   🌼 🗄 🗙
🗈 🛇   top 🔻   🞯   Filter All levels 🔻   1 Issue: 🗖 1   🏚
not available
not available
19:15:19.700 19:15:19.699 AC>>: loginStateChanged: isLogin=true "login" configurePhone.js:50
19:15:19.700 19:15:19.700 phone>>> loginStateChanged: login <u>configurePhone.js:50</u>
19:15:19.700 CallUIManager: handle register success     CallUIManager.tsx:2713
19:15:19.794 AgentAssistManager: updating configuration parameters: <u>AgentAssistManager.ts:355</u>
19:15:19.794     AgentAssistManager: Agent user update:     AgentAssistManager.ts:356       {"agentUsername":"1003"}
19:15:19.794 AgentAssistManager: Connection update: {"servicePath":"/agentAssist/socket.io","serviceUrl":" <u>https://vaibeta.westeurope.</u> <u>cloudapp.azure.com</u> "}
19:15:19.822 AgentAssistManager: initiate <u>AgentAssistManager.ts:384</u>
19:15:19.822 AgentAssistAsyncTask - connect: starting AgentAssistManager.ts:27
19:15:19.822 AgentAssistManager: connecting to service with <u>AgentAssistManager.ts:390</u> configuration: {"servicePath":"/agentAssist/socket.io","serviceUrl":" <u>https://vaib</u> <u>eta.westeurope.cloudapp.azure.com</u> "}
19:15:19.823 AgentAssistServiceAdapterSocketIO: <u>AgentAssistServiceAdapterSocketIO.ts:19</u> initiating socket io
19:15:19.826 AgentAssistManager: connection status event: <u>AgentAssistManager.ts:114</u> {"connectionStatus":{"connectionState":"connecting"}}
19:15:19.847 AgentAssistAsyncTask - connect: waiting for completion AgentAssistManager.ts:57
8 19:15:20.142 ➤ GET <u>https://vaibeta.westeurope.cloudapp.azure.com/agentAssis</u> <u>polling_js:353</u> <u>t/socket.io/?token=undefined&amp;EIO=4&amp;transport=polling&amp;t=09aVNKH</u> net::ERR_CERT_COMMON_NAME_INVALID
19:15:20.143 AgentAssistServiceAdapterSocketIO: <u>AgentAssistServiceAdapterSocketIO.ts:41</u> socket error event: xhr poll error
19:15:20.144 AgentAssistManager: connection status event: <u>AgentAssistManager.ts:114</u> {"connectionStatus":{"connectionState":"disconnected","lastError":{"message":"xhr poll error"}}}
19:15:20.164 AgentAssistAsyncTask - connect: completed <u>AgentAssistManager.ts:45</u>

**4.** To accept this certificate, copy the request URL to a new tab and navigate there. The following message will appear:



5. Click the Advanced button to show the following:



- 6. Click "Proceed to ......"; the browser accepts the certificate.
- 7. Reloading the client uses the applied configuration, and the connection will succeed.

This page is intentionally left blank.

#### **International Headquarters**

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

**Documentation Feedback:** https://online.audiocodes.com/documentation-feedback

©2024 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-14163

