

PUBLIC DOCUMENT

NetMatch-S CI User Guide SBC Configuration for WEBEX Calling

16-05-2024



Document History

Document released version	Document released date	Notes
1.0	10-01-2023	First Version with NMSCI release 5.8.0-20240111
1.1	19-03-2024	Added chapter 4 (Webex Calling Side configuration) Added chapter 2 (Multi-tenant configuration on SBC side)
1.2	16-05-2024	Added paragraph 3.3 (Caveats)

Abstract

This document is the operator guide relevant to the SBC Configuration in particular oriented to Webex Calling to PSTN interworking.



Table of contents

1	INTRODUCTION	.5
2	MULTI-TENANT CONFIGURATION ON SBC SIDE	.5
3	MAIN ASSUMPTIONS	.6
3.1	Media Bypass option	.6
3.2	Call Transfer scenarios	.6
3.3	Caveats	.6
3.3.1	OPUS support	.6
3.3.2	High Availability	.6
3.3.3	Media Optimisation	.7
3.3.4	Max Concurrent calls	.7
3.3.5	Media Optimisation	7
3.3.6	SBC Maintenance management	7
3.3.7	Reference Software release and hardware requirements	7
3.3.8	Options	7
3.3.9	US Federal Environment	.7
4	WEBEX CALLING SIDE CONFIGURATION	.8
4.1	Multitenancy configuration1	0
5	CONFIGURING ITALTEL'S SBC NETMATCH-S CLOUD INSIDE FOR NO MEDI	Α
BYPA	SS SCENARIOS1	2
5.1	Prerequisites1	2
5.2	Login to the product1	3
5.3	License Management Interface1	3
5.4	Network configuration1	4
5.4.1	Subnet	4
5.4.2	IP Interface Addresses	17
5.5	How to configure DNS Service1	9
5.5.1	How to configure DNS/ENUM Service Manager	20
5.5.2	How to configure DNS/ENUM Interfaces	21
5.5.3	How to configure DNS/ENUM Peers	22
5.5.4	How to configure DNS/ENUM Routing Tables	23
5.6	How to manage Certificate	25
5.6.1	Create Certificate Signing Request (CSR)	25
5.6.2	Update Certificate Signing Request (CSR)	27
5.6.3	Import CA Certificate	29
5.6.4	Create CA Profile	31
5.6.5	Create Trustiness Profile	33
5.7	How to import SIP Manipulations	35
5.8	How to create SIP Profiles	37
5.8.1	Create SIP Profiles for No Media Bypass option	37
5.9	How to create Media Interfaces	39
5.10	How to create Media Domains	12
5.10.1	Create Webex Calling Media Domain for No Media Bypass option	12
5.10.2	Create PSTN Media Domain for No Media Bypass option	13
5.11	How to create SIP Interfaces	5
5.11.1	Create SIP Interface for PSTN side	16
5.11.2	Create SIP Interface for Webex Calling side	17
5.12	How to create SIP Peers and SIP Peer Group on PSTN side	0
5.12.1	Create SIP Peers on PSTN side	50



5.12.2	Create SIP Peer Groups on PSTN side	53
5.13	How to create SIP Domains	55
5.13.1	Create SIP Domain for PSTN side for No Media Bypass option	55
5.13.2	Create SIP Domain for Webex Calling side for No Media Bypass option	61
5.14	How to create Transcoding Rules	65
5.14.1	Create Transcoding Rules from Webex Calling to PSTN	66
5.14.2	Create Transcoding Rules from PSTN to Webex Calling	67
5.15	How to create Interconnection	68
5.15.1	Create Interconnection from PSTN to Webex Calling for No Media Bypass option	69
5.15.2	Create Interconnection from Webex Calling to PSTN for No Media Bypass option	71



1 Introduction

This document shows how to connect Italtel's SBC named NetMatch-S CI (also referred to as simply "the Product" in the remainder of the document) to Webex Calling and refers to the Italtel SBC configuration only. For configuring **Webex Calling** side, the Cisco's cloud-calling product, please refer to <u>https://developer.webex.com/docs/webex-calling-overview</u>.

This document is meant for IT or telephony experts.

2 Multi-tenant configuration on SBC side

One of the allowed configurations foreseen by Cisco is to have an SBC certified with Webex Calling interoperability and hosted in the SP network, whilst providing PSTN interworking to the connected Enterprises' Webex Calling tenants.

The Italtel SBC supports this configuration and offers PSTN connectivity through the SIP trunking functionality, enabling Webex Calling to be used as office phone system.

In this scenario the SBC can be hosted in a Service Provider's network, serving in a centralized way the PSTN voice interworking service for the connected Enterprises' Webex tenants. The SBC can virtualized in "slices" (SIP Interfaces) and each one of them, dedicated to one enterprise, has a dedicated IP Address announced on the public network towards Cisco Webex Calling platform: each instance of SBC, at a configuration level, is split into several interfaces (each one of them with its own "IP:Port" socket and its own TLS certificate) shown externally to the public network.





3 Main Assumptions

3.1 Media Bypass option

The product has been certified for the Non-Media Bypass option scenarios "without ICE media path optimization", refer to Cisco documentation:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/AltDesigns/PA-WbxCall.pdf

3.2 Call Transfer scenarios

As per the Call Transfer Scenarios, the product has been certified without supplementary services SIP REFER enable on NetMatch-S CI, refer to Cisco documentation:

https://help.webex.com/en-us/article/jr1i3r/Configure-Local-Gateway-on-Cisco-IOS-XE-for-Webex-Calling#id_100573

The protocol validation option considered for Refer method should not be present in "Allow" SIP header received from the SBC.

3.3 Caveats

3.3.1 OPUS support

NetMatch-S CI supports OPUS with SHA1_80 encryption. GCM_256 encryption is not supported at the moment

3.3.2 High Availability

The product can be deployed either in High Availability (HA) mode or in a Single (or noHA) mode.

From the perspective of the VNFC's (the subcomponent it is made of), when deployed in HA mode, they can be deployed in 1+1 scheme or in 2N scheme or N+1 (N+M) scheme.

1+1 scheme means 1 is working and the other one is in stand-by.

2N scheme means the component are all in Active mode (i.e. working) and there will be double the number of strictly needed components so that:

- in normal mode the components work with half of their capacity
- if a server fails, half of the components will be working still capable of serving the whole traffic.

Let's call it overprovisioning and this case the overprovisioning is N+N = 2N. This scheme applies to the deployment over a couple of hardware support (e.g. blades or servers).

In a more complex datacenter where each component can be installed with complex antiaffinity rules and thus over numerous blades / servers, the N+1 mode can be adopted, meaning an overprovisioning of 1 component (all Active). The system will be dimensioned so that the traffic can be supported by N subcomponents and can face a single subcomponent failure, with no service disruption. Also N+M scheme can be applied with M as the overprovisioning level.



3.3.3 Media Optimisation

Media Optimisation is under test and will be available next releases.

3.3.4 Max Concurrent calls

The product can be delployed with different sizes and can scale from 50 sessions to 20k+, depending on the needs.

3.3.5 Media Optimisation

The solution is deployed within the Service Provider's network and be used as a multi-tenant SBC solution where customer is offered with PSTN access through a local gateway.

3.3.6 SBC Maintenance management

If the product is deployed in HA mode (which is the most used model), each functionality (SIP, Media, Operation and Maintenance) is redundant and can survive to the fault of the working element. The software upgrade of such a network element can be done with no service disruption, by orchestrating the change of each redundant functions. This way there's no need of putting the network element in maintenance mode (therefore it is transparent to the Wx Calling platform).

Anyway, if needed, the SBC can be put in maintenance mode for any reason, at SIP Interface level (i.e. trunk). That case from the Wx Calling point of view the IP Address exposed by the product will answer to the Options with 503 response message.

Same apply in case of license expiration (503 to any request).

3.3.7 Reference Software release and hardware requirements

The reference release supporting Wx Calling IW is 5.8 and upper.

If the product is deployed as a virtual application in a DC the minimum requirements are 8vCPU and 8GB RAM. The product is scalable to higher performances with different footprints in terms of vResources.

3.3.8 Options

The SBC marks the Webex Calling node as down solely based on the response to OPTIONs and not for the INVITE messages.

3.3.9 US Federal Environment

The platform is not tested for US Federal Environment.



4 Webex Calling side configuration

Before to configure Netmatch SBC, if is necessary to configure the trunk on Control Hub, according to the guidelines in the following link: <u>Configure trunks, route groups, and dial plans for Webex Calling</u> The required steps are:

• Add a "certificate based" Trunk

Add Trunk

Location	
This location is where the trunk is physically co	onnected. To create a new location, visit the Locations page.
HQ - Milano Caldera	$\overline{}$
Name	
TrunkNMS X	
Trunk Type	
Choose the right trunk type for this local gates	way. Learn more on trunk type
Certificate based	
Device Type	
Cisco Unified Border Element	
e Device Type should be "Italtel	Netmatch-S)
Enterprise Session Border Controller (SBC) Add	ress
Select the type and enter an FQDN or SRV addre You must have the domain for your SBC's FQDN,	ess for Webex Calling to reach out to your Enterprise SBC. /SRV claimed or verified [2] before you can use this address. Manage your

• FQDN				
○ SRV				
Hostname *	Domain *		Port *	
ItaltelNMS ×	italtel.com	\checkmark	5061	×
Valid address				
FQDN				
ItaltelNMS.italtel.com:5061				
Maximum number of concurrent calls *				

The trunk is successfully created:

domains

Italtel and Italtel Logo are registered trademarks of Italtel SpA. All contents are Italtel SpA Copyright 2024. All rights reserved. This document is intended for the addressee(s) only and is confidential and/or may contain legally privileged information; it may not be reproduced or distributed in any form without Italtel's prior written consent.



Add Trunk



TrunkNMS Successfully Created.

Visit Route Group page to add trunk(s) to a route group. Visit Locations page to configure PSTN connection to individual locations. Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

Trunk Info

Status 🛈

Unknown

Webex Calling edge proxy address (FQDN)

peering1.eun.sipconnect.bcld.webex.com:5062 peering2.eun.sipconnect.bcld.webex.com:5062 peering3.eun.sipconnect.bcld.webex.com:5062 peering4.eun.sipconnect.bcld.webex.com:5062

Webex Calling edge proxy address (SRV)

eun01.sipconnect.bcld.webex.com

On NMS configuration it will be used the SRV configuration, as Cisco recommends.

The trunk is created and can be associated to a given location on Webex Calling

Calling			
Numbers Virtual Lines	Call Routing Manag	ged Gateways Features	B PSTN Service Setti
Trunk Route Group Dial Pl	ans Verify Call Routing Zon	e Trusted Network Edge	
Trunk SIP trunks provide connect accessed via the Local Gat	vity to a customer-owned PSTN s eway configuration page.	ervice and to an on-premises IP	PBX deployment. These were pre
Name	Location	Trunk Type	In Use
TrunkNMS	HQ - Milano Caldera	Certificate based	No



4.1 Multitenancy configuration

It is possible to configure multitenancy, on Webex Calliing side, in two different ways

• Different IP different FQDN

Ex Customer 1 FQDN : Customer1.italtel.com (IP 138.132.80.80)

Enterprise Session Border Controller (SBC) Address						
Select the type and enter an You must have the domain fo domains	FQDN or SRV address for Webex Calling or your SBC's FQDN/SRV claimed or verifi	to reach out to your Enterprise SBC. ied I before you can use this address. Ma	nage your			
FQDN						
⊖ SRV						
Hostname *	Domain *	Port *				
Customer1	× italtel.com	 ✓ 5061 	×			
✓ Valid address						
FQDN						
Customer1.italtel.com:506	1					

Ex Customer 2 FQDN : Customer2.italtel.com (IP 138.132.80.90)

Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC. You must have the domain for your SBC's FQDN/SRV claimed or verified 🗅 before you can use this address. Manage your domains

Domain *		Port *	
italtel.com	~	5061	×
	Domain *	Domain *	Domain * Port * italtel.com 5061

 Same IP (different port), different FQDN Ex Customer 1 FQDN : Customer1.italtel.com (IP 138.132.80.80:5061)



Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC. You must have the domain for your SBC's FQDN/SRV claimed or verified 🖸 before you can use this address. Manage your domains

FQDN			
⊖ SRV			
Hostname *	Domain *	Port *	
Customer1	× italtel.com	5061	×
Valid address			
FQDN			
Customer1.italtel.com:5061			

Ex Customer 2 FQDN : Customer2.italtel.com (IP 138.132.80.80:5062)

Enterprise Session Border Controlle	er (SBC) Address		
Select the type and enter an FQDN You must have the domain for your domains	or SRV address for Webex Callin SBC's FQDN/SRV claimed or veri	g to reach out to your Enterprise SBC. ified 🕻 before you can use this address. Manage	e your
• FQDN			
SRV SRV			
Hostname *	Domain *	Port *	
Customer2	× italtel.com	 ✓ 5062 	×
Valid address			
FQDN			
Customer2.italtel.com:5062			



5 Configuring Italtel's SBC Netmatch-S Cloud Inside for No Media Bypass scenarios

This section shows how to configure Italtel' SBC for interworking with Webex Calling. Some hints and GUI snapshots relevant to a sample case of configuration are inserted in the document to ease the explanation of the configuration and some fields filling: they are highlighted in **yellow** background or shown in tables. They are based on the example scheme shown below in section 5.1.

5.1 Prerequisites

Before you begin the configuration, make sure you have the following information available for the product you want to pair:

- Public IP address
- SRV Proxy name
- Public certificate
- Low Level Design

Here below an example of LLD is shown for No Media Bypass.





5.2 Login to the product

NetMatch-S CI provides an Advanced Graphical User Interface (GUI) through HTTP/HTTPS connection using a dedicated management address.

Type the URL of NetMatch-S CI (e.g. https://138.132.66.69:8443/NMSCI-WebGui/) in your browser to access the GUI.



Type username and password in the **Authentication** form and click **Sign in** to log into the system.

5.3 License Management Interface

The **License Management Service** enables the product to deliver specific features, referred to the purchase made by the customer on the set of features that the product is able to offer.

After the product has been installed, no default license is available; therefore, the product will not offer any functionality.

To obtain a valid license, follow the steps below:

Click Licenses in the left side menu, to open the License information page.

Netmatch-S CI WebGui	=	😐 PNF 📢	Europe/Berlin	O Mon, 01 Apr 2019 17:06:00	■ 4° 🖻 4	🕽 itaitei 🛛 \varTheta
	Licenses					
Dashboard	Request Code					
al Performance <	pzPIMzMgAgWBiwvMzWJp4MjCFh3LTDIA6Yk98wCOT8VJsZngg5Gc3uBW3Nm0wuJVlzR5gNkai2DdGZdFbc0Z5lidEN1h8dGCNoPUy11DeSSY1QKRTyl4	4nQjhMAyAA6A	AHAAeAw0eDjQ5	eNjiU2PZTGY5GNmoM2dNTcc0n	nMzaczrODbM2fMz6gzpł	Mz6MwC
∴ Alarms <		CarmDoQA IM	ykaxiiviC+vaw1E1		IT ODEZIZNJQUADAADA	AJAAVAR
Licenses	Despense Code					
♀ Network Configuration <	Response Code					
SBC Configuration <						
査 Troubleshooting <						R
🗲 System <	CheckResponseCode SelectRequestCode					
	Current					ø
	// Feature			Expiration	Status	
	1. SIP_SESSION				Disabled	
	2. AUDIO_TU_SESSION			-	Disabled	
	3. REG_CACHE				Disabled	
	4. P_CSCF			-	Disabled	



- Copy Request Code and send it to Point of Contact
- Insert the Response Code, obtained by Italtel reference, in the Response Code Box:

Licenses
Request Code
VYpaMzMgAgWFwvMDWJ25Mz5BhCAH7Ns6Qm3tMANnCIKZZJPB0YMDxcz5MnoJ4ha0Dg5CNjXBOfZXPRNGYXJRj8aFmMtxQ0ZktVVkl5GzAAIAAxAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Response Code
AVSEACO-TRADEORAGETIDE INDATION GRITTE DOUBDICHT PASADAN ANT ANT DAUBE AVEZ DUCTOR THINDED TO INFORMATION OF DE LEGNINGERATOR TRADEORATION AND THE NODE/INTERNAL AND ANT ANT
CheckResponseCode SelectRequestCode

• Click "CheckResponseCode" button and verify the License in now ACTIVE with the following Features MTF, SIP_SESSION, AUDIO_TU_SESSION, TLS, WEBEX_CALLING, SRTP:

#	Feature	Expiration	Status
1.	MTP CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR CONTRACT	2030-01-01 00:59:59	Enabled
2.	SP_SESSION	2030-01-01 00:59:59	1000
З.	AUDIO_TU_SESSION	2080-01-01 00:59:59	100
4.	REG_CACHE	-	Disabled
5.	P_CSCF	-	Disabled
6.	ΠL	-	Disabled
7.	CDR	-	Disabled
8.	Q05	-	Disabled
9.	TUS	2030-01-01 00:59:59	Enabled
10.	ATCF	-	Disabled
11.	MSTEAMS	-	Disabled
12.	ARNT	-	Disabled
13.	SKIP	2080-01-01 00:59:59	Enabled
14.	SDP_SCREENING	-	Disabled
15.	SYS_UM	-	Disabled
16.	SIPREC	-	Disabled
17.	WEEK_OALUNG	2030-01-01 00 59 59	Enabled

5.4 Network configuration

In the product, you have to configure subnets to be used for SIP signaling and media.

5.4.1 Subnet

To configure the subnets, follow the steps below:

• Click **Network Configurations/Subnet** in the left side menu, to open the configuration page:

Italtel and Italtel Logo are registered trademarks of Italtel SpA. All contents are Italtel SpA Copyright 2024. All rights reserved. This document is intended for the addressee(s) only and is confidential and/or may contain legally privileged information; it may not be reproduced or distributed in any form without Italtel's prior written consent.





Then to access the **Create Subnet** view, click on + New button



The Create Subnet view will be displayed:

Create Subnet

a_0 - ETH_VIRT - sip-media_0

We suggest creating one subnet associated to the physical Interface sip-media_0 according to your network design, like in the following examples:

Create Subnet	
Settings	Physical Interface
Name	sip-media 0 ETH VIRT - sip-media 0
subnet_webex	
VLAN	sip-media_1 - ETH_VIRT - sip-media_1
Gateway	
IPv4 135:132:66:1	
Netmask	
265 266 266 128 (/25) ×	

- In the Name field, insert a descriptive (logical) name to be used as subnet.
- In the VLAN field, the dropdown menu on the left-hand side of the VLAN ID field allows you to specify whether the VLAN should be tagged or untagged. If the VLAN is tagged, the ID is used as an actual tag and will be added to each Ethernet frame that is sent on a trunk. Untagged VLANs have ID equal to -1.
- In the Gateway field, Virtual IP address of the gateway to be used to access to the external network. IPv4 or IPV6 addresses are supported.
- In the Gateway field, Netmask for the gateway address. You specify the netmask by choosing the relevant integer value In the dropdown menu on the right-hand side. (The system will automatically display the netmask in dotted form in the left-hand field). When editing the form fields the Gateway box you must insert a valid IP address and the Netmask drop-down menu will propose a choice between all possible valid subnet mask values.



Netmask	
255.255.255.128 (/25)	~
252.0.0.0 (/6)	
254.0.0.0 (/7)	
255.0.0.0 (/8)	
255.128.0.0 (/9)	
255.192.0.0 (/10)	
255.224.0.0 (/11)	
255.240.0.0 (/12)	
255.248.0.0 (/13)	
255.252.0.0 (/14)	
255.254.0.0 (/15)	
255.255.0.0 (/16)	
255.255.128.0 (/17)	
255.255.192.0 (/18)	
255.255.224.0 (/19)	
255.255.240.0 (/20)	
255.255.248.0 (/21)	
255.255.252.0 (/22)	
255.255.254.0 (/23)	
255.255.255.0 (/24)	
255.255.255.128 (/25)	·

• In the **Physical Interface** field, any physical network interface is a named software representation by the operating system of the O&M to the user to enable him to configure the hardware or virtual network device

Name	VLAN	Gateway	Netmask	Physical Interface
subnet_webex	Untagged	138.132.65.1	255.255.255.128 /25	sip-media_0

If everything is correctly configured, upon clicking save the list view with the new subnet will be displayed:

Subnets								+ New
Subnets 1								
Show 10 🗸 entries							Search:	
Name	1 Physical Interface	11 Туре	1 Mode	IT VLAN	1 Netmask	1 Gateway	Actions	
subnet_webex	sip-media_0 - ETH_VIRT	IPV4	UNTAGGED		255.255.255.128	138.132.65.1		۹ 🖊 💼
Showing 1 to 1 of 1 entries								Previous 1 Next

5.4.2 IP Interface Addresses

This section describes how new IP interface addresses can be configured in the product for Media and SIP Interface.

To configure the IP interface Addresses, follow the steps below:

 click IP Interface Addresses in the Network Configuration menu, and then click on button:

Netmatch-S CI WebGui	=	Direct Access	ഥ p32v39u-oam-0	O CET	@ Tue, 23 Jun 2020 16:07:52	4ª ⊠	👤 italtei	0
	IP Interface Address						+ Ne	~
Dashboard	IP Interface Address 0							
al Performance <	No IP Interface Address configured							
🗘 Alarms 🗸								
Licenses								
Network Configuration								
» Subnets								
IP Interface Addresses								
» ICMP Setting								
 TTL Setting 								



Ŷ

• For each subnet created you can select to a choice between all possible valid IP, according to you network design, like in this example:

For Webex Calling side 138.132.65.52:

Create IP Interface Address

Network Interfaces

Subnet

subnet_webex - 138.132.65.1/255.255.255.128 (0@sip-media_0)

Address

138.132.66.62

NAT

DISABLED

For PSTN side 138.132.65.53:

Create IP Interface Address Network Interfaces Subnet sud_pstn - 138.132.66.1/255.255.0 (66@sip-media_1) Address 188.132.66.63

DISABLED	,

A list view with the IP Interface Address will be displayed at the end of the configurations:

IP Interface Add	Iress				+ New
IP Interface Address 🕖					
Show 10 v entries					Search:
Address	11. Subnet Name	11 Netmask	.↓† Gateway	11 Vlan	11 Actions
138.132.65.52	subnet_webex	255.255.255.128/25	138.132.65.1	UNTAGGED	
138.132.65.53	sud_pstn	255.255.255.128/25	138.132.65.1	UNTAGGED	
Showing 1 to 2 of 2 entries					Previous 1 Next



5.5 How to configure DNS Service

This feature allows operators to configure all the resources needed to perform DNS queries to external servers.

In order to access the configuration sub-menu, choose **SBC Configuration > DNS/ENUM Service** link into the side menu:

Netmatch-S CI WebG	Netmatch-S CI WebGui							
Licenses								
Vetwork Configuration								
SBC Configuration	~							
» Media Interfaces								
» Media Domains								
» SIP Interfaces								
SIP Profiles								
» SIP Peers								
» SIP Peer Groups								
SIP Domains								
Transcoding Rules								
» Rerouting Rules								
» Interconnections								
DNS/ENUM Service	*	7						
» Manager								
» Interfaces								
» Peers								
» Routing Tables		J						
» Digit Manipulations								
» SIP Manipulations								
» TLS Certificates								
Emergency Service Nur	n.							



5.5.1 How to configure DNS/ENUM Service Manager

This section describes how to globally enable or disable queries to a DNS or ENUM server in order to access the configuration page, choose **Manager** Link into the sub-menu.

DNS Servers	3		
DNS/ENUM Manage	ers 🚺		
Show 10 • entries			Search:
Name	1 DNS Servers Queries	1 ENUM Servers Queries	11 Actions
internal	true	true	۹ 🖌
Showing 1 to 1 of 1 entrie	S		Previous 1 Next

By choosing the modify action *k*, the appropriate form will be presented in which it is possible to enable or disable the DNS or ENUM queries separately.

You have to disable ENUM feature with false and enable DNS feature (default value true):

Server Settings	
Capabilities	
DNS Servers Queries	
true	~
ENUM Servers Queries	
false	~

To apply the changes, choose the save button.



5.5.2 How to configure DNS/ENUM Interfaces

This section describes how to configure the external interface, in terms of IP Address and Port, to be used for DNS queries.

In order to access the configuration page, choose Interfaces Link into the sub-menu.

The List DNS/ENUM Interfaces, if any configured, is displayed:

DNS/ENUM Interfaces	+ New
DNS/ENUM Interfaces 0	
No DNS/ENUM Interface found	

Click **+** New to create a new Interface, the following view is displayed:

General Settings	
Name	
Division	
Administrative Status	
InService	~
Destanal Saliinaa	
Protocol Settings Subnet	
Protocol Settings Subnet subnet_webex - 138.132.65.1/255.255.128/25 (VLAN 0)	
Protocol Settings Subnet subnet_webex - 138.132.65.1/255.255.128/25 (VLAN 0) Address	
Protocol Settings Subnet subnet_webex = 138.132.65.1/255.255.128/25 (VLAN 0) Address 150.7.2.165.52	
Protocol Settings Subnet subnet_webex - 138:132:65.1/255:255.255.128/25 (VLAN 0) Address 101:132:65:62 Transport Protocol	

- In the **Name** field, insert a descriptive (logical) name to be used for this Interface. This is meant for the user's convenience only and does not affect the queries.
- The administrative status field is used to manage the update operations upon this interface.
- By filling the 'Subnet' and 'Address' fields, select the external address to be assigned to the Interface that can reach a DNS Server (e.g. 138.132.65.52) according to your network design.
- Begin by searching and selecting one of the configured **Subnet**. The subnet list is available through a live search, which allows the dynamic search of the subnet name
- Then choose in the drop-down menu one of the **IP Interface Addresses** configured for the selected subnet

Parameter Value



Name	DNSInt
Administrative status	InService
Subnet	subnet_webex
Address	138.132.65.52

Once the form is completely filled in, click on solution to complete the creation; then the DNS Interfaces list page will be shown.

DNS/ENUM	I Interfaces			+ New
DNS/ENUM Interf	aces 🚺			
Show 10 🗸 entr	es			Search:
Name	1 DNS/ENUM Interface	↓↑ Subnet	1 Administrative Status	11 Actions
DNSint	UDP/138.132.65.52	subnet_teams	✓ InService	۹ 🖊 🔒
Showing 1 to 1 of 1 ent	ries			Previous 1 Next

5.5.3 How to configure DNS/ENUM Peers

This section describes how to configure the parameters for every external DNS server to be interrogated (e.g. Public DNS Server IP = 8.8.8.8).

In order to access the configuration page, choose **Peers** Link into the sub-menu.

The List DNS/ENUM Peers, if any configured, is displayed:

DNS/ENUM Peers	+ New
Dns/Enum Peers 0	
No DNS/ENUM Peer found	

Click on **Here** button to access the form for configuring the DNS peer parameters.

Create DNS/ENUM Peer		
General Settings		Probe Settings
Name		Probe timer (sec.)
dns		30
DNS/ENUM Interface		Waiting Response timer (msec.)
DNSint	~	3000
Control Status		Keep after TTL
UNLOCKED	~	false 🗸
Peer Type		ENUM Probe Selection
DNS	~	
IP Address		DNS Probe Domain
6.8.6.6		
Port Transport Protocol		
53 UDP	~	



The following describe only the information that you have to change or insert:

- Name is a symbolic label to refer to the DNS peer
- IP Address and Port of the remote DNS
- Waiting Response timer is the maximum time waited for a remote server to reply back (expressed in milliseconds)

Parameter	Value
Name	dns
IP Address	8.8.8.8
Waiting Response Timer	3000

Once the form is completed, click on solution to apply the configuration and return to the DNS/ENUM Peer list page.

5.5.4 How to configure DNS/ENUM Routing Tables

This section describes how to configure a group of alternative remote peer referring to the same DNS Server in order to apply load balancing or high availability policies.

In this example only 1 DNS is considered (e.g. 8.8.8.8)

In order to access the configuration page, choose **Routing Tables** Link into the sub-menu.

The List DNS/ENUM Routing Tables, if any configured, is displayed.

Click on + New button to go to the creation page:

Create DNS/ENUM Routing Table

Settings		DNS/ENUM Peer list			
Name		Name		Role	
dins		DNS - dns - 8.8.8.8:53 UDP	~	MASTER ~	-
Zone Validation Mode			+ Add		
GENERIC	~				
DNS/ENUM Routing Table Type					
DNS	~				
Scan Mode					
MASTER_SLAVE	~				

The following describes only the information that you have to change or insert:

Name is a symbolic label to refer to this specific Routing Table (e.g. dns)

Once the form is completed, click on <a>Save button to apply the configuration and return to the DNS/ENUM Routing Tables list page:

Italtel and Italtel Logo are registered trademarks of Italtel SpA. All contents are Italtel SpA Copyright 2024. All rights reserved. This document is intended for the addressee(s) only and is confidential and/or may contain legally privileged information; it may not be reproduced or distributed in any form without Italtel's prior written consent.



DNS/ENUM	Routing Tables				+ New
DNS/ENUM Routing	Tables 1				
Show 10 🗸 entries					Search:
Name	↓li Type	1 Scan mode	1 Dns/Enum Peers	11 Actions	
dns	DNS	FAILOVER_MECHANISM	[M] dns - 8.8.8.63	۹ 🖌 🕯	
Showing 1 to 1 of 1 entrie	s				Previous 1 Next



5.6 How to manage Certificate

The section below shows how to manage a certificate. The certificate is used by the SBC to authenticate the connection with Webex Calling.

5.6.1 Create Certificate Signing Request (CSR)

This mode provides the generation of Certificate Signing Request (CSR) on NetMatch-S CI.

Ne	etmatch-S CI WebGui	
÷	Licenses	
Y	Network Configuration <	
Ø	SBC Configuration ~	
	Media Interfaces	
	Media Domains	
	SIP Interfaces	
	SIP Profiles	
	SIP Peers	
	SIP Peer Groups	
	SIP Domains	
	Transcoding Rules	
	Rerouting Rules	
	Interconnections	
	DNS/ENUM Service <	
	Digit Manipulations	
	SIP Manipulations	
»	TLS Certificates	
	Emergency Service Num.	



Certificate Signing Request General General General Certificate Signing Request General Genera	S Certificates			+ Import Certificate	+ Import CA Certifica	ate
Certificate Signing Request C Cancel < Same				+ Create Self-Sigr	ed 🕂 Request CS	SR
General Extensions Security	ı Request			< Cancel	✓ Save	
		General Extensions	Security			
Name (Identifier) Authority Info Access Key Encryption Algorithm		Authority Info Access	Key Encryption Algorithm			
relisional PBE SHA13DES			PBE SHA1 3DES			
Key Size			Key Size			
Subject Information SIP Extensions 2048		SIP Extensions	2048			
Common Name (CN) Subject Alternative Names Signiture Algorithm		Subject Alternative Names	Signiture Algorithm			
remold table core - SHATwithRSA		nms02 itsitei eem	- SHA1withRSA			
Organizational Unit (OU) + Add		+ Add				
Reserve						
Organization (O)						
Locality (L)						
Mano						
State (S)						
MA CONTRACTOR OF CONTRACTOR						
Country (C)						
r de la companya de l						
Email Address (E)						
Password						

The fields to fill in:

General

name = the name of the certificate. (e.g., cert-webex-ok)

Subject Information

Common Name (CN) = User Certificates: You should enter the person's full name. Mandatory, it cannot be null. (e.g.nms02.italtel.com)

Organizational Unit (OU) = the Organizational Unit field can be used to differentiate between different divisions within an organization. Mandatory, it cannot be null. (e.g. Research)

Organization (O) = the name you specify for the Organization field should be the legal name for your organization that is registered with the appropriate city, state, or country/region authority. Mandatory, it cannot be null. (e.g. Italtel)

Locality (L) = the Locality field denotes the city that the organization resides in. Mandatory, it cannot be null. (e.g. Milano)

State (S) = the State or Province field specifies where the organization is physically located. Mandatory, it cannot be null. (e.g. Italia)

Country (C) = requires country/region code. Mandatory, 2 or 3 specific characters of a country/region. (e.g. IT)

EmailAddress (E) = the e-mail of the person who generate the request. Mandatory, has to present e-mail specific characters. (e.g. <u>mario.rossi@italtel.com</u>)

Password = password. Mandatory, composed at least of six characters

General Extensions (e.g. Italtel12345)

Italtel and Italtel Logo are registered trademarks of Italtel SpA. All contents are Italtel SpA Copyright 2024. All rights reserved. This document is intended for the addressee(s) only and is confidential and/or may contain legally privileged information; it may not be reproduced or distributed in any form without Italtel's prior written consent.



Authority Info Access (AIA) = the authority information access extension indicates how to access information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data. Optional.

SIP Extensions

Subject Alternative Name (SAN) = the subject alternative name extension allows identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate. Defined options include an Internet electronic mail address, a DNS name, an IP address, and a Uniform Resource Identifier (URI). Mandatory. (e.g. nms02.italtel.com)

This value is the SBC FQDN, the same value will be set into the ' Forced Local FQDN ' in WEBEX CALLING SIP DOMAIN

Security settings

In this panel, the used security settings are shown, as Key Encryption Algorithm, Key Size and Signature Algorithm.

At the End click on Save button

Click to download the CSR file, as seen in figure below:

Tls Certifica	tes 📵										
Show 10	✓ entries							Sea	rch:		
Name 💵	Type ↓†	Subject	Ĵ↑	Issuer	ţţ	\ F	/alid ⁼rom	ļĵ	Valid Until	.↓↑	Actions
cer-webex- ok	Certificate Signing	CN=nms02.italtel.com, C=IT, ST=Italtel, L=Milano, E=massimiliano.nucita@italtel.com, OU=Research, O=Italtel		-		-			-		<u></u> ± ★ 🛍

Then send the CSR to the Certification Authority

5.6.2 Update Certificate Signing Request (CSR)

Then once received the signed certificate, the user can update the CSR clicking the update-icon



Then import cert-webex-ok,pem (signed certificate received):



Upload Signed Certificate for: cer-webex-ok

Upload Signed Certificate

Certificate file

Scegli file cert-webex-ok.pem

Please use PEM format

Upload

At the end, you have a list like this:

Vanage TLS Certificates					ificate	🕂 İm	port C	A Certificate
				+ Create	e Self-	Signed	+ F	equest CSR
TIs Certificates 🕐								
Show 10 v entries				Sea	rch:			
Name <u>↓</u> ≜ Type ↓† Subject	ĴĴ	Issuer	ĴĴ	Valid From	11	Valid Until	11	Actions
cert-webex- ok CN=nms02.ltaitei.com, C=, ST=, L=, E=, OU=, O=		CN=R3, C=US, ST=, L=, E=, OU=, O=Let's Encrypt		Fri Oct 2 14:59:23 CEST 20	7 23	Thu Jan 2 13:59:22 CET 2024	25 4	±



5.6.3 Import CA Certificate

This mode provides importing of a Certification Authority (CA) certificate for NetMatch-S CI and Webex Calling.

Netmatch-S CI WebGui					
÷	Licenses				
Y	Network Configuration <				
Ø	SBC Configuration ~				
	Media Interfaces				
	Media Domains				
	SIP Interfaces				
	SIP Profiles				
	SIP Peers				
	SIP Peer Groups				
	SIP Domains				
	Transcoding Rules				
	Rerouting Rules				
	Interconnections				
	DNS/ENUM Service <				
	Digit Manipulations				
	SIP Manipulations				
»	TLS Certificates				
	Emergency Service Num.				

Manage TLS Certificates + Import CA Certificate
+ Create Self-Signed + Mequest CBM



Upload a new CA certificate

Upload new certificate				
Name				
ISRG				
Certificate file				
Scegli file ISRG.pem				
Please use PEM format				
Upload				

The fields to fill in:

Name = the name of the certificate. (e.g. ISRG)

Certificate file = the CA certificate file .pem (e.g. ISRG.pem)

Upload a new CA certificate

Upload new certificate					
Name					
IdenTrust					
Certificate file					
Scegli file idenTrust.pem					
Please use PEM format					
Lipload					

The fields to fill in:

Name = the name of the certificate. (e.g. IdenTrust)

Certificate file = the CA certificate file .pem (e.g. IdenTrust.pem)



Upload a new CA certificate

Upload new certificate

Name
letsEncrypt
Certificate file
Scegli file letsEncrypt.pem
Please use PEM format

Upload

The fields to fill in:

Name = the name of the certificate. (e.g. letsEncrypt)

Certificate file = the CA certificate file .pem (e.g. letsEncrypt.pem)

At the end, you have a list like this:

idenTrust	Certification Authority	CN=IdenTrust Commercial Root CA 1, C=US, ST=, L=, E=, OU=, O=IdenTrust	CN=IdenTrust Commercial Root CA 1, C=US, ST=, L=, E=, OU=, O=IdenTrust	Thu Jan 16 19:12:23 CET 2014	Mon Jan 16 19:12:23 CET 2034	±
ISRG	Certification Authority	CN=ISRG Root X1, C=US, ST=, L=, E=, OU=, O=Internet Security Research Group	CN=ISRG Root X1, C=US, ST=, L=, E=, OU=, O=Internet Security Research Group	Thu Jun 04 13:04:38 CEST 2015	Mon Jun 04 13:04:38 CEST 2035	± 前
letsEncrypt	Certification Authority	CN=R3, C=US, ST=, L=, E=, OU=, O=Let's Encrypt	CN=ISRG Root X1, C=US, ST=, L=, E=, OU=, O=Internet Security Research Group	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025	<mark>⊥</mark> 前

Note: If you have more files of root-ca provided by CA, please import all and then create a CA Profile.

5.6.4 Create CA Profile

This mode allows you to the create a Certification Authority Profile with list of (CA) for NetMatch-S CI and Webex Calling.



Netmatch-S CI WebGui

v

ß	SBC	Configur	ation

- » Media Interfaces
- » Media Domains
- » SIP Interfaces
- » SIP Profiles
- » SIP Peers
- » SIP Peer Groups
- » SIP Domains
- » Transcoding Rules
- » Rerouting Rules
- » Interconnections
- DNS/ENUM Service
- » Digit Manipulations
- » SIP Manipulation
- » TLS Certificates
- » TLS Profile
 - » CA Profiles
- » Trustiness Profile Rule
- » Emergency Service Num.
- » AR&NT

The following describes the information that you have to create a new CA Profile:

Click on **+**New to create a new CA Profile; then the following view is displayed:





And then with 🚬 insert in list the CA that you need to insert in you CA Profile

The following describes only the information that you have to change or insert to create a new CA Profile.

In the **Name** field, insert a descriptive (logical) name to be used for this CA profile. This name will be used to associate the SIP Interface (e.g. webEx-CA-list).

At the end, you have a list like this:

CA Profiles	+ New
CA Profiles 1	
Show 10 v entries	Search:
Name	11 Actions
webEx-CA-list	۹ 🖊 🛢
Showing 1 to 1 of 1 entries	Previous 1 Next

5.6.5 Create Trustiness Profile

This mode allows you to insert a new trustiness rule that can be formed by the admitted domain, the admitted CA or both.

SBC Configuration Media Interfaces Media Domains Media Domains SIP Interfaces SIP Profiles SIP Profiles SIP Peers SIP Peer Groups SIP Domains Transcoding Rules Rerouting Rules Interconnections DNS/ENUM Service Digit Manipulations TLS Certificates TLS Profile > Trustiness Profile Rules AR&NT	Netmatch-S CI WebGui
 Media Interfaces Media Domains SIP Interfaces SIP Profiles SIP Peers SIP Peer Groups SIP Domains Transcoding Rules Rerouting Rules Interconnections Interconnections IDNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile AR Profiles Trustiness Profile Rules Emergency Service Num. AR&NT 	SBC Configuration
 Media Domains SIP Interfaces SIP Profiles SIP Peers SIP Peer Groups SIP Domains Transcoding Rules Interconnections Interconnections DNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile AR Profiles Trustiness Profile Rules Emergency Service Num. AR&NT 	» Media Interfaces
 » SIP Interfaces » SIP Profiles » SIP Peers » SIP Peer Groups » SIP Domains » Transcoding Rules » Transcoding Rules » Interconnections © INS/ENUM Service < » Digit Manipulations » SIP Manipulations » TLS Certificates » TLS Profile > Marigues Profile Rules » Trustiness Profile Rules » Emergency Service Num. » AR&NT 	» Media Domains
 » SIP Profiles » SIP Peers » SIP Peer Groups » SIP Domains » Transcoding Rules » Transcoding Rules » Transcoding Rules » Interconnections » Interconnections Ø DNS/ENUM Service > DNS/ENUM Service > DIgit Manipulations » SIP Manipulations » TLS Certificates » TLS Profile > CA Profiles » Trustiness Profile Rules » Emergency Service Num. » AR&NT 	» SIP Interfaces
 » SIP Peers » SIP Peer Groups » SIP Domains » Transcoding Rules » Rerouting Rules » Rerouting Rules » Interconnections © DNS/ENUM Service < » Digit Manipulations » SIP Manipulations » TLS Certificates » TLS Profile > CA Profiles » Trustiness Profile Rules » Emergency Service Num. » AR&NT 	» SIP Profiles
 » SIP Peer Groups » SIP Domains » SIP Domains » Transcoding Rules » Rerouting Rules » Interconnections Ø DNS/ENUM Service Ø DIGIt Manipulations » SIP Manipulations » TLS Certificates » TLS Profile * CA Profiles » Trustiness Profile Rules » Emergency Service Num. » AR&NT 	» SIP Peers
 SIP Domains Transcoding Rules Rerouting Rules Interconnections DNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile ARAProfiles Emergency Service Num. AR&NT 	» SIP Peer Groups
 Transcoding Rules Rerouting Rules Interconnections DNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile AR&NT 	» SIP Domains
 Rerouting Rules Interconnections DNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile AR&NT 	» Transcoding Rules
 Interconnections DNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile CA Profiles Trustiness Profile Rules Emergency Service Num. AR&NT 	» Rerouting Rules
 DNS/ENUM Service < Digit Manipulations SIP Manipulations TLS Certificates TLS Profile CA Profiles Trustiness Profile Rules Emergency Service Num. AR&NT 	» Interconnections
 » Digit Manipulations » SIP Manipulations » TLS Certificates » TLS Profile » CA Profiles » Trustiness Profile Rules » Emergency Service Num. » AR&NT 	DNS/ENUM Service <
 » SIP Manipulations » TLS Certificates » TLS Profile » CA Profiles » Trustiness Profile Rules » Emergency Service Num. » AR&NT 	 Digit Manipulations
 TLS Certificates TLS Profile CA Profiles Trustiness Profile Rules Emergency Service Num. AR&NT 	» SIP Manipulations
 TLS Profile CA Profiles Trustiness Profile Rules Emergency Service Num. AR&NT 	» TLS Certificates
CA Profiles Trustiness Profile Rules Emergency Service Num. AR&NT	» TLS Profile
 Trustiness Profile Rules Emergency Service Num. AR&NT 	» CA Profiles
 Emergency Service Num. AR&NT 	» Trustiness Profile Rules
» AR&NT	» Emergency Service Num.
	» AR&NT



The following describes the information that you have to create a new Trustiness Profile Rule:

Click on **+** New to create a new Trustiness Profile; then the following view is displayed:

Create Trustiness Profile Rule			✓ Cancel ✓ Save
Settings	Rules		
Name			Q +
webex			
	Allowed Domains	Allowed CAs	
	eun01.sipconnect.bold.webex.com	IdenTrust	-

With + Add insert Domain and CA of Webex Calling allowed in your Trustiness Profile

The following describes only the information that you have to change or insert to create a new Trustiness Profile.

In the **Name** field, insert a descriptive (logical) name to be used for this Trustiness profile. This name will be used to associate the SIP Interface (e.g. webex).

In the **Allowed Domains** field, insert a Name of the allowed domain (e.g. eun01.sipconnect.bcld.webex.com)

In the **Allowed CAs** field, insert a Name of the allowed Certification Authority (e.g. IdenTrust)

Click <a>Save to confirm the creation of Trustiness Profile.

Parameter	Value
Name	webex
Allowed Domains	eun01.sipconnect.bcld.webex.com
Allowed CAs	IdenTrust

At the end for example you have:

Trustiness Profiles		+ New
Trustiness Profile Rule 1		
Show 10 v entries		Search:
Name	1 Number of Rules	↓↑ Actions
webex	1	۹ 🖊 📋
Showing 1 to 1 of 1 entries		Previous 1 Next



5.7 How to import SIP Manipulations

For those scenarios, where different equipment vendors provide different SIP implementations or where particular SIP profiles are required by the interconnected Service Providers/Enterprises, the product provides the SIP Manipulation feature to ensure the adaptation of SIP signalling interfaces.

The product is able to insert, delete or modify any SIP field in the received SIP messages, before forwarding them.

The access to the SIP Manipulation functionality is available through the **SIP Manipulations** item inside the **SBC Configuration** menu. Choosing this one, the list of the already available Sip Manipulations rules is displayed, if any.

Netmatch-S CI WebGui			
÷	Licenses		
Y	Network Configuration <		
Ø	SBC Configuration ~		
>	Media Interfaces		
*	Media Domains		
*	SIP Interfaces		
	SIP Profiles		
»	SIP Peers		
*	SIP Peer Groups		
>	SIP Domains		
>	Transcoding Rules		
≫	Rerouting Rules		
۲	Interconnections		
	DNS/ENUM Service <		
>	Digit Manipulations		
*	SIP Manipulations		
*	TLS Certificates		
	Emergency Service Num		



A Sip manipulation rule can also be imported into the SBC.

In this configuration is necessary to import these Sip Manipulation:

- sipManipulation_userPhoneWebex.json
- sipManipulation_userPhone.json
- sipManipulation_outPstnWebex.json

sipManipulation userPhoneWebex.json sipManipulation userPhone.json sipManipulation_userPhoneWebex.json

💿 Apri							×
	uesto PC > Desktop >				v Ŭ 0	erca in Desktop	م
Organizza 👻 Nuova ci	artella					***** *	. ?
sip.i4web20200 ^	Nome	Ultima modifica	Тіро	Dimensione			-
OneDrive	santo	11/06/2020 14:32	File	6 KB			
	ServerCertificate.pem	15/07/2020 14:45	File PEM	3 KB			
lesto PC	🗋 signal	17/06/2020 16:22	File	12 KB			
📘 Desktop	sipManipulation_AccessIN.json	16/06/2020 11:05	File JSON	2 KB			
🗎 Documenti	sipManipulation_OPTION_IN (1).json	16/06/2020 11:05	File JSON	2 KB			
🔈 Download	sipManipulation_OPTION_IN.json	10/06/2020 13:36	File JSON	2 KB			
http://www.agini	sipManipulation_OPTION_OUT (1).json	16/06/2020 11:06	File JSON	4 KB			
h Musica	sipManipulation_OPTION_OUT.json	10/06/2020 13:36	File JSON	5 KB			
Occetti 3D	sipManipulation_userPhone (1).json	23/07/2020 14:46	File JSON	2 KB			
Midaa	sipManipulation_userPhone.json	17/07/2020 10:46	File JSON	2 KB			
Video	tcp22	27/04/2020 17:26	File	103 KB			
Disco locale (C:	TEAMS-PSTN.txt	23/07/2020 13:39	Documento di testo	44 KB			
🤳 Disco locale (D	TEAMS-PSTN-HoldResumeTEAMS.txt	05/06/2020 17:14	Documento di testo	35 KB			
🐦 piredda (\\icsa\	🚾 tes_trace_11910.rar	15/07/2020 17:42	Archivio WinRAR	63 KB			
A Poto	ses_trace_11920.rar	15/07/2020 17:07	Archivio WinRAR	16 KB			,

Then, if the operation is successful, the Sip Manipulation appears in the list and you can use them subsequently in a Sip Domain and Sip Interface configuration, if needed.

SIP Manipulations				New name or suffix	↑ Import	Export All	+ New
SIP Manipulations							_
Show 10 🗸 entries					Search:		
Name	11 Description	11 Xml	1 Actions				
replaceln	in Sip Interface MSTEAMS	sipScreaningTrigger_replaceIn.xml	+ 9. 🖊 📋				
userPhone	Insert user=phone	sipSorveningTropper_userPhone.xml	+ Q 🖊 🛎				

Italtel and Italtel Logo are registered trademarks of Italtel SpA. All contents are Italtel SpA Copyright 2024. All rights reserved. This document is intended for the addressee(s) only and is confidential and/or may contain legally privileged information; it may not be reproduced or distributed in any form without Italtel's prior written consent.

Apri

Annulla


5.8 How to create SIP Profiles

A SIP Profile is a set of SIP protocol settings that is possible to associate to a SIP domain. These settings include standard SIP timer configuration and White/Blacklist management on both SIP Methods and SIP headers. It is possible to associate the same SIP profile to different SIP domains. In order to create a SIP Profiles, select **SBC Configuration >> SIP Profiles** in the main menu:

Ne	etmatch-S CI WebG	Gui	
e.	Licenses		
¥	Network Configuration	<	
Ø	SBC Configuration	~	
	Media Interfaces		
	Media Domains		
	SIP Interfaces		
»	SIP Profiles	$\langle =$	
	SIP Peers		
	SIP Peer Groups		
	SIP Domains		
	Transcoding Rules		
	Rerouting Rules		
	Interconnections		
8	DNS/ENUM Service	<	
	Digit Manipulations		
	SIP Manipulations		
	TLS Certificates		
	Emergency Service Nu	m.	

5.8.1 Create SIP Profiles for No Media Bypass option

The following describes the information that you have to change or insert to create a Sip Profiles for No Media Bypass options:

Click on **to create a new SIP profile; then the following view is displayed:**



Create SIP Profile				< Canon	10
Settings		Incoming Managed	SIP Methods	Incoming Managed SIP Headers	_
None		Cares			
and Million			+A11	Filter Modally	
		Filter Modelity		using SYSTEM_DEFAULTS	
SIP Timers		Base Lat			
Liner C				Protocione Manusco d RAD Line Man	
110	040	Outersine Managed	CID Mathewie	Outgoing Managed SIP Headers	
Dates 0		Colgony mereges	or monus	♥ kiti	
32	1410	Caret		Filter Modally	
			◆ A.81	using SYISTEM_DEFAULT8	
33000	mar	Filter Modelity			
		Base Lat			
1898 11 540					
		Enable Notification 8	Events		
timer tz					
			₩ A8		
VGW options					
Timer wait response from vGW					
206		msec			
Timer wait response from protected vGW					
200		msec			
Rerouting trigger responses					
49 					
1					
-					
♣ Ada					
Kerculung Malch Type					
ORECT		v.			

The following describes only the information that you have to change or insert to create a new SIP Profile.

In the **Name** field, insert a descriptive (logical) name to be used for this SIP profile. This name will be used to associate the SIP profile during the configuration of a SIP Domain

The **Incoming Managed SIP Methods** and **Outgoing Managed SIP Methods** sections allow configuring separately two list of methods to be accepted or rejected in the corresponding directions of SIP messages. A **Filter Modality** (Disabled / Blacklist / Whitelist) is associated to each methods list to define the application criteria.

To add SIP methods to the list, click +Add and select the chosen method from the drop-down menu.

For each list is possible to set the Filter Modality.

SIP Headers in a Blacklist, as well as those outside a Whitelist, will be removed from SIP message if not mandatory.

In VGW options Tab set 200 msec in Timer wait response from vGW and in Timer wait response from protected vGW (this value is used for the duration of SIP T1 when Peer is resolved by DNS), the Rerouting Match Type in set to DIRECT for rerouting on value of these Rerouting trigger responses: 408, 3xx, 5xx if add

Parameter	Value	
Name	noreferWebex	





Incoming Managed SIP Methods	REFER
Filter modality	Blacklist
Outgoing Managed SIP Methods	REFER
Filter Modality	Blacklist
Timer waits response from VGW	200
Timer waits response from protected VGW	200
Rerouting Match Type	DIRECT
Rerouting Trigger Responses	408, 3, 5

Click Save to confirm the creation of SIP Profile.

At the end the following view is displayed:

SIP Profiles												+ New
Sip Profiles (
Show 10 🗸 entries											Search:	
Name 🕸	Timer T1 (msec)	1 Timer T2 (sec)	1 Timer C (sec)	1 Timer D (sec)	1 Timer H (msec)	1 IN Methods	UT Methods	IN Headers	OUT Headers	1 Notification Events	1 VGW options	11 Actions
norefer	500	40	180	32	32000	REFER	REFER	ALLOW ALL	ALLOW ALL		SET	۹ 🖊 💼
noreferWebex	500	40	180	32	32000	REFER	REFER	ALLOWALL	ALLOWALL		SET	۵ 🗸 🗈
refer	500	40	180	32	32000	ALLOW ALL	INFO	ALLOW ALL	ALLOW ALL		SET	۹ 🖊 🗎
SYSTEM_DEFAULTS	500	40	180	32	32000	ALLOW ALL	ALLOW ALL	ALLOW ALL	ALLOW ALL			
Showing 1 to 4 of 4 entries												Previous 1 Next

For Methods and Headers columns, the green character means "allow" (Whitelist modality) while the red character means "reject" (Blacklist modality).

5.9 How to create Media Interfaces

In order to create a Media Interface, select **SBC Configuration >> Media Interfaces** in the main menu:





You have to configure 2 media interfaces.

Click on **+** New to create a first new Media Interface the following view is displayed:

Media Interface for Webex Calling side:

As reported in Cisco Port Reference for Webex calling (<u>https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Webex-Calling</u>) the media ports on local gateway must be configured **from port 8000 to 48198**.

Create Media Interface

Settings	Network Interfaces
Name	Subnet
media_north_webex	subnet_webex 138.132.65.1/255.255.255.128/25 (VLAN 0) ·
UDP Port Range (first-last)	Address
10000 - 12001	100.102.05.52



Media Interface for PSTN side:

Create Media Interface	
Settings	Network Interfaces
Name	Subnet
media_south_pstn	subnet_teams - 138.132.65.1/255.255.255.128/25 (VLAN 0) -
UDP Port Range (first-last)	Address
10000 - 12001	108 192 66 63

The **Name** field is a label identifying the Media Interface to recall it during the configuration of the SIP Interface.

The **UDP Port Range** field is used to assign a range of UDP ports to the media interface.

In the '**Network Interfaces**' panel, select the external address to be assigned to the Media Interface between those who are provided according to your network interface configurations.

First, you search and select one of the configured **Subnet** as follow; the list is available through a useful live search, which allows the dynamic search of the subnet name.

Then choose in the drop-down menu one of the **IP Interface Addresses** configured for the selected subnet.

Name	First UDP Port	Last UDP Port	Subnet	Address
media_north_webex	10000	12001	subnet_webex	138.132.65.52
media_south_pstn	10000	12001	subnet_pstn	138.132.65.53

Click <a>Save to confirm the creation of Media Interface.

At the end, for example we have:

Media Interfaces				+ New
MediaInterfaces 2				
Show 10 🗸 entries				Search
Name	Ilà Subnet	I Ip Address	.IT Port range	1 Actions
media_north_webex	subnet_webex	138 132 65 52	10000 - 12001	۹ \min
media_south_pstn	subnet_teams	138.132.65.53	10000 - 12001	Q. 🔳
Showing 1 to 2 of 2 entries				Provious 1 Next



5.10 How to create Media Domains

In order to create a Media Domain, select **SBC Configuration >> Media Domains** in the main menu:

Ne	etmatch-S CI Web	Gui	
÷	Licenses		
Y	Network Configuration	<	
ß	SBC Configuration	~	
	Media Interfaces		
»	Media Domains	\leftarrow	
	SIP Interfaces		
	SIP Profiles		
	SIP Peers		
	SIP Peer Groups		
	SIP Domains		
	Transcoding Rules		
	Rerouting Rules		
	Interconnections		
	DNS/ENUM Service	<	
	Digit Manipulations		
	SIP Manipulations		
	TLS Certificates		

» Emergency Service Num.

You have to configure 2 media Domains for Team side and PSTN side.

Click on **Here** to create a new Media Domain; the following view is displayed:

5.10.1 Create Webex Calling Media Domain for No Media Bypass option

The following describes the information that you have to change or insert to create Webex Calling Media Domain for No Media Bypass options:



Create Media Domain

Settings		
-		
Name		
dom webex		
		-
Media Release		
DISABLED	~	,
SRTP		
MANDATORY	×	
lceType		
DISABLED	Ŷ	r.

This section includes configuration parameters for media domain.

The **Name** field is a label identifying the Media Domain to recall it during the configuration of the SIP Interface.

In case of **SRTP** feature enabled, it is possible to configure the SRTP Type field.

The Direct Routing Interface requires the use of SRTP only, so you need to configure the SBC to operate the same way.

Name	SRTP	
dom_webex	MANDATORY	

5.10.2 Create PSTN Media Domain for No Media Bypass option

The following describes the information that you have to change or insert to create PSTN Media Domain:

Create Media Domain

Settings	
Name	
dom_south_ostn	
Media Release	
DISABLED	~
SRTP	
DISABLED	~
ІсеТуре	
DISABLED	~

This section includes configuration parameters for media domain.

The **Name** field is a label identifying the Media Domain to recall it during the configuration of the SIP Interface.



Name					
dom_south_pstn					

At the end for example you have 2 Media Domains

Media Domains					+ New
MediaDomains 4					
Show 10 v entries				Se	arch:
Name	11 SRTP	1 Media Release	.↓† Ice Type	11 Actions	11
dom_sud_pstn	DISABLED	DISABLED	DISABLED		۹ 🗡 📋
dom_webex	MANDATORY	DISABLED	DISABLED		۹ 🖊 🗎
SYSTEM_DEFAULTS	DISABLED	DISABLED	DISABLED		٩
Showing 1 to 4 of 4 entries					Previous 1 Next



5.11 How to create SIP Interfaces

This section shows how to configure a SIP Interface. A SIP Interface defines a listening port and protocol type (UDP, TCP, or TLS) for SIP signalling traffic on a specific logical IP network interface.

In order to create a SIP Interface, select **SBC Configuration >> SIP Interfaces** from the main menu:



Click **Them** to create a new SIP Interface: the following view is displayed:



reate SIP Interface		Canal ZSru
General Settings	SIP Settings	Security Control List
Name	Subnet	Automatic SCL
ste_south_este	subnet_seams - 158 198 65 1-466 266 266 108346 (VLAN +	fahe 🗸
Interface Type	Address	* Add
Generic 👻	138.132.66.68	Security Control Type
Administrative Status	Transport Protocol	DisABLED V
InService v	UDP 👻	
6IP Domain Inbound Policy Type	Port	0
All traffic V	5060	SIP Manipulations
	TLS	Inbound rule
	false 🗸 🗸	None Y
	Enable Check MTU	Outbound rule
	false 🗸 🗸	cutPsinWebex
	Cause Q.850	<u>-</u>
	0 DISADI FD -	
	Emergency Service management	
	false 🗸	
>		· · · · · · · · · · · · · · · · · · ·

5.11.1 Create SIP Interface for PSTN side

The following describes the information that you have to change or insert to create a sip Interface on PSTN side:

In the Name field, insert a descriptive (logical) name to be used for this SIP Interface.

In the 'SipSetting' panel, select the external address to be assigned to the Sip Interface, between those provided according to your network interface configurations.

First, search and select one of the configured **Subnet** as follow; the list is available through a useful live search, which allows the dynamic search of the subnet name.

Then choose in the drop-down menu one of the **IP Interface Addresses** configured for the selected subnet.

Then add SIP Manipulation in Outbound Rule, choosing in the drop-down menu.

Click **Save** to confirm the creation of Sip Interface.

Parameter	Value
Name	sip_south_pstn
Subnet	subnet_pstn
Address	138.132.65.53
Transport	UDP
SIP Manipulation Outbound	outPSTNwebex

At the end for example you have:

SIP Interfaces						+ New
SIP Interfaces						
Show 10 🗸 entries						Search:
Name	Interface	↓† Subnet	J† TLS	1 TLS Port	1 Administrative Status	1 Actions
sip_south_pstn	UDP/138.132.65.53:5060	subnet_teams	false	-	✓ InService	۹ 🖊 🗯
Showing 1 to 1 of 1 entries						Previous 1 Next



5.11.2 Create SIP Interface for Webex Calling side

The following describes only the information that you have to change or insert to create a sip Interface on Webex Calling side:

In the Name field, insert a descriptive (logical) name to be used for this SIP Interface.

In the 'Sip Settings' panel, select the external address to be assigned to the Sip Interface between those provided according to your network interface configurations.

First, search and select one of the configured **Subnet** as follow; the list is available through a useful live search, which allows the dynamic search of the subnet name.

Then choose in the drop-down menu one of the **IP Interface Addresses** configured for the selected subnet.

In the **Transport Protocol** field, choose the transport protocol to be used for SIP signalling.

In the **TLS** field, you can enable TLS feature

Then add SIP Manipulation in Inbound and Outbound Rule, choosing in the drop-down menu.

Click **Click** to confirm the creation of Sip Interface.

Parameter	Value
Name	sip_webex
Subnet	subnet_webex
Address	138.132.65.52
Transport	ТСР
TLS	true
TLS Version	1.2



SIP Settings
Subnet
subnet_webex 138.132.65.1/255.255.255.128/25 (VLAN -
Address
1 38 132 65 52
Transport Protocol
TOP 🗸
FE L4 Termination
false 🗸
Port
5060
TLS
true 🗸 🗸
Enable Check MTU
false 🗸
Cause Q.850
0 DISABLED -
Emergency Service management
false 🗸

_

When **TLS** field is true, a new 'TLS Setting' panel appear:



TLS Settings	
TLS Port	
5061	
TLS Certificate	
cert-webex-ok - [CRT]	~
Trusted TLS CAs	
webEx-CA-list (CAProfile)	~
Authentication Type	
BILATERAL	~
Trustiness Profile	
webex	~
Add P-Served-User from certificate	
false	~
TLS Version	0
1.2	~

Under TLS Settings you have to change or insert the following parameters:

TLS Certificate (select Cert-webex-ok for Webex Calling) Trusted TLS CAs (select WebEx-CA-List for Webex Calling) Authentication Type (select BILATERAL for Webex Calling) Trustiness Profile (select webex for Webex Calling) TLS Version TLS version (ALL, 1.0, 1.1 or 1.2) (select 1.2 for Webex Calling)

To create the sip Interface on Webex Calling side you have to change or insert only the highlighted fields:



General Settings	SIP Settings	Security Control List
Lana .	lubret	Automatio 80L
de nation	week lands and an exception of the second se	tana 🗸
interface Type	Address	
Generic 🗸 🗸	INCREASE AND A DECEMBER OF	Beaufity Control Type
Administrative Italus	Transport Protocci	DISALED
itäavisa 🗸 🗸	100 V	
SP Domain Inbound Policy Type	FE L4 Termination	SIP Manipulations
Al lizatio	taise V	Industrial fulle
	Port	None V
	5050	Outboard rule
	TA	None V
	tui V	
	Enable Check NTU	
	tess 🗸	
	Ceute Q.350	
	Editable +	
	Emergency Jervice management	
	DSABLE ¥	
	Enable ELIN Emergency Jervice	
	tase V	
	Enable Emergency Celiback	
	tase V	
	TI S Satiana	
	The desiries	
	TLI Port	
	TLI Cetificate	
	www.ipai	
	Thethed TL 8 CA4	
	weeks-heats (not-cons)	
	Authenticetion Type	
	1.000 V	
	Truthess Profile	
	V	
	Add P-Served-User from serificate	
	···· ·	
	TL3 Version 0	

At the end for example you have:

SIP Interfaces					♦ New
SIP Interfaces ()					
Show 10 v entries					Search
Name II: SIP Interface	Subnet	IT TLS	TLS Port	Administrative Status	1 Actions
sip_webex TOP/138 132.65 52.5060	subnet_webex	tue	5061	✓ InService	a 🗡 🔹
sip_south_pstn UDP/138.132.65.53.5050	subnet_learns	false		✓ InService	۹ 🖌 🛛
Showing 1 to 2 of 2 entries					Previous 1 Next

5.12 How to create SIP Peers and SIP Peer Group on PSTN side

5.12.1 Create SIP Peers on PSTN side

In order to create a SIP Agent (only for PSTN side), select **SBC Configuration >> SIP Peers** submenu in the main menu:





Click **+** New to create a new SIP Peer; the following view is displayed:

The following describes the information that you have to change or insert to create a sip Peer on PSTN side:



Create SIP Peer

Settings				Probe Settings	
Name				Probe Method	Probe On Request
pstn				OPTIONS Y	Disabled 🗸
Administrative Status				Probe Domain	Probe Timer
InService			~	First connected 🗸	60
IP Address					
52.178.167.0				Call Admission Control	
Port	Transport Protocol			Max Act Sess. (CAC)	Max In Sess. (CAC IN)
5060	UDP		~		
Enable TLS		TLS Port		Max Out Sess (CAC OUT)	May CDS
false	~	5061		0	0
Peer Shared				Max In CPS	Max Out CPS
false	~			0	0
				Max In Bandwidth (Kbit/Sec)	Max Out Bandwidth (Kbit/Sec)
				0	0
				Max Bandwidth (Kbit/Sec)	
				0	

In the **Name** field, insert a descriptive (logical) name to be used for this SIP Agent. This name will be used to associate the SIP Agent during the configuration of the Hunting Group.

In the IP Address and Port fields enter the IP address and port of the remote SIP agent.

The other fields depend of your configuration in PSTN side, for example if you need probe method or other.

Name	Status	IP Address	Port	Transport	Probe Method
pstn	InService	52.178.167.0	5060	UDP	OPTIONS

At the end for example you have

SIP Pe	eers											+ New
SIP Peers	5 1											
Show 10	✓ entries										Search:	
Name J	Li Address	1 Port	Transport	11 TLS 11	TLS Port	1 Probe Method	↓† Probe On Req	1 Probe Domain	↓† Shared	1 Administrative Status	1 Operational State	11 Actions
pstn	52.178.167.0	5060	UDP	false	5061	OPTIONS	Disabled	pstn.com	false	✓ InService	✓ InService	۹ 🖊 🕯
Showing 1 to	o 1 of 1 entries											Previous 1 Next



5.12.2 Create SIP Peer Groups on PSTN side

In order to create a SIP Peer Group (only for PSTN side), select SBC Configuration >> SIP Peer Groups from the main menu:

Netm	Gui	
🖬 Lice	enses	
Y Net	twork Configuration	¢
C SB	C Configuration	~
» Me	edia Interfaces	
» Me	dia Domains	
» SIF	P Interfaces	
» SIF	P Profiles	
» SIF	P Peers	24
» SIF	P Peer Groups	
» SIF	^o Domains	
» Tra	anscoding Rules	
» Re	routing Rules	
» Inte	erconnections	
I DN	IS/ENUM Service	<
» Dig	git Manipulations	
» SIF	^o Manipulations	
» TL	S Certificates	
» En	nergency Service Ni	ım.

Click + New to create a new SIP Peer Group; the following view is displayed:



The following describes the information that you have to change or insert to create a sip Peer Groups on PSTN side:

Create SIP Peer Group						<
Settings		SIP Peer list				
Name		Name	Max Call (for SIG)	Status		
gr_pstr		pstn - 52,178 167 0,5080 UDP	<mark>∽</mark> 1	InService	~	-
Administrative Status			+ Add			
InService	~					
Enable TLS						
false	~					

In the **Name** field, insert a descriptive (logical) name to be used for this Hunting Group. This name will be used to associate the Hunting Group in a SIP Domain. (e.g. gr_pstn).

In this example, we suppose you have in PSTN side just one Peer in one Peer Group.

Name	Status	Peer List
gr_pstn	InService	pstn

At the end for example you have:

SIP Peer Groups					+ New
SIP Peer Groups 1					
Show 10 v entries					Search:
Name 💷 Scan mode	IT TLS	11 SIP Peers	1 Administrative Status	1 Operational Status	1 Actions
gr_pstn -	false	pstn - 52.178.167.0:5060	✓ InService	✓ InService	۹ 🖌 📋
Showing 1 to 1 of 1 entries					Previous 1 Next



5.13 How to create SIP Domains

In order to create a SIP Domain, select **SBC Configuration >> SIP Domains** in the main menu:

Netmatch-S CI WebGui					
÷	Licenses				
Y	Network Configuration <				
Ø	SBC Configuration ~				
	Media Interfaces				
	Media Domains				
	SIP Interfaces				
	SIP Profiles				
	SIP Peers				
	SIP Peer Groups				
»	SIP Domains				
	Transcoding Rules				
	Rerouting Rules				
	Interconnections				
8	DNS/ENUM Service <				
	Digit Manipulations				
	SIP Manipulations				
	TLS Certificates				
	Emergency Service Num				

5.13.1 Create SIP Domain for PSTN side for No Media Bypass option

Click **+** New to create a new SIP Domain; the following view is displayed:

The following describes the information that you have to change or insert to create SIP Domain PSTN for each section.



In the Settings Logical section, you can provide the following information:

Create SIP Domain	
Settings	MTF Interworking Logical
pstn:com	
SIP Interface	
sip_south_pstn	*
Media Interface	
media_south_psin	· · · · · · · · · · · · · · · · · · ·
Media Domain	
dom_south_pstn	¥.
SIP Profiles	
SYSTEM_DEFAULTS	~
Туре	
GENERIC	~
DNS Query	
DISABLED 🗸	
ENUM Query	
DISABLED 🗸	
Enable TLS	
false	~

The Name field, a string identifier.

The **Sip Interface** field (drop-down menu) will show all the SIP Interfaces previously configured on the system, and that will be used for signalling flows exchange.

In the **Media Interface** field (drop-down menu) will show all the Media Interface previously configured on the system, and that will be used for media flows exchange.

In the **Media Domain** field (drop-down menu) will show all Media Domain previously configured on the system, and that will be used for media different features configured, like a profile with different configuration.

Parameter	Value
Name	pstn.com
Sip Interface	sip_south_pstn
Media Interface	media_south_pstn
Media Domain	dom_south_pstn



In the **Settings Interworking** section, you can provide the following information:

Settings	MTF (menvorking) Logical
Enable Call Forwarding Loop Prevention	Send SDP after PRACK
false 🗸	false 🗸
Provisional Response ACK	Update Interworking
Disabled V	Enable 🗸
Enable Multiple Redirect Contacts Handling	Enable Origin
faise	faise 🗸
Multiple Redirect Contact Handling	SIP DSCP 0
Paralel	Disabled 🗸
Forced Request URI	Audio DSCP 0
tus 🗸 🗸	Disabled 🗸
Request URI Host Mode	Video DSCP 0
false 🗸	Disabled 🗸
Force Host PAI	Other DSCP 0
DISABLED	Disabled 🗸
Route Header Stripping	Trunk Group Value
tos 🗸 🗸	
Replace Domain In Route	Trunk Context Value
false	
Include User phone parameter in URIs	Send Trunk Group
false 🗸	false 🗸
Treatment info Diversion Inbound Side	Enable NAT presence
None 🗸	false 🗸
Treatment info Diversion Outbound Side	Media Latching
None	None 🗸
Destination Redirection Policy	Route Header Use to Routing
no action	Priority 🗸
Call Deflection	
false	

The **Forced Request URI** field sets the Forced replacement of the Request-URI with the IP address and destination port.

The **Route Header Stripping** field Enabling to strip the top most route typically inserted by NM-S-CI on outgoing side.

Parameter	Value
Forced Request URI	True
Route Header Stripping	True



5.13.1.1 Adding SIP, Digit and SDP Manipulations

In addition, it is possible to associate to a SIP Domain one or more manipulation rules. You can associate SIP and Digit Manipulations previously configured and one or more SDP Manipulations. All these settings can be defined for Inbound and Outbound direction.

In the following example, for all calls incoming into the selected SIP domain, the SIP Manipulation "**userPhone**" (previously imported) is applied in the Inbound Side:

SIP Manipulations	Outbound	Inbound
Apply rule		
userPhone		~



In the following example, for all Domain Role and call side, insert these SDP Manipulations

Inbound/Incoming

Inbound/Incoming				
Action		Param		
Remove Media Stream	m=video			
Remove Line	m=application			
	Outbound	Inbound		
SDP Manipulation	IS			
Incoming				
Action				
Remove Media Stream		~		
Media to remove				
m=video				
Incoming				
Action				
Remove Media Stream		~		
Media to remove				
m=application				

Outbound/Incoming

Outbound/Incoming			
Action Param			
Remove Media Stream	m=video		
Remove Line	m=application		



C	Outbound	Inbound
SDP Manipulations		
Incoming		
Action		
Remove Media Stream		~
Media to remove		
m=video		
Action		
Remove Media Stream		~
Media to remove		
m=application		

Note: In the SDP Manipulation section, you can also introduce, for example, an action to remove SDP codec that SBC must not forward to PSTN domain.



5.13.2 Create SIP Domain for Webex Calling side for No Media Bypass option

Click **+** New to create a new SIP Domain the following view is displayed:

The following describes the information that you have to change or insert to create SIP Domain WEBEX for each section.

In the **Settings Logical** section, you can provide the following information:

₣ Settings			MTF Interworking	Logical
SIP Interface				
16TMSGRK				1
Media Interfaces				
Media Interface		Role		
media_noth_viebex		EXTERNAL	~	-
	+ Add			
Media Domain				
dom_webex				~
\$IP Profiles				
and all titles				~
Туре				
Type -veces				~
Type IVEET Emergency Service Management Type				~
Type VEET: Emergency Service Management Type Not Managed	~			v
Type VEED Emergency Service Management Type Not Managed DNS Routing Table	V Probe Method		Probe Timer	~
Type VEED Emergency Service Management Type Not Managed DNS Guery DNS Routing Table Etitsbjsch Cfr	Probe Method v v v	v	Probe Timer	~
Type Stock Emergency Service Management Type Not Managed DNS Guery DNS Routing Table EtiteDyst Sty Proxy Name Sty	♥ Probe Method ♥ 40% 40,5	v	Probe Timer 00	v
Type Stock Emergency Service Management Type Not Managed DNS Query DNS Routing Table CityEpito SKV Proxy Name SKV Pr	Probe Method	~	Probe Timer 60	~
Type Stock Emergency Service Management Type Not Managed DNS Query SKV Proxy Name ExtCl SecuritsSicoch megniciter ENUM Query Statu En	♥ Probe Method ♥ Notiness	v	Probe Timer 60	~
Type Stock Emergency Service Management Type Not Managed DNS Routing Table CNS Query SRV Proxy Name ExUED to the Stock mission coder ENUM Query DISABLED Stock Stoc	v Probe Method v d⊂t wijs	v	Probe Timer 00	~
Type Stock Service Management Type Rot Managed DNS Govery DNS Govery Stock Service Servi	v Probe Method v v⊂r eive	v	Probe Timer 00	~
Type	Probe Method	v	Probe Timer 00	~

The Name field, a string identifier.

The **Sip Interface** field (drop-down menu) will show all the SIP Interfaces previously configured on the system, and that will be used for signalling flows exchange.

In the **Media Interface** field (drop-down menu) will show all the Media Interface previously configured on the system, and that will be used for media flows exchange.

In the **Media Domain** field (drop-down menu) will show all Media Domain previously configured on the system, and that will be used for media different features configured, like a profile with different configuration.

The **SIP Profiles** (drop-down menu) will show all profiles previously configured on the system in order to choose one of them to apply a particular set of values for the typical SIP parameters (Timers, Allowed Methods, Allowed Headers, etc.).

In case of No Media Bypass option select noreferWebex

The **DNS Query** select box provides the opportunity to enable the respective queries.

The **DNS routing** Table provides the list of Routing Tables configured for DNS service.

The **Probe Method** provides the different modalities to probe.

In the Enable TLS field, select true.



In the **Type** field, select a SIP domain type.

The SRV Proxy name field, insert the domain name to discover the access edge service and performing a DNS SRV lookup

In the **Forced Local FQDN** field, the FQDN (Fully Qualified Domain Name) specified in this field overwrites the domain part of the Contact and Record Route Headers.

This value is the SBC FQDN, the same value set into the 'Subject Alternative Names [SAN]' field in the TLS certificate.

Parameter	Value
Name	sip_webex.com
SIP Interface	sip_webex
Media Interface	media_north_webex
Media Domain	dom_north_webex
SIP Profiles	noreferWebex
Туре	WEBEX
DNS Query	ENABLED
DNS Routing Tabled	dns
Probe Method	OPTIONS
SRV Proxy name	eun01.sipconnect.bcld.webex.com
Enable TLS	True
Forced Local FQDN	nms02.italtel.com

In the **Settings Interworking** section, you can provide the following information:

Estings	MTF Interworking Logical
Enable Call Forwarding Loop Prevention	Send SDP after PRACK
false	false 🗸
Provisional Response ACK	Update Interworking
Disabled V	Enable 🗸
Enable Multiple Redirect Contacts Handling	Enable Origin
false 🗸	false 🗸
Multiple Redirect Contact Handling	SIP DSCP 0
Parallel 🗸	Disabled V
Forced Request URI	Audio DSCP 0
tue 🗸 🗸	Disabled V
Request URI Host Mode	Video DSCP 0
false 🗸	Disabled V
Force Host PAI	Other DSCP 0
DISABLED 🗸	Disabled V
Route Header Stripping	Trunk Group Value
false 🗸	
Replace Domain In Route	Trunk Context Value
false 🗸	
Include User phone parameter in URIs	Send Trunk Group
false 🗸	false 🗸
Treatment info Diversion Inbound Side	Enable NAT presence
None Y	false 🗸
Treatment info Diversion Outbound Side	Media Latching
None 🗸	None
Destination Redirection Policy	Route Header Use to Routing
no action 🗸	Priority 🗸
Call Deflection	
false 🗸	



The **Forced Request URI** field sets the Forced replacement of the Request-URI with the IP address and destination port.

Parameter	Value
Forced Request URI	True

In the Settings MTF section, you can provide the following information:

laia Anchoring Enty Offer faise Ringback Tone raise Ringback Tone faise Cold Presence ort Zero Anchoring Faite Condition faise Multi Dialog Anchoring faise Multi Dialog Anchoring faise Request Mode Anchor faise Cold Presence	Settings	MTF Interworking Logical
false false false index oreed Anchoring false /ul>	Media Anchoring	Early Offer
aread Anchoring Ringback Tone false Ialse p Speed Anchoring Early Media Condition false SDP Presence ort Zero Anchoring Multi Dialog Anchoring false Multi Dialog Anchoring false Request Mode Anchor false false mote Media Bypass Fallback Timer false false	false	r false v
false p Speed Anchoring Early Media Condition false false ort Zero Anchoring Multi Dialog Anchoring false false moty Reinvite Anchoring Ialse emote Media Bypass false jo false false false false jo false false jalse false false	Forced Anchoring	Ringback Tone
p Speed Anchoring Early Media Condition false SDE Presence ort Zero Anchoring Multi Dialog Anchoring false Talse mpty Reinvite Anchoring Request Mode Anchor emote Media Bypass Talseck On Refer false Sol Enclose enchore Fallback Timer active On Refer Sol Enclose false Sol Enclose	false	✓ false ✓
false SDP Presence ort Zero Anchoring Multi Dialog Anchoring false false moty Reinvite Anchoring Request Mode Anchor false alse emote Media Bypass false ender Media Anchor false Anchor ender Media Bypass false Anchor ender Media Bypass false Anchor ender Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor false Anchor </td <td>Up Speed Anchoring</td> <td>Early Media Condition</td>	Up Speed Anchoring	Early Media Condition
and Zero Anchoring Multi Dialog Anchoring false false mpty Reinvite Anchoring Request Mode Anchor false false emote Media Bypass false Anchor enter Anchor false Anchor efer Anchor false Anchor false false Anchor false false Anchor enter Anchor false Anchor false false Anchor false Anchor fal	false	SDP Presence V
false * false * mpty Reinvite Anchoring Request Mode Anchor false * emote Media Bypass Fallback On Refer ender Anchor false false * efer Anchor false false * false * active On Refer 30 false * false *<	Port Zero Anchoring	Multi Dialog Anchoring
mpty Reinvite Anchoring Request Mode Anchor false false enote Media Bypass Fallback On Refer false alse efer Anchor falsek Timer false 30 active On Refer fallback Response Codes Inclusive false falsek Response Codes false false aling ID On Refer false Tansferor Fallback Response Codes	false	✓ false ✓
false	Empty Reinvite Anchoring	Request Mode Anchor
ende Media Bypass Fallback On Refer false false efer Anchor Fallback Timer false 30 false Fallback Response Codes Inclusive false false false false false Fallback Response Codes Inclusive false false false false	false	r false v
false false false false false Fallback Timer 30 audrive On Refer Fallback Response Codes Inclusive false false false false false false false	Remote Media Bypass	Fallback On Refer
fallback Timer fallback Timer iadive On Refer false	false	✓ false ✓
false 30 active On Refer Fallback Response Codes Inclusive false * alling ID On Refer Fallback Response Codes Transferor *		Fallback Timer
Image: Construction of the second	felee	30
aling ID On Refer Transferor Tran	10.90	Fallback Response Codes Inclusive
alling ID On Refer Transferor Transferor	Inactive On Refer	false
alling ID On Refer	10150	Fallback Response Codes
Transferor	Calling ID On Refer	
	Transferor	

The Modality and Early Media Condition fields are used to define the tone emission mode

Parameter	Value
Early Media Condition	SDP Presence



5.13.2.1 Adding SIP, Digit and SDP Manipulations

In addition, it is possible to associate to the SIP Domain one or more manipulation rules. You can associate SIP and Digit Manipulations previously configured and one or more SDP Manipulations. All these settings can be defined for Inbound and Outbound directions.

In the following example, for all call inbound side to the domain the previously imported SIP Manipulation "**userPhoneWebex**" is applied in Inbound Side:



At the end, you have (for example):

SIP Domains								+ New
Domains (3)								
Show 10 🖌 entries								Search:
Name	1 SIP Interface	IT Policy	IT SIP Profile	Media Interface	1 Media Domain	11 Def	IT TLS	11 Actions
pstn.it	sip_sud_pstn - [138.132.66.68 : 5060]	INGRESS_ADDRESS	SYSTEM_DEFAULTS	media_sud_pstn - 138.132.66.68.[10000- 12001]	dom_sud_pstn		false	۹ 🖊 🗯
webex	sip_webex - [138.132.65.47 : 5060]	INGRESS_ADDRESS	norefer	media_north_webex - 138.132.65.47:[10000 12001]	dom_webex		true	۹ 🗡 🗎
Showing 1 to 5 of 5 entries								Previous 1 Next



5.14 How to create Transcoding Rules

In order to create a Transcoding Rule, select **SBC Configuration >> Transcoding Rules** in the main menu:

Then the Transcoding Rules List is displayed.

N	etmatch-S CI WebGui	
÷	Licenses	
Y	Network Configuration <	
Ø	SBC Configuration ~	
>	Media Interfaces	
	Media Domains	
	SIP Interfaces	
	SIP Profiles	
	SIP Peers	
	SIP Peer Groups	
	SIP Domains	
»	Transcoding Rules	
	Rerouting Rules	
	Interconnections	
8	DNS/ENUM Service <	
	Digit Manipulations	
	SIP Manipulations	
	TLS Certificates	



5.14.1 Create Transcoding Rules from Webex Calling to PSTN

Click **+** New to create a new Transcoding Rule, the following view is displayed:

The following describes the information that you have to change or insert to create rule Webex Calling-PSTN:

Create Transcoding Rule		B Deixke ✓ Edit ■ List al
Settings	Origin SIP Peer	Destination SIP Peer
Name	Type	Type
WEBEXNEPSTN	Meedx VI	eaterway 🗸
Transcoding Type		
PROACTIVE	Origin codecs	Destination codecs
Use Global PTime	Additional priori codess	Additional destination poders
Do not set a common ptime for all codecs 🗸 🗸	077A × A	ema VIA
SRTP Interworking	07/1N 🗸 🗸	वर्ताता 🗸 🗸
tue 🗸	9724 V R	G7284 🗸 🔍
Fax Transcoding	Minimum origin codeos	Minimum destination codeos
DISABLED V		
	Over DTUE	Destrution DTUP
	Ongin DTMP	Destination DTMP
	InBand DTMF	inBand DTMF
	false 🗸 🗸	false 🗸 🗸
	rfo2833 DTMF	rfo2833 DTMF
	ta 💙	ta 🗸 🗸
	Received Telephone-Event Payloads	Received Telephone-Event Payloads
	Sent Telephone-Event Payload	Sent Telephone-Event Payload
	sipinto DTMF	sipinto DTMF
	false 🗸 🗸	false 🗸 🗸
	KPML DTMF	KPML DTMF
	false 🗸 🗸	false 🗸 🗸
	Origin Additional Capabilities	Destination Additional Capabilities
	RTP/RTCP Port Multiplexing	RTPIRTCP Port Multiplexing
	false 🗸 🗸	faise 🗸 🗸
	Disable RTCP Passthrough	Disable RTCP Passthrough
	false 🗸 🗸	faise 🗸 🗸

In the Settings section, you can provide the following information:

Name, a string identifier.

In tab **Origin SIP Peer,** field **Type**, specify the type of terminals present on the call side in order to compose the SDP with attributes congruent to these terminals.

In tab **Destination SIP Peer,** field **Type**, specify the type of terminals present on the call side in order to compose the SDP with attributes congruent to these terminals.

In tab Origin Codecs and Destination Codecs add codecs G711A, G711U and G729A.

In tab **Origin DTMF** and **Destination DTMF**, in **rfc2833 DTMF** field set dual-tone multi-frequency (DTMF) signalling as specially marked RTP packets according to **RFC2833**.

Parameter	Value
Name	WEBEXvsPSTN
Origin SIP Peer Type	WEBEX
Destination SIP Peer Type	GATEWAY
Origin Codecs	G711A, G711U, G729A
Origin DTMF – rfc2833 DTMF	True
Destination Codecs	G711A, G711U, G729A
Destination DTMF – rfc2833 DTMF	True



5.14.2 Create Transcoding Rules from PSTN to Webex Calling

Click **+** New to create a new Transcoding Rule, the following view is displayed.

The following describes the information that you have to change or insert to create rule PSTN-Webex Calling:

Create Transcoding Rule		Cetter ZEda in Latal
Settings	Origin SIP Peer	Destination SIP Peer
Name	Туре	Туре
PSTNWWEDEK	onew 🗸	WEBBX 👻
Transcoding Type		
PROACTIVE	Origin codecs	Destination codecs
Use Global PTime	Additional origin codeos	Additional destination orders
Do not set a common ptime for all codeos 🗸 🗸	011A ∨ R	011A V R
SRTP Interworking	काम्य 🗸 🕹	97HU 🗸 🤘
true 🗸 🗸	6720A 🗸 🗸	G120A 🗸 🗸
Fax Transcoding	Minimum origin codecs	Minimum destination codecs
DISABLED 🗸		
	Origin DTMF	Destination DTME
	- Provide Table	In the second seco
	fate V	false V
	4-2023 DTME	
	Received Telephone. Event Davloyde	Received Telephone-Event Pevinede
	House have been provide a memory of provide	HOUTED HERPHONE LIVER UPDAV
	Sant Talanhona, Evant Pavloyd	Sant Talanhona-Evant Pevinad
	ern respirent stern regione	win inspirite stan region
	siginfo DTMF	siginfo DTMF
	false 🗸	false 🗸
	KPML DTMF	KPML DTMF
	faise 🗸	false 🗸
	Origin Additional Canabilities	Destination Additional Canabilities
	faire Control Numpering	fairea
	Nuclei 2722 Basthouse	Deable 2729 December 24
	Insule Rice Passenough	false V

In the **Settings** section, you can provide the following information:

Name, a string identifier.

In tab **Origin SIP Peer** field **Type** specify the type of terminals present on the call side in order to compose the SDP with attributes congruent to these terminals.

In tab **Destination SIP Peer** field **Type** specify the type of terminals present on the call side in order to compose the SDP with attributes congruent to these terminals.

In tab Origin Codecs and Destination Codecs add codecs G711A, G711U and G729A.

In tab **Origin DTMF** and **Destination DTMF**, in field rfc2833 send dual-tone multi-frequency (DTMF) signalling as specially marked RTP packets according to RFC2833.

Parameter	Value
Name	PSTNvsWEBEX
Origin SIP Peer Type	GATEWAY
Destination SIP Peer Type	WEBEX
Origin Codecs	G711A, G711U, G729A
Origin DTMF – rfc2833 DTMF	True
Destination Codecs	G711A, G711U, G729A
Destination DTMF – rfc2833 DTMF	True



At the end, you will have (for example):

Transcoding Rules				+ New
Transcoding Rules				
Show 10 🗸 entries				Search:
Name	11 Transcoding Type	11 Fax Transcoding Type	11 Actions	
PSTNeWEBEX	PROACTIVE	DISABLED	۹. 🗡 🗯	
WEBEXvsPSTN	PROACTIVE	DISABLED	Q 🖊 🗯	
Showing 1 to 4 of 4 entries				Previous 1 Next

5.15 How to create Interconnection

To create, customize and view the interconnections with additional (optional) features, select **SBC Configuration >> Interconnections** in the main menu.



Click + New to create a new interconnection, the following view is displayed (with Transcoding Rule associated)



5.15.1 Create Interconnection from PSTN to Webex Calling for No Media Bypass option

The following describes the information that you have to change or insert to create an interconnection PSTN-Webex Calling:

Create Interconnection					K Cancel 🛛 🗸 Save
Origin domain		Settings		Destination domain	
Name		Туре		Name	
converse in the second s		Rule based routing	~	weber	
Peer Type		Trustiness		Peer Type	
SIP Face Broop	v	UNTRUSTED	~		~
SIP Peer Group Name		ChargingTrustiness		Peer Type	
gr_osh_webex	×	UNTRUSTED	~	WEBEX	
SIP Peer List	Max call	Topology hiding		Rerouting Rule	
pstn-webEx1 - 138.132.49.130.5082 UDP	1	DISABLED	~	No Rerouting Rule	~
ostn-webEx2 - 138.132.49.131:5082 UDP	1	Transcoding Rule			
		PS INVERSE	~	Destination codecs	
SIP Peer Scan Mode		Transcoding Type			
NOND_NOBN		PROACTIVE		Additional destination codecs	
Рег Тура		Fax Transcoding Type		G711U	v e,
UNIEVED .		DISABLED		G729A	v @.
Route Header Use for Nouting		SRTP Passthrough		Minimum destination orders	
Priorey		false	*		
Origin codecs		Media Inactivity Detection		Destination MTF Settings	
Additional origin codecs		Detection		Media Anchoring	
0711A	v 9.	DISABLED	*	faise	
G711U	v @.	Initial Inactivity Timer		Forced Anchoring	
G729A	v @.	120		false	
Minimum origin codecs		Subsequent Inactivity Timer		Up Speed Anchoring	
		30		false	
Origin MTF Settings				Port Zero Anchoring	
Media Anchoring		Pouting Bules		faise	
		Rounny Rules		Empty Reinvite Anchoring	

In **Orig Domain** tab for **Name** field (select pstn.com).

In **Orig Domain** tab for **Peer Type** field (select Sip Peer Group).

In Orig Domain tab for Sip Peer Group Name field (select gr_pstn).

In Settings tab for Transcoding Rule field (select PSTNvsWEBEX).

In **Destination Domain** tab for **Name** field (select sip_webex.com).

In **Routing Rules** tab push on Add Number routing policy and insert REMOTE route number that identify destination .

Parameter	Value
024388497	
Number	
Route Number	
+39024388497	
Number	
Route Number	
Routing Rules	

Origin Domain



Name	pstn.com	
Peer Type	Sip Peer Group	
SIP Peer Group Name	gr_pstn	
Settings		
Trascoding Rule	PSTNvsWEBEX	
Туре	e Rule Based routing	
Destination Domain		
Name	sip_webex.com	



5.15.2 Create Interconnection from Webex Calling to PSTN for No Media Bypass option

The following describes the information that you have to change or insert to create an interconnection Webex Calling-PSTN:

Create Interconnection				K Cancel 🗸 Save
Origin domain	Settings	-	Destination domain	
Name	Туре		Name	
where the second s	Rule based routing	~	and materials. A	
Peer Type	Trustiness		Peer Type	
. v	TRUSTED	~	SIP Peer Group	×
Petr Type	ChargingTrustiness		SIP Peer Group Name	
WEBEX	UNTRUSTED	~	g. path weber	~
Route Header Use for Routing	Topology hiding		SIP Peer List	Max call
Priority	DISABLED	~	pstn-webEx1 - 138.132.49.130.5052 UDP	1
	Transooding Rule			
	WEDEAUSRATN	~	pstn-webEx2 - 138.132.49.131.5052 UDP	1
Orgin codecs	Transcoding Type		SIP Peer Scan Mode	
Additional origin codecs	PROACTIVE		ROUND_ROBIN	
0711A 🗸 🔍	Fax Transcoding Type		Peer Type	
G711U V Q	DISABLED		GATEWAY	
G729A 🗸 🤘	10 TB Pacethraunah		Rerouting Rule	
Minimum origin codecs	hisa	~	No Rerouting Rule	~
Origin MTF Settings		_		
Hole Anderson	Media Inactivity Detection		Destination codecs	
Neola Anchoring	Detection		Additional destination codecs	
1994	DISABLED	~	G711A	~ @
Forced Anchoring	Initial Inactivity Timer		G711U	Y R
1318	120		G729A	∀ @
Up Speed Anchoring	Subsequent Inactivity Timer		Minimum destination codeos	
false	30			
Port Zero Anchoring			Destination MTE Settings	
false			Deservation and Security	

- In Orig Domain tab for Name field.
- In Settings tab for Trustiness field.
- In Settings tab for Transcoding Rule field.
- In Destination Domain tab for Name field.
- In **Destination Domain** tab for **Peer Type** field.
- In **Destination Domain** tab for **Sip Peer Group** Name field.

In **Routing Rules** tab push on Add Number routing policy and insert REMOTE route number that identify destination .



Routing Rules

Route Number
Number
+39
Route Number
Number
0039
Route Number
Number
342

Parameter	Value		
Origin Domain			
Name Sip_webex.com			
Se	ttings		
Trustiness	TRUSTED		
Transcoding Rule	WEBEXvsPSTN		
Туре	Rule Based routing		
Destination Domain			
Name	pstn.com		
Peer Type	Sip Peer Group		
SIP Peer Group Name	gr_pstn		


At the end, you will have (for example):

Interconnections													+ New
Interconnections 🕑													
Show	10 🗸 entries											Search:	
ld .	🗄 Origin	11 Origin Peer Group 11	Destination 11	Destination Peer Group	Туре	Route	1 Routing Po	licy 👫 Transcoding Rule 🕼	Trustiness 🕸	ChargingTrustiness	Topology Hiding 🔱	Media Inactivity Detection	↓† Actions
0	pstn.com	gr_pstn	pstnhub-ppe.skype.net		Static routing	Priority	-	PSTNvsTEAMS	TRUSTED	UNTRUSTED	DISABLED	DISABLED	۹ 🖌 💼
1	pstnhub- ppe.skype.net	-	pstn.com	gr_pstn	Static routing	Priority		TEAMSvsPSTN	TRUSTED	UNTRUSTED	HIDE_HEADER	DISABLED	۹ 🖊 💼
Showi	ng 1 to 2 of 2 entries												Previous 1 Next

Italtel and Italtel Logo are registered trademarks of Italtel SpA. All contents are Italtel SpA Copyright 2024. All rights reserved. This document is intended for the addressee(s) only and is confidential and/or may contain legally privileged information; it may not be reproduced or distributed in any form without Italtel's prior written consent.