

Oracle SBC with Microsoft Teams Direct Routing

Technical Application Note



Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Contents

2////////

1	REVIS	ION HISTORY	6
2	INTEN	DED AUDIENCE	6
3	VALID	ATED ORACLE SOFTWARE VERSIONS	6
4	RELA	TED DOCUMENTATION	7
	4.1 O	RACLE SBC	7
	4.2 M	ICROSOFT TEAMS	7
5	ABOU	T TEAMS DIRECT ROUTING	7
Ŭ	5.1 P	I ANNING DIRECT ROUTING	7
	5.2 M	EDIA BYPASS VS NON MEDIA BYPASS	8
	5.3 IN	IFRASTRUCTURE REQUIREMENTS	8
	5.4 D	NS REQUIREMENTS	8
	5.4.1	SBC Domain Names	9
	5.4.2	Adding the SBC Domain to Microsoft O365	9
	5.4.3	Creating a User in Microsoft O365	11
	5.5 C	ONNECT THE SBC TO THE TEAMS TENANT	13
	5.5.1	Remote Connection to Teams via Powershell	13
	5.5.2	Connect the Oracle SBC	14
	5.5.3	Configuring User Online Voice Settings	15
	5.5.4	Configure Voice Routing for Direct Routing	15
6	ORAC	LE SBC CONFIGURATION	18
	6.1 S	YSTEM-CONFIG	20
	6.1.1	NTP-Sync	20
	6.2 N	ETWORK CONFIGURATION	21
	6.2.1	Physical Interfaces	21
	6.2.2	Network Interfaces	22
	6.3 S	ECURITY CONFIGURATION	22
	6.3.1	Certificate Records	22
	6.3.2	TLS Profile	28
	6.3.3	Media Security	29
	6.4 TI		32
	6.4.1	Media Profiles	32
	6.4.2		33
	6.4.3		34
	6.4.4		35
	6.5 IVI	EDIA CONFIGURATION	35
	0.0.1	Neula Manager	30 27
	0.5.2	Realin Coning	31 20
	0.0.3		30
	661	Sin-Confia	20
	662	Replaces Header Support	<u>⊿∩</u>
	662	Sin Manipulation	- - -0 //1
	661	Sin Interface	12 71
	0.0.4		40

////

6.6.5 Session Agents 6.6.6 Session Group 6.7 ROUTING CONFIGURATION	43 44 45
6.8 SIP ACCESS CONTROLS	
7.1 MICROSOFT TEAMS CONFIGURATION ASSISTANT	
 8 VERIFY CONNECTIVITY. 8.1 ORACLE SBC OPTIONS PINGS. 8.2 MICROSOFT SIP TESTER CLIENT. 	54 54 54
9 SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS:	
9.1 TERMINOLOGY	55
9.2 REQUIREMENTS FOR INVITE MESSAGES AND FINAL RESPONSES	
9.3 REQUIREMENTS FOR OPTIONS MESSAGES	
9.3.1 Contact Header-OPTIONS:	
10 MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS	
11 APPENDIX A	
11 APPENDIX A 11.1 ORACLE SBC TDM WITH TEAMS	 58 58
11 APPENDIX A 11.1 ORACLE SBC TDM WITH TEAMS 11.1.1 Interface Requirements	58 58 58
 11 APPENDIX A	58 58 58 58
 11 APPENDIX A	58 58 58 58 58 58 58
 11 APPENDIX A	58 58 58 58 58 58 58 60
 11 APPENDIX A	58 58 58 58 58 58 60 60 62
 11 APPENDIX A	58 58 58 58 58 58 60 60 62 62
 11 APPENDIX A	58 58 58 58 58 58 60 60 62 62 62 64
 11 APPENDIX A	58 58 58 58 58 58 60 60 62 62 62 62 64
 11 APPENDIX A	58 58 58 58 58 58 60 60 62 62 62 62 64 64
 11 APPENDIX A	58 58 58 58 58 60 60 62 62 62 64 64 64 64 64
 11 APPENDIX A	58 58 58 58 58 58 60 60 62 62 62 62 62 64 64 64 64 64 64 64 68 69

///*

2/11/11/2



This Page is left Intentionally Blank

1 Revision History

Document Version	Description	Revision Date
1.1	 Document Based on 9.0 Release Removed sip manipulations for Teams Added Config Assistant Section 	11-16-2021
1.2	 Removed Session Translation for E911 Removed sip-all fqdn Added new Access Controls 	01-05-2022
1.3	 Enable refer call xfer on realm Added RespondOptionsManip 	07-15-2022
1.4	 Added DigiCert Global Root G2 as root certificate Modified TLS Profile 	08-22-2022
1.5	Modified powershell cmdlet	03-14-2023
1.6	Modified Cert record config requirements	02-12-2024
1.7	Removed reference to ping- response parameter and added notes for using tls-global config in ACLI	07/20/2024

2 Intended Audience

This document describes how to connect the Oracle SBC to Microsoft Teams Direct Routing. This paper is intended for IT or telephony professionals.

Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.

3 Validated Oracle Software Versions

All testing was successfully conducted with the Oracle Communications SBC versions:

SCZ830, SCZ840, SCZ900

These software releases with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 3950 (Release SCZ9.0.0 Only)
- AP 4600
- AP 4900 (Release SCZ9.0.0 Only)
- AP 6350
- AP 6300
- VME

Please visit <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers</u> for further information

4 Related Documentation

4.1 Oracle SBC

- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Reference Guide
- Oracle® Enterprise Session Border Controller Release Notes
- Oracle® Enterprise Session Border Controller Configuration Guide
- Oracle® Enterprise Session Border Controller Security Guide

4.2 Microsoft Teams

- <u>Microsoft Teams Direct Routing Overview</u>
- <u>Microsoft Teams Direct Routing Configuration</u>
- <u>Microsoft Teams Public Trusted Certificate for the SBC</u>

5 About Teams Direct Routing

Microsoft Phone System Direct Routing lets you connect a supported, customer-provided Session Border Controller (SBC) to Microsoft Phone System. With this capability, for example, you can configure on-premises Public Switched Telephone Network (PSTN) connectivity with Microsoft Teams client

With Direct Routing, you can connect your SBC to almost any telephony trunk or interconnect with third-party PSTN equipment. Direct Routing enables you to:

- Use virtually any PSTN trunk with Microsoft Phone System.
- Configure interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

5.1 Planning Direct Routing

When planning to configure MSFT Teams Direct Routing with the Oracle SBC, the following prerequisites are required: Please read through the following information before proceeding.

- <u>Microsoft Phone System Licensing</u>
- Fully Qualified Domain Name for your Session Border Controller
- Public trusted certificate for the Oracle SBC

5.2 Media Bypass vs Non Media Bypass

When planning and setting up Microsoft Teams Phone System Direct Routing, one of the main features you need to pay attention to is whether or not you enable media bypass in your Teams tenant, or leave it disabled. This feature changes the way media flows on calls.

The default configuration is to have Media Bypass disabled, which forces the Microsoft phone system media processors to anchor media for all calls. In other words, all media packets will flow from the Oracle SBC to Microsoft phone system, and from there, to the Teams client.

Media bypass enables you to shorten the path of media traffic and reduce the number of hops in transit for better performance. With media bypass, media is kept between the Oracle Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System. Media bypass leverages protocols called **Interactive Connectivity Establishment** (ICE) on the Teams client and <u>ICE lite</u> on the Oracle SBC. These protocols enable Direct Routing to use the most direct media path for optimal quality

For more information, please see "About Media Bypass with Direct Routing"

5.3 Infrastructure Requirements

The table below shows the list of infrastructure prerequisites for deploying Direct Routing.

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	
SIP Trunks connected to the SBC	
Office 365 tenant	
Domains	
Public IP address for the SBC	See Microsoft's Plan Direct Routing document and
Fully Qualified Domain Name (FQDN) for the SBC	Microsoft Trusted Root Program
Public DNS entry for the SBC	with Included
Public trusted certificate for the SBC	CA Certificate List
Firewall ports for Direct Routing signaling	
Firewall IP addresses and ports for Direct Routing media	
Media Transport Profile	
Firewall ports for client media	

5.4 DNS Requirements

You must create DNS records for domains in your network that resolve your Oracle SBC. Before you begin, the following is required for every Oracle SBC you want to pair:

• Public IP address

• FQDN resolving to the Public IP address

5.4.1 SBC Domain Names

The SBC domain name must be from one of the names registered in Domains of the tenant. You cannot use the *.onmicrosoft.com tenant for the FQDN name of the SBC.

The following table shows examples of DNS names registered for the tenant, whether the name can be used as an FQDN for the SBC, and examples of valid FQDN names:

DNS name	Can be used for SBC FQDN	Examples of FQDN names
contoso.com	Yes	Valid names:
		sbc1.contoso.com
		ssbcs15.contoso.com
		europe.contoso.com
contoso.onmicrosoft.com	No	Using *.onmicrosoft.com domains
		is not supported for SBC names

5.4.2 Adding the SBC Domain to Microsoft O365

The steps below will walk you through adding/registering your Oracle SBC domain in Microsoft O365.

To add, modify or remove domains you **must** be a **Global Administrator** of a <u>business or enterprise plan</u>. These changes affect the whole tenant, Customized administrators or regular users won't be able to make these changes

1. Go to the admin center at https://admin.microsoft.com. Enter your credentials to access the Microsoft 365 admin center

	Microsoft 365 admin center	P Search
=		Oracle
ŵ	Home	
8	Users \checkmark	Recommended based on your Office download setting …
⁹ 2 ⁶	Teams & groups $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	
	Billing ~	Get new Office features every month
٢	Settings \checkmark	Customer feedback from organizations like yours has shown that users have a better You get updates
ß	Setup	experience with Office when their features are updated more often. Don't wait six months to update your Office apps. Give your users more powerful tools to stay productive in Office as soon as those tools are available.
Adn	nin centers	
U	Teams	View recommendation

2. Go to the Settings > Domain's page, click Add Domain

	Microsoft 365 admin cent	er				✓ Search
=			Home	> Domains		
ŵ	Home		Dor	nains		
8	Users	\sim				
የ ድ	Teams & groups	\sim	+ Ac	ld domain 🗔 Buy domain 🖒 Refresh		
	Billing	\sim				
<u>نې</u>	Settings	^ /		Domain name ↑		Status
	Domains			telechat.o-test06161977.com (Default)	:	No services selected
	Search & intelligence		_			-
	Org settings			customers.telechat.o-test06161977.com	÷	No services selected
	Integrated apps			solutionslab.onmicrosoft.com	:	✔ Healthy

3. Enter the name of the domain you want to add, then select "Use this domain" at the bottom

	Microsoft 365 admin center	
≡	Domains > Add domain	
ណ៍		
8	Add domain	
የቋየ		Add a domain
	Domain name	
٢	Connect domain	If you already own a domain like contoso.com, you can add it to your account here.
P		Domain name
	O Finish	telechat.o-test06161977.com

4. Next, choose how you want to verify that you own the domain. For the purposes of this example, we select "Add a TXT record" select continue.



5. Follow the instructions on the screen. Once complete, select "verify" to complete the process



In this application note, we are using the following FQDN that is registered in Microsoft O365 to pair the Oracle SBC to Microsoft Teams Direct Routing Interface. Since our SBC is deployed behind NAT, we will only be displaying the private IP addresses configured on the SBC.

Public IP Address	FQDN Name
<public ip="" nat="" of="" or="" sbc=""></public>	telechat.o-test06161977.com

Next, we can create a User and assign Microsoft Phone System license.

5.4.3 Creating a User in Microsoft O365

After your Domain has been added and verified in Microsoft O365, the domain must be activated by adding at least one licensed user with the SIP address matching that registered domain.

The steps below will outline how to add a user and assign privileges and licenses to that user.

1. In the <u>Microsoft 365 admin center</u>, go to **User management**, and select Add user.

iii Microsoft 365 admin center	♀ Search
=	Home > Active users
ŵ Home	Active users
A Users ^	
Active users Contacts	📏 Add a user 🔒 Multi-factor authentication 💍 Refresh 👌 Delete user 🔍 Reset password 📋 Manage product licenses 🧏 Manage roles \cdots

2. Fill in the required fields for basic information of the user and select Next

Add a user		
Basics	Set up the basi	cs
	To get started, fill out some b	asic information about who you're adding as a user.
Optional settings		
O Finish	First name	Last name
	Solutionslab	Oracle
	Display name *	
	Solutionslab Oracle	
	Username *	Domains
	sloracle	@ telechat.o-test06161977.com <
	Automatically create a pass	word
	Password *	
		Strong 💿
	Require this user to change	their password when they first sign in
	Send password in email up	on completion

11/1/

- 3. Assign the user a product license. To allow for Microsoft Teams Direct Routing, the following licenses must be assigned to users
 - Microsoft 365 Phone System
 - Office 365 E3

Add a user	
Basics	Assign product licenses
Product licenses	
	Assign the licenses you'd like this user to have.
Optional settings	
Finish	Select location *
	Licenses (0)*
	Assign user a product license
	Microsoft 365 Phone System You're out of licenses and we can't automatically buy it for you. Go to subscriptions to buy one.
	Microsoft Teams Exploratory 199 of 200 licenses available
	Office 365 E3 You're out of licenses and we can't automatically buy it for you. Go to subscriptions to buy one.

4. Finally, select Roles and add any additional Profile info to the user account. Select next, and follow the on screen instructions to complete the addition of the user.

Add a user	
Basics	Optional settings
Product licenses Optional settings	You can choose what role you'd like to assign for this user, and fill in additional profi information.
O Finish	Roles (User: no administration access)
	Profile info

5.5 Connect the SBC to the Teams tenant

The following describes how to configure your Teams tenant to accept a connection from the Oracle SBC. It will also cover how to enable your users for Direct routing, and the basics on how to setup call routing.

There are two ways to configure Microsoft Teams to accept a connection from the SBC. Using the Microsoft Teams admin center GUI, or by using the CLI in powershell.

In this example, we'll connect to Teams online via powershell and provide some examples of a basic configuration.

In order you use Powershell to connect to your Teams tenant, you must first follow the step outlined in <u>Set up your computer for Windows Powershell</u>

5.5.1 Remote Connection to Teams via Powershell

To establish a remote connection to your Teams tenant via powershell, you must first run the following commands and enter your admin credentials when prompted:

- Import-Module MicrosoftTeams
- \$credential = Get-Credential
- Connect-MicrosoftTeams



You will be prompted for your admin credentials twice in order to gain access to the tenant. Once logged in, you will see something similar to the following:



5.5.2 Connect the Oracle SBC

Use the New-CsOnlinePSTNGateway cmdlet to connect the SBC to the tenant. In a PowerShell session, type the following, and then press Enter:

"New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignalingPort <SBC SIP Port> -MaxConcurrentSessions <Max Concurrent Sessions the SBC can handle> -Enabled \$true"

PS C:\WINDOWS\system32> New-CsOnlinePSTNGateway -Fqdn telechat.o-test06161977.com -SipSignalingPort 5061 -MaxConcurrentSessions 500 -Enabled Strue -MediaBypass Senabled

Although not provided in the example config, we also recommend setting the option "SendSipOptions" to \$true. For a complete list of other options and configurable fields on the Teams PSTN Gateway, please refer to the following <u>SBC Settings</u>

You can control media bypass for each SBC by using the **Set-CSOnlinePSTNGateway** command with the **-MediaBypass** parameter set to true or false

After your PSTNGatway is configured, use the <u>Get-CsOnlinePSTNGateway</u> cmdlet to verify that the SBC is present in the list of paired SBCs. Type the following in a remote PowerShell session, and then press Enter:

Get-CsOnlinePSTNGateway -Identity <FQDN>

Identity: telechat.o-test06161977.comInboundTeamsNumberTranslationRules: {}OutboundPstnNumberTranslationRules: {}OutboundPstnNumberTranslationRules: {}OutboundPstnNumberTranslationRules: {}Fqdn: telechat.o-test06161977.comSipSignalingPort: 5061FailoverTimeSeconds: 10ForwardCallHistory: TrueForwardPai: TrueSendSipOptions: TrueMaxConcurrentSessions: 500Enabled: TrueGatewaySiteId:GatewaySiteLbrEnabled: FalseFailoverResponseCodes: 408,503,504PidLoSupported: FalseMediaRelayRoutingLocationOverride:ProxySbc:BypassMode: NoneDescriptions:	PS C:\WINDOW5\system32> Get-CsOnline	PSTNGateway -id telechat.o-test06161977.com
	Identity InboundTeamsNumberTranslationRules InboundPstnNumberTranslationRules OutboundTeamsNumberTranslationRules OutboundPstnNumberTranslationRules Fqdn SipSignalingPort FailoverTimeSeconds ForwardCallHistory ForwardCallH	<pre>: telechat.o-test06161977.com : {} : {} : {} : {} : {} : {} : {} : telechat.o-test06161977.com : 5061 : 10 : True : True : True : True : True : True : False : False : False : 408,503,504 : False : None</pre>

5.5.3 Configuring User Online Voice Settings

Earlier is the application note, we created a user and assigned that user the proper licenses. The next step is to configure the user's online phone settings.

Since we'll be managing the user's phone number online, we'll use the following powershell cmdlet:

Set-CsPhoneNumberAssignment -Identity "<User name>" -EnterpriseVoiceEnabled \$true

Set-CsPhoneNumberAssignment -Identity "<User name>" -PhoneNumber <phone number> -PhoneNumberType <phonenumbertype>

PS C:\WINDOWS\system32> Set-CsPhoneNumberAssignment -id teamsuser2@telechat.o-test06161977.com -EnterpriseVoiceEnabled \$true
PS C:\WINDOWS\system32> Set-CsPhoneNumberAssignment -id teamsuser2@telechat.o-test06161977.com -PhoneNumber +17814437248 -PhoneNumberType DirectRoutin

It's recommended, but not required, that the phone number used is configured as a full E.164 phone number with country code

5.5.4 Configure Voice Routing for Direct Routing

We'll now go through how to configure voice routing for Phone System Direct Routing.

Please see "Configure Voice Routing for Direct Routing" for more details and in depth examples.

1. Create a PSTN Usage named "US and Canada"

Set-CsOnlinePstnUsage -Identity Global -Usage US and Canada"

PS C:\WINDOWS\system32> Set-CsOnlinePstnUsage -Identity Global -Usage "US and Canada"

2. Verify that the usage was created by entering:

Get-CSOnlinePSTNUsage



3. We'll create a voiceroute to point traffic to the our SBC (PSTNGatway)

New-CsOnlineVoiceRoute -Identity "Bedford 1" -NumberPattern .* -OnlinePstnGatewayList telechat.o-test06161977.com -Priority 1 -OnlinePstnUsages "US and Canada"

PS C:\WINDOWS\system32> New-CsOnlineVoiceRoute -Identity "Bedford 1" -NumberPattern .* -OnlinePstnGatewayList telechat.o-test06161977.com -Priority 1 -OnlinePstnUsages "US and Canada"

4. Verify it's been created with

Get-CSOnlineVoiceRoute

PS C:\WINDOWS\system32>	get-csonlinevoiceroute -id "Bedford 1'
Identity	: Bedford 1
Priority	: 1
Description	: .
NumberPattern	: .*
OnlinePstnUsages	: {US and Canada}
OnlinePstnGatewayList	: {telechat.o-test06161977.com}
BridgeSourcePhoneNumber	:
Name	: Bedford 1

5. Now, we'll create a Voice Routing policy

New-CsOnlineVoiceRoutingPolicy "US Only" -OnlinePstnUsages "US and Canada"

PS C:\WINDOWS\system32> New-CsOnlineVoiceRoutingPolicy "US Only" -OnlinePstnUsages "US and Canada"

Get-CSOnlineVoiceRoutingPolicy



6. Lastly, we'll assign the policy to users:

Grant-CsOnlineVoiceRoutingPolicy -Identity "teamsuser1" -PolicyName "US Only"



This concludes the basic setup in Microsoft Teams tenant to pair the SBC, assign DID's to users, and create voice routing for Phone System Direct Routing.

We'll now move on to configuring the Oracle SBC.

6 Oracle SBC Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Microsoft Teams Direct Routing Interface.

If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Microsoft Teams Phone System Direct Routing is by utilizing the <u>Configuration Assistant</u>.

If an existing SBC is being used to interface with Microsoft Teams, follow the steps in this chapter to successfully configure the Oracle SBC.

Below shows the connection topology example for MSFT Teams for both Media Bypass and Non Media Bypass deployments

There are multiple connections shown:

- Teams Direct Routing Interface on the WAN
- Service provider Sip trunk terminating on the SBC





There are two methods for configuing the OCSBC, ACLI, or GUI.

For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element.

This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the <u>ACLI configuration guide</u>.

To access the OCSBC GUI, enter the management IP address into a web brower. When the login screen appears, enter the username and password to access the OCSBC.

Once you have access to the OCSBC GUI, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left hand side of the screen.

Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change for the connection to MSFT Teams Phone System Direct routing to function properly.

Note: the configuration examples below were captured from a system running the latest GA software, 9.0.0

ORACL	ORACLE Enterprise Session Border Controller									
NN3900-101 10	NK6900-10 10188/k4186 52/90.0 GA (Build 54) Deshboard Configuration									
Configuration	View Configuration	Q								
media-manager		•	Configuration Objects	nfiguration Objects						
security		•								
session-router		•	Name	Description						
oustern.			access-control	Configure a static or dynamic access control list						
system		,	account-config	Configure Quality of Service accounting						
			authentication-profile	Configure authentication profile						
			certificate-record	Create, generate, and import a certificate						

6.1 System-Config

To enable system level functionality for the OCSBC, you must first enable the system-config

GUI Path: system/system-config

ACLI Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)
- Transcoding Core (This field is only required if you have deployed a VME SBC)

ORACLE Enterprise Session Border Controller							
NN3900-101 10.138.194.136 SCZ9	2.0.0 GA (Build 54)						
Configuration View Configuration	on Q						
media-manager	•	Modify System Config					
security	•						
session-router	•	Hostname	telechat.o-test06161977com				
system	•	Description	SBC connecting PSTN Sip Trunk to Microsoft Teams Phone System Direct Routing				
fraud-protection							
host-route		Location	Burlington, MA				

• Click OK at the bottom

6.1.1 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration, but recommended.

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-sync

ORACLE Enterprise Session Border Controller							
NN3900-101 10.138.194.136	SCZ9.0.0 GA (Build 54)						
Configuration View Confi	guration Q						
media-manager	•	Modify NTP Config					
security	•						
session-router	•	Server	216.239.35.0 🗙				

• Select OK at the bottom

Now we'll move on configuring network connection on the SBC.

6.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with MSFT Teams Direct Routing, the other to connect to PSTN Network. The slots and ports used in this example may be different from your network setup.

6.2.1 Physical Interfaces

GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

• Click Add, use the following table as a configuration example:

Config Parameter	Teams	PSTN
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0

Note: Physical interface names, slot and port may vary depending on environment

ORACLE Enterprise Session Border Controller								
NN3900-101 10.138.194.136 SCZ9.0.0 F	Patch 2 (Build 172))						
Configuration View Configuration	Q							
media-manager	•	Phy Int	Phy Interface					
security	•							
session-router	•	_						
system	-	[C] t	t 1	🛓 / G 🖻				
		Action	Sel	Name	Operation Type	Port	Slot	
fraud-protection		:		s0p0	Media	0	0	
host-route								
http-client		:		s1p0	Media	0	1	

6.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

• Click Add, use the following table as a configuration example:

Configuration Parameter	Teams	PSTN
Name	s1p0	s0p0
IP Address	10.1.3.4	10.1.2.4
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.3.1	10.1.2.1
DNS Primary IP	8.8.8.8	
DNS Domain	Telechat.o-test06161977.com	

ORACLE Enterprise Session Border Controller									
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2	Sektronical-b-/SBC-1 SC/200 Patch 2 (Baldel 72) Databased Configuration								Configuration
Configuration View Configuration	Q								
media-manager	•	Networ	rk Inte	rface					
security	•								
session-router									
system		🗅 t	1 1	🛓 🖉 🙃 🍵					
-,		Action	Sel	Name	Sub Port Id	Description	Hostname	IP Address	
fraud-protection				s0p0	0			10.1.2.4	
host-route		· ·							
http-client				slpO	0			10.1.3.4	

• Click OK at the bottom of each after entering config information

Next, we'll configure the necessary elements to secure signaling and media traffic between the Oracle SBC and Microsoft Phone System Direct Routing.

6.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Teams Direct Routing Interface.

Microsoft Teams Direct Routing only allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by Certificate Authorities (CAs) that are part of the <u>Microsoft Trusted</u> <u>Root Certificate Program</u>. A list of currently supported Certificate Authrities can be found at:

Public trusted certificate for the SBC

6.3.1 Certificate Records

"Certificate-records" are configuration elements on Oracle SBC which capture information for a TLS certificate such as common-name, key-size, key-usage etc.

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC's configuration.

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

For the purposes of this application note, we'll create three certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certificate signed by this authority)
- DigiCert Global G2 Cert (Microsoft Presents the SBC a certificate signed by this authority)

Note: The DigiCert RootCA is only part of this example, as that is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

6.3.1.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Microsoft to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN and the extended key usage list must contain both serverAuth and clientAuth. In this example our common name will be **telechat.o-test06161977.com.** You must also give it a name. All other fields are optional, and can remain at default values.

To Configure the certificate record:

Click Add, and use the following example to configure the SBC certificate

ORACLE Enterprise Set	ssion Border (Controller	
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2 (Build 17	72)	
Configuration View Configuration	Q		
media-manager	Þ	Add Certificate Record	
security	•	Name	CDCC VIII + 1 T
authentication-profile		Hame	SBCCertificatefor leams
certificate-record		Country	US
tls-global		State	MA
tls-profile		Locality	Burlington
session-router	•	Organization	Engineering
system	Þ	Unit	
		Common Name	telechat.o-test-06161977.com
		Key Size	2048 💌
		Alternate Name	
		Trusted	✓ enable
		Key Usage List	digitalSignature 🗙
			keyEncipherment 🗙
		Extended Key Usage List	serverAuth 🗙 clientAuth 🗙

• Click OK at the bottom

Next, using this same procedure, configure certificate records for the Root CA certificates

6.3.1.2 Root CA and Intermediate Certificates

6.3.1.2.1 Go Daddy Root

The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

6.3.1.2.2 DigiCert Global Root G2

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by DigiCert Global Root G2. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: DigiCert Global Root G2



6.3.1.2.3 Baltimore Root

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by Baltimore Cyber Baltimore CyberTrust Root. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate.

You can download this certificate here: https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem

Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	Baltimore Root	GoDaddy Root	DigiCert Global Root G2
Common Name	Baltimore CyberTrust Root	Go Daddy Class2 Root CA	DigiCert Global Root G2
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256

ORACL	E Enterprise	Session Bo	rder Co	ntroller						Û 🗕	admin 👻
NN3950-101 10.13	8.194.101 SCZ9.	.0.0 Patch 3 (E	Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
onfiguration	View Configuratio	on Q							Discard	😧 Verify	B Save
media-manager	•	Certific	ate Re	ecord							
security	•										
authentication-pro	ofile										
certificate-record			<u>n</u> 1	🛃 🗹 РКС5	2 / 1 1				Search		Q
certificate record		Action	Select	Name	Country	State	Locality	Organization	Unit	Comm	on Name
tls-global		÷		BaltimoreRoot	US	MA	Burlington	Engineering		Baltim	ore CyberT
tls-profile session-router	►	:		DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCe	rt Global Re
system	•	:		GoDaddyRoot	US	MA	Burlington	Engineering		GoDad	ldy Class2 F
		:		SBCCertificateforTea.	. US	California	Redwood City	Oracle Corporation		telecha	at.o-test06'
								-	•		

At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.

ORACL	E Enterprise S	ession Bo	rder Co	ntroller									0 🗸	admin 🔻
NN3950-101 10.130	8.194.101 SCZ9.0.0	D Patch 3 (E	uild 290)					Dashb	oard Co	onfiguration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q											😟 Verify	🖹 Save
media-manager	•	Certificate Record												
security	Ψ													
authentication-pro	ofile		5. ↑	T	DIVICITA							Soarch		0
certificate-record		Action	Select	Name	E PRCSIZ	Co	Confirm		cality	Ore	anization	Unit	Comr	non Name
tls-global				Raltimore	Poot		Do you want to activ	vate the configuration?	rdington	Enc	neering		Paltin	oore CuberT
tls-profile		:		Datamoren		0.			Junigton	LIIE	sincering		Daicin	Iore cyberr
session-router	•	:		DigiCertGlo	obalRootG2	US	Confir	m Cancel	urlington	Dig	iCert	www.digicert.com	DigiC	ert Global R
system	•	:		GoDaddyR	oot	US		МА	Burlington	Eng	gineering		GoDa	ddy Class2 F
		:		SBCCertific	ateforTea	US		California	Redwood City	Ora	cle Corporation		telech	nat.o-test06

6.3.1.3 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. This is not required for any of the Root CA or intermidiate certificates that have been created.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

ORACL	LE Ent	terprise Se	ession Bo	rder Co	ntroller						Û 🔺	admin 🔻	
NN3950-101 10.	138.194.101	SCZ9.0.0) Patch 3 (E	Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System	
Configuration	View Cor	nfiguration	Q							Discard	😟 Verify	🖪 Save	
media-manager			Certificate Record										
security	security 🔹												
authentication-j	profile		D f	₽	.↓. K pkcs12					Search		0	
certificate-recor	d		Action	Select	Name	Country	State	Locality	Organization	Unit	Comm	ion Name	
tls-global			:		BaltimoreRoot	US	MA	Burlington	Engineering		Baltim	ore CyberT	
tls-profile												101110	
session-router		•	:		DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCe	ert Global Re	
system		•	:		GoDaddyRoot	US	MA	Burlington	Engineering		GoDad	ldy Class2 F	
			:		SBCCertificateforTea	US	California	Redwood City	Oracle Corporation		telech	at.o-test06′	

Generate certificate response

Copy the following information and send to a CA authority



Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

6.3.1.4 Import Certificates to SBC

Once certificate signing request has been completed - import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.

ORACL	Enterprise S	ession Bo	order Co	ntroller						Û 🔺	admin 👻	
NN3950-101 10.1	38.194.101 SCZ9.0.0) Patch 3 (E	Build 290				Dashboard	Configuration	Monitor and Trace	Widgets	System	
Configuration	View Configuration	Q							Discard	😧 Verify	Save	
media-manager	•	Certificate Record										
security	▼					. .						
aumentication-p			Ē; ⊥	₽ PKCS12	/ ि ₫				Search		Q	
certificate-record	1	Action	Select	Name	Country	State	Locality	Organization	Unit	Comm	non Name	
tls-global		:		BaltimoreRoot	US	MA	Burlington	Engineering		Baltim	ore CyberT	
tls-profile				DigiCartGlabalDootG2	110		Purlington	DigiCort	www.digicort.com	DigiC	ort Global Dr	
session-router	•	:		Digicei (Giobaikoo(Gz	03	MA	Burnington	Digicent	www.digicer.com	Digice		
system	•	:		GoDaddyRoot	US	MA	Burlington	Engineering		GoDad	ddy Class2 F	
		:		SBCCertificateforTea	US	California	Redwood City	Oracle Corporation		telech	at.o-test06′	

1111110

• Once pasted in the text box, select Import at the bottom, then save and activate your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

6.3.2 TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

• Click Add, use the example below to configure

ORACLE	Enterprise	Session Border Controller						Û 🗕	admin 🔫
NN3950-101 10.138.1	194.101 SCZ9.0).0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration v	/iew Configuratior	n Q					Discard	😟 Verify	🖹 Save
media-manager	Þ	Modify TLS Profile							
security	•								*
authentication-profi	ile	Name	TLSTeams						
certificate-record		End Entity Certificate	SBCCertificateforTeams	*					
tls-global		Trusted Ca Certificates	BaltimoreRoot 🗙						- 1
tls-profile			DigiCertGlobalRootG2 ×						
session-router	•								
system	Þ	Cipher List	DEFAULT 🗙	1.					- 1
		Verify Depth	10	(Range: 010)					- 11
		Mutual Authenticate	🗸 enable						
		TLS Version	tlsv12	,					
		Options							-
		ОК	Back						

• Select OK at the bottom

Next, we'll move to securing media between the SBC and Microsoft Teams.

6.3.3 Media Security

This section outlines how to configure support for media security between the OCSBC and Microsoft Teams Direct Routing.

6.3.3.1 SDES-Profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured. The only crypto-suite option supported by Microsoft is AES_CM_128_HMAC_SHA1_80 and must be included in the crypto list

In the SBC's GUI, on the bottom left, you will need to enable the switch "Show All" to access the media security configuration elements.

GUI Path: security/media-security/sdes-profile

ACLI Path: config t→security→media-security→sdes-profile

• Click Add, and use the example below to configure

	ssion Border (Controller	
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2 (Build 1	72)	
Configuration View Configuration	Q		
media-manager	•	Modify Sdes Profile	
security	•		
admin-security		Name	TeamsSRTP
auth-params		Crypto List	AES_CM_128_HMAC_SHA1_80 ×
authentication		Srtp Auth	✓ enable
authentication-profile		Srtp Encrypt	✓ enable
cert-status-profile		SrTCP Encrypt	✓ enable
certificate-record		Mki	enable
factory-accounts		Egress Offer Format	same-as-ingress 💌
ike	- F	Use Ingress Session Params	
ipsec	- ×	Options	
local-accounts		Key	
media-security	•	Salt	
dtls-srtp-profile		Srtp Rekey On Re Invite	enable
media-sec-policy		Lifetime	31

Please note, if you have media bypass enabled in your environment, the lifetime value of 31 is required for Teams clients to decrypt SRTP packets sent by the Oracle SBC.

• Select OK at the bottom

6.3.3.2 Media Security Policy

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Microsoft Teams, the other for non secure media facing PSTN.

GUI Path: security/media-security/media-sec-policy

ACLI Path: config t→security→media-security→media-sec-policy

• Click Add, use the examples below to configure

ORACLE Enterprise Set	sion Border (Controller	
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2 (Build 1	72)	
Configuration View Configuration	Q		
media-manager	•	Add Media Sec Policy	
security	•		
admin-security		Name	TeamsMediaSecurity
auth-params		Pass Through	enable
authentication		Options	
authentication-profile		⊿ Inbound	
cert-status-profile		Profile	TeamsS 🔻
certificate-record		Mode	srtp 💌
factory-accounts		Protocol	sdes 🛛 🔻
actory accounts		Hide Egress Media Update	enable
ike	- F		
ipsec	•	Outbound	
local-accounts		Profile	TeamsS 💌
		Mode	srtp 💌
media-security	•	Protocol	sdes 🗸 🔻

1111110

ORACLE Enterprise Ses	ision Bo	order Controller	
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2 (I	Build 172)	
Configuration View Configuration	Q		
media-manager	•	Add Media Sec Policy	,
security	•		
admin-security	•	Name	PSTNNonSecure
auth-params		Pass Through	enable
authentication		Options	
authentication-profile		⊿ Inbound	
cert-status-profile		Profile	+
certificate-record		Mode	rtp 💌
factory-accounts		Protocol	none 💌
ike	•	Hide Egress Media Update	enable
ipsec	•	Outbound	
la sel se su de		Profile	•
iocal-accounts		Mode	rto
media-security	•	Protocol	·
			none 🔻

• Select OK at the bottom of each when finished

This finishes the security configuration portion of the application note. We'll now move on to configuring media and transcoding.

6.4 Transcoding Configuration

Transcoding is the ability to convert between media streams that are based upon disparate codecs. The OCSBC supports IP-to-IP transcoding for SIP sessions, and can connect two voice streams that use different coding algorithms with one another

6.4.1 Media Profiles

For different codecs and media types, you can setup customized media profiles that serve to police media values and define media bandwidth policies.

SILK & CN offered by Microsoft teams are using a payload type which is different than usual, so to support this, we configure the following media profiles on the SBC.

This is an optional configuration, and only needs to be implemented on the SBC if you are planning to use the SILK codec or wideband comfort noise between the SBC and Microsoft Phone System Direct Routing.

GUI Path: session-router/media-profile

ACLI Path: config t→session-router→media-profile

Configure three media profiles to support the following:

- Silk Wideband
- Silk Narrowband
- CN

Click Add, then use the table below as an example to configure each:

Parameters	Silk	Silk	CN
Subname	narrowband	wideband	wideband
Payload-Type	103	104	118
Clock-rate	8000	16000	0

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2	(Build 172)								Dashboard Configuration M	Ionit
Configuration View Configuration	Q									
account-config	^	Media	Profile	e						
account-group										
allowed-elements-profile		D 1	t. ±	/ 6 🏛						Se
class-profile	•	Action	Sel	Name	Subname	Media Type	Payload Type	Transport	Clock Rate	
enforcement-profile		1		CN	wideband	audio	118	RTP/AVP	0	
enum-config		:		SILK	narrowband	audio	103	RTP/AVP	8000	
filter-config		•								
h323	- E	1		SILK	wideband	audio	104	RTP/AVP	16000	

• Select OK at the bottom or each after entering the required values

6.4.2 Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the Oracle SBC the ability to add, strip, and reorder codecs for SIP sessions.

While transcoding media codecs is optional, Microsoft does require the SBC generate Comfort Noise and RTCP packets towards Teams if the connection on the other side of the SBC (PSTN, IPPBX, etc..) does not support either. In order to satisfy this requirement, the SBC uses transcoding resources to generate those packets, which does require a codec policy be configured and assigned.

GUI Path: media-manager/codec-policy

ACLI Path: config t→media-mangaer→codec-policy

Here is an example config of a codec policy used for the SBC to generate CN packets towards Teams.

ORACLE Enterprise Session Border Controller											
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)											
Configuration View Configuration Q											
media-manager 🗸 👻	Add Codec Policy										
codec-policy											
dns-alg-constraints	Name	addCN									
dns-config	Allow Codecs	* X									
ice-profile	Add Codecs On Egress										
media-manager	Order Codecs										
media-policy	Packetization Time	20									

If you have chosen to configure the <u>media profiles</u> in the previous section to use SILK or wideband CN, you would set your codec policy to add them on egress. Here is an example:

ORACLE Enterprise Session Border Controller				
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)				
Configuration View Cor	nfiguration Q			
media-manager	•	Modify Codec Policy		
codec-policy				
dns-alg-constraints		Name	addCNandSILK	
dns-config		Allow Codecs	* ×	
ice-profile		Add Codecs On Egress	CN 🗙 SILK::wideband 🗙	

Lastly, since some SIP Trunks may have issues with the codecs being offerened by Microsoft Teams, you can create another codec policy to remove unwanted or unsupported codecs from the request/responses to your Sip Trunk provider.

ORACLE Enterprise Session Border Controller					
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)					
Configuration View Configuration	Q				
media-manager	•	Modify Codec Policy			
codec-policy					
dns-alg-constraints		Name	SipTrunkCodecs		
dns-config		Allow Codecs	* X SILK:NO X		
ice-profile			G722:NO X PCMA:NO X		
media-manager		Add Codecs On Egress	PCMU 🗙		
media-policy		Order Codecs			
msrp-config		Packetization Time	20		

• Select OK at the bottom

6.4.3 RTCP Policy

The following RTCP policy needs to be configured for the Oracle SBC to generate RTCP sender reports toward Microsoft Teams.

GUI Path: media-manager/rtcp-policy

ACLI Path: config t→media-manger→rtcp-policy

• Click Add, use the example below as a configuration guide

ORACLE Enterprise Session Border Controller				
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)				
Configuration View Configuration Q				
media-manager 🗸 🔻	Add RTCP Policy			
codec-policy				
dns-alg-constraints	Name	rtcpGen		
dns-config	RTCP Generate	all-calls 🔹		
ice-profile	Hide Cname	enable		

FYI, for the SBC to generate RTCP sender reports to Teams, the realm in which this policy is assigned must also have a codec policy assigned. This is to evoke the required transcoding resources needed to generate RTCP packets.

Select OK

6.4.4 ICE Profile

Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE STUN lite mode) enables an Advanced Media Termination client to perform connectivity checks, and can provide several STUN servers to the browser. ICE STUN support requires configuring an ICE Profile

The use of ICE is required only if using Teams with Media Bypass enabled.

This is the only Oracle SBC configuration difference between Media Bypass and Non Media Bypass deployments.

GUI Path: media-manager/ice-profile

ACLI Path: config t→media-manger→ice-profile

• Click Add, use the example below as a guide to configure

ORACLE Enterprise Session Border Controller				
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)				
Configuration View Configuration Q				
media-manager 🔹 🔻	Add Ice Profile			
codec-policy				
dns-alg-constraints	Name	Ice		
dns-config	Stun Conn Timeout	10		
ice-profile	Stun Keep Alive Interval	15		
ice-prome	Stun Rate Limit	100		
media-manager	Mode	NONE		

In some environments, it may be necessary to change the default values for Stun Conn Timeout, Stun Keep Alive Interval, and Stun Rate Limit to a value of 0 (zero).

Select OK at the bottom.

This concludes the configuration for transcoding and Advanced Media Termination options on the SBC. We can now move to setup Media.

6.5 Media Configuration

This section will guide you through the configuration of media manager, realms and steering pools, all of which are required for the SBC to handle signaling and media flows toward Teams and PSTN.

6.5.1 Media Manager

To configure media functionality on the SBC, you must first enabled the global media manager

GUI Path: media-manager/media-manager

ACLI Path: config t→media-manager→media-manager-config

The following two hidden options are recommended for the global media manager when interfacing with Microsoft Teams Phone System Direct Routing.

- audio-allow-asymmetric-pt: Provides transcoding support for asymmetric dynamic payload types enables the Oracle® Session Border Controller to perform transcoding when the RTP is offered with one payload type and is answered with another payload type.
- xcode-gratuitous-rtcp-report-generation: This option allows the Oracle SBC to generate a Real-Time Transport Control Protocol (RTCP) Receiver Report separately from the default Sender-Receiver Report (RFC 3550). This option requires a reboot to take effect.

ORACLE Enterprise Session Border Controller				
NN3900-101 10.138.194.136 SCZ Configuration View Configurat	9.0.0 Patch 2 (Build 17 ion Q	72)		
media-manager codec-policy	Ŧ	Add Media Manager		
media-manager		This object has not been o	created. Start editing and click OK to a	
media-policy		State	✓ enable	
realm-config		Flow Time Limit	86400	
steering-pool		Initial Guard Timer	300	
security	•	Subsq Guard Timer	300	
session-router		TCP Flow Time Limit	86400	
Session router		TCP Initial Guard Timer	300	
system	•	TCP Subsq Guard Timer	300	
		Hnt Rtcp	enable	
		Algd Log Level	NOTICE	
		Mbcd Log Level	NOTICE	
		Options	audio-allow-asymmetric-pt X xcode-gratuitous-rtcp-report- generation X	

Click OK at the bottom


Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

GUI Path; media-manger/realm-config

ACLI Path: config t→media-manger→realm-config

• Click Add, and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

Config Parameter	Teams Realm	PSTN Realm
Identifier	Teams	SipTrunk
Network Interface	s0p0:0	s1p0:0
Mm in realm	\checkmark	\checkmark
Media Sec policy	TeamsSecurityPolicy	PSTNNonSecure
Teams-FQDN	telechat.o-test06161977.com	
Teams-fqdn-in-uri	\checkmark	
Sdp-inactive-only	\checkmark	
RTCP mux	\checkmark	
Refer Call Transfer	Enabled	
ice profile	ICe (required for media bypass only)	
Codec policy	addCN	SipTrunkCodecs
RTCP policy	rtcpGen	
Access-control-trust-level	HIGH	HIGH

Also notice the realm configuration is where we assign some of the elements configured earlier in this document. IE...

- Network Interface
- Media Security Policy
- Ice Profile (optional, only required if using Media Bypass)
- Codec Policy (optional on the PSTN Realm)
- RTCP Policy

ORACLE Enterprise Session Border Controller					
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)					
Configuration View Configuration Q					
media-manager 🔹	Realm Cor	nfig			
codec-policy					
dns-alg-constraints	_				
dns-config	🕒 🖻	1 1 1			
	Action Sel	Identifier	Description	Addr Prefix	Network Interfaces
ice-profile	: [SIPTrunk	Realm Facing Sip Trunk	0.0.0.0	s1p0:0.4
media-policy	: 0	Teams	Realm Facing Microsoft Teams	0.0.0.0	s0p0:0.4

• Select OK at the bottom of each

6.5.3 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN. The other facing Teams.

GUI Path: media-manger/steering-pool

ACLI Path: config t→media-manger→steering-pool

Click Add, and use the below examples to configure

ORACLE Enterprise Session Border Controller				
SolutionsLab-vSBC-1 SCZ9.0.0	Patch 2 (Build 172)			
Configuration View Configur	ration Q			
media-manager	•	Modify Steering Pool		
codec-policy				
media-manager		IP Address	10.1.2.4	
media-policy		Start Port	10000	
realm-config	End I		10999	
realm-comig		Realm ID	SipTrunk	•

ORACLE Enterprise Session Border Controller					
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2	(Build 1	72)			
Configuration View Configuration	Q				
media-manager	•	•	Modify Steering Pool		
codec-policy					
media-manager			IP Address	10.1.3.4	
media-policy			Start Port	10000	
			End Port	10999	
realm-config			Realm ID	Teams	•

• Select OK at the bottom

We will now work through configuring what is needed for the SBC to handle SIP signaling.

6.6 Sip Configuration

This section outlines the configuration parameters required for processing, modifying and securing sip signaling traffic.

6.6.1 Sip-Config

To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

ACLI Path: config t→session-router→sip-config

There are only two recommended changes/additions to the global Sip Config.

- Set the home realm ID parameter to Teams Realm, and add the following hidden option:
- Max-udp-length=0: Setting this option to zero (0) forces sipd to send fragmented UDP packets. Using this option, you override the default value of the maximum UDP datagram size (1500 bytes; sipd requires the use of SIP/TCP at 1300 bytes).

ORACLE Enterprise Session Border	Controller	
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 1	172)	
Configuration View Configuration Q		
security		
session-router 🔹	Add SIP Config	
access-control	This object has not been cre	ated. Start editing and click OK to a
account-config	State	✓ enable
filter-config	Dialog Transparency	✓ enable
ldap-config	Home Realm ID	Teams v
local-policy	Egress Realm ID	
local-routing-config	Nat Mode	None
media-profile	Registrar Domain	
session-agent	Registrar Host	
session-group	Registrar Port	0
session-recording-group	Init Timer	500
session-recording-server	Max Timer	4000
session-translation	Trans Expire	32
sip-config	Initial Inv Trans Expire	0
sin-feature	Invite Expire	180
sp reade	Session Max Life Limit	0
sip-interface	Enforcement Profile	•
sip-manipulation	Red Max Trans	10000
sip-monitoring	Options	max-udp-length=0 🗙

• Select OK at the bottom

6.6.2 Replaces Header Support

The Oracle® Session Border Controller supports the Replaces header in SIP messages according to RFC 3891. The header, included within SIP INVITE messages, provides a mechanism to replace an existing early or established dialog with a different dialog. The different dialog can be used for Microsoft Teams services such as call parking, attended call transfer and various conferencing features.

The Oracle SBC's support for Replaces header is required to properly interwork with Microsoft Teams, but Microsoft Teams does not support the use of Replaces header. In other words, Microsoft sends Replaces to the SBC, the SBC cannot send Replaces to Microsoft.

To configure support for Replaces, we configure the following:

6.6.2.1 Sip Feature

The sip feature configuration element allow the SBC to support the Replaces value in the SIP Require and Supported Headers to and from Microsoft Teams.

GUI Path: session-router/sip-feature

ALCI Path: config t→session-router→sip-feature

Click add and use the following to configure:

ORACLE Enterprise Session Border Controller					
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2	(Build 17	2)		
Configuration View Configuration	Q				
security	►	*			
session-router	•		Add SIP Feature		
access-control		ι.	Name	replaces	
account-config			Realm	-	
account coming		ъ.	(Call)	leams	•
filter-config			Support Mode Inbound	Pass	•
ldap-config			Require Mode Inbound	Pass	•
local-policy			Proxy Require Mode Inbound	Pass	•
local-routing-config			Support Mode Outbound	Pass	•
media-profile			Require Mode Outbound	Pass	•
session-agent			Proxy Require Mode Outbound	Pass	•

Click OK at the bottom

6.6.2.2 Sip Profile

Sip Profile, once configured and assigned to a sip interface, will act on a Replaces header when received by Microsoft teams to replace a dialog.

GUI Path: session-router/sip-feature

ALCI Path: config t→session-router→sip-profile

The toggle switch "Show All" on the bottom left must be enabled to reveal the sip-profile option.

ORACLE Enterprise Session Border Controller				
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)				
Configuration View Configuration Q				
service-health				
session-agent	Add SIP Profile			
session-agent-id-rule	Name	forreplaces		
session-constraints	Redirection	inherit	•	
session-group	Ingress Conditional Cac Admit	inherit	•	
session-recording-group	Egress Conditional Cac Admit	inherit	•	
session-recording-server	Forked Cac Bw	inherit	•	
session-router	Cnam Lookup Server		•	
session-timer-profile	Cnam Lookup Dir	egress	•	
session-translation	Cnam Unavailable Ptype			
sip-advanced-logging	Cnam Unavailable Utype			
sip-config	Replace Dialogs	enabled	•	

• Click OK at the bottom

6.6.3 Sip Manipulation

To ensure the SBC generates a 200OK response to SIP Options messages received from Teams, we'll configure the following sip-manipulation rule

GUI Path: session router/sip manipulation

ACLI Path: config t→session-router→sip-manipulation

Click Add, and use the following example to configure:

-				
ORACLE Enterprise Ses	sion Border Contro	oller		
NN3950-101 10.138.194.101 SCZ9.0.0 P	atch 3 (Build 290)			
Configuration View Configuration	Q			
media-manager	Þ	Add SIP Manipulation		
security	►			
session-router	•	Name	RespondOptions	
access-control		Description	Sip Manipulation to respond locally to SIP Options pings	
account-config				
filter-config		Split Headers		
ldap-config		Join Mandau		
local-policy		Join Headers		
local-routing-config		CfgRules		
media-profile				
session-agent				
session-group				
session-recording-group				
session-recording-server				
session-translation				
sip-config				
sip-feature				
sip-interface				No rules to display. Please add.
sip-manipulation				Add 🗸

111/1/1

Next, under CfgRules, select "header rule" in the "Add" drop down menu:

	ORACLE Enterprise Session Border Controller					
NN3950-101 10.138.194.101 SCZ	9.0.0 Patch 3 (Build 290)					
Configuration View Configurat	tion Q					
media-manager	•	Add Sip manipulation / h	neader rule			
security	►					
session-router		Name	RejectOptions			
access-control		Header Name	From			
account-config		Action	reject	•		
filter-config		Comparison Type	case-sensitive	•		
ldap-config		Msg Type	request	•		
local-policy		Methods				
local-routing-config		Match Value				
media-profile		New Value	200 OK	I		

• Click OK at the bottom when finished

6.6.4 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

Configure two sip interfaces, one associated with PSTN Realm, and the other for Teams.

GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

Click Add, and use the table below as an example to configure:

Config Parameter	SipTrunk	Teams
Realm ID	SipTrunk	Teams
Sip-Profile		forreplaces
Sip Port Config Parmeter	Sip Trunk	Teams
Address	10.1.2.4	10.1.3.4
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TeamsTLSProfile
Allow anonymous	agents-only	all
In Manipulationid		RespondOptions

ORACLE Enterprise Session Border Controller					
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)					
Configuration View Configuration Q					
service-health					
session-agent	SIP Interface				
session-agent-id-rule	session-agent-id-rule				
session-constraints	C; ť	1 1	🛓 🖉 🗇 🗇		
session-group	Action	Sel	State	Realm ID	
session-recording-group	:		enabled	SIPTrunk	
session-recording-server	:		enabled	Teams	

Notice this is where we assign the TLS profile configured under the <u>Security</u> section of this guide, the sip-profile which allows the SBC to act on the Replaces header when received by Microsoft Teams, and the sip-manipulation which ensures the SBC responds locally to SIP Options.

• Select OK at the bottom of each when applicable

6.6.5 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

ACLI Path: config t→session-router→session-agent



• Click Add, and use the table below to configure:

Config parameter	Session Agent 1	Session Agent 2	Session Agent 3
Hostname	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.com	sip3.pstnhub.microsoft.com
Port	5061	5061	5061
Transport method	StaticTLS	StaticTLS	StaticTLS
Realm ID	Teams	Teams	Teams
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	10	10	10
Refer Call Transfer	enabled	enabled	enabled

ORAC	ORACLE Enterprise Session Border Controller											
SolutionsLab-vS	Soknowskab-v58C-1 10114 SC2V0.0 Parch 2 (kuld 172) Dashboard Configuration Monit											
Configuration	View Configuration	Q										
security		Þ	*									
session-router		*		Sessio	sion Agent							
access-control	4											
account-confi	e			D 1	<u>د</u> 1	± / 6 ±						Se
filter-config				Action	Sel	Hostname 👻	IP Address	Port	State	App Protocol	Realm ID	
Idap-config						sip3.pstnhub.microsoft.com		5061	enabled	SIP	Teams	
local-policy						sip2.pstnhub.microsoft.com		5061	enabled	SIP	Teams	
local-routing-o	config			1		sip.pstnhub.microsoft.com		5061	enabled	SIP	Teams	

Next, we'll configure a session agent for PSTN.

ORACLE Enterprise Session Border Controller									
SolutionaLab-v58C-1 SC290.0 Patch 2 (Build 172)								Dashboard	Configuration
Configuration View Configuration Q	L								
rph-profile	*	Session Ag	ent						
service-health									
session-agent		_							
session-agent-id-rule			1 2 / 6 1						
-		Action Sel.	. Hostname	IP Address	Port	State	App Protocol	Realm ID	
session-constraints		: -	10.1.2.30	10.1.2.30	5060	enabled	SIP	SipTrunk	
session-group									

• Select OK at the bottom

6.6.6 Session Group

A session agent group allows the SBC to create a load balancing model:

All three Teams session agents configured above will be added to the group. The session agents listed under destination must be in this order, and the strategy must be set to HUNT.

GUI Path: session-router/session-group

ACLI Path: config t→session-router→session-group

• Click Add, and use the following as an example to configure:

	Controller	
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 17	72)	
Configuration View Configuration Q		
local-response-map	Add Session Group	
local-routing-config		
media-profile	Group Name	TeamsGRP
net-management-control	Description	1
q850-sip-map		
qos-constraints	State	✓ enable
response-map	App Protocol	SIP 🔻
rph-policy	Strategy	Hunt 💌
rph-profile	Dest	sip.pstnhub.microsoft.com 🗙
service-health		sip2.pstnhub.microsoft.com 🗙
session-agent		sip3.pstnhub.microsoft.com 🗙
session-agent-id-rule	Trunk Group	
session-constraints	Sag Recursion	✓ enable
session-group	Stop Sag Recurse	401,407

• Click OK at the bottom

6.7 Routing Configuration

Now that a majority of the signaling, security and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls from Microsoft Teams to our Sip trunk, and vice versa...

GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy

	ssion Border C	Controller		
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2 (Build 17	72)		
Configuration View Configuration	Q			
media-manager	•	Modify Local Policy		
security	•			
session-router	•	From Address	**	
access-control	- 1-	To Address	* X	
account-config	- 1-	Source Realm	Teams 🗙	
filter-config	- 11	Description	Route calls from Teams Phone	
ldap-config			System Direct Routing to PSTN	
local-policy				
local-routing-config		State	✓ enable	
media-profile	- 11	Policy Priority	none 🔻	
session-agent	- 11	Policy Attributes		
session-group	- 11			
session-recording-group	- 11			
session-recording-server	- 11			
session-translation	- 11			
sip-config	- 11			
sip-feature	- 11			
sip-interface	- 11			\mathbf{U}
sip-manipulation	- 11			No policy attribute to display. Please add.
sip-monitoring				Add

111111

After entering values for to and from address and source realm, click Add under policy attribute to configure the next hop destination.

ORACLE Enterprise Session Border Controller								
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)								
Configuration View Conf	iguration Q							
media-manager	<u>۲</u>	Modify Local policy / policy	y attribute					
security								
session-router	•	Next Hop	10.1.2.30	•				
access-control		Realm	SipTrunk	•				
account-config		Action	none	•				

Next, we'll setup routing from our SIP Trunk to Microsoft Teams:

ORACLE Enterprise Session Border	Controller			
NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build	172)			
Configuration View Configuration Q				
media-manager	Modify Local Policy			
security 🕨				
session-router 🔹	From Address	* X		
access-control	To Address	* X		
account-config	Source Realm	SIPTrunk 🗙		
filter-config	Description			
ldap-config				
local-policy				
local-routing-config	State	🖌 enable		
media-profile	Policy Priority	none 🔻		
session-agent	Policy Attributes			
session-group				
session-recording-group				
session-recording-server				
session-translation				
sip-config				
sip-feature			(\cdot)	
sip-interface			\mathbf{U}	
sip-manipulation			No policy attribute to displ	ay. Please add.
sip-monitoring			Add	
	orise Session Border (Controller		
NN3900-101 10.138.194.136	SCZ9.0.0 Patch 2 (Build 1	172)		
Configuration View Config	uration Q			
media-manager	•	Add Local policy / policy	attribute	
security		. ,, ,		
,		Next Hop		
session-router	-	nextrop	sag:TeamsGRP	•
access control		Realm	Teams	
access-control		A stars		
account config		Action	replace-uri	

Select OK when applicable on each screen ٠

account-config

All transfers that use an SIP Refer message must go through the <u>Microsoft Teams infrastructure</u>. When the Microsoft SIP proxy sends an SIP Refer message to the Oracle SBC, an SIP Invite message should be returned to the SIP proxy, not to PSTN or to any other destination. It is true even if the call is transferred to an external PSTN number. To accommodate this requirement, we can configure another routing policy on the Oracle SBC to ensure call Invites generated by the SBC off SIP REFER's are routed properly.

	: p - a		
	ssion Border C	ontroller	
NN3900-101 10.138.194.136 SCZ9.0.0	Patch 2 (Build 17	2)	
Configuration View Configuration	Q		
media-manager	•	Modify Local Policy	
security	•		
session-router	•	From Address	* X
access-control		To Address	sip.pstnhub.microsoft.com 🗙
account-config		Source Realm	Teams 🗙
filter-config			
ldap-config		Description	Policy to route invites for correct transfer routing.
local-policy			
local-routing-config		State	✓ enable
media-profile		Policy Priority	none 💌

ORACLE Enterprise Session Border Controller							
NN3900-101 10.138.194.136	SCZ9.0.0 Patch 2 (Build 17	72)					
Configuration View Conf	figuration Q						
media-manager	•	Add Local policy / policy	attribute				
security	► 1						
session-router	-	Next Hop	sag:TeamsGRP	•			
access-control		Realm	Teams	•			
account-config		Action	replace-uri	•			

• Select OK when applicable.

6.8 SIP Access Controls

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

Please note, DDOS values are specific to platform and environment. For more detailed information please refer to the Oracle Communications SBC Security Guide.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

- 1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high
- 2. Set the access control trust level on public facing realms to HIGH

Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

Use this example to create ACL's for all MSFT Teams subnets. This example can be followed for any of the public facing interfaces, ie...SipTrunk, etc...

GUI Path: session-router/access-control

ACLI Path: config t→session-router→access-control

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14, and 52.120.0.0/14.

ORACLE Enterprise Session Border Controller							
SolutionsLab-vSBC-1 10.1.1.4 SCZ9.0.0 Patch 2 (Build 172)							
Configuration View Configuration	Q						
media-manager	•	Modify Access Control					
security	•						
session-router	-	Realm ID	Teams	•			
access-control		Description					
account-config							
filter-config		Source Address	52.112.0.0/14				
ldap-config		Destination Address	0.0.0.0				
local-policy		Application Protocol	SIP	•			
local-routing-config		Transport Protocol	ALL				
media-profile		Access	permit	•			
session-agent	- 1	Average Rate Limit	0				
session-group		Trust Level	high	•			

• Select OK at the bottom

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone System Direct Routing.

7 Oracle SBC Configuration Assistant

When you first log on to the E-SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the E-SBC provides the Configuration Assistant. The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic between the SBC and Microsoft Teams Phone System. You can use the Configuration Assistant for the initial set up to make to the basic configuration. See "Configuration Assistant Operations" in the Web GUI User Guide and "Run Configuration Assistant" in the ACLI Configuration Guide

Configuration assistant is available starting in release nnSCZ840P5 and nnSCZ900p2.

7.1 Microsoft Teams Configuration Assistant

The screenshots below are from an Oracle SBC GUI running 900p2.

For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:

Solution	d.ab-vSBC-1 1011.4	- SC290.0 Patch 2 (Build 172)		Dashboard	Configuration	Monitor and 1
System	Configuration Assis	1947) 			Crown MA CLIER	ne no
File Mano	agement	Configuration Assistant - Select Deployment				×
System Operations	Select a PBX Template	Select a SIP Trunk Template			st 🗲	
	ZoomPhone v	Select PBX Template to list the corresponding SIP Sid	de template			
		Microsoft Teams v				
		Microsoft ACS v				
		Cisco v				
	Avaya Session Manager v					
	GenericPBX v					
		GenesysPureEngage v				
		PureCloud v				
		Upload a Configuration	Upload a Template			
		Drag and Drop	Drag and Drop	+		
		Select a file or drop one here.	Select a file or drop one here.			
		Please click below link for additional template packages. https://www.oracle.com/technical-resources/documentation/acme-packet.html				

Under PBX template, we'll select Microsoft Teams template. This brings up a list of available sip trunk templates.

ZoomPhone v	VerizonRetaillpTrunking v	
Microsoft Teams u		
MICHODIC REALLS V	TwilioSIPTrunking v	
Aicrosoft Teams v [MSFTTeamsOnly gz]	GenericSipTrunk v	
escription : witcrosort i teams tempiate enables you to configure and connect our Session Border Controller to Microsoft Teams direct routing service and our PSTN provider.	IntelepeerSipTrunking v	
Avaya Session Manager v	ATTIPtrunking v	
GenericPBX v	BellCanadatrunking v	
GenesysPureEngage v	OrangeBTIP v	
PureCloud v		
Ipload a Configuration	Upload a Template	
Drag and Drop Select a file or drag one here. +	Drag and Drop Setct a file or drop one here. +	

Select a sip trunk template and click next at the top to access the Notes page. Pay close attention to the information here, as this is a list of warnings, pre-requisites and recommendations:

Configuration Assistant - Notes		×
Back	Next >	
PBX Template Notes for Microsoft Teams v	SIP Trunk Template Notes for GenericSipTrunk v	
Warning: - Proceeding with the Configuration Assistant results in erasing the existing configuration.	Warning: - Proceeding with the Configuration Assistant results in erasing the existing configuration.	
Pre-requisites:	Pre-requisites:	
Connect Port 0 of the Session Border Controller (SBC) to your network. Entwer that Transcoding resources are installed on your system (Hardware only). Add the SBTP license to the system. Table the Advanced entitlement on the system. Session Capacity in the entitlement. Set Session Capacity in the entitlement on the system. Set Session Capacity in the entitlement on the system. Set Session Capacity in the entitlement on the system. Set Session Capacity in the entitlement on the system.	This template is used to configure generic settings to connect the SBC to PSTN services Connect Port 1 of the Session Border Controller (SBC) to your network. Ensure that Transcoding resources are situatiled on your system (Virtual Machine Edition only). Configure at least one Transcoding core on your system (Virtual Machine Edition only). This template supports ONLV UDP/TCO configuration. Set Session Capacity in the entitlement. Set the system time.	

Clicking "Next" on the Notes page triggers the configuration assistant to do a system check. This ensures that all the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page providing the opportunity to setup entitlements, add license keys, etc...before moving on to the configuration. Once all requirements for your selected templates have been satisfied, you can proceed to the configuration pages.

Config	uration Assist	ant - Microsoft Tea	ams Network									×
	< Back	1	2	3	(4)	5	6	7	8	9	Skip 🔪	
		Microsoft Teams Network	Media	Transcoding	Trusted Certificate	SBC Certificate	PSTN Network	PSTN Session Agent	Transcoding	Additional Configuration		
				Let's cor	nfigure the interfac	e that communica	tes with Microso	oft Teams				
					Realm Name 💿							^
					Dert Marchar (2)		Required					
					Port 0		*					н
					Slot Number ®		Required					
					Slot 0		₩ Required					н
					Network IP Addre	ss ®						н
							Required					
					Network IP subne	t mask O						н
					Network Gateway	IP Address 🕲	Required					11
							Required					
					Primary DNS serve	er IP Address 🕲						*

Follow the instructions on each page. Any field that is labeled required must contain an entry.

Once you have entered all information in required fields on all pages, select the option to Review in the top right of the screen:

ssistant - Addition	al Configuration	1							×
0	0	0	O	0	O	Ø	0	9	Review
Microsoft Teams Network	Media	Transcoding	Trusted Certificate	SBC Certificate	PSTN Network	PSTN Session Agent	Transcoding	Additional Configuration	
			Lets cor	figure Session Ag	ent Capabilities				
			Do you want to ena	ble OPTIONS towards PS	TN? @ No	Yes			
			Do you want SBC to PSTN?	handle call transfer from	1 No	Yes			
			Do you want to ena toward your PSTN	ble session translation or provider?	⑦ №	Yes			
	Issistant - Addition	Issistant - Additional Configuration	Issistant - Additional Configuration	Issistant - Additional Configuration	Account Teams Media Transcoding Trusted Certificate SBC Certificate SBC Certificate C	Image: Section 1 - Additional Configuration Image: Section 1 - Section 2	Image: Second Teams Media Transcoding Trusted Certificate SEC Certificate PSTN Network PSTN Second Agent Microarch Teams Media Transcoding Trusted Certificate SEC Certificate PSTN Network PSTN Second Agent Do you want to enable OPTIONS towards PSTN? No Ves Do you want to enable OPTIONS towards PSTN? No Ves Do you want to enable GPTIONS towards PSTN? No Ves Ves No Ves Do you want to enable GPTIONS towards PSTN? No Ves No Ves Do you want to enable Section translation on toward your PSTN provider? No Ves	Image: Section 1 Configuration Image: Section 1 Configuration Microsoft Teams Media Transcoding Transcoding Trusted Cettificate SBC Cettificate PSTN Network PSTN Session Agent Transcoding Microsoft Teams Media Transcoding Trusted Cettificate SBC Cettificate PSTN Network PSTN Session Agent Transcoding Do you want to enable OPTIONS towards PSTN? N No Ves No Ves PSTN? Do you want to enable call transfer from toward your PSTN provider? No Ves Do you want to enable session translation on toward your PSTN provider? No Ves	Additional Configuration Image: Configure Section Con

The left side of the review page contains all of the entries added on each page and allows for editing each page individually if necessary.

The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.

uration Assistant - Sumr	nary				Download 👻
Microsoft Teams Network		/ Edit		Configuration	
Realm Name	Port Number				
Teams	Port 0				CODV
Slot Number	Network IP Address				- copy
Slot 0	10.1.3.4				
Network IP subnet mask	Network Gateway IP Address				
0 330 320 320 320 320 320	10171		name	BaltimoreRoot	
200.200.200.0	10.1.5.1		common-name	Baltimore CyberTrust Root	
Primary DNS server IP Address	DNS Domain		certificate-record	TeamsCSR	
8.8.8.8	telechat.o-test06161977.com		state	California	
			locality	Redwood City	
			unit	Oracle CORD-LABS BOSTON	
			common-name	telechat.o-test06161977.com	
Media		🧷 Edit	codec-policy	DCTUC- 4 - D - 3 /	
Do you want to enable Media Bypass?			allow-codecs	*	
blad			add-codecs-on-egress	PCMU	
enabled			codec-policy	TerrefederDelieu	
			allow-codecs	*	
			add-codecs-on-egress	CN SILK	
Transcoding		A Edit	http-server		
		/ Euit	ice-profile	webserverinstance	
Do you want to enable transcoding fea	tures (Comfort Noise, RTCP)? Do you want to select media codecs (SBC t	o Microsoft Teams)?	name	ice	
enabled	enabled		stun-conn-timeout	0	
Select media codecs			local-policy	0	
			from-address	*	
SILK			to-address	* 	
			source-realm policy-attribute	Sipirunk	
			next-hop	SAG:TeamsGrp	
Trusted Cortificate			realm	Teams	
nusteu certificate		/ Edit	local-policy		

1111111

Once all the information has been reviewed and accepted, click Apply.

The SBC now presents the Epilogue.

Configurati	on Assistant - Epilogue		×
Back	Perform the following actions when the system come	up to complete the deployment ::	Confirm
	Actions to be performed for Microsoft Teams v Security: - If you opted to generate a CSR during the SBC certificate provisioning step, please make sure to import the signed certificate after the reboot. - If you are going to use the SBC to interwork between SRTP and RTP, please make sure you assign the media security policy named "RTP" to the realm with non secure media.	Actions to be performed for GenericSipTrunk v No more actions required for this template	

Confirm, and then select reboot to apply the new configuration to the SBC.

Configuration Assistant - Apply Confirmation	
	If you proceed, the system erases the existing configuration and reboots.
	Back Reboot
	_

8 Verify Connectivity

8.1 Oracle SBC Options Pings

After you've paired the OCSBC with Direct Routing using the New-CsOnlinePSTNGateway PowerShell cmdlet, validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing.

While in the Oracle SBC GUI, Utilize the "Widgets" to check for OPTIONS to and from the SBC.

• At the top, click "Wigits"

This brings up the Wigits menu on the left hand side of the screen

GUI Path: Signaling/SIP/Method Options

ORACLE Enterprise Session Barder Controller										
SolutionsLab-V3BC1 10114 SC2P00.Parch 2 (Build 172) Dearboard										
Widgets										
Client Trans		*								
SIP Codecs			Method options							
SIP Errors										
Interface	•		Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total		
Methods			OPTIONS Requests	27	31	17	39	2301		
Method Ack			Retransmissions	0	0	0	0	0		
Mathead Dura			200 OK	24	28	14	33	1283		

• Looking at both the **Server Recent** and **Client Recent**, verify the counters are showing OPTIONS Requests and 2000K responses.

8.2 Microsoft SIP tester Client

SIP Tester client is a sample PowerShell script that you can use to test Direct Routing Session Border Controller (SBC) connections in Microsoft Teams. This script tests basic functionality of a customer-paired Session Initiation Protocol (SIP) trunk with Direct Routing.

The script submits an SIP test to the test runner, waits for the result, and then presents it in a human-readable format. You can use this script to test the following scenarios:

- Outbound and inbound calls
- Simultaneous ring
- Media escalation
- Consultative transfer

Download the script and Documentation here:

Sip Tester Client script and documentation

9 Syntax Requirements for SIP Invite and SIP Options:

Microsoft Teams Hybrid Voice Connectivity interface has requirements for the syntax of SIP messages. This section covers high-level requirements to SIP syntax of Invite and Options messages. The information can be used as a first step during troubleshooting when calls don't go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

9.1 Terminology

- Recommended not required, but to simplify the troubleshooting, it is recommended to configure as in examples as follow
- Must strict requirement, the system does not work without the configuration of these parameters

9.2 Requirements for Invite Messages and Final Responses

Picture 1 Example of INVITE and 2000K message

INVITE sip:17815551345@sip.pstnhub.microsoft.com:5061;user=phone;transport=tls SIP/2.0 Via: SIP/2.0/TLS 10.1.3.4:5061;branch=z9hG4bKcm87o2205o1rkbb1vnp0.1 Max-Forwards: 65 From: "Test" <sip:+17815551212@telechat.o-test06161977.com:5060;user=phone>;tag=19fc69fc0a020100 To: <sip:+17815551345@10.1.2.4:5060;user=phone> Call-ID: 1-19fc69fc0a020100.318f0133@68.68.117.67 CSeq: 2 INVITE Contact: <sip:+17815551212@telechat.o-test06161977.com:5061;user=phone;transport=tls>;sip.ice Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER User-Agent: T7100/3.0 Supported: 100rel Content-Type: application/sdp Content-Length: 550 X-MS-SBC: Oracle/AP3900/8.4.0p7

SIP/2.0 200 Ok FROM: <sip:+ 17815551212@10.1.2.4:5060;user=phone>;tag=e520638efffffff2c68c TO: <sip:+ 17815551345@telechat.o-test06161977.com:5060;user=phone>;tag=19ec632b0a020100 CSEQ: 1 INVITE CALL-ID: 1-19ec632b0a020100.74184225@68.68.117.67 VIA: SIP/2.0/TLS 52.114.32.169:5061;branch=z9hG4bKf74789d Contact: <sip:+17815551345@telechat.o-test06161977.com:5061;user=phone;transport=tls>;sip.ice Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER Server: T7100/1.0 Content-Type: application/sdp Content-Length: 477 Supported: timer,replaces Session-Expires: 1800; refresher=uas X-MS-SBC: Oracle/AP3900/8.4.0p7-ws

9.2.1 Contact Header-Invite and Final Response

- Must have the FQDN sub-domain name of a specific Teams tenant for media negotiation in both requests and final responses.
- Syntax: Contact:: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>
- MSFT Direct Routing will reject calls if not configured correctly

9.3 Requirements for OPTIONS Messages

Example of OPTIONS message

OPTIONS sip:sip.pstnhub.microsoft.com:5061;transport=tls SIP/2.0 Via: SIP/2.0/TLS 10.1.3.4:5061;branch=z9hG4bKumatcr30fod0o13gi060 Call-ID: 4cf0181d4d07a995bcc46b8cd42f924002000sg52@10.1.3.4 To: sip:ping@sip.pstnhub.microsoft.com From: <sip:ping@sip.pstnhub.microsoft.com>;tag=0b8d8daa0f6b1665b420aa417f5f4b18000sg52 Max-Forwards: 70 CSeq: 3723 OPTIONS Route: <sip:52.114.14.70:5061;Ir> Content-Length: 0 Contact: <sip:ping@telechat.o-test06161977.com:5061;transport=tls> Record-Route: <sip:telechat.o-test06161977.com > X-MS-SBC: Oracle/AP3900/8.4.0p7-ws

9.3.1 Contact Header-OPTIONS:

- When sending OPTIONS to the Direct Routing Interface Interface "Contact" header should have SBC FQDN in URI
- hostname along with Port & transport parameter set to TLS.
- Syntax: Contact: sip: <FQDN of the SBC:port;transport=tls>
- If the parameter is not set correctly, Teams Direct Routing Interface will not send SIP Options to the SBC

10 Microsoft Teams Direct Routing Interface characteristics

The following table contains the technical characteristics of the Direct Routing Interface. Microsoft, in most cases, uses RFC standards as a guide during the development. However, Microsoft does not guarantee interoperability with SBCs even if they support all the parameters in table 1 due to specifics of implementation of the standards by SBC vendors. Microsoft has a partnership with some SBC vendors and guarantees their device's interoperability with the interface. All validated devices are listed on Microsoft's site. Microsoft only supports the validated devices to connect to Direct Routing Interface. Oracle is one of the vendors who have a partnership with Microsoft.

Category	Parameter	Value	Comments
	SIP Interface FQDN	Refer to Microsoft documentation	
	IP Addresses range for SIP interfaces	Refer to Microsoft documentation	
	SIP Port	5061	
Ports and IP	IP Address range for Media	Refer to Microsoft documentation	
	Media port range on Media Processors	Refer to Microsoft documentation	
	Media Port range on the client	Refer to Microsoft documentation	
	SIP transport	TLS	
	Media Transport	SRTP	
	SRTP Security Context	DTLS, SIPS Note: DTLS is not supported until later time. Please configure SIPS at this moment. Once support of DTLS announced it will be the recommended context	https://tools.ietf.org/html/rfc5763
Transport	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	
and Security	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP mux helps reduce number of required ports
	Supported Certification Authorities	Refer to Microsoft documentation	
	Transport for Media Bypass (of configured)	ICE-lite (RFC5245) – recommended, · Client also has Transport Relays	
		· G711	
		 Silk (Teams clients) 	
	Audio codecs	 Opus (WebRTC clients) - Only if Media Bypass is used; 	
		· G729	
		· G722	
Codecs		 CN Required narrowband and wideband 	
		· RED – Not required	
	Other codecs	• DTMF – Required	
		 Events 0-16 Silence Suppression – Not required 	· · ·

1/1

2/11/11/2

11 Appendix A

11.1 Oracle SBC TDM with Teams

Oracle® designed the Time Division Multiplexing (TDM) functionality for companies planning to migrate from TDM to SIP trunks by using a hybrid TDM-SIP infrastructure, rather than adopting VoIP-SIP as their sole means of voice communications. The TDM interface on the Oracle® Enterprise Session Border Controller (E-SBC) provides switchover for egress audio calls, when the primary SIP trunk becomes unavailable. You can use TDM with legacy PBXs and other TDM devices.

- Only the Acme Packet 1100 and the Acme Packet 3900 platforms support TDM, which requires the optional TDM card.
- TDM supports bidirectional calls as well as unidirectional calls.
- TDM operations require you to configure TDM Config and TDM Profile, as well as local policies for inbound and outbound traffic.
- The software upgrade procedure supports the TDM configuration.
- Options for the Acme Packet 1100 and the Acme Packet 3900 platforms include CallingLine Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP).
- Options for the Acme Packet 1100 platform include the four-port Primary Rate Interface (PRI), the Euro ISDN Basic Rate Interface (BRI), and the Foreign Exchange OfficeForeign Exchange Subscriber (FXO-FXS) card.

11.1.1 Interface Requirements

- PRI—Digium1TE133F single-port or Digium 1TE435BF four-port card.
- BRI-Digium 1B433LF four-port card
- FXS—Digium 1A8B04F eight-port card, green module (ports 1-4)
- FXO—Diguim 1A8B04F eight-port card, red module (ports 5-8)

Oracle SBC Time Division Multiplexing (TDM) functionality has been fully tested with Microsoft Teams Phone System Direct Routing.

For further information on the setup and configuration of TDM on the Oracle SBC, please refer to the <u>TDM</u> <u>Configuration Guide</u>

12 Appendix B

12.1 Oracle SBC deployed behind NAT

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network.

The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

• The private IP address must be the same IP as configured on both the SIP Interface and Steering Pool

• The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config.

The SPL is applied to the Teams side SIP interface.

GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.1.3.4

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.

ORACLE Enterprise Ses	sion Border C	ontroller	
SolutionsLab-vSBC-2 SCZ9.0.0 Patch 2	(Build 172)		
Configuration View Configuration	Q		
media-manager	•	Modify SIP Interface	
security	•		U
session-router	-	Session Max Life Limit	0
access-control		Proxy Mode	.
account-config		Redirect Action	•
filter-config		Nat Traversal	none 🔻
Idap-config		Nat Interval	30
		TCP Nat Interval	90
local-policy		Registration Caching	enable
local-routing-config		Min Reg Expire	700
media-profile		Registration Interval	7400
session-agent		Route To Registrar	3000
session-group		Conurad Natwork	enable
session-Bronh		Secured Network	enable
session-recording-group		Uri Fqdn Domain	
session-recording-server		Options	
session-translation		SPL Options	HeaderNatPublicSipIfIp=52.151.136.203

You will need to apply these options to every sip interface on the SBC that is connected through a NAT.

13 Appendix C

13.1 Ringback on Inbound Calls to Teams and Early Media

In certain deployments, on certain call flows, PSTN callers may experience silence on inbound calls to Microsoft Teams instead of an expected ring back tone.

When Teams receives an INVITE, after sending a 183 with SDP response back to the Oracle SBC, Teams does not play ring back. Microsoft's expectation is the Oracle SBC will signal appropriately to the Sip Trunk in order for local ring back to be generated.

To properly signal the trunk to play the ring back, the SBC presents a 180 Ringing response to the trunk instead of the 183 Session Progress received from Teams.

In order to accommodate the 183 with SDP message that signal early media in cases of simultaneous ringing set to IVR, etc... we inspect the SDP of the 183 received before converting it to 180 Ringing.

If the SDP of the 183 does not contain the IP address of SBC (which is the case when Teams clients have simultaneous ringing set to IVRs), we use a sip manipulation to strip the SDP from the 183. Next, we convert the 183 response to a 180 Ringing before forwarding it to the Sip Trunk.

Due to the complexity of this sip manipulation, the SBC ACLI output has been provided.

GUI Path: Session Router/sip-manipulation

ACLI Path: config t→session-router→sip-manipulation

This sip manipulation will be applied as the in-manipulationid on the Teams Sip Interface.

sip-manipulation name Checkfor183 header-rule check183 name header-name @status-line manipulate action reply msg-type Invite methods element-rule is183 name type status-code action store comparison-type pattern-rule match-value 183 mime-sdp-rule name if183 reply msg-type methods Invite action manipulate boolean comparison-type match-value \$check183.\$is183 sdp-session-rule name au action manipulate sdp-line-rule checkclineforsbcip name type С action store comparison-type pattern-rule match-value ^(.(?!(10.1.3.4))).*\$ mime-sdp-rule name delete183SDP msg-type reply methods Invite action delete comparison-type boolean match-value \$if183.\$au.\$checkclineforsbcip header-rule name change183to180 @status-line header-name manipulate action boolean comparison-type \$if183.\$au.\$checkclineforsbcip match-value element-rule changestatus name status-code type replace action match-value 183 180 new-value element-rule name changereasonphrase type reason-phrase replace action match-value Session Progress Ringing new-value

This sip manipulation will be applied as the In Manipulationid on the Teams Sip Interface:

Note: If there is an existing Sip Manipulation rule already assigned as the in-manipulation-id on either the realm or sip interface, these rules would need to be added to that <u>existing manipulation</u>.

GUI Path: Session Router/Sip Interface

ACLI Path: config t→session-router→sip-interface

ORACLE Enterprise Session Border Controller							
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2	(Build 1	172)					
Configuration View Configuration	Q						
security	►	•					
session-router			Modify SIP Interface				
		ы.	Registration Interval	3600			
access-control			Route To Registrar	enable			
account-config			6	enable			
films and in			Secured Network	enable			
niter-conng			Uri Fqdn Domain				
ldap-config			Options				
local-policy			options				
			SPL Options				
local-routing-config			Truct Mode				
media-profile			Hust Mode	all 🔻			
session-agent			Max Nat Interval	3600			
session-agent			Stop Recurse	401,407			
session-group			Port Map Start	0			
session-recording-group			Port Map Fail	0			
			Port Map End	0			
session-recording-server			In Manipulationid	Checkfor183			
session-translation			Out Manipulationid	Checkfor183			

13.2 Oracle SBC Local Media Playback

13.2.1 Ringback on Transfer

During a call transfer initiated by Microsoft Teams, the calling party does not hear a ring back tone while the Oracle SBC is acting on the sip REFER received from Microsoft. In order to avoid this period of silence, we utilize the Oracle SBC's local playback feature.

Once configured, the Oracle SBC has the ability to generate ringback upon receipt of the sip REFER from Microsoft.

First, you must create a media file.



Media files of ringback tones are uploaded to /code/media to the Oracle SBC. This file differs based on your media generation method and must be raw media binary. For Transcoding based RBT, ensure that the files RAW PCM 16-bit MONO samples, sampled at 8-khz encapsulated with little-endian formatting and cannot exceed 4.8 MB.

Next, upload the file to the /code/media directory on the Oracle SBC.

ad

ORACLE Enterprise Session Border C	ontroller
SolutionsLab-vSBC-1 SCZ90.0 Patch 2 (Build 172)	Dashboard Configuration Monitor and Trace Widgets Syntax
Configuration Assistant	Force H4 Switchover 💿 Beacont 🕹 🕹 🔥 eff Informati
File Management v	Playback Media
Backup Configuration	
Configuration CSV	
Local Route Table	
Fraud Protection Table	
Log	
Audit Log	
Playback Media	
Software Image	\bigcirc
SPL Plug In	\bigcirc
Configuration Template	No playback media to display. Please refresh or upload playback media.
System Operations	Refresh Upload
	Upload file x
	LS_Ringback_tone.raw
	Upload Cancel sh or upload playback media.

Lastly, we'll assign this file to the realm facing PSTN, and set the trigger for the SBC to generate local ringback toward PSTN:

GUI Path: media manager/realm-config

ACLI Path: config t→media-manager→realm-config

	rise Session Border	Controller		
SolutionsLab-vSBC-1 SCZ9.0.0	Patch 2 (Build 172)			
Configuration View Configu	ration Q			
media-manager	•	Modify Realm Config		
codec-policy		Sm Icsi Match For Invite		
media-manager				
media-policy		Sm Icsi Match For Message		
realm-config		Ringback Trigger	refer	•
steering-pool		Ringback File	ringback10sec.pcm	

• Select OK at the bottom, and save and activate your configuration.

14 Appendix D

14.1 Configuration for Emergency Calling

As part of Oracle's continued partnership with Microsoft, the Oracle Communications Session Border Controller is fully certified with Microsoft Teams Direct Routing for E911 compatibility as well as an Elin Capable Gateway.

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers

For more information on how to configure emergency services in your Microsoft Teams Tenant, please refer to the documentation at the link below.

https://docs.microsoft.com/en-us/microsoftteams/what-are-emergency-locations-addresses-and-call-routing

https://docs.microsoft.com/en-us/microsoftteams/configure-dynamic-emergency-calling

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure#configure-voice-routing

The following will outline how to configure your Oracle SBC to handle E911 from Microsoft Teams, as well as setting up Oracle SBC Elin Gateway configuration.

14.1.1 E911

14.1.2 Emergency Session Handling

The Oracle® Enterprise Session Border Controller provides a mechanism to handle emergency sessions from non-allowed endpoints/agents. An endpoint is designated as non-allowed if it fails the admission control criteria specified by the allow-anonymous parameter in the Sip Inerface/SIP Ports configuration element. To enable this feature, you will need to configure the following:

- Local Policy to Match and Route emergency calls to correct destination with policy priority set to emergency
- Enable anonymous-priority on Ingress Sip Interface

Note: This is just a configuration example. This note assumes any session agents or session group for PSAP has already been configured:

14.1.2.1 Local Policy Route for Emergency Calls

GUI Path: session-router/local-policy

ACLI Path: config t→session-router—local-policy

ORACLE Enterprise Session Border Controller							
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)							
Configuration View Configuration	Q						
codec-policy	•	Modify	Local	Policy			
media-manager							
media-policy		From Add	ress		* X		
realm-config		To Addres	is		1911	× 911 × +1911 ×	
steering-pool		Source Re	alm		Tear	ns 🗙	
security	•	Descriptio	n				
session-router	•	Description			Local	policy to route emergency	calls
access-control							
account-config		State			🗸 en	able	
filter-config		Policy Price	ority		emerg	gency	•
ldap-config		Policy Attr	ibutes				
local-policy		D;	/ [6 @			
local-routing-config		Action	Sel	Next Hop		Realm	Actio
media-profile		:		sag:e911group		SipTrunk	none

You would also configure a policy attribute to route emergency calls to their proper destination. In this example, we have created a SAG called e911 as the destination for all emergency calls. For instructions on how to configure <u>Session Agents</u> or <u>Session Groups</u>, please click the links for examples.

Next, we'll enable anonymous-priority field in Sip-Interface: For more information on how this feature works, please see the <u>SBC Configuration Guide, Chapter 4.</u>

GUI Path: Not available in the SBC GUI at this time

ACLI Path: config t→session-router→sip-interface

sip-interface	
realm-id	Teams
sip-port	
address	10.1.3.4
port	5061
transport-protocol	TLS
tls-profile	TeamsTLSProfile
allow-anonymous	agents-only
in-manipulationid	Checkfor183
anonymous-priority	emergency
sip-profile	forreplaces

14.1.2.2 Net-Management Control

The Oracle Communications Session Border Controller supports network management controls for multimedia traffic specifically for static call gapping and 911 exemption handling. These controls limit the volume or rate of traffic for a specific set of dialed numbers or dialed number prefixes (destination codes).

To enable network management controls on your Oracle Communications Session Border Controller, you set up the net-management-control configuration and then enable the application of those rules on a per-realm basis. Each network management control rule has a unique name, in addition to information about the destination (IP address, FQDN, or destination number or prefix), how to perform network management (control type), whether to reject or divert the call, the next hop for routing, and information about status/cause codes. For more information about Network Management Controls, please refer to the <u>Configuration Guide, Chapter</u> <u>11</u>.

GUI Path: session-router/net-management-control

ACLI Path: config t→session-router→net-management-control

Use the below example to configure net-management-control and assign it to the Teams realm. Please note, net-management-control Realm parameter is not available through the GUI, so it must be enabled via ACLI to the appropriate realm.

	Parder Controller				
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)					
Configuration View Configuration Q	l l				
local-response-map	Add Net Manage	ment Control			
local-routing-config					
media-profile	Name	EmergencyRoute			
net-management-control	State	enable			
q850-sip-map	Туре	priority	•		
qos-constraints	Value	0			
response-map	Treatment	divert	•		
rph-policy	Next Hop	sag:e911group	•		
rph-profile	Realm Next Hop	SipTrunk	•		
service-health	Protocol Next Hop	SIP	•		
cossion-acont	Status Code	503			
session-agent	Cause Code	63			
session-agent-id-rule	Gap Rate Max Count	0			
session-constraints	Gap Rate Window Size	0			
session-group	Destination Identifier	911 🗙			

2////////

Note: Net-Management-Controls do not adhere to any constraints configured on your SBC due to the emergency nature of the call flows handled by this element.

realm-config identifier description network-interfaces mm-in-realm media-sec-policy rtcp-mux ice-profile teams-fqdn teams-fqdn teams-fqdn-in-uri sdp-inactive-only in-translationid access-control-trust-level net-management-control codec-policy rtcp-policy	Teams Realm facing Teams s1p0:0.4 enabled TeamsMediaSecurity enabled ice telechat.o-test06161977.com enabled 911removeplus high enabled addCN rtcpGen
---	--

14.1.2.3 Session Constraints for E911

In order for the SBC to have the ability to handle emergency calls in high volume environment, we recommend configuring and applying session constraints for each realm on your SBC to allow a small portion of your licensed sessions to be allocated to emergency calls.

The below example is a very basic constraint setup limiting the number of calls allowed to traverse a realm. For the purposes of this example, we assume there are 100 licensed sessions on the SBC, so we'll limit the number of calls on the realms to 90, leaving 10 licensed session for emergency calls. Again, as noted above, when net management controls are configured to handle emergency traffic, constraints do not apply to those calls.

GUI Path: session-router/session-constraints

ACLI Path: config t→session-router→session-constraints

ORACLE Enterprise Session Border Controller					
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)					
Configuration View Configuration Q					
iwf-config	*	Add Consists Constraints			
ldap-config					
local-policy		Name	E911Contraints		
local-response-map		State	✓ enable		
local-routing-config		Max Sessions	90		

And now we'll assign this constraint to a realm:

ORACLE Enterprise Session Border Controller				
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)				
Configuration View Configuration) Q			
media-manager	•	Modify Realm Config		
codec-policy		KICF FUILY	rtcpGen	•
dns-alg-constraints		Constraint Name	E911Contraints	•

• Select OK at the bottom of each element when finished

14.2 Elin Gateway

The Oracle® Enterprise Session Border Controller supports E911 ELIN for Teams-enabled Enterprises using the ELIN Gateway SPL option. Enable this option in the global SPL configuration. The Oracle® Enterprise Session Border Controller supports up to 300 ELIN numbers simultaneously and it can reuse numbers allowing a greater number of emergency calls

For more information about the SBC's Emergency Location Identification Number (ELIN) Gateway Support, please refer to the <u>9.0.0 Configuration Guide, Starting on Page 20-29</u>

GUI Path: system/spl-config

ACLI Path: config t→system→spl-config

The only entry required to enable support for Elin Gateway is:

Elin-Gateway=<value>

Valid Values are either 30 or 60. This determines how long (minutes) the SBC will retain the mapping in memory. Default value is 30. For the purposes of testing, we increased that value to 60 minutes, as shown in the example below.

An optional configuration parameter:

Elin-Add-PSAP=<value>

Where <value> is one or more PSAP numbers. For multiple numbers, place the numbers within quotes, separate the numbers with a comma, and use no spaces. A single number does not require enclosure in quotes.

Examples: Elin-Add-PSAP=999 and Elin-AddPSAP="999,000,114"

By Default, Oracle delivers the SBC preconfigured with the 911 and 112 Public Safety Answering Point (PSAP) callback numbers

ORACLE Enterprise Session Border Controller			
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 1	72)		
Configuration View Configuration Q			
fraud-protection	•	Modify SPL Config	
host-route			
http-client		SPL Options	Elin-Gateway=60,Elin-Add-PSAP=933
http-server		Plugins	

• Select OK at the bottom of the page when finished adding the options

14.2.1 Sip-Manipulation for Teams ELIN

By Default, the Oracle SBC with Elin SPL enabled, looks at the <NAM> field in the metadata of an Invite to extract the ELIN numbers and the FROM User uri for mapping. Since Microsoft Teams sends the ELIN information in an <Elin> field, and to avoid any issues due to ani masking on the Teams side, we have created the following sip-manipulation rule to move the information in the <Elin> field to the <Nam> field, and we replace the User part of the FROM header with the user part of the PAI. The manipulation gets assigned to either the Teams Realm or Sip Interface, and assures proper Elin mapping in the SBC.

Note: If there is an existing Sip Manipulation rule already assigned as the in-manipulation-id on either the realm or sip interface, these rules would need to be added to that <u>existing manipulation</u>.



ALCI Path: config t→session-router→sip-manipulation

While this can be configured via the GUI, we are using the ACLI output to provide an example config for ease of viewing.

11/1/1

sip-manipulation	
name	ELIN_Support
header-rule	
name	StoreElin
header-name	Content-Type
action	store
msg-type	request
methods	Invite
element-rule	
name	storeelin
parameter-name	application/pidf+xml
type	mime
action	Store
companson-type	pattern-rule
header-rule	(<elin>)(.)(</elin>)
name	ReplaceNam
header-name	
action	manipulate
msa-type	request
methods	Invite
element-rule	
name	changenam
parameter-name	application/pidf+xml
type	mime
action	find-replace-all
comparison-type	pattern-rule
match-value	(<nam>)(.*)(</nam>)
new-value	\$1+\$StoreElin.\$storeelin.\$2+\$3
neader-rule	
hame	From
action	FIUII
msa-type	request
methods	Invite
element-rule	invito
name	changeuser
type	uri-user
comparison-type	pattern-rule
new-value	\$PAI_USER.\$0

15 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all of the configuration elements used in our examples, including some of the optional configuration features outlined throughout this document. Be aware that not all parameters may be applicable to every Oracle SBC setup, so please take this into consideration if planning to copy and paste this output into your SBC.

access-control	
realm-id	Teams
source-address	52.112.0.0/14
application-protocol	SIP
trust-level	high
access-control	
realm-id	Teams
source-address	52.120.0.0/14
application-protocol	SIP
trust-level	high
certificate-record	
name	BaltimoreRoot
common-name	Baltimore CyberTrust Root
certificate-record	
name	DigiCertGlobaRootG2
common-name	DigiCert Global Root G2
certificate-record	
name	DigiCertRoot
common-name	DigiCert Global Root CA
certificate-record	
name	SBCCertificateforTeams
state	California
locality	Redwood City
organization	Oracle Corporation
unit	Oracle CGBU-LABS BOSTON
common-name	telechat.o-test06161977.com
certificate-record	
name	WebServerInstance
state	California
locality	Redwood City
organization	Oracle Corporation
unit	Oracle CGBU-LABS BOSTON
common-name	telechat.o-test06161977.com
codec-policy	Cia Trumb Carda as
name	
allow-codecs	SILK:NU G722:NU PCMA:NU
add-codecs-on-egress	PCMU
codec-policy	
name	
allow-codecs	CN
adu-codecs-on-egress	CIN
nup-server	webServerInstance
http. state	dischlad
https.state	
nups-state	
us-prome	webservennstance

ice-profile name ice local-policy from-address 1911 to-address 911 +1911 source-realm Teams description Local policy to route emergency calls policy-priority emergency policy-attribute sag:e911group next-hop SipTrunk realm local-policy from-address to-address source-realm SipTrunk description Route calls from PSTN to Microsoft Teams Phone System Direct Routing policy-attribute next-hop sag:TeamsGrp realm Teams action replace-uri local-policy from-address to-address source-realm Teams description Route Calls from Teams Phone System Direct Routing to PSTN policy-attribute next-hop 10.1.2.30 realm SipTrunk media-manager options audio-allow-asymmetric-pt xcode-gratuitous-rtcp-report-generation media-profile name CN wideband subname payload-type 118 media-profile SILK name subname narrowband payload-type 103 clock-rate 8000 media-profile name SILK wideband subname payload-type 104 16000 clock-rate media-sec-policy **PSTNNonSecure** name media-sec-policy **TeamsMediaSecurity** name inbound TeamsSRTP profile mode srtp
protocol sdes outbound profile TeamsSRTP mode srtp protocol sdes net-management-control EmergencyRoute name type priority treatment divert next-hop sag:e911group realm-next-hop SipTrunk protocol-next-hop SIP destination-identifier 911 network-interface name s0p0 ip-address 10.1.2.4 netmask 255.255.255.0 gateway 10.1.2.1 network-interface name s1p0 ip-address 10.1.3.4 255.255.255.0 netmask gateway 10.1.3.1 ntp-config 216.239.35.0 server phy-interface s0p0 name operation-type Media phy-interface s1p0 name operation-type Media slot 1 realm-config identifier SipTrunk description Realm facing PSTN network-interfaces s0p0:0.4 enabled mm-in-realm media-sec-policy **PSTNNonSecure** access-control-trust-level high codec-policy SipTrunkCodecs ringback-trigger refer ringback-file ringback10sec.pcm realm-config identifier Teams description **Realm facing Teams** network-interfaces s1p0:0.4 mm-in-realm enabled media-sec-policy **TeamsMediaSecurity** enabled rtcp-mux ice-profile ice teams-fqdn telechat.o-test06161977.com teams-fqdn-in-uri enabled sdp-inactive-only enabled access-control-trust-level high net-management-control enabled codec-policy addCN

refer-call-transfer enabled rtcp-policy rtcpGen rtcp-policy name rtcpGen all-calls rtcp-generate sdes-profile name **TeamsSRTP** lifetime 31 session-agent hostname 10.1.2.30 ip-address 10.1.2.30 realm-id SipTrunk ping-method **OPTIONS** ping-interval 30 session-agent hostname e911.com ip-address 10.1.2.10 realm-id SipTrunk description Route emergency calls to this destination. session-agent sip.pstnhub.microsoft.com hostname 5061 port **StaticTLS** transport-method realm-id Teams **OPTIONS** ping-method ping-interval 10 refer-call-transfer enabled session-agent hostname sip2.pstnhub.microsoft.com 5061 port transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 10 refer-call-transfer enabled session-agent hostname sip3.pstnhub.microsoft.com port 5061 transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 10 refer-call-transfer enabled session-group group-name TeamsGrp sip.pstnhub.microsoft.com dest sip2.pstnhub.microsoft.com sip3.pstnhub.microsoft.com sag-recursion enabled 401,407,480 stop-sag-recurse session-group group-name e911group

description	Session Group for emergency calls
dest	e911.com
sag-recursion	enabled
home-realm-id	Teams
options	max-udp-length=0
allow-pani-for-trusted-only	disabled
add-ue-location-in-pani	disabled
npli-upon-register	disabled
sip-feature	
name	replaces
require-mode-inbound	Page
require-mode-outbound	Pass
sip-interface	1 400
realm-id	SipTrunk
sip-port	
address	10.1.2.4
allow-anonymous	agents-only
sip-interface	-
realm-ld	Ieams
sip-port address	10 1 3 /
nort	5061
transport-protocol	TLS
tls-profile	TeamsTLSProfile
allow-anonymous	all
in-manipulationid	RespondOptions
anonymous-priority	emergency
sip-profile	forreplaces
sip-manipulation	Charlefor 193
header-rule	Checkiol 103
name	check183
header-name	@status-line
action	manipulate
msg-type	reply
methods	Invite
element-rule	
name	IS183
type	status-code
comparison-type	nattern-rule
match-value	183
mime-sdp-rule	
name	if183
msg-type	reply
methods	Invite
action	manipulate
comparison-type	boolean Cabaak482 Cia482
match-value	\$CHECK 183.\$IS 183
name	au
action	manipulate
sdp-line-rule	
name	checkclineforsbcip

2/11/1/10

////

type С action store comparison-type pattern-rule match-value ^(.(?!(10.1.3.4))).*\$ mime-sdp-rule name delete183SDP msg-type reply methods Invite action delete comparison-type boolean match-value \$if183.\$au.\$checkclineforsbcip header-rule change183to180 name header-name @status-line action manipulate boolean comparison-type match-value \$if183.\$au.\$checkclineforsbcip element-rule name changestatus type status-code replace action 183 match-value 180 new-value element-rule name changereasonphrase reason-phrase type action replace match-value Session Progress new-value Ringing sip-manipulation name ELIN_Support header-rule StoreElin name header-name Content-Type action store msg-type request methods Invite element-rule name storeelin application/pidf+xml parameter-name type mime action store comparison-type pattern-rule match-value (<ELIN>)(.*)(</ELIN>) header-rule ReplaceNam name Content-Type header-name action manipulate request msg-type Invite methods element-rule name changenam parameter-name application/pidf+xml type mime find-replace-all action comparison-type pattern-rule

match-value (<NAM>)(.*)(</NAM>) \$1+\$StoreElin.\$storeelin.\$2+\$3 new-value header-rule **PAItoFrom** name From header-name action manipulate request msg-type methods Invite element-rule name changeuser type uri-user comparison-type pattern-rule new-value **\$PAI USER.\$0** sip-manipulation name **RespondOptions** header-rule name **RejectOptions** From header-name action reject msg-type request OPTIONS methods 200 OK new-value sip-profile forreplaces name replace-dialogs enabled spl-config spl-options Elin-Gateway=60, Elin-Add-PSAP=933 steering-pool ip-address 10.1.2.4 start-port 10000 end-port 10999 realm-id SipTrunk steering-pool ip-address 10.1.3.4 start-port 10000 end-port 10999 realm-id Teams system-config hostname oraclesbc.com description SBC connecting PSTN Sip Trunk to Microsoft Teams Phone System Direct Routing location Burlington, MA transcoding-cores 1 tls-global session-caching enabled tls-profile TeamsTLSProfile name end-entity-certificate **SBCCertificateforTeams** trusted-ca-certificates **BaltimoreRoot** DigiCertGlobalRootG2 mutual-authenticate enabled tls-profile name WebServerInstance end-entity-certificate WebServerInstance **BaltimoreRoot** trusted-ca-certificates DigiCertRoot



CONNECT WITH US



o oracle.com

Oracle Corporation, World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065, USA

Worldwide Inquiries Phone: +1.650.506.7000 Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, did including imply warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615