

Configuring the Oracle SBC with Microsoft Teams Direct Routing Carrier Hosting Model

**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.

## **1** Contents

2.1       ORACLE SEC       5         2.2       MICROSOFT TEAMS       5         3       REVISION HISTORY       6         4       INTENDED AUDIENCE       7         5       VALIDATED ORACLE VERSIONS       7         6       ABOUT TEAMS DIRECT ROUTING       7         7       INFRASTRUCTURE REQUIREMENTS       8         8       CONFIGURATION       9         8.1.1       Prerequisites       11         8.1.2       SEC Domain Name       11         8.1.3       SEC Domain Name       11         8.1.4       SEC Domain Name       12         9       ORACLE SEC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync       15         9.12       Network Configuration       16         9.13       Physical Interfaces       16         9.14       Network Configuration       17         9.2.1       Centrificate Records       17         9.2.2       TLS Profile       22         9.3.3       TRANSCONICURATION       26         9.3.4       Media Profiles       26         9.3.3       TRANSCONING CONTEGURATION	2	RELA	TED DOCUMENTATION	5
2.2       MICROSOFT TEAMS.       5         3       REVISION HISTORY       6         4       INTENDED AUDIENCE       7         5       VALIDATED ORACLE VERSIONS       7         6       ABOUT TEAMS DIRECT ROUTING.       7         7       INFRASTRUCTURE REQUIREMENTS.       8         8       CONFIGURATION       9         8.1.1       Prerequisites       11         8.1.2       About SBC Domain Name in Carrier Tenant.       11         8.1.3       SBC Domain Name in Carrier Tenant.       12         9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces.       16         9.1.4       Network Interfaces.       16         9.1.5       YSTEM-CONFIGURATION.       23         9.2       PL: Ortificate Records       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.3.3       TRANSCONICURATION       26         9.3.4       Media Profiles       26		2.1 (	ORACLE SBC	5
3       REVISION HISTORY		2.2	MICROSOFT TEAMS	5
4       INTENDED AUDIENCE       7         5       VALIDATED ORACLE VERSIONS       7         6       ABOUT TEAMS DIRECT ROUTING       7         7       INFRASTRUCTURE REQUIREMENTS       8         8       CONFIGURATION       9         8.1.1       Prerequisites       11         8.1.2       About SEC Domain Name       11         8.1.3       SBC Domain Name       11         8.1.4       SBC Domain Name in Carrier Tenant       11         8.1.4       SBC Domain Name in Carrier Tenant       11         8.1.4       SBC Domain Name in Carrier Tenant       11         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync       15         9.1.2       Network Configuration       16         9.1.3       Network Interfaces       16         9.1.4       Network Interfaces       16         9.1.2       Certificate Records       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.3       TRANSCODINC CONFIGURATION       26         9.3.1       Media Security       23         9.4       MEDIA CONFIGURATION       29 </td <td>3</td> <td>REVI</td> <td>SION HISTORY</td> <td>6</td>	3	REVI	SION HISTORY	6
5       VALIDATED ORACLE VERSIONS	4	INTE	NDED AUDIENCE	7
6       ABOUT TEAMS DIRECT ROUTING.	5	VALI	DATED ORACLE VERSIONS	
7       INFRASTRUCTURE REQUIREMENTS.       8         8       CONFIGURATION       9         8.1.1       Prerequisites       11         8.1.2       About SBC Domain Name       11         8.1.3       SBC Domain Name in Carrier Tenant.       11         8.1.4       SBC Domain in Customer Tenant.       12         9       ORACLE SBC CONFIGURATION       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces.       16         9.1.4       Network Configuration       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.3       TRANSCONING CONFIGURATION       26         9.3.2       Odde Policies       26         9.3.3       RTANSCONING CONFIGURATION       26         9.3.4       ICE Profile       28         9.4.1       Media Manager       29         9.4.1       Media Manager       29         9.4.1       Media Manager       29         9.4.1       Media Manager       29         9.5.5       Sip-Config       33         9.5	6	AROI		7
7       INFRASTRUCTORE REQUIREMENTS	7		ACTRUCTURE REQUIREMENTS	
8       CONFIGURATION       9         8.1.1       Prerequisites       11         8.1.2       About SEC Domain Name       11         8.1.3       SEC Domain Name in Carrier Tenant.       11         8.1.4       SBC Domain in Customer Tenant.       12         9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces.       16         9.1.4       Network Interfaces.       16         9.1.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.3       TRANSCOINC CONFIGURATION       26         9.3.1       Media Security       23         9.3.2       Codee Policies       26         9.3.3       RTCP Policy       28         9.4       Media Profiles       29         9.4.4       Media Amager       29         9.4.3       Steering Pools       31         9.5.1       Sip CONFIGURATION       32         9.5.2	/	INFK	ASTRUCTURE REQUIREMENTS	ð
8.1.1       Prerequisites       11         8.1.2       About SBC Domain Name       11         8.1.3       SBC Domain In Customer Tenant       11         8.1.4       SBC Domain in Customer Tenant       12         9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.5       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.4.4       Media Configuration       26         9.3.4       ICE Profile       28         9.4.4       Media Anager       29         9.4.1       Media Manager       29         9.4.2       Realm Config       33         9.5.1	8	CONF	FIGURATION	
8.1.2       About SBC Domain Name       11         8.1.3       SBC Domain in Customer Tenant.       11         8.1.4       SBC CONFIGURATION       12         9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.2       Certificate Records       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Code Policies       26         9.3.3       RTCP Policy       28         9.4       MEDIA CONFIGURATION       29         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Co		8.1.1	Prerequisites	
8.1.3       SBC Domain Name in Carrier Tenant.       11         8.1.4       SBC Domain in Customer Tenant.       12         9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.4       Network Interfaces       16         9.1.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3.1       Media Profiles       26         9.3.2       Code Policies       26         9.3.3       RTCP Policy       28         9.4       MeDIA CONFIGURATION       29         9.4.1       Media Manager       29         9.4.2       Realm Config       33         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4		8.1.2	About SBC Domain Name	
8.1.4       SBC Domain in Customer Tenant       12         9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces.       16         9.1.4       Network Interfaces.       16         9.1.5       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security.       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.4       MEDIA CONFIGURATION       29         9.4.1       Media Manager       29         9.4.1       Media Manager       29         9.4.1       Media Manager       30         9.5       SIP CONFIGURATION       32         9.5.1       Sip Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip		8.1.3	SBC Domain Name in Carrier Tenant	
9       ORACLE SBC CONFIGURATION       14         9.1       SYSTEM-CONFIG       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.4       Network Interfaces       16         9.1.4       Network Interfaces       16         9.1.4       Network Interfaces       16         9.1.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Code c Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       29         9.4.4       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5.5       Sip ConFiguration		8.1.4	SBC Domain in Customer Tenant	
9.1       SYSTEM-CONFIG.       14         9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.5       SECURTY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       29         9.4.4       Realm Config       29         9.4.4       Realm Config       30         9.4.2       Realm Config       30         9.5.5       Sip ConFigURATION       32         9.5.6       Sersion Agents       36         9.5.7       Sip ConFiguration       32 <td>9</td> <td>ORAC</td> <td>CLE SBC CONFIGURATION</td> <td></td>	9	ORAC	CLE SBC CONFIGURATION	
9.1.1       NTP-Sync.       15         9.1.2       Network Configuration       16         9.1.3       Physical Interfaces.       16         9.1.4       Network Interfaces.       16         9.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       29         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       Sip Config       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Router Config       38 <td></td> <td>9.1 .</td> <td>System-Config</td> <td></td>		9.1 .	System-Config	
9.1.2       Network Configuration       16         9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.4       Network Interfaces       16         9.1.5       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       28         9.4.4       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Group       37         9.6       Routing Config <td< td=""><td></td><td>9.1.1</td><td>NTP-Sync</td><td></td></td<>		9.1.1	NTP-Sync	
9.1.3       Physical Interfaces       16         9.1.4       Network Interfaces       16         9.1.4       Network Interfaces       16         9.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       29         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Group       37         9.6       ROUTING CONFIGURATION       38         9.6.1       LRT       38		9.1.2	Network Configuration	
9.1.4       Network Interfaces       16         9.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       29         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Group       37         9.6.1       LRT       38         9.6.1       LRT       38         9.6.1       LRT       38         9.6.3		9.1.3	Physical Interfaces	
9.2       SECURITY CONFIGURATION       17         9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       28         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Group       37         9.6       ROUTING CONFIGURATION       38         9.6.1       LRT       38         9.6.2       Local Routing Config       39		9.1.4	Network Interfaces	
9.2.1       Certificate Records       17         9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.3.4       ICE Profile       28         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       Sip ConFiguRATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Group       37         9.6       Routing Config       38         9.6.1       LRT       38         9.6.2       Local Routing Config       39         9.6.4       Local Policy Config       40         9.6.4       Local Policy Configuration       40 <td></td> <td>9.2</td> <td>Security Configuration</td> <td></td>		9.2	Security Configuration	
9.2.2       TLS Profile       22         9.2.3       Media Security       23         9.3       TRANSCODING CONFIGURATION       26         9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       26         9.3.4       ICE Profile       28         9.3.4       ICE Profile       29         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       33         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Group       37         9.6       ROUTING CONFIGURATION       38         9.6.1       LRT       38         9.6.1       LRT       38         9.6.2       Local Routing Config       39         9.6.3       Session Router Config       39         9.6.4       Local Policy Configuration       40		9.2.1	Certificate Records	
9.2.3       Media Security		9.2.2	TLS Profile	
9.3       TRANSCODING CONFIGURATION		9.2.3	Media Security	
9.3.1       Media Profiles       26         9.3.2       Codec Policies       26         9.3.3       RTCP Policy       28         9.3.4       ICE Profile       28         9.4       MEDIA CONFIGURATION       29         9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Group       37         9.6       ROUTING CONFIGURATION       38         9.6.1       LRT       38         9.6.2       Local Routing Config       39         9.6.3       Session Router Config       39         9.6.4       Local Policy Configuration       40         9.7       SIP ACCESS CONTROLS       44		9.3 '	TRANSCODING CONFIGURATION	
9.3.2Codec Policies269.3.3RTCP Policy289.3.4ICE Profile289.3.4ICE Profile289.4MEDIA CONFIGURATION299.4.1Media Manager299.4.2Realm Config309.4.3Steering Pools319.5SIP CONFIGURATION329.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.3.1	Media Profiles	
9.3.3RTCP Policy		9.3.2	Codec Policies	
9.3.4ICE Profile289.4MEDIA CONFIGURATION299.4.1Media Manager299.4.2Realm Config309.4.3Steering Pools319.5SIP CONFIGURATION329.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.3.3	RTCP Policy	
9.4MEDIA CONFIGURATION299.4.1Media Manager299.4.2Realm Config309.4.3Steering Pools319.5SIP CONFIGURATION329.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.7SIP ACCESS CONTROLS44		9.3.4	ICE Profile	
9.4.1       Media Manager       29         9.4.2       Realm Config       30         9.4.3       Steering Pools       31         9.5       SIP CONFIGURATION       32         9.5.1       Sip-Config       33         9.5.2       Replaces Header Support       34         9.5.3       Sip Interface       35         9.5.4       Session Agents       36         9.5.5       Session Group       37         9.6       ROUTING CONFIGURATION       38         9.6.1       LRT       38         9.6.2       Local Routing Config       39         9.6.3       Session Router Config       40         9.6.4       Local Policy Configuration       40         9.7       SIP Access Controls       44		9.4 I	Media Configuration	
9.4.2Realm Config309.4.3Steering Pools319.5SIP CONFIGURATION329.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.7SIP ACCESS CONTROLS44		9.4.1	Media Manager	
9.4.3Steering Pools319.5SIP CONFIGURATION329.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.4.2	Realm Config	
9.5SIP CONFIGURATION329.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.4.3	Steering Pools	
9.5.1Sip-Config339.5.2Replaces Header Support349.5.3Sip Interface359.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.5	SIP CONFIGURATION	
9.5.2Replaces Header Support		9.5.1	Sip-Config	
9.5.3Sip Interface		9.5.2	Replaces Header Support	
9.5.4Session Agents369.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.5.3	Sip Interface	
9.5.5Session Group379.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.5.4	Session Agents	
9.6ROUTING CONFIGURATION389.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.5.5	Session Group	
9.6.1LRT389.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.6	ROUTING CONFIGURATION	
9.6.2Local Routing Config399.6.3Session Router Config409.6.4Local Policy Configuration409.7SIP ACCESS CONTROLS44		9.6.1	LRT	
9.6.3Session Router Config		9.6.2	Local Routing Config	
9.6.4 Local Policy Configuration		9.6.3	Session Router Config	
9.7 SIP ACCESS CONTROLS 44		9.6.4	Local Policy Configuration	
		9.7	SIP Access Controls	

/ / / 1

10 VERIFY CONNECTIVITY	
10.1 OCSBC OPTIONS PING	
10.2 MICROSOFT SIP TESTER CLIENT	
11 SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS:	
11.1 TERMINOLOGY	
11.2 REQUIREMENTS FOR INVITE MESSAGES	
11.2.1 Contact.Header Invite:	
11.3 REQUIREMENTS FOR OPTIONS MESSAGES	
11.3.1 Contact Header OPTIONS:	
11.4 MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS	
12 APPENDIX A	
12.1 SBC Behind NAT SPL configuration	
13 APPENDIX B	
13.1 RINGBACK ON INBOUND CALLS TO TEAMS AND EARLY MEDIA	
13.2 ORACLE SBC LOCAL MEDIA PLAYBACK	
13.2.1 Ringback on Transfer	
13.2.2 Media Files	
14 ACLI RUNNING CONFIGURATION	

### 2 Related Documentation

### 2.1 Oracle SBC

- Oracle® Enterprise Session Border Controller ESBC Configuration Guide
- Oracle® Enterprise Session Border Controller ACLI Reference Guide
- Oracle® Enterprise Session Border Controller Release Notes
- https://docs.oracle.com/cd/F12246\_01/doc/sbc\_scz900\_security.pdf

### 2.2 Microsoft Teams

- <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure</u>
- <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users</u>
- <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc</u>

# 3 Revision History

Version	Date Revised	Description of Changes
1.0	04/17/2019	Initial publication
1.1	10/09/2019	<ul> <li>Added GUI Configuration</li> <li>Firmware Version 8.3</li> <li>Modified Due to changes in MSFT Concept of Hosting Model</li> </ul>
1.2	03/26/2020	<ul> <li>Modified TLS Profile Config</li> <li>Change LRT example</li> <li>Added additional customer domain information</li> </ul>
1.3	04/29/2020	<ul> <li>Added Alert</li> <li>Add Important Information Section</li> </ul>
1.4	06/08/2020	<ul> <li>Changed Running Config Output</li> <li>Added Appendix C with Notes</li> <li>Added notes regarding Sip Manipulation and new release</li> </ul>
1.5	01/07/2022	Removed Reference to sip-all fqdn
1.6	03/31/2022	<ul> <li>9.0 Refresh</li> <li>Removed sip manips</li> <li>Added ACLs for new Teams subnets</li> </ul>
1.7	08/21/2022	<ul> <li>Added DigiCert Global G2 Root Certificate config and screenshots</li> <li>Modified TLS Profile</li> </ul>
1.8	07/20/2024	<ul> <li>Removed reference to ping- response parameter and added notes for using tls-global config in ACLI</li> </ul>

## 4 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 +.

# 5 Validated Oracle Versions

Microsoft has successfully conducted testing with the Oracle Communications SBC versions:

SCZ830/SCZ840/SCZ900

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

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

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

# 6 About Teams Direct Routing

Microsoft Teams Direct Routing allows a customer provided SBC to connect to Microsoft Phone System. The customer provided SBC can be connected to almost any telephony trunk or interconnect 3rd party PSTN equipment. The scenario allows:

- Use virtually any PSTN trunk with Microsoft Phone System.
- Configure interoperability between customer-owned telephony equipment, such as 3rd party PBXs, analog devices, and Microsoft Phone System

# 7 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 <u>Plan Direct Routing</u> 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	

# 8 Configuration

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

Below shows the connection topology example for MSFT Teams Carrier Model. There are multiple connections shown:

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



These instructions cover configuration steps between the Oracle SBC and Microsoft Teams Direct Routing Interface. The interconnection of other entities, such as connection of the SIP trunk, 3rd Party PBX and/or analog devices are not covered in this instruction. The details of such connection are available in other instructions produced by the vendors of retrospective components.

The below illustration and table are the Tenant Domain Structure used for this Application Note.



New Domain Name	Туре	Registered Tenant	Certificate SAN for SBC	Tenant Default Domain	FQDN presented in Contact header when sending Calls
Customers.telechat.0-test06161977.com	Base	Carrier	*.cusotmers.telechat.o- test06161977.com	Telechat.o-test06161977.com	NA, this is a service tenant, no users Sbc1.Customers.telechat. 0-test06161977.com
Sbc1.Customers.telechat.0- test06161977.com	Subdomain	Customer	*.cusotmers.telechat.o- test06161977.com	Solutionslab.cgbubedford.com	Sbc1.Customers.telechat. 0-test06161977.com
Sbc2.Customers.telechat.0- test06161977.com	Subdomain	Customer	*.cusotmers.telechat.o- test06161977.com	Woodgrovebank.us	Sbc2.Customers.telechat. 0-test06161977.co

### 8.1.1 Prerequisites

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- FQDN name for each registered subdomain representing individual tenants using the multitenant Direct Routing Trunk. Each FQDN must resolve to the Public IP address
- Public certificate, issued by one of the supported CAs (refer to <u>Related Documentation</u> for details about supported Certification Authorities).

#### 8.1.2 About SBC Domain Name

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 domain name. For example, on the picture below, the administrator registered the following DNS names for the tenant:

DNS Name	Can Be Used For SBC	Example of FQDN names
*.customers.adatum.biz	YES	Valid FQDN: <ul> <li>Sbc50.customers.adatum.biz</li> <li>Sbc51.customer.adatum.biz</li> <li>Ussbcsl5.customers.adataum.biz</li> <li>Europe.customers.adatum.biz</li> </ul> Invalid FQDN: <ul> <li>Sbc1.customers.europe.adatum.biz</li> <li>(this would require registering domain name "Europe.adatum.biz")</li> </ul>
adatumbiz.onmicrosoft.com	NO	Using *.onmicrosoft.com domains is not supported for SBC names

### 8.1.3 SBC Domain Name in Carrier Tenant

Below is an example of registered DNS names in the Carrier Tenant:

- Carrier Default Domain: telechat.o-test06161977.com
- Carrier Subdomain: customers.telechat.o-test06161977.com

Note: The above FQDN's are examples only and not to be used outside of this document. Please use FQDN's that are applicable to your environment.

	Microsoft 365 admin cent	er		
		<	Home > Domains	
ŵ	Home		View All domains	Q
R	Users	$\sim$	Domain name	Status
x	Groups	^	telechat.o-test06161977.com (Default)	Setup complete
	Groups		customers.telechat.o-test06161977.com	Setup complete
	Billing	$\sim$	solutionslab.onmicrosoft.com	Setup complete

After you have registered a domain name, you need to activate it by adding at least one licensed user with the SIP address matching the created base domain.

In the below example we have created the user <u>carriertest@customers.telechat.o-test06161977.com</u> in the carrier tenant to activate the carrier base domain:

	Microsoft 365 admin center		
	<	Home > Active users	
ŵ	Home	◯ Refresh         Views         All users         ▼         Search users         ✓	
8	Users ^	Display name Username	Status
	Active users	carrier test carriertest@customers.telechat.o-test06161977.	c Office 365 E5

### 8.1.4 SBC Domain in Customer Tenant

For each customer tenant, you must register a subdomain that belongs to a carrier that points to a customer tenant.

In the below example:

- Customer Tenant Default Domain: solutionslab.cgbubedford.com
- Carrier subdomain: sbc1.customers.telechat.o-test06161977.com

Note: The above FQDN's are examples only and not to be used outside of this document. Please use FQDN's that are applicable to your environment.

	Microsoft 365 admin center		
≡		Oracle	
ŵ	Home	Domains	
8	Users ^		
	Active users	+ Add domain 🗇 Buy domain 🖒 Refresh	
	Contacts	Domain name	Status
	Guest users	solutionslab.cgbubedford.com (Default)	Healthy
	Deleted users		
æ	Groups	productslab.onmicrosoft.com	🥑 Healthy
×	Groups v	sbc1.customers.telechat.o-test06161977.com	✓ Healthy

Same as the carrier tenant above, once you register the domain, you must activate it by adding at least one licensed user with the SIP address matching the carrier subdomain in the customer tenant.

Below, we have added the user <u>teamscustomer1@sbc1.customers.telechat.o-test06161977.com</u> to activate the carrier subdomain in the customer tenant.

	Microsoft 365 admin center		
=		Oracle	
ŵ	Home	Active users	
8	Users ^		
1	Active users	옷, Add a user 🖉 Add multiple users 👌 Multi-factor authentication 🖒 Refresh 🞍 Export Users \cdots	
	Contacts	Display name ↓ Username	Licenses
	Guest users	teams customer1 : teamscustomer1@sbc1.customers.telechat.o-test06161977.com	Office 365 E5

#### For the purposes of this example, the following IP address and FQDN's are used:

#### Note: all fqdn's listed below resolve to the same public IP address

FQDN Names	Public IP Address
customers.telechat.o-test06161977.com	141.146.36.68
sbc1.customers.telechat.o-test06161977.com	
sbc2.customers.telechat.o-test06161977.com	

# 9 Oracle SBC Configuration

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 accessed the OCSBC, 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 connection to MSFT Teams Direct routing to function properly.

Please note, the below configuration example assumes Media Bypass is enabled on the MSFT Teams Tenant. For differences in the OCSBC configuration for Non Media Bypass, please see Appendix A

ORACL	ORACLE Enterprise Session Border Controller						
NN3950-100 10	NN8/50-100 10138194100 SC290.0 Patch 3 (Build 245)						
Configuration View Configuration Q							
media-manager		•	Configuration Objects				
security		tty >					
session-router		•	Name	Description			
sustem			access-control	Configure a static or dynamic access control list			

### 9.1 System-Config

To configure 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 Ses	sion Border (	Controller	
NN3950-100 10.138.194.100 SCZ9.0.0	Patch 3 (Build 2	245)	
Configuration View Configuration	Q		
media-manager	×	Modify System Config	
security	•		
session-router	•	Hostname	customers.telechat.o-test06161977.cor
system	•	Description	Carrier SBC for Teams Carrier Hosting Model
fraud-protection			
host-route		Location	Burlington, MA
http-client		Mib System Contact	
http-server		Mib System Name	
network-interface		Mib System Location	
ntp-config		Acp TLS Profile	•
phy-interface		SNMP Enabled	✓ enable

• Click the OK at the bottom of the screen

### 9.1.1 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

	e Session Border	Controller
NN3950-100 10.138.194.100 SCZ	9.0.0 Patch 3 (Build	245)
Configuration View Configuration	on Q	
media-manager	•	Add NTP Config
security	•	
session-router	•	This object has not been created. Start editing and click OK to add.
system	•	Server 216.239.35.0 🗙
fraud-protection		

• Select OK at the bottom

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

### 9.1.2 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.

### 9.1.3 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 Sess	ion Border Co	ntroller					
NN3950-100 10.138.194.100 SCZ9.0.0 P	Patch 3 (Build 245	5)					
Configuration View Configuration	Q						
media-manager	•	Phy Int	erface	•			
security	•						
session-router	•	_					
system		[]; 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

### 9.1.4 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	S0p0	S1p0
IP Address	141.146.36.68	10.1.2.4
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	10.1.2.1
DNS Primary IP	8.8.8.8	
DNS Domain	telechat.o-test06161977.com	

	ession Border Co	ntroller												
NN3950-100 10.138.194.100 SCZ9.0.	0 Patch 3 (Build 24	5)	Dashboard											
Configuration View Configuration	Q													
media-manager	•	Netwo	work Interface											
security	•													
session-router	•													
system	*		£ 1	/ 6 6										
		Action	Sel	Name	Sub Port Id	Description	Hostname	IP Address						
fraud-protection				s0p0	0			141.146.36.68						
host-route														
http-client		1		slp0	0			10.1.2.4						

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

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

### 9.2 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

#### 9.2.1 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 wildcard certificate)
- Go Daddy sCert (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 (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.

#### 9.2.1.1 SBC End Entity Certificate

The SBC's end entity certificate is based on the Carrier Model domain structure outlined in the <u>Configuration</u> section of this document. This certificate record must include the following:

• Common name: Carrier Base Domain (customers.telechat.o-test06161977.com)

• Alternate Name: \*.Carrier Base Domain (\*.customers.telechat.o-test06161977.com)

To Configure the certificate record:

• Click Add, and configure the SBC certificate as shown below:

ORACLE Enterprise Set	ssion Border C	ontroller	
NN3950-100 10.138.194.100 SCZ9.0.0	Patch 3 (Build 2	45)	
Configuration View Configuration	Q		
media-manager	Þ	Modify Certificate Record	
security	•		
authentication-profile		Name	TeamsCarrierCert
certificate-record		Country	US
tls-global		State	California
tls-profile		Locality	Redwood City
session-router	•	Organization	Oracle Corporation
system	•	Unit	
		Common Name	customers.telechat.o-test06161977.cor
		Key Size	2048 🔻
		Alternate Name	*.customers.telechat.o-test06161977.o
		Trusted	✓ enable
		Key Usage List	digitalSignature 🗙
			keyEncipherment 🗙

• Click OK at the bottom

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

#### 9.2.1.2 Root CA and Intermediate Certificates

#### 9.2.1.2.1 GoDaddy CA

The following, DigitCertRoot, 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.

#### 9.2.1.2.2 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

#### 9.2.1.2.3 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	Enterprise Se	ession Bor	rder Co	ntroller						Û 🔺	admin 👻
NN3950-101 10.1	38.194.101 SCZ9.0.0	) Patch 3 (B	uild 290	)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q							Discard	😧 Verify	🖺 Save
media-manager	Þ	Certific	ate Re	ecord							
security	•										
authentication-p	rofile		1. 1.		/ G @				Search		Q
certificate-record	1	Action	Select	Name	Country	State	Locality	Organization	Unit	Comm	non Name
tls-global		:		BaltimoreRoot	US	МА	Burlington	Engineering		Baltim	ore CyberT
tls-profile session-router	•	:		DigiCertGlobalRootG2	US	МА	Burlington	DigiCert	www.digicert.com	DigiCe	ert Global Re
system	•	:		GoDaddyRoot	US	МА	Burlington	Engineering		GoDad	dy Class2 F
		:		TeamsCarrierCert	US	California	Redwood City	Oracle Corporation		telech	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 Enterp	orise Session B	order Co	ntroller						Û 🔺	admin 🔫
NN3950-101 10.13	18.194.101 S	CZ9.0.0 Patch 3	(Build 290	)			Dashbo	ard Configuration	Monitor and Trace	Widgets	Systam
Configuration	View Configu	uration Q								😟 Verity	🖹 Save
media-manager	►	Certif	icate Re	ecord							
security											
authentication-pr	rofile	D	₫. <u>↑</u>	± ₽KCS12					Search		Q
certificate-record		Action	Select	Name	Co	Confirm	cality	Organization	Unit	Comn	non Name
tls-global		:		BaltimoreRoot	US	Do you want to activate the configuration	? urlington	Engineering		Baltin	nore CyberT
tis-profile session-router	+	:		DigiCertGlobalRootG2	US	Confirm Cancel	urlington	DigiCert	www.digicert.com	DigiC	ert Global Ro
system	►	:		GoDaddyRoot	US	МА	Burlington	Engineering		GoDa	ddy Class2 F
		:		TeamsCarrierCert	US	California	Redwood City	Oracle Corporation	1	telech	at.o-test06'
		4									

#### 9.2.1.3 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:

NN3950-101 10.138.194	.101 SCZ9.0.	.0 Patch 3 (I	Build 290	)			Dashboard	Configuration	Monitor and Trace	Widgets	System
onfiguration	/ Configuration	Q							Discard	😟 Verify	🖪 Sa
media-manager	•	Certifi	cate Re	ecord							
security	•										
authentication-profile		D:	± 10 ±	▲ PKCS12	/ ₲ ₫				Search		Q
certificate-record		Action	Select	Name	Country	State	Locality	Organization	Unit	Comm	ion Name
tls-global		:		BaltimoreRoot	US	МА	Burlington	Engineering		Baltim	iore Cyber
session-router	Þ	:		DigiCertGlobalRootG2	US	MA Burlington	Burlington	DigiCert	www.digicert.com	DigiCe	rt Global I
system	•	:		GoDaddyRoot	US	MA	Burlington	Engineering		GoDad	ldy Class2:
		:		TeamsCarrierCert	US	California	Redwood City	Oracle Corporation		telecha	at.o-test0
		4									

Generate certificate response
Copy the following information and send to a CA authority
<ul> <li>BEGIN CERTIFICATE REQUEST</li> <li>MIC7jCCAdYCAQAwbDELMAkGAIUEBhMCVVMxCzAJBgNVBAgTAkIBMRMwEQYDVQQH</li> <li>EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEIMcMGAIUEAxMcdGVis</li> <li>ZWNoYXQubyI0ZXNOLTA2MTYxOTc3LmNvbTCCASIWDQYJKoZIhvcNAQEBBQADggEP</li> <li>ADCCAQoCggEBAK+uhx7951uhDGVQWvv4EoZE68WDLIDYPPYJWbvL5uW2K9y3Yn</li> <li>s40ca4ZuZWmrLNLLIZFV9x9R5XzQ4mv4BiJuVDCBCbowuautu/gxXSKIRESpfDZh</li> <li>NaAGUJrvAfvacyPz7KsyrJKgchzs0FNNJPDAaQsDQjuoFCDUbt0AIZ6xDFxpCdIF</li> <li>nhq+dtB7gAtCdWE/V6r4PAf1Idj82YT4YBAWQwQJ2vGn+yc2FtEPSmHIbWEICV</li> <li>s40G4U2TMSI/JAVcpF+jsJc8xsvtF±2r24REfCrcrm0llg0HRvEgYTluUteFo1y</li> <li>d/00avPYHgkkn250HQ2IwaMIIkMxpBjlpUCAwEAAaA9MDsGCSqGSIb3DQEJDjEu</li> <li>MCwwCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCcSqAQUFBwMBBggrBgEFBQcDAjAN</li> <li>BgkqhkiG9w0BAQ=FAAOCAQEAnBLJuRPL82rAQDIB3I2JeOf3tacevMQeCIGcdFCf</li> <li>uLcuKMvjBYkJweOrtDWvBZ901D2YbyuVNxPLbiD5JudWbJBAWud+9693VUVQb</li> <li>/UR5rooNKwQI0fJMNmuPMWI3/p7kVs1tk8aSwF6IHNx+k56MrR4SYFqV/z2C01s</li> <li>PeTYRy0VGYSQs0h5T5kcU0xjEXPJSK2pdQz8YGbIAbKZXcp1n7zJEwgtodmRnhZ</li> <li>r7Gm45145JA8Q0ped3H83aFg0Q8twMeVj9znA0ogle/g==</li> <li>END CERTIFICATE REQUEST</li> </ul>

Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, **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.

#### 9.2.1.4 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.

ORACLE	Enterpris	e Session Bo	order Co	ontroller						Û▲ 6	admin 👻
NN3950-101 10.138.19	94.101 SCZ9	2.0.0 Patch 3 (E	Build 290	))			Dashboa	rd Configuration	Monitor and Trace	Widgets	System
Configuration vi	iew Configurati	on Q							Discard	😧 Verify	🗄 Sa
media-manager	Þ	Certific	cate Re	ecord							
security	•				~						
authentication-profil	le	P	д. ·								6
certificate-record		L <sup>2</sup>	u¦ ⊥ Select	Name	Country	E‡ L≦	locality	Organization	Search	Commo	Q
tls-global		:	Jelect	BaltimoreRoot		ма	Burlington	Engineering	onix	Baltimo	ore Cybe
tls-profile				BaltimoreRoot			bunngton	Engineering		Datanio	ine cyber
session-router	•	:		DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCer	t Global
system	►	:		GoDaddyRoot	US	MA	Burlington	Engineering		GoDado	dy Class2
		:		TeamsCarrierCert	US	California	Redwood City	Oracle Corporati	on	telechat	t.o-testC
Format		try-all		•							
Import Certificat	e										
Format		try-all		•							
import Metriou		<ul> <li>File</li> <li>Paste</li> </ul>									
Paste		BEGIN C IMIHNIC CBW WGBACERA WGBACERA WGBACERA JMSkwJWP WGAQCYQ JMSkwJWP SMAAWADAY SMAAWADAY SMAAWADAY SMAAWADAY SMAAWADAY SMAAWADAY	ERTIFICA IggAwlBA 4AOWW2 DBP VQQGE VQQGE CBUTFM IggM2U5 DOGEwJV DOGEwJV	ATE A BIQC3C/HB ANBgkqhkiG JVUEV/MB UNIEnQgSW JBE UNIEnQgSW JBE UNIENQ AEFWOJMTA NTIaMIGKM VU2ETMBEG							

• 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:

#### 9.2.2 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

ORACL	Ent	erprise S	ession Border Controller								Û 🔺	admin 🔫
NN3950-101 10.	138.194.101	SCZ9.0.0	) Patch 3 (Build 290)					Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Con	figuration	Q							Discard	😧 Verify	B Save
media-manager	•	•	Modify TLS Profile									
security		,										
authentication-p	orofile		Name		TLSTeams							- 1
certificate-recor	d		End Entity Certificate		SBCCertificateforTeams	Ŧ						- 1
tls-global			Trusted Ca Certificates		BaltimoreRoot 🗙							- 1
tls-profile					DigiCertGlobalRootG2 🗶							
					GoDaddyRoot 🗙							
session-router	•	•	Cipher List									
system	•		-		DEFAULT 🗙	/	:					
			Verify Depth		10		(Range: 010)					- 11
			Mutual Authenticate		✓ enable							
			TLS Version		tlsv12	Ŧ						
			Options									-
			(	эк	Back							

• Select OK at the bottom

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

### 9.2.3 Media Security

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

#### 9.2.3.1 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

ORACLE Enterprise Ses	sion Border C	ontroller	
NN3950-100 10.138.194.100 SCZ9.0.0	Patch 3 (Build 24	45)	
Configuration View Configuration	Q		
media-manager	•	Modify Sdes Profile	
security	-		
admin-security	•	Name	SDES
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	•	Use Ingress Session Params	
ipsec	•	Options	
local-accounts		Key	
media-security	•	Salt	
dtls-srtp-profile		Srtp Rekey On Re Invite	
media-sec-policy		Lifetime	31

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

#### 9.2.3.2 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	ssion Border C	Controller		
NN3950-100 10.138.194.100 SCZ9.0.0	Patch 3 (Build 2	(45)		
Configuration View Configuration	Q			
auth-params		Modify Media Sec Policy		
authentication		Name	TeamsSRTP	
authentication-profile		Pass Through	enable	
cert-status-profile		Options	chabic	
certificate-record				
factory-accounts		Inbound		
ike		Profile	SDES 💌	
inc.		Mode	srtp	•
ipsec	•	Protocol	sdes	
local-accounts		Hide Egress Media Update	enable	
media-security	-			
dtls-srtp-profile		Outbound		
media-sec-policy		Profile	SDES 🔶	
media see poncy		Mode	srtp	▼
sdes-profile		Protocol	sdes	•

ORACLE Enterprise Ses	sion Border C	Controller		
NN3950-100 10.138.194.100 SCZ9.0.0	Patch 3 (Build 2	245)		
Configuration View Configuration	Q			
auth-params	•	Modify Media Sec Policy		
authentication		Name	PSTNNonSecure	
authentication-profile		Pass Through	enable	
cert-status-profile		Options		
certificate-record				
factory-accounts		🖌 Inbound		
ike	•	Profile	+	
insec		Mode	rtp	•
ipsee		Protocol	none	•
local-accounts		Hide Egress Media Update	enable	
media-security	-			
dtls-srtp-profile		Outbound		
the second s		Profile	•	
media-sec-policy		Mode	rtp	•
sdes-profile		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 advanced media termination features and transcoding.

### 9.3 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

### 9.3.1 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. 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										
NN3950-100 10.138.194.100 SCZ9.0.0	NR9590-100 10188194100 5C790.0 Patch 3 (Build 245) Configuration Monit										Monit
Configuration View Configuration	nfiguration View Configuration Q										
account-group	•										
allowed-elements-profile			Media I	Profile							
class-profile	•										
enforcement-profile	- 1		<b>[</b> ] f	t 1	🛓 / G 🗎						St
enum-config	- 1		Action	Sel	Name	Subname	Media Type	Payload Type	Transport	Clock Rate	
filter-config	- 1		÷		CN	wideband	audio	118	RTP/AVP	16000	
h323	•		:		SILK	narrowband	audio	103	RTP/AVP	8000	
http-alg	- 1		:		SILK	wideband	audio	104	RTP/AVP	16000	

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

#### 9.3.2 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. 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 $\rightarrow$  media-mangaer $\rightarrow$  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						
NN3950-100 10.138.194.100 SCZ9	NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)						
Configuration View Configuration	n Q						
media-manager	•	Modify Codec Policy					
codec-policy							
dns-alg-constraints		Name	addCN				
dns-config		Allow Codecs	* ×				
ice-profile		Add Codecs On Egress	CN X				
media-manager		Order Codecs					

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	ORACLE Enterprise Session Border Controller							
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)								
Configuration View Configuration	Q							
media-manager	•	Modify Codec Policy						
codec-policy								
dns-alg-constraints		Name	addSilkandCN					
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							
NN3950-100 10.138.194.100	NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)						
Configuration View Confi	guration Q						
media-manager	•	Modify Codec Policy					
codec-policy							
dns-alg-constraints		Name	SipTrunkCodecs				
dns-config		Allow Codecs	* x     PCMA:no x				
ice-profile			SILK:no 🗙 G/22:no 🗙				
media-manager		Add Codecs On Egress	PCMU 🗙				

• Select OK at the bottom

### 9.3.3 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							
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)							
Configuration View Configuration Q							
media-manager 🔹 🔻	Modify RTCP Policy						
codec-policy							
dns-alg-constraints	Name	rtcpGen					
dns-config	RTCP Generate	all-calls 🔹					

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

#### 9.3.4 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							
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)							
Configuration View Configuration Q							
media-manager 👻	Modify Ice Profile						
codec-policy							
dns-alg-constraints	Name	ice					
dns-config	Stun Conn Timeout	0					
ice-profile	Stun Keep Alive Interval	0					
	Stun Rate Limit	0					
media-manager	Mode	NONE					

When deploying the Oracle SBC with Microsoft Teams, we recommend changing the default values for Stun Conn Timeout, Stun Keep Alive Interval, and Stun Rate Limit to a value of 0 (zero) from their default values.

• 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.

#### 9.4 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.

#### 9.4.1 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	r Controller	
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build	d 245)	
Configuration View Configuration Q		
media-manager 🗸 🔻	Modify Media Manager	
codec-policy		500
dns-alg-constraints	Subsq Guard Timer	300
dos-config	TCP Flow Time Limit	86400
	TCP Initial Guard Timer	300
ice-profile	TCP Subsq Guard Timer	300
media-manager	Hnt Rtcp	enable
media-policy	Algd Log Level	NOTICE 💌
msrp-config	Mbcd Log Level	NOTICE 🔻
playback-config	Options	audio-allow-asymmetric-pt 🗙
realm-config		xcode-gratuitous-rtcp-report-
realm-group		generation ×
rtcp-policy		

• Click OK at the bottom

### 9.4.2 Realm Config

#### **Nested Realm for Teams**

Nested Realms is an OCSBC feature that supports hierarchical realm groups. One or more realms may be nested within a higher order realm. This allows the OCSBC to separate each tenant the Carrier Model SBC is servicing.

In this example we will create two realms facing MSFT Teams.

A parent realm for Teams and a child realm for a customer tenant. The parent realm will contain the carrier base domain, and the Tenant realm will contain the customer's carrier subdomain.

We'll also be creating a third, standalone realm facing PSTN.

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 three realms used in this configuration example

Config Parameter	Teams Realm	Tenant Realm	PSTN Realm
Identifier	Teams	Teams_Cust1	SipTrunk
Network Interface	s0p0:0	s0p0:0	s1p0:0
Mm in realm	$\checkmark$	$\checkmark$	$\checkmark$
Media Sec policy	TeamsSRTP	TeamsSRTP	PSTNNonSecure
Teams-FQDN	Customers.telechat.o- test06161977.com	Sbc1.customers.telechat.o- test06161977.com	
Teams-fqdn-in-uri	$\checkmark$	$\checkmark$	
Sdp-inactive-only	$\checkmark$	$\checkmark$	
RTCP mux	$\checkmark$	$\checkmark$	
ice profile	Ice (required for media bypass only)	Ice (required for media bypass only)	
Codec policy	addCN	addCN	SipTrunkCodecs
RTCP policy	rtcpGen	rtcpGen	
Access-control-trust-level	HIGH	HIGH	HIGH
Parent Realm		Teams	

Additional Realms can be added, one for each customer tenant the Oracle SBC is servicing. The carrier subdomain registered in each tenanr needs to be added under the "Teams-FQDN" parameter in the realm.

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								
NN3950-100 10.138.194.100 SCZ9.0.0 P	NN3950-100 10138.194.100 SCZ9.0.0 Patch 3 (Build 245)							
Configuration View Configuration Q								
media-manager Realm Config								
codec-policy								
media-manager								
media-policy		D t	1. 1	🕹 🧷 🔁 🖻				
includ policy		Action	Sel	Identifier	Description	Addr Prefix	Network Interfaces	
realm-config		:		SIPTrunk	Realm Facing PSTN	0.0.0.0	s1p0:0	
steering-pool								
security	►			Teams	Carrier Tenant Facing Teams Direct Routing Inte	0.0.0.0	s0p0:0	
session-router	Þ	÷		Teams_Cust1	Realm to service Customer, woodgrovebank.us	0.0.0.0	s0p0:0	

• Select OK at the bottom of each

### 9.4.3 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						
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3	3 (Build 245)					
Configuration View Configuration Q						
media-manager	Modify Steering Pool					
codec-policy						
dns-alg-constraints	IP Address	10.1.2.4				
dns-config	Start Port	10000				
ice-profile	End Port	19999				
ice-prome	Realm ID	SIPTrunk				

ORACLE Enterprise Session Border Controller							
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)							
Configuration View Configuration Q							
media-manager 🗸 👻	Modify Steering Pool						
codec-policy							
dns-alg-constraints	IP Address	141.146.36.68					
dns-config	Start Port	20000					
ice-profile	End Port	29999					
	Realm ID	Teams 🔹					

• Select OK at the bottom

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

### 9.5 Sip Configuration

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

### 9.5.1 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).

NN3950-100 10138194100 SCZ90 0 Patch 3 (Build 2	ontroller		
Configuration View Configuration Q			
security	Modify SIP Config		
session-router 💌			
access-control	State	✓ enable	
account-config	Dialog Transparency	✓ enable	
filter-config	Home Realm ID	Teams	•
ldap-config	Egress Realm ID		•
local-policy	Nat Mode	None	•
local-routing-config	Registrar Domain	*	
media-profile	Registrar Host	*	
session-agent	Registrar Port	5060	
session-group	Init Timer	500	
session-recording-group	Max Timer	4000	
session-recording-server	Trans Expire	32	
	Initial Inv Trans Expire	0	
session-translation	Invite Expire	180	
sip-config	Session Max Life Limit	0	
sip-feature	Enforcement Profile		•
sip-interface	Red Max Trans	10000	
sip-manipulation	Options	max-udp-length=0 🗙	

• Select OK at the bottom

### 9.5.2 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:

#### 9.5.2.1 Sip Feature

The sip feature configuration element allows 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 Ses	ssion E	Border C	Controller		
NN3950-100 10.138.194.100 SCZ9.0.0	Patch	3 (Build 2	245)		
Configuration View Configuration	Q				
security	►	*			
session-router	•		Modify SIP Feature		
access-control			Name	replaces	
account-config			Realm	Teams	
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

#### 9.5.2.2 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						
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build	1 245)					
Configuration View Configuration Q						
session-constraints	Modify SIP Profile					
session-group						
session-recording-group	Name	forreplaces				
session-recording-server	Redirection	inherit	•			
session-router	Ingress Conditional Cac Admit	inherit	•			
session-timer-profile	Egress Conditional Cac Admit	inherit	•			
session-translation	Forked Cac Bw	inherit	•			
sip-advanced-logging	Cnam Lookup Server		•			
sip-config	Cnam Lookup Dir	egress	•			
sip-feature	Cnam Unavailable Ptype					
sip-feature-caps	Cnam Unavailable Utype					
sin-interface	Replace Dialogs	enabled				

• Click OK at the bottom

#### 9.5.3 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. You only need to configure a single sip interface facing Microsoft Teams Direct Routing. All realms for customers tenants inherit the sip interface from the Teams parent realm

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	141.146.36.68
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TeamsTLSProfile
Allow anonymous	agents-only	all
in-manipulationid		RespondOptions

ORACLE Enterprise Session Border Controller								
NN3950-100 10.138.194.100 SCZ9.0.0 Pate	NN3950-100 10138194100 SC29.0.0 Patch 3 (Build 245)							
Configuration View Configuration Q								
rph-policy	•	SID Inte	orfaco					
rph-profile			indee					
service-health								
session-agent		🗅 t	1 1	🛃 🖉 🖸 🗇				
carrien agent id rule		Action	Sel	State	Realm ID	Description		
session-agent-iu-rue		:		enabled	SIPTrunk	Sip Interface facing PSTN		
session-group		÷		enabled	Teams	Sip Interface facing Microsoft Teams Dir		

Notice this is where we assign the TLS profile configured under the <u>Security</u> section of this guide, and the <u>sipprofile</u> which allows the SBC to act on the Replaces header when received by Microsoft Teams.

• Select OK at the bottom of each when applicable

#### 9.5.4 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

You will need to configure three Session Agents for the Microsoft Direct Routing Interface

• 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

ORACLE Enterprise Session Border Co	ontroller								
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 24	45)							Dashboard Config	uration Monit
Configuration View Configuration Q									
media-profile	redis-profile Session Agent								
net-management-control									
q850-sip-map		1: ±	1 / 6 8						Si
qos-constraints	Action	Sel	Hostname	IP Address	Port	State	App Protocol	Realm ID	
response-map	:		sip.pstnhub.microsoft.com		5061	enabled	SIP	Teams	
rph-policy			sip2.pstnhub.microsoft.com		5061	enabled	SIP	Teams	
rph-profile service-health	:		sip3.pstnhub.microsoft.com		5061	enabled	SIP	Teams	

Next, we'll configure a session agent for PSTN

ORACLE Enterprise Session Border Cor	ntroller								
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)							Dashboard	Configuration	
Configuration View Configuration Q									
rph-profile ^	Session A	ion Agent							
service-health									
session-agent	_								
session-agent-id-rule	🗅 🕸								
	Action Sel	Hostname	IP Address	Port	State	App Protocol	Realm ID		
session-constraints	: 0	10.1.2.30	10.1.2.30	5060	enabled	SIP	SipTrunk		

• Select OK at the bottom

### 9.5.5 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:

ORACLE Enterprise Session Border C	ontroller	
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 2	45)	
Configuration View Configuration Q		
media-profile	Modify Session Group	
net-management-control	Course Manua	
q850-sip-map	Group Name	TeamsGRP
qos-constraints	Description	
response-map		
rph-policy	State	✓ enable
rph-profile	App Protocol	SIP
service-health	Strategy	Hunt 💌
session-agent	Dest	sip.pstnhub.microsoft.com 🗙
session-agent-id-rule		sip2.pstnhub.microsoft.com 🗙
session-constraints		sip3.pstnhub.microsoft.com 🗙
session-group	Trunk Group	
session-recording-group	Sag Recursion	💽 enable

• Click OK at the bottom

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

### 9.6 Routing Configuration

This section outlines how to configure the OCSBC to route Sip traffic to and from Microsoft Teams Direct Routing Interface.

The OCSBC has multiple routing options that can be configured based on environment. For this example configuration, we are utilizing the OCSBC's multistage local policy routing feature along with DID separation via local route table.

A routing stage signifies a re-evaluation of local policy based on the results of a local policy lookup. In the simplest, single stage case, the Session Border Controller performs a local policy lookup on a SIP message's Request URI. The result of that local policy lookup is a next hop FQDN, IP address, ENUM lookup, or LRT lookup; that result is where the Session Border Controller forwards the message. In the multistage routing model, that resultant next hop is used as the lookup key for a second local policy lookup

### 9.6.1 LRT

The OCSBC supports LRT, an XML document that contains either E164 telephone numbers or strings-to-SIP-URI mappings. An iLRT is configured and transferred from the development environment to the OCSBC /code/Irt directory. After installation and configuration, the LRT is available for SIP Request routing. For more information on creating and configuring LRT, please see the <u>OCSBC 9.0 Configuration Guide</u>, Chapter 8.

The following is an example Lrt file, once created, will be placed in the /code/lrt directory on the OCSBC

xml version="1</td <td>.0" encoding="UTF-8" standalone="yes"?&gt;</td>	.0" encoding="UTF-8" standalone="yes"?>
<localroutes td="" xml<=""><td>ns:xsi="http://www.w3.org/2001/XMLSchema-instance"&gt;</td></localroutes>	ns:xsi="http://www.w3.org/2001/XMLSchema-instance">
Customer 1 T</td <td>enant: solutionslab.cαbubedford.com/sbc1.customers.telechat.o-test06161977.com&gt;</td>	enant: solutionslab.cαbubedford.com/sbc1.customers.telechat.o-test06161977.com>
<route></route>	
	anort singa-"ragay"s 10 shan 10 @chat austamara talaabat a taat06161077 aanta/nayts
la su ta	<iext type="regex">:". :sip.io@suct.customers.telechat.o-testoorora/r.com:</iext>
<route></route>	
	<user type="E164">17814437247</user>
	<next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
<routes< td=""><td></td></routes<>	
	<user type="E104">17814437243<user></user></user>
	<next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
Customer 2 Te</td <td>enant – woodgrovebank.us/sbc2.customers.telechat.o-test06161977.com&gt;</td>	enant – woodgrovebank.us/sbc2.customers.telechat.o-test06161977.com>
<route></route>	
	<user tyne="F164">17814437243-/user&gt;</user>
	anot supple 2 rot 2 rot 10 the 10 and 1
la ser la	<pre><next type="regex">: : :sip.iv@sbc2.customers.telechat.o-testororora/r.com;<mext></mext></next></pre>
<route></route>	
	<user type="E164">17814437244</user>
	<pre><next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next></pre>
<route></route>	
	(1551  type = 104 + 1/0.1443/300 (1051)
	<next type="regex">!"."!sip:\U@sbc2.customers.telechat.o-testU61619//.com!</next>

The LRT file, once created, can be copied to the /code/Irt directory of the SBC via SFTP to the management IP, or uploaded through the GUI:

#### 9.6.1.1 GUI Upload of LRT File

- At the top, click on the System Tab
- Left Hand side, expend File Management and select Local Route Table
- Click Upload
- Browse to select file to upload to SBC
- Check box "Activate LRT file after upload"
- Click Upload

ORACLE Enterprise Session Border O		
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 2	245)	
System Configuration Assistant		
File Management 💌	Local Route Table	
Backup Configuration		
Configuration CSV		
Local Route Table		
Fraud Protection Table		
Log		
Audit Log		
Playback Media		Upload file 🗙 🗙
Software Image		tamsLRT.xml.gz
SPL Plug In		<ul> <li>Activate the LRT file after upload</li> </ul>
Configuration Template		Upload Cancel S
System Operations		

### 9.6.2 Local Routing Config

After moving the DID-range-based LRT to the /code/Irt directory on the OCSBC, use the following procedure to specify the file's location, and the lookup method.

GUI Path: session-router/local-routing-config

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

Click Add, use the following as an example to configure

Note: the file name field below is the full name of the LRT file that has been placed in the /code/lrt directory on the OCSBC

ORACLE Enterprise Session Border Controller								
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 245)								
Configuration View Configuration Q								
security								
session-router 🔻	Add Local Routing Config							
access-control	Name	TeamsLRT						
account-config	File Name	TeamsLRT.xml.gz						
filter-config	Prefix Length	0						
ldap-config	String Lookup	enable						
local-policy	Retarget Requests	✓ enable						
local-routing-config	Match Mode	exact 💌						

### 9.6.3 Session Router Config

Session router config allows for the SBC to perform multistage routing.

GUI Path: session-router/session-router

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

Use the following example to configure session router config:

ORACLE Enterprise Session Border C	ontroller			
NN3950-100 10.138.194.100 SCZ9.0.0 Patch 3 (Build 2	45)			
Configuration View Configuration Q				
local-response-map	Add Session Router			
local-routing-config				
media-profile	This object has not been	created	1. Start editing	and click OK to a
net-management-control	State		🗸 enable	
q850-sip-map	System Number Type		Pots	•
qos-constraints	Match Lp Src Parent Realm		enable	
response-map	Nested Realm Stats		enable	
rph-policy	Reject Message Threshold		0	
rph-profile	Reject Message Window		10	
	Force Report Trunk Info	enable		
	Additional Lp Lookups	1		(Range: 05)
	Max Routes Per Lookup	0		(Range: 0999999999)
	Total Lp Routes	0		(Range: 0999999999)
	Multi Stage Src Realm Override	🗸 enable		

Click OK at the bottom

### 9.6.4 Local Policy Configuration

Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

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

To route Sip traffic to and from Microsoft Teams Direct Routing Interface, the following local policies will need to be configured.

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

ORACLE Enterprise Ses	sion B	order Cor	troller					
NN3950-100 10.138.194.100 SCZ9.0.0	Patch 3	5 (Build 245	)					
Configuration View Configuration	Q							
account-group allowed-elements-profile		•	Modify	Local	Policy			
class-profile	►		From Add	ress		* X		
enforcement-profile			To Addres	S		* ×		
enum-config filter-config			Source Re	alm		SIPT	runk 🗙	
h323	►		Descriptio	n				
http-alg								
iwf-config			State			🗸 en	able	
ldap-config			Policy Price	ority		none		•
local-policy			Policy Attr	ibutes				
local-response-map			D,	/	ē 🗇			
local-routing-config			Action	Sel	Next Hop		Realm	Action
media-profile			:		Irt:TeamsLRT		SIPTrunk	none

#### Policy Attribute:

	ssion Bor	rder Controller		
Configuration	D Patch 3 (E	Build 245)		
Configuration	Ч.			
account-group		<ul> <li>Modify Local</li> </ul>	policy / policy attribute	
allowed-elements-profile			policy / policy attribute	
class-profile	•	Next Hop	Irt:TeamsLRT	•
enforcement-profile		Realm	SIPTrunk	-
enum-config		Action	none	•
filter-config		Terminate Recursio	on enable	
h323	- <b>F</b>	Cost	0	
http-alg		State	✓ enable	
iwf-config		App Protocol		•
ldap-config		Lookup	multi	•

The above local policy utilizes the <u>Irt /local-routing-config</u>- outlined previously in this document. This is a way to identify the terminating tenant/subdomain when the core network ie..SIPTrunk, does not identify the target in the Request-Uri host. When the target subdomain/tenant is identified in the Request-Uri host, the following local policies will route directly to Teams Group by to-address match.

• Call from Sip Trunk to Customer 1 Tenant:

ORACLE Enterprise Se	ession Borde	r Controller						
NN3950-100 10.138.194.100 SCZ9.0.	0 Patch 3 (Buil	ld 245)						
Configuration View Configuration	Q							
media-manager	•	Mod	ify Loca	l Policy				
security	•							
session-router	-	From /	ddress		* ×			
access-control	- 1	To Add	ress		sbc1	.customers.telechat.o-		
account-config	- 1				test ×	06161977.com		
filter-config								
ldap-config	- 1	Source	Realm		SIPT	runk 🗙		
local-policy		Descri	otion					
local-routing-config	- 1							
media-profile								
session-agent	- 1	State			🗸 en	able		
session-group	- 1	Policy	Priority		none		•	
session-recording-group		Policy	Attributes					
session-recording-server	- I.	D	P	ā 🗇				
session-translation		Actio	n Sel	Next Hop		Realm	Actio	on
sip-config		:		sag:TeamsGRP		Teams_Cust1	repla	ace-uri

#### Policy Attribute:

ORACLE Enterprise Session Border Controller								
NN3950-100 10.138.194.100 SCZ9	9.0.0 Patch 3 (Buil	ld 245)						
Configuration View Configuration	n Q							
media-manager	•	Modify Local policy	/ policy attribute					
security	• • •							
session-router	-	Next Hop	sag:TeamsGRP	•				
access-control		Realm	Teams_Cust1	•				
account-config		Action	replace-uri	•				
filter-config	- 1	Terminate Recursion	enable					
ldap-config		Cost	0					
local-policy		State	✓ enable					
	_	App Protocol		•				
local-routing-config	- 1	Lookup	single	•				

• Click OK at the bottom

Using the above example, continue for each customer tenant being hosted by this OCSBC.

Next, we'll configure a local policy to route all traffic from Teams Direct Routing to Sip Trunk

	sion Border	Controller					
Configuration View Configuration	Q Q	d 245)					
account-group	•						
allowed-elements-profile		Mod	fy Loca	l Policy			
class-profile	•	From A	ddress		* ×		
enforcement-profile	- 1	To Add	ress				
enum-config	- 1	Source	Pealm		×		
filter-config		Source	Reditti		Tear	ms 🗙	
h323		Descrip	tion				
http-alg	- 1						
iwf-config	- 1	State			🖌 en	able	
ldap-config		Policy I	riority		none		•
local-policy		Policy	ttributes				
local-response-map		D,	1				
local-routing-config		Actio	Sel	Next Hop		Realm	Action
media-profile		:		10.1.2.30		SIPTrunk	none

### Policy Attribute:

	ORACLE Enterprise Ses	sion B	order C	Controller		
N	N3950-100 10.138.194.100 SCZ9.0.0	Patch 3	3 (Build 2	245)		
Co	Niew Configuration	Q				
	account-group		*			
	allowed-elements-profile			Modify Local policy / polic	y attribute	
	class-profile	►		Next Hop	10.1.2.30	•
	enforcement-profile			Realm	SIPTrunk	•
	enum-config			Action	none	•
	filter-config			Terminate Recursion	enable	
	h323	►		Cost	0	
	http-alg			State	✓ enable	
	iwf-config			App Protocol		•
	ldap-config			Lookup	single	•

• Click OK at the bottom of each when applicable:

### 9.7 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 only 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 Teams realm.

Use this example to create ACL's for both 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						
NN3950-100 10	.138.194.100 SCZ9.0.0	Patch 3	3 (Build 24	5)		
Configuration	View Configuration	Q				
media-manager		•	*	Modify Access Control		
codec-policy						
media-manager				Realm ID	Teams	•
media-policy				Description		
realm-config						
steering-pool				Source Address	52.112.0.0/14	_
security		۲		Destination Address	0.0.0.0	
session-router				Application Protocol	SIP	
access-control				Transport Protocol	ALL	•
account-config				Access	permit	

• Click OK at the bottom

The SBC configuration is now complete. Move to verify the connection with Microsoft Direct Routing Interface.

# **10 Verify Connectivity**

### **10.1 OCSBC Options Ping**

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

While in the OCSBC GUI, utilize "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/Methods/Method OPTIONS

C	ORACLE Enterprise Session Border Controller									
N	N8950-100 10188194100 SC290.0 Patch 3 (Build 245) Deshboard Configuration Monitor							Monitor a		
Wid	igets									
	Client Trans	•	Method options							
	SIP Codecs									
	SIP Errors									
	Interface	•	Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total	Clier	nt PerMax
	Methods		OPTIONS Requests	19	2299	12	19	2299	12	
	metrous	*	Retransmissions	0	0	0	0	0	0	
	Method Ack		200 OK	19	2299	12	19	2299	12	
	Method Bye		Transaction Timeouts	0	0	0	0	0	0	
	Method Cancel		Locally Throttled	0	0	0	0	0	0	

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

### **10.2 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

# 11 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.

### 11.1 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

### **11.2 Requirements for Invite Messages**

Picture 1 Example of INVITE message

INVITE sip:17814437383@sbc1.customers.telechat.o-test06161977.com;transport=tls SIP/2.0 Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bK3rfq6u10d8f8fonro0k0.1 From: sip:9785551212@sbc1.customers.telechat.o-test06161977.com;transport=tls:5061;tag=0A7C0BFE To: <sip: 17814437383@sip.pstnhub.microsoft.com:5061> Call-ID: F3154A1E-F3AE-4257-94EA-7F01356AEB55-268289@192.168.4.180 CSeq: 1 INVITE Content-Length: 245 Content-Type: application/sdp Contact: <sip:9785551212@sbc1.customers.telechat.o-test06161977.com:5061;user=phone;transport=tls> Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE User-Agent: Oracle SBC

### 11.2.1 Contact.Header Invite:

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

### **11.3 Requirements for OPTIONS Messages**

Picture 2 Example of OPTIONS message

OPTIONS sip:sip.pstnhub.microsoft.com:5061;transport=tls SIP/2.0 Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bKumatcr30fod0o13gi060 Call-ID: 4cf0181d4d07a995bcc46b8cd42f924002000sg52@155.212.214.173 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;lr> Content-Length: 0 Contact: <sip:ping@customers.telechat.o-test06161977.com 5061;transport=tls> Record-Route: <sip: customers.telechat.o-test06161977.com >

### 11.3.1 Contact Header OPTIONS:

- When sending OPTIONS to the Direct Routing Interface, the "Contact" header should have SBC FQDN in URI. This will be the FQDN registered in the carrier tenant.
- 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 back to the SBC

### **11.4 Microsoft Teams Direct Routing Interface characteristics**

Table 1 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 Name	Refer to Microsoft documentation	
	IP Addresses range for SIP interfaces	Refer to Microsoft documentation	
Ports and IP	SIP Port	5061	
	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 and Security	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	
	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	
	Audio codecs	<ul> <li>G711</li> <li>Silk (Teams clients)</li> <li>Opus (WebRTC clients) - Only if Media Bypass is used;</li> <li>G729</li> <li>G722</li> </ul>	
Codecs	Other codecs	<ul> <li>CN</li> <li>Required narrowband and wideband</li> <li>RED – Not required</li> <li>DTMF – Required</li> <li>Events 0-16</li> <li>Silence Suppression – Not required</li> </ul>	

# 12 Appendix A

### 12.1 SBC Behind NAT SPL configuration

This configuration is needed when your SBC is behind a NAT device. This is configured to avoid loss in voice path and SIP signaling.

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 as the SIP Interface and steeping pool IP address, both of which must match
- 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.

To configure SBC Behind NAT SPL Plug in, Go to session-router->sip-interface->spl-options and input the following value, save and activate.

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.0.4.4

Here HeaderNatPublicSipIfIp is the public interface ip and HeaderNatPrivateSipIfIp is the private ip configured on the OCSBC.

ORACLE Enterprise Session Border Controller				
NN3950-100 10.138.194.100 SCZ9.	0.0 Patch 3 (B	uild 245)		
Configuration View Configuration	Q			
media-manager	•	Modify SIP Interface		
security	•	TCP Nat Interval	90	
session-router	•	Registration Caching	enable	
access-control		Min Reg Expire	300	
account-config		Registration Interval	3600	
filter-config		Route To Registrar	enable	
ldap-config		Secured Network	enable	
local-policy		Uri Fqdn Domain		
local-routing-config		Options	1	
media-profile	_	SPL Options	HeaderNatPublicSipIfIp=52:151.236.202	

• This configuration needs to be applied to each Sip Interface in the OCSBC configuration that is deployed behind a Nat Device

# 13 Appendix B

### 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 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.

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 Checkfor183 name header-rule check183 name @status-line header-name manipulate action msg-type reply methods Invite element-rule is183 name type status-code action store comparison-type pattern-rule match-value 183 mime-sdp-rule if183 name msg-type reply methods Invite action manipulate comparison-type boolean \$check183.\$is183 match-value sdp-session-rule name au action manipulate sdp-line-rule checkclineforsbcip name type С action store comparison-type pattern-rule match-value ^(.(?!(141.146.36.68))).\*\$ mime-sdp-rule delete183SDP name msg-type reply Invite methods action delete comparison-type boolean match-value \$if183.\$au.\$checkclineforsbcip header-rule change183to180 name @status-line header-name action manipulate comparison-type boolean match-value \$if183.\$au.\$checkclineforsbcip element-rule name changestatus status-code type replace action match-value 183 new-value 180 element-rule name changereasonphrase reason-phrase type replace action match-value Session Progress new-value Ringing

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

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	SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)						
Configuration View Configuration	Q						
security	►						
session-router			Modify SIP Interface				
		а.	Registration Interval	3600			
access-control			Route To Registrar	enable			
account-config			Secured Network				
filter-config			Securearitement	enable			
			Uri Fqdn Domain				
Idap-config			Options				
local-policy							
local-routing-config			SPL Options				
modia profile		Trust Mode	all	•			
media-profile		Max Nat Interval	3600				
session-agent			Stop Recurse	401.407			
session-group				401,407			
			Port Map Start	0			
session-recording-group			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 can generate ringback upon receipt of the sip REFER from Microsoft.

First, you must create a media file.

### 13.2.2 Media Files

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.

GUI Path: System/Playback Media/Upload

ORACLE Enterprise Session Border	r Controlle	
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)	Dashbourd Configuration Monitor and Trace	Widgets System
System Configuration Assistant	Force H4 Switchover 🛛 🔿 Reboot	🛃 Support information
File Management v	Playback Media	
Backup Configuration		
Configuration CSV		
Local Route Table		
Fraud Protection Table		
Log		
Audit Log		
Playback Media		
Software Image		
SPL Plug In	( )	
Configuration Template	No playback media to display. Please refresh or upload playback media.	
System Operations	Markets Update	

Playback Media		
	Upload file	×
	US_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

ORACLE Enterprise Session Border Controller					
SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)	SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)				
Configuration View Configuration Q					
media-manager 👻	Modify Realm Config				
codec-policy	Sm Icsi Match For Invite				
media-manager	Shricsi Materi For invite				
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 ACLI Running Configuration**

Below is a complete output of the running configuration used to create this application note. This output includes all 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	Toomo
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	DigiCertRoot
common-name	DigiCert Global Root CA
certificate-record	·
name	TeamsCarrierCert
state	California
locality	Redwood City
organization	Oracle Corporation
common-name	customers.telechat.o-test06161977.com
alternate-name	*.customers.telechat.o-test06161977.com
codec-policy	
name	OptimizeCodecs
allow-codecs	* SILK:NO G722:NO

add-codecs-on-egress codec-policy	PCMU
name allow-codecs	addCN *
add-codecs-on-egress	CN
http-server	
name	webServerInstance
ice-profile	ing
name stun-conn-timeout	
stun-keep-alive-interval	0
local-policy	č
from-address	*
to-address	*
source-realm	SIPTrunk
policy-attribute	
realm	IIT. I CAMSER I SIDTruck
lookup	multi
local-policy	man
from-address	*
to-address	sbc1.customers.telechat.o-test06161977.com
source-realm	SIPTrunk
policy-attribute	Turne
next-nop	sag: LeamsGRP
action	renlace-uri
local-policy	
from-address	*
to-address	*
source-realm	Teams
policy-attribute	40.4.0.00
next-nop	10.1.2.30 SIDTruck
local-routing-config	SIPTIUNK
name	TeamsLRT
file-name	TeamsLRT.xml.gz
media-manager	
media-profile	
name	CN
subname	
clock-rate	16000
media-profile	10000
name	SILK
subname	narrowband
payload-type	103
clock-rate	8000
name	SII K
subname	wideband
payload-type	104
clock-rate	16000
media-sec-policy	
name	RTP
media-sec-policy	TeamsSPTD
name	

inbound profile SDES mode srtp protocol sdes outbound SDES profile mode srtp protocol sdes network-interface s0p0 name ip-address 141.146.36.68 255.255.255.192 netmask 141.146.36.65 gateway dns-ip-primary 8.8.8.8 dns-ip-backup1 8.8.4.4 dns-domain customers.telechat.o-test06161977.com network-interface name s1p0 10.1.2.4 ip-address 255.255.255.0 netmask gateway 10.1.2.1 ntp-config 216.239.35.0 server phy-interface name s0p0 operation-type Media phy-interface name s1p0 operation-type Media slot realm-config identifier SIPTrunk **Realm Facing PSTN** description network-interfaces s1p0:0 enabled mm-in-realm media-sec-policy RTP access-control-trust-level high codec-policy **OptimizeCodecs** ringback-trigger refer ringback-file US\_Ringback\_tone.raw realm-config identifier Teams description Carrier Tenant Facing Teams Direct Routing Interface network-interfaces s0p0:0 enabled mm-in-realm qos-enable enabled media-sec-policy TeamsSRTP rtcp-mux enabled ice-profile ice customers.telechat.o-test06161977.com teams-fqdn teams-fqdn-in-uri enabled sdp-inactive-only enabled in-manipulationid **RespondOptions** access-control-trust-level high codec-policy addCN rtcp-policy rtcpGen realm-config

Teams Cust1 identifier description Realm to service Customer, woodgrovebank.us. network-interfaces s0p0:0 enabled mm-in-realm TeamsSRTP media-sec-policy rtcp-mux enabled ice-profile ice teams-fqdn sbc1.customers.telechat.o-test06161977.com teams-fqdn-in-uri enabled sdp-inactive-only enabled access-control-trust-level high codec-policy addCN rtcp-policy rtcpGen rtcp-policy rtcpGen name rtcp-generate all-calls sdes-profile name SDES AES\_CM\_128\_HMAC\_SHA1\_32 crypto-list AES\_CM\_128\_HMAC\_SHA1\_80 31 lifetime session-agent 10.1.2.30 hostname ip-address 10.1.2.30 realm-id SIPTrunk session-agent hostname sip.pstnhub.microsoft.com port 5061 transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 10 refer-call-transfer enabled session-agent hostname sip2.pstnhub.microsoft.com port 5061 transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 10 refer-call-transfer enabled session-agent hostname sip3.pstnhub.microsoft.com 5061 port transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 10 refer-call-transfer enabled session-group TeamsGRP group-name sip.pstnhub.microsoft.com dest sip2.pstnhub.microsoft.com sip3.pstnhub.microsoft.com

session-router additional-lp-lookups 1 multi-stage-src-realm-override enabled sip-config home-realm-id Teams registrar-domain registrar-host registrar-port 5060 max-udp-length=0 options sip-message-len 0 extra-method-stats enabled allow-pani-for-trusted-only disabled add-ue-location-in-pani disabled npli-upon-register disabled sip-feature replaces name Teams realm Pass require-mode-inbound require-mode-outbound Pass sip-interface realm-id **SIPTrunk** Sip Interface facing PSTN description sip-port address 10.1.2.4 allow-anonymous agents-only sip-interface realm-id Teams description Sip Interface facing Microsoft Teams Direct Routing sip-port address 141.146.36.68 port 5061 transport-protocol TLS TLSTeamsCarrier tls-profile in-manipulationid Checkfor183 sip-profile forreplaces sip-manipulation Checkfor183 name header-rule name check183 header-name @status-line action manipulate reply msg-type Invite methods element-rule is183 name type status-code action store pattern-rule comparison-type match-value 183 mime-sdp-rule name if183 msg-type reply methods Invite action manipulate comparison-type boolean \$check183.\$is183 match-value

sdp-session-rule name au action manipulate sdp-line-rule checkclineforsbcip name type С action store pattern-rule comparison-type match-value ^(.(?!(141.146.36.68))).\*\$ 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 new-value Ringing element-rule changestatus name status-code type replace action match-value 183 new-value 180 element-rule changereasonphrase name reason-phrase type action replace match-value Session Progress sip-monitoring match-any-filter enabled monitoring-filters sip-profile name forreplaces replace-dialogs enabled steering-pool ip-address 10.1.2.4 start-port 10000 end-port 19999 realm-id **SIPTrunk** steering-pool ip-address 141.146.36.68 start-port 20000 end-port 29999 realm-id Teams system-config hostname customers.telechat.o-test06161977.com description Carrier SBC for Teams Carrier Hosting Model Burlington,MA location NOTICE system-log-level snmp-agent-mode v1v2

tls-global session-caching

tls-profile name end-entity-certificate trusted-ca-certificates

mutual-authenticate

enabled

TLSTeamsCarrier TeamsCarrierCert BaltimoreRoot DigiCertGlobalRootG2 enabled

ORACLE

#### CONNECT WITH US

O blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

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 © 2020, 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, including implied 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