Oracle SBC integration with Cisco CUCM and Microsoft Teams Enterprise 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.

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of Changes</th>
<th>Date Revision Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Oracle SBC integration with Cisco CUCM and Microsoft Teams Enterprise Model</td>
<td>21st February 2020</td>
</tr>
</tbody>
</table>
Table of Contents

1. INTENDED AUDIENCE .................................................................................................................. 5
2. DOCUMENT OVERVIEW ............................................................................................................... 5
3. INTRODUCTION ............................................................................................................................ 7
   3.1. AUDIENCE ............................................................................................................................ 7
   3.2. REQUIREMENTS ..................................................................................................................... 7
   3.3. ARCHITECTURE ...................................................................................................................... 8
4. CONFIGURING THE CISCO CUCM .............................................................................................. 9
   4.1. Configuring a new SIP Trunk ................................................................................................. 9
   4.2. Configure a new Route Pattern ............................................................................................ 11
5. REQUIREMENTS TO CONFIGURE MICROSOFT TEAMS DIRECT ROUTING ............................ 14
   5.1. TENANT REQUIREMENTS ..................................................................................................... 14
   5.2. LICENSING REQUIREMENTS ............................................................................................... 14
   5.3. DNS REQUIREMENTS .......................................................................................................... 14
   5.4. SBC DOMAIN NAMES ......................................................................................................... 14
   5.5. PUBLIC TRUSTED CERTIFICATE FOR THE SBC ............................................................ 16
6. CONFIGURE TEAMS DIRECT ROUTING .................................................................................... 17
   6.1. ESTABLISH A REMOTE POWERSHELL SESSION ............................................................ 17
   6.2. PAIR THE SBC TO THE TENANT ......................................................................................... 18
   6.3. ENABLE USERS FOR DIRECT ROUTING ............................................................................ 20
   6.4. ASSIGN A PHONE NUMBER TO THE USER ........................................................................ 21
   6.5. CONFIGURE VOICE ROUTING ............................................................................................ 21
7. MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS ............................ 23
8. CONFIGURING THE SBC .............................................................................................................. 25
   8.1. VALIDATED ORACLE SBC VERSION ..................................................................................... 25
9. NEW SBC CONFIGURATION ......................................................................................................... 25
   9.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC .................................................... 25
   9.2. CONFIGURE SBC USING WEB GUI ..................................................................................... 30
   9.3. CONFIGURE SYSTEM-CONFIG ............................................................................................ 32
   9.4. CONFIGURE PHYSICAL INTERFACE VALUES ..................................................................... 33
   9.5. CONFIGURE NETWORK INTERFACE VALUES ..................................................................... 34
   9.6. ENABLE MEDIA MANAGER ................................................................................................... 37
   9.7. CONFIGURE REALMS ........................................................................................................... 38
   9.8. ENABLE SIP-CONFIG ............................................................................................................. 39
   9.9. CONFIGURING A CERTIFICATE FOR SBC .......................................................................... 40
   9.10. TLS-PROFILE ....................................................................................................................... 44
   9.11. CONFIGURE SIP INTERFACES ............................................................................................ 45
   9.12. CONFIGURE SESSION-AGENT ........................................................................................... 46
   9.13. CONFIGURE SESSION-AGENT GROUP .............................................................................. 50
   9.14. CONFIGURE LOCAL-POLICY ................................................................................................ 51
   9.15. CONFIGURE MEDIA PROFILE AND CODEC POLICY ....................................................... 53
   9.16. CONFIGURE STEERING-POOL ........................................................................................... 56
   9.17. CONFIGURE SDES PROFILE .............................................................................................. 57
   9.18. CONFIGURE MEDIA SECURITY PROFILE ......................................................................... 58
   9.19. CONFIGURE RTCP POLICY AND RTCP MUX .................................................................. 59
10. EXISTING SBC CONFIGURATION.................................................................61
APPENDIX A .................................................................................................62
1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Microsoft Teams Direct Routing Enterprise Model and Cisco CUCM.

2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between on premises Cisco CUCM and Microsoft's Teams Enterprise Model (Cloud based) using Oracle SBC. The solution contained within this document has been tested using Oracle Communication OS 830m1p2 version. Our scope of this document is only limited to testing Teams Enterprise Model with Cisco CUCM.

Microsoft Teams Direct Routing lets you connect a supported, customer-provided Session Border Controller (SBC) to Microsoft Phone System. With Direct Routing, you can connect your SBC to almost any telephony trunk or interconnect with third-party Public Switched Telephone Network (PSTN) equipment. Direct Routing enables you to:

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

Microsoft Teams works on two different methods which is given below:

1) Media bypass

Media bypass shortens the path of media traffic and reduces the number of hops in transit for better performance. With media bypass, media is kept between the Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System. For more information on media bypass, please read the links given below.


https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-MB.pdf

2) Non-media bypass

Without media bypass, when a client makes or receives a call, both signaling and media flow between the SBC, the Microsoft Phone System, and the Teams client. For more information on media bypass, please read the links given below.

https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-NONMB.pdf
Cisco Unified Call Manager provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management and is the core call control application of the collaboration portfolio.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Cisco CUCM 11.5 environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Cisco CUCM Server associated parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

Please note that the IP address, FQDN and config name and its details given in this document is used as reference purpose only. The same details cannot be used in customer config and the end users can use the configuration details according to their network requirements.

For additional information on CUCM 11.5, please visit

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Teams Direct Routing Enterprise Model with Cisco CUCM 11.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 11.5 server configuration, Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

3.2. Requirements

- Fully functioning Cisco UCM 11.5
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.3.0 version
- Teams Direct Routing Enterprise Model running Teams Client.

The below revision table explains the versions of the software used for each component:

This table is Revision 1 as of now:

<table>
<thead>
<tr>
<th>Software Used</th>
<th>CUCM Version</th>
<th>SBC Version</th>
<th>Teams Client version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 1</td>
<td>11.5</td>
<td>8.3.0</td>
<td>1.3.00.362 (64-bit) (Windows) v.2020.1.14.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>i.USWE2.2 (Mobile)</td>
</tr>
</tbody>
</table>
3.3. Architecture

The configuration, validation and troubleshooting is the focus of this document and will be described in three phases:

- Phase 1 – Configuring the Cisco Unified Call Manager v11.5 for Oracle SBC
- Phase 2 – Configuring the Teams Direct Routing Enterprise Model.
- Phase 3 – Configuring the Oracle SBC
4. Configuring the Cisco CUCM

Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

4.1. Configuring a new SIP Trunk

01) Go to Device ----- Trunk ----- Add New
02) Select Trunk Type – SIP Trunk and then Click Next
03) In the Device Name field, enter the SIP Trunk name and optionally provide a description.
04) In the Device Pool drop-down list, select a device pool id created already else select Default
05) Enter the Destination Address and Destination Port of the SBC under SIP Information.
06) Select appropriate SIP profile and SIP trunk security profile from the dropdown menu.
07) Click Save
### Trunk Configuration

**Status**

- Status: Ready

**Trunk Information**

- **Trunk Type**: SIP Trunk
- **Device Protocol**: SIP
- **Trunk Service Type**: None(Default)

### Device Information

- **Product**: SIP Trunk
- **Device Protocol**: SIP
- **Trunk Service Type**: None(Default)
- **Device Name**: 3900-SBC
- **Description**: 3900-SBC
- **Device Pool**: Default
- **Common Device Configuration**: < None >
- **Call Classification**: Use System Default
- **Media Resource Group List**: < None >
- **Location**: Hub_None
- **AAP Group**: < None >
- **Tunneled Protocol**: None

* - Indicates required item.
4.2. Configure a new Route Pattern

01) Go to Call Routing ------ Route/Hunt ------ Route Pattern and click Add New
02) Enter a Route Pattern according to the network requirements and calling plan.
03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.
04) Click Save.
### Route Pattern Configuration

**Pattern Definition**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern</td>
<td>^7814+43XXXX</td>
</tr>
<tr>
<td>Route Partition</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Description</td>
<td>RouteToSBCTeams</td>
</tr>
<tr>
<td>Numbering Plan</td>
<td>-- Not Selected --</td>
</tr>
<tr>
<td>Route Filter</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>MLPP Precedence*</td>
<td>Default</td>
</tr>
<tr>
<td>Apply Call Blocking Percentage</td>
<td></td>
</tr>
<tr>
<td>Resource Priority Namespace Network Domain</td>
<td>&lt; None &gt;</td>
</tr>
<tr>
<td>Route Class*</td>
<td>Default</td>
</tr>
<tr>
<td>Gateway/Route List</td>
<td>3900-SBC</td>
</tr>
<tr>
<td>Route Option</td>
<td></td>
</tr>
</tbody>
</table>
The route pattern that has been created is shown below:

![Route Pattern Image]

The created SIP trunk associated with the route pattern is shown below:

![SIP Trunk Image]

With these steps, the CUCM config to the SBC is complete.
5. Requirements to Configure Microsoft Teams Direct Routing

If you are planning to configure direct routing with Oracle SBC, you must ensure that the following prerequisites are completed before proceeding further:

- Tenant requirements
- Licensing and other requirements
- SBC domain names
- Public trusted certificate for the SBC
- SIP Signaling: FQDNs

5.1. Tenant Requirements

Make sure that you have a custom domain on your O365 tenant. Here we have created an account soladmin@solutionslab.onmicrosoft.com.

Likewise create an account, which is not the default domain created for your tenant. For more information https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sbc-domain-names

5.2. Licensing Requirements

Make sure that the following license requirements are met by the Direct routing users.(ie the users must be assigned the following licenses in Office 365)

- Microsoft Phone System
- Microsoft Teams + Skype for Business Plan 2 if included in Licensing SKU

5.3. DNS Requirements

Create DNS records for domains in your network that resolve to your SBC. Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- FQDN name resolving to the Public IP address

5.4. SBC Domain Names

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

For example, on the picture below, the administrator registered the following DNS names for the tenant:
<table>
<thead>
<tr>
<th>DNS Name</th>
<th>Can be used for SBC FQDN</th>
<th>Examples of FQDN names</th>
</tr>
</thead>
<tbody>
<tr>
<td>woodgrovebank.us</td>
<td>Yes</td>
<td>Valid names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc1.woodgrovebank.us;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ussbscs15.woodgrovebank.us</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• europe.woodgrovebank.us</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Valid name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc1.europe.woodgrovebank.us (requires registering domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name europe.atatum.biz in “Domains” first)</td>
</tr>
<tr>
<td>woodgrovebankus.onmicrosoft.com</td>
<td>No</td>
<td>Using *.onmicrosoft.com domains is not supported for SBC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>names</td>
</tr>
<tr>
<td>hybrdvoice.org</td>
<td>Yes</td>
<td>Valid names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc1.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ussbscs15.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• europe.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Valid name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sbc1.europe.hybridvoice.org (requires registering domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name europe.hybridvoice.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hybridvoice.org in “Domains” first)</td>
</tr>
</tbody>
</table>

Please activate and register the domain of tenant.
In this document the following FQDN and IP is used as an example:

<table>
<thead>
<tr>
<th>Public IP</th>
<th>FQDN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.212.214.172</td>
<td>oracleesbc2.woodgrovebank.us</td>
</tr>
</tbody>
</table>

5.5. Public trusted certificate for the SBC

It is necessary to set up a public trusted certificate for direct routing. This certificate is used to establish TLS connection between Oracle SBC and MS Teams. The certificate needs to have the SBC FQDN in the subject, common name, or subject alternate name fields.

For root certificate authorities used to generate SBC certificate, refer Microsoft documentation.

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc
6. Configure Teams Direct Routing

The SBC has to be paired with the direct routing interface for direct routing to work. To achieve this follow the below steps

6.1. Establish a remote PowerShell session

The first step is to download Microsoft PowerShell. For more information and downloading the client, visit Microsoft's website

https://docs.microsoft.com/en-us/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell.

To establish a remote connection, follow the below steps

Open PowerShell and type in the below commands

- Import-Module SkypeOnlineConnector
- $userCredential = Get-Credential
- $sfbSession = New-CsOnlineSession -Credential $userCredential
- Import-PSSession $sfbSession

PowerShell prompts for a username and password. Enter the tenant username and password. Tenants are used in pairing the SBC with the direct routing interface.
Now the remote connection is established. Check whether the remote connection is proper by using the below command “Get-Command *onlinePSTNGateway*”

The command will return the four functions shown here that will let you manage the SBC.

6.2. Pair the SBC to the tenant

To pair SBC to the tenant, type the command as shown below. Here the FQDN used is oraclesbc.woodgrovebank.us

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

For more information, please visit the Microsoft documentation here:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure#connect-to-skype-for-business-online-by-using-powershell
After pairing, we can check whether the SBC is present in the list of paired SBC’s by typing in the command:

Get-CsOnlinePSTNGateway -Identity oraclesbc2.woodgrovebank.us

The details of the gateway are listed when the above command is entered.

Verify whether the enabled parameter is set to true.
The OPTIONS ping from the SBC is now responded with 200OK.
Once there are incoming options to the direct routing interface, it starts sending OPTIONS to the SBC.

<table>
<thead>
<tr>
<th>Identity</th>
<th>oraclesbc2.woodgrovebank.us</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fqdn</td>
<td>oraclesbc2.woodgrovebank.us</td>
</tr>
<tr>
<td>SipSignallingPort</td>
<td>oraclesbc2.woodgrovebank.us</td>
</tr>
<tr>
<td>FailoverTimeSeconds</td>
<td>10</td>
</tr>
<tr>
<td>ForwardCallHistory</td>
<td>True</td>
</tr>
<tr>
<td>ForwardPai</td>
<td>True</td>
</tr>
<tr>
<td>SendSipOptions</td>
<td>True</td>
</tr>
<tr>
<td>MaxConcurrentSessions</td>
<td>True</td>
</tr>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>MediaBypass</td>
<td>True</td>
</tr>
<tr>
<td>GatewaySiteId</td>
<td>False</td>
</tr>
<tr>
<td>GatewaySiteLbrEnabled</td>
<td>False</td>
</tr>
<tr>
<td>FailoverResponseCodes</td>
<td>408, 503, 504</td>
</tr>
<tr>
<td>GenerateRingingWhileLocatingUser</td>
<td>True</td>
</tr>
<tr>
<td>PidFloSupported</td>
<td>False</td>
</tr>
<tr>
<td>MediaRelayRoutingLocationOverride</td>
<td>None</td>
</tr>
<tr>
<td>ProxySbc</td>
<td>None</td>
</tr>
<tr>
<td>BypassMode</td>
<td>None</td>
</tr>
</tbody>
</table>
6.3. Enable Users for Direct Routing.

To add users, create a user in Office 365 and assign a license. Here the following user is created:

teamsuser1@woodgrovebank.us

Here the following license is added
- Office 365 Enterprise E5 (including SfB Plan2, Exchange Plan2, Teams, and Phone System)

Verify whether the user is homed in Skype for business Online by issuing the below command in PowerShell

“Get-CsOnlineUser -Identity "<User name>" | fl RegistrarPool”

Here the “infra.lync.com” verifies that the user is homed.

PS C:\WINDOWS\system32> Get-CsOnlineUser -Identity teamsuser1 | fl RegistrarPool
RegistrarPool : sippoolsn23a15.infra.lync.com
6.4. Assign a phone number to the User

After creating a user, a phone number and voice mail has to be assigned through Powershell. Enter the below command for assigning a phone number.

Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:<E.164 phone number>

The phone number used has to be configured as a full E.164 phone number with country code.

6.5. Configure Voice Routing

Voice Routing is performed by the direct routing Interface based on the following elements

- Voice Routing Policy
- PSTN Usages
- Voice Routes
- Online PSTN Gateway

Here is an example to configure routes, PSTN usage, voice routing policy and assigning the policy to user.

1. Create the PSTN Usage "US and Canada".

2. Verify this by executing the command below

3. Configure voice route as shown below. Here all calls are routed to the same SBC.

   This is achieved by using -NumberPattern ".*" Set-CsOnlineVoiceRoute -id "Bedford 1" -NumberPattern ".*" -OnlinePstnGateway List oraclesbc2.woodgrovebank.us –Priority 1
4. Verify the configuration by typing in the following command: `Get-CsOnlineVoiceRoute`

```
Identity : Oracle_US
Priority  : 3
Description: (~\d+[0-9][\d])$
OnlinePstnUsages : {Oracle_US}
OnlinePstnGatewayList : {sbc2.customers.telechat.o-test06161977.com, oraclesbc2.woodgrovebank.us}
Name      : Oracle_US
```

5. Create a Voice Routing Policy "US Only" and add to the policy the PSTN Usage "US and Canada.". Use the following command:

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

This can be verified through the following command:

```
PS C:\Users\gabalakr> Get-CsOnlineVoiceRoutingPolicy
Identity : Global
OnlinePstnUsages : {}
Description : 
RouteType : 
Identity : Tag:US Only
OnlinePstnUsages : {US and Canada}
Description : 
RouteType : BYOT
```

6. Grant to user teamsuser1 a voice routing policy by using PowerShell

```
PS C:\WINDOWS\system32> Grant-CsOnlineVoiceRoutingPolicy -Identity "teamsuser1" -PolicyName "US Only"
```
7. Validate the same using the PowerShell command as shown below

```
PS C:\Users\gabalakr> Get-CsOnlineVoiceRoutingPolicy
Identity : Global
OnlinePstnUsages : {}
Description : 
RouteType : 

Identity : Tag:US Only
OnlinePstnUsages : {US and Canada}
Description : 
RouteType : BYOT
```

7. Microsoft Teams Direct Routing Interface Characteristics

The Table below 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.

<table>
<thead>
<tr>
<th>Ports and IP</th>
<th>SIP Interface FQDN Name</th>
<th>Refer to Microsoft documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP Addresses range for SIP interfaces</td>
<td>Refer to Microsoft documentation</td>
</tr>
<tr>
<td>SIP Port</td>
<td>5061</td>
<td></td>
</tr>
<tr>
<td>IP Address range for Media</td>
<td>Refer to Microsoft documentation</td>
<td></td>
</tr>
<tr>
<td>Media port range on Media Processors</td>
<td>Refer to Microsoft documentation</td>
<td></td>
</tr>
<tr>
<td>Media Port range on the client</td>
<td>Refer to Microsoft documentation</td>
<td></td>
</tr>
<tr>
<td>Transport and Security</td>
<td>SIP transport</td>
<td>TLS</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>-----</td>
</tr>
<tr>
<td>Media Transport</td>
<td>SRTP</td>
<td></td>
</tr>
<tr>
<td>SRTP Crypto Suite</td>
<td>AES_CM_128_HMAC_SHA1_80, non-MKI</td>
<td>DTLS-SRTP is not supported</td>
</tr>
<tr>
<td>Control protocol for media transport</td>
<td>SRTCP (SRTCP-Mux recommended)</td>
<td>Using RTCP mux helps reduce number of required ports</td>
</tr>
<tr>
<td>Supported Certification Authorities</td>
<td>Refer to Microsoft documentation</td>
<td></td>
</tr>
<tr>
<td>Transport for Media Bypass</td>
<td>ICE-lite (RFC5245) – recommended, Client also has Transport Relays</td>
<td></td>
</tr>
</tbody>
</table>

**Audio codecs**
- G711
- G722
- Silk (Teams clients)
- Opus (WebRTC clients) - Only if Media Bypass is used:
  - G729

**Other codecs**
- DTMF – Required
- Events 0-16
- CN
- Required narrowband and wideband
- RED – Not required
- Silence Suppression – Not required
8. Configuring the SBC

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

8.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.3 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- VME

9. New SBC configuration

If the customer is looking to setup a new SBC from scratch, please follow the section below.

9.1. Establishing a serial connection to the SBC

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None
Power on the SBC and confirm that you see the following output from the boot-up sequence:

Enter the default password to log in to the SBC. Note that the default SBC password is “acme” and the default super user password is “packet”.

Both passwords have to be changed according to the rules shown below.
Now set the management IP of the SBC by setting the IP address in bootparam to access bootparam. Go to Configure terminal->bootparam.

Note: There is no management IP configured by default.

```
NN3900-101# conf t
NN3900-101(configure)# bootparam
'. '= clear field; ' - ' = go to previous field; q = quit
Boot File          : /boot/nnsCZ830mlp2.bz
IP Address         : 172.18.255.101
VLAN               : 0
Netmask            : 255.255.0.0
Gateway            : 172.18.0.1
IPv6 Address       :
IPv6 Gateway       :
Host IP            :
FTP username       : vxftp
FTP password       : vxftp
Flags              :
Target Name        : NN3900-101
Console Device     : COM1
Console Baudrate   : 115200
Other              :

NOTE: These changed parameters will not go into effect until reboot. Also, be aware that some boot parameters may also be changed through PHY and Network Interface Configurations.
```

Setup product type to Enterprise Session Border Controller as shown below.

To configure product type, type in setup product in the terminal

```
NN3900-101# setup product
WARNING:
Alteration of product alone or in conjunction with entitlement changes will not be complete until system reboot
Last Modified 2019-06-04 11:51:56
1 : Product      : Enterprise Session Border Controller
Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]:
```
Enable the features for the ESBC using the setup entitlements command as shown.

Save the changes and reboot the SBC.

```
Entitlements for Enterprise Session Border Controller
Last Modified: Never

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Session Capacity</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Admin Security</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Data Integrity (FIPS 140-2)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Transcode Codec AMR Capacity</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Transcode Codec AMRWS Capacity</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Transcode Codec EVRCC Capacity</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Transcode Codec EVRCE Capacity</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Transcode Codec EVS Capacity</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Transcode Codec OFUS Capacity</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Transcode Codec SILK Capacity</td>
<td>0</td>
</tr>
</tbody>
</table>

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 1

Session Capacity (0-128000) : 500
Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 3

*******************************************************
CAUTION: Enabling this feature activates enhanced security functions. Once saved, security cannot be reverted without resetting the system back to factory default state.
*******************************************************

Admin Security (enabled/disabled) : 
Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 5

Transcode Codec AMR Capacity (0-102375) : 50
Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 2

Advanced (enabled/disabled) : enabled
Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 10

Transcode Codec OPUS Capacity (0-102375) : 50
Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 11

Transcode Codec SILK Capacity (0-102375) : 50
```

The SBC comes up after reboot and is now ready for configuration.
Go to configure terminal->system->web-server-config.

Enable the web-server-config to access the SBC using Web GUI. Save and activate the config.

```
NN3900-101(web-server-config)# state enabled
NN3900-101(web-server-config)# done
web-server-config
  state enabled
  inactivity-timeout 5
  http-state enabled
  http-port 80
  https-state disabled
  https-port 443
  http-interface-list GUI
  tls-profile
  last-modified-by admin@172.18.0.130
  last-modified-date 2020-02-20 02:46:51
```

**NN3900-101(web-server-config)# exit
**NN3900-101(system)# save
**NN3900-101(system)# exit
**NN3900-101(configure)# exit
**NN3900-101# save-config
checking configuration

Results of config verification:
  4 configuration warnings
Run 'verify-config' for more details

Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
*NN3800-101# activate-config
activate-config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
9.2. Configure SBC using Web GUI

In this app note, we configure SBC using the WebGUI.

The Web GUI can be accessed through the url https://<SBC_MGMT_IP>.

The username and password is the same as that of CLI.

Go to Configuration as shown below, to configure the SBC.
Kindly refer to the GUI User Guide given below for more information.

https://docs.oracle.com/cd/F13782_01/doc/esbc_scz830_webgui.pdf

The expert mode is used for configuration.

Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.
9.3. Configure system-config

Go to system->system-config

For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/cd/F13782_01/doc/esbc_scz830_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration. If there is no transcoding involved, then the above step is not needed.
9.4. Configure Physical Interface values

To configure physical Interface values, go to System->phy-interface.

You will first configure the slot 0, port 0 interface designated with the name s0p0. This will be the port plugged into your inside (connection to the PSTN gateway) interface. Teams is configured on the slot 0 port 1. Below is the screenshot for creating a phy-interface on s0p0

Create a similar interface for Teams as well from the Web GUI. The table below specifies the values for both teams and Trunk.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Trunk(s0p0)</th>
<th>MSTeams(s0p1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>Media</td>
<td>Media</td>
</tr>
</tbody>
</table>

![Screenshot of creating a phy-interface on s0p0](image.png)
9.5. Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure two interfaces, one for Teams side and one for CUCM side.

The table below lists the parameters, to be configured for both the interfaces.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Teams side Network Interface</th>
<th>CUCM side Network interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>s0p0</td>
<td>s1p1</td>
</tr>
<tr>
<td>Host Name</td>
<td>oraclesesbc2.woodgrovebank.us</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>155.212.214.172</td>
<td>10.232.50.50</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>155.212.214.1</td>
<td>10.232.50.1</td>
</tr>
<tr>
<td>DNS-IP Primary</td>
<td>8.8.8.8</td>
<td></td>
</tr>
<tr>
<td>DNS-domain</td>
<td>Woodgrovebank.us</td>
<td></td>
</tr>
</tbody>
</table>
### Modify Network Interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>kdp1</td>
<td></td>
</tr>
<tr>
<td>Sub port id</td>
<td>0</td>
<td>(Range: 0.4093)</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>oracleesbc2.woodgrovebank.us</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>155.212.214.172</td>
<td></td>
</tr>
<tr>
<td>Pri utility addr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sec utility addr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>155.212.214.1</td>
<td></td>
</tr>
<tr>
<td>Heartbeat</td>
<td></td>
<td>(Range: 0.5555)</td>
</tr>
<tr>
<td>Heartbeat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heartbeat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heartbeat</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Modify Network Interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartbeat</td>
<td>0</td>
<td>(Range: 0.5555)</td>
</tr>
<tr>
<td>Retry count</td>
<td>0</td>
<td>(Range: 0.5555)</td>
</tr>
<tr>
<td>Retry timeout</td>
<td>1</td>
<td>(Range: 1.65535)</td>
</tr>
<tr>
<td>Health score</td>
<td>0</td>
<td>(Range: 0.100)</td>
</tr>
<tr>
<td>DNS IP primary</td>
<td>8.8.8.8</td>
<td></td>
</tr>
<tr>
<td>DNS IP backup1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS IP backup2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS domain</td>
<td>woodgrovebank.us</td>
<td></td>
</tr>
<tr>
<td>DNS timeout</td>
<td>11</td>
<td>(Range: 0.429467295)</td>
</tr>
<tr>
<td>DNS max ttl</td>
<td>86400</td>
<td>(Range: 30..2073600)</td>
</tr>
</tbody>
</table>
9.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager and configure the below option for generating rtcp reports.

audio-allow-assymmetric-pt
xcode-gratuitous-rtcp-report-generation

Go to Media-Manager->Media-Manager
9.7. Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below. The name of the Realm can be any relevant name according to the user convenience.

In the below case, Realm name is given as Teams (SBC to Teams)

Similarly, Realm name is given as CUCMRealm (SBC to CUCM)
9.8. Enable sip-config

SIP config enables SIP handling in the SBC. Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below.
To configure sip-config, Go to Session-Router->sip-config.

In options add max-udp-length =0.
           inmanip-before-validate
9.9. Configuring a certificate for SBC

Microsoft Teams Direct Routing Interface only allows TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted certification authorities.

The step below describes how to request a certificate for SBC External interface and configure it based on the example of DigiCert. The process includes the following steps:

1) Create a certificate-record – “Certificate-record” are configuration elements on Oracle SBC which captures information for a TLS certificate – such as common-name, key-size, key-usage etc.

   The following certificate-records are required on the Oracle SBC in order for the SBC to connect with Microsoft Teams

   - SBC – 1 certificate-record assigned to SBC
   - Root – 1 certificate-record for root cert
   - Intermediate – 1 certificate-record for intermediate (this is optional – only required if your server certificate is signed by an intermediate)

2) Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority

3) Deploy the SBC and Root/Intermediary certificates on the SBC

Step 1 – Creating the certificate record

Go to security->Certificate Record and configure a certificate for SBC as shown below.
Follow the same steps and create following intermediate and root certificates.

-BaltimoreRoot: This certificate is always required for MS Teams.

See the link here, to get some additional information

-DigiCertRoot
-DigiCertInter

The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>DigicertInter</th>
<th>BaltimoreRoot</th>
<th>DigiCertRoot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common-name</td>
<td>DigiCert SHA2 Secure Server CA</td>
<td>Baltimore CyberTrust Root</td>
<td>DigiCert Global Root CA</td>
</tr>
<tr>
<td>Key-size</td>
<td>2048</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>Key-usage-list</td>
<td>digitalSignature keyEncipherment</td>
<td>digitalSignature keyEncipherment</td>
<td>digitalSignature keyEncipherment</td>
</tr>
<tr>
<td>Extended-key-usage-list</td>
<td>serverAuth</td>
<td>serverAuth</td>
<td>serverAuth</td>
</tr>
<tr>
<td>key-algor</td>
<td>rsa</td>
<td>rsa</td>
<td>rsa</td>
</tr>
</tbody>
</table>
Step 2 – Generating a certificate signing request

(Only required for the SBC’s end entity certificate, and not for root CA certs)

Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- Select the certificate and generate certificate on clicking the “Generate” command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.

- Also, note that a save/activate is required
Step 3 – Deploy SBC & root/intermediate certificates

Once certificate signing request have 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 done, issue save/activate from the WebGUI.

Repeat the steps for the following certificates:

- BaltimoreRoot
- DigiCertInter
- DigiCertRoot.

At this stage all the required certificates have been imported to the SBC.
9.10. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go to security-> TLS-profile config element and configure the tls-profile as shown below
9.11. Configure SIP Interfaces.

Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please ensure that the IP address allocated to the SIP interface is the FQDN resolvable address. i.e. if you issue command nslookup from another computer, “oracleesbc2.woodgrovebank.us” – it should resolve to 155.212.214.172. Note that the IP should be publicly routable IP address.

Note:

- TLS-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from Teams server
Similarly, Configure Internal IP under sip-port of sip-interface for CUCM side.

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address. Now configure where the SBC sends the outbound traffic.

9.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Configure the session-agent for Teams with the following parameters. Go to session-router->Session-Agent.

- hostname to “sip.pstnhub.microsoft.com”
- port 5061
- realm-id – needs to match the realm created for teams
- transport set to “StaticTLS”
- refer-call-transfer set to enabled
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs
Follow above steps to create 2 more sessions for:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

Note: Please note that all signaling SHOULD only point to sip/sip2/sip3.pstnhub.microsoft.com – no signaling should be sent to sip-all.pstnhub.microsoft.com FQDN. The sip-all.pstnhub.microsoft.com FQDN is only used for longer DNS TTL value.

Similarly, Configure the session-agent for CUCM side with the following parameters.
Go to session-router->Session-Agent.

- Host name to FQDN of CUCM which is “CUCM-Cisco.pe.oracle.com” in this case.
- The same value is configured in Cisco CUCM under System --- Enterprise Parameter ----Cluster FQDN
- port 5060
- realm-id – needs to match the realm created for CUCM.
- transport set to “UDP+TCP”
9.13. Configure session-agent group

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

Go to Session-Router->Session-Group.

Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

To make calls from Teams to CUCM, the following config is required:
To make calls from CUCM to Teams, please configure the below local policy.
9.15. Configure Media Profile and Codec Policy

The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required

SILK & CN offered by Microsoft teams are using a payload type which is different than usual. Configure the media-profile as shown below,
Go to Session-Router->Media-profile
Configure media profiles similarly, for silk codec also as given below.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>SILK-1</th>
<th>SILK-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subname</td>
<td>narrowband</td>
<td>wideband</td>
</tr>
<tr>
<td>Payload-Type</td>
<td>103</td>
<td>104</td>
</tr>
<tr>
<td>Clock-rate</td>
<td>8000</td>
<td>16000</td>
</tr>
</tbody>
</table>

After creating media profile, create codec-policy, addCN, to add comfort noise towards Teams and apply it on the realm for Teams.

Go to media manager ---- codec policy.
Go to media manager ---- realm config and assign the codec policy to the Teams realm
9.16. Configure steering-pool

Steering-pool config allows configuration to assign IP address(es), ports & a realm.
9.17. Configure sdes profile

Please go to →Security → Media Security → sdes profile and create the policy as below.

Microsoft only supports AES_CM_128_HMAC_SHA1_80 encryption.
9.18. Configure Media Security Profile

Please go to ➔ Security ➔ Media Security ➔ media Sec policy and create the policy as below:
Create Media Sec policy with name SDES for the Teams side which will have the sdes profile created above. Assign this media policy to the Teams Realm.

Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the CUCM side which will use only TCP/UDP as transport protocol. Assign this media policy to the CUCMRealm.
9.19. Configure RTCP Policy and RTCP Mux

The RTCP policy needs to be configured in order to generate RTCP reports towards Teams. It is then applied on the Teams realm.

Go to Media-manager->rtcp-policy to configure rtcp-policy.
Please add the above policy to Ream Teams and also enable support for RTCP-Mux in the realm.
10. Existing SBC configuration

If the SBC being used with Microsoft Teams is an existing SBC with functional configuration with a SIP trunk, following configuration elements are required:

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- Enable DNS
- New sip-interface
- New session-agent
- New-Session-Agent-Group
- New steering-pools
- New Local-policy
- Media-profile
- Codec-policy
- SDES Profile
- Media-ssec-Policy
- RTCP policy
- RTCP-mux

Please follow the steps mentioned in the above chapters to configure these elements.
### Appendix A

Following are the test cases that are executed as part of Teams Direct Routing Enterprise Model with CUCM.

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Test Cases Executed</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Device supports ptime of 20 ms for an inbound call to CUCM user</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>Device sends its own FQDN in the contact header</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>Device (CUCM Endpoint) accepts call from Teams user where the user's calling line identity is set to anonymous</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>Teams user places inbound call from CUCM on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>5</td>
<td>Teams user places outbound call to CUCM on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>6</td>
<td>Teams user places outbound call to CUCM on hold for over 15 minutes and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>7</td>
<td>Inbound CUCM Call to Teams blind transferred to second Teams User</td>
<td>Pass</td>
</tr>
<tr>
<td>8</td>
<td>Outbound CUCM call from Teams user blind transferred to second Teams User</td>
<td>Pass</td>
</tr>
<tr>
<td>9</td>
<td>Inbound CUCM Call to Teams consultatively transferred to Teams User</td>
<td>Pass</td>
</tr>
<tr>
<td>10</td>
<td>Outbound CUCM call from Teams user consultatively transferred to Teams User</td>
<td>Pass</td>
</tr>
<tr>
<td>11</td>
<td>CUCM user calls Teams user that simultaneously rings second TEAMS/CUCM user and second user answers</td>
<td>Pass</td>
</tr>
<tr>
<td>12</td>
<td>CUCM user calls Teams user that is forwarded to second CUCM/TEAMS user</td>
<td>Pass</td>
</tr>
<tr>
<td>13</td>
<td>CUCM User calls Teams user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer’s SIP trunk</td>
<td>Pass</td>
</tr>
<tr>
<td>14</td>
<td>Teams user calls CUCM user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer’s SIP trunk</td>
<td>Pass</td>
</tr>
<tr>
<td>15</td>
<td>Teams user calls an IVR number and navigates through the IVR menu after call connection</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Result</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>16</td>
<td>Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR</td>
<td>Pass</td>
</tr>
<tr>
<td>17</td>
<td>Device sends comfort noise packets to Direct Routing interface when CUCM user mutes an outbound call</td>
<td>Pass</td>
</tr>
<tr>
<td>18</td>
<td>Device sends comfort noise packets to Direct Routing interface when CUCM user mutes an inbound call</td>
<td>Pass</td>
</tr>
<tr>
<td>19</td>
<td>Teams user mutes inbound call from CUCM and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>20</td>
<td>Device must provide SRTCP for a transcoded inbound call when service provider or gateway does not send SRTCP</td>
<td>Pass</td>
</tr>
<tr>
<td>21</td>
<td>Device must provide SRTCP for a transcoded outbound call when service provider or gateway does not send SRTCP</td>
<td>Pass</td>
</tr>
<tr>
<td>22</td>
<td>Device must provide SRTCP for an inbound call that doesn’t involve transcoding when service provider or gateway does not send SRTCP</td>
<td>Pass</td>
</tr>
<tr>
<td>23</td>
<td>Device must provide SRTCP for an outbound call that doesn’t involve transcoding when service provider or gateway does not send SRTCP</td>
<td>Pass</td>
</tr>
<tr>
<td>24</td>
<td>Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the offer</td>
<td>Pass</td>
</tr>
<tr>
<td>25</td>
<td>Device must respond with a=rtcp-mux attribute in the SDP response if the offer contains the same attribute</td>
<td>Pass</td>
</tr>
</tbody>
</table>