
# Microsoft Teams Phone Mobile with Oracle SBC

**Technical Application Note**

ORACLE

COMMUNICATIONS

# Disclaimer

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

## Contents

**This Page is Intentionally left Blank**

# 1 Revision History

| Document Version | Description | Revision Date |
|---|---|---|
| Rev 1.1 GA | Updated release | 02-08-2024 |

# 2 Intended Audience

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

# 3 Validated Oracle Software Versions

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

SCZ920 or above.

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

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

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

# 4 Related Documentation

## 4.1 Oracle SBC

- https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/aclireference/acli-reference-guide.pdf
- https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/releasenotes/sbc-release-notes.pdf
- https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/configuration/sbc-configuration-guide.pdf

### 4.2 Microsoft Teams

https://cloudpartners.transform.microsoft.com/partner-gtm/operators/teams-phone-mobile

## 5 About Teams Phone Mobile

Microsoft Teams Phone Mobile is an intuitive, mobile-first Microsoft Teams experience that allows business users to access Teams capabilities through their mobile identity on both their native dialler and any Teams endpoint. The solution delivers cellular network quality of service to Teams communications, while allowing customers to enforce business policies, reduce costs, and improve the user experience for the growing mobile workforce. Through Teams Phone Mobile, Microsoft will collaborate closely with mobile network operators (MNOs), leveraging their unique mobile assets, including 5G technologies, to build a differentiated, high-quality, connected, and immersive mobile experience that can evolve with worldwide mobility trends.

### 5.1 Customer Benefits

- Create a unified business communication experience. Enables an inclusive workplace for mobile, remote, hybrid, and office workers by providing a reliable communication solution to work securely from either their native dialer or from the Teams app on any device.
- Reduce costs and eliminate redundancies. Allows customers to eliminate fixed lines for their mobile and remote workers and reduce international, long-distance, and intra-company mobile costs.
- Streamline management and governance. Provisions access usage and manages telephony services for all employees from one centralized place – the Office 365 portal. Provides enterprises the ability to enforce business policies, including security, compliance, and data governance protocols, even with wireless-only, 5G users.
- Deliver a business-grade mobile communications solution. Allows mobile network operators to build on future innovation of their 5G networks through partnership with Microsoft, empowering digital transformation for enterprise customers with a high-quality and differentiated user experience.

For a list of operators participating in the Microsoft Teams Phone Mobile program and the countries or regions where their service is available, see Microsoft 365 Teams Phone Mobile.

### 5.2 Plan for Teams Phone Mobile

Please follow below Microsoft Learn article to know more about Planning and configuring Teams Phone Mobile.

https://learn.microsoft.com/en-us/microsoftteams/operator-connect-mobile-plan

Ensure your organization has eligible Microsoft 365 services:

- Teams Phone System SKU or E5 with Teams
- Teams Phone Mobile add-on SKU

Below link provides details about configuring your Microsoft Teams Services for enabling Teams Phone Mobile.

https://learn.microsoft.com/en-us/microsoftteams/operator-connect-mobile-configure

### 5.3 Media Bypass vs Non-Media Bypass

Teams Phone Mobile can only work in Non-Media Bypass mode.

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

### 5.4 Teams Phone Mobile Call Scenarios

- Each user is allocated with Operator's mobility number along with a SIM (Physical or eSIM). The mobile number is also used as User's Teams Identity.
- Intra Tenant (users in the same tenants Teams to Teams) calls are handled within the MS Teams network. However, Teams to Native dialer calls are routed to the mobile network operator to enable mobile default dialer ringing.
- Inter-tenant (between different CUGs (Closed User Group)) calls between Teams clients are routed back to Partner mobile operators (supplier of Number) for termination to called party or the partner can redirect back via Interconnect link Microsoft Azure Peering Service Voice (MAPSV) to Microsoft Azure Phone System.
- Outbound call – _Teams client to non-Teams number: Call is handed over to mobile operator by Microsoft for termination to called party.
- Inbound call – _non-Teams number to Teams client: Call is handed over to Microsoft by mobile operator for termination to called party.
- Users can initiate or receive calls from Teams Client on desktop, laptop, mobile over-the-top (OTT) or tablet. In addition, user call also uses the Mobile Native dialer to initiate or receive calls.
- International roaming users will be able to make / receive calls under standard roaming arrangements. In some countries, due to regulatory constraints, calls between Teams client and PSTN may be restricted.
- Number portability shall be applicable as per respective Geography regulatory rules.

### 5.5 Reference Breakdown

| | |
|---|---|
| OC-SBC | Oracle Operator Connect SBC supporting Teams Phone Mobile Service |
| VoLTE | Voice over LTE- Mobile default dialler |
| MSFT | Mirosoft |

| | |
|---|---|
| TPM | Teams Phone Mobile |
| Native Dialler | Default Dialler of User Client |
| On-Net | Users calls within the same Mobile network |
| Off-Net | Users calls within different operators networks |
| BreakOut | Call towards PSTN |
| MO | Mobile Originated Call |
| MT | Mobile Terminated Call |
| APP | Call from Teams App |
| OC-SBC | OperatorConnect SBC supporting Teams Phone Mobile Service |
| VoLTE | Voice over LTE- Mobile default dialler |
| MSFT | Mirosoft |
| TPM | Teams Phone Mobile |
| Native Dialler | Default Dialler of User Client |
| On-Net | Users calls within the same Mobile network |
| Off-Net | Users calls within different operators networks |
| BreakOut | Call towards PSTN |

# 6 OC-SBC Interworking & Media requirements.

To integrate Teams into an Operators IMS Core, the Oracle SBC are the most valuable option as they are proven and interworks between a 3GPP defined platform (Carriers IMS Core) and non-3GPP Voice platform (Microsoft Teams).

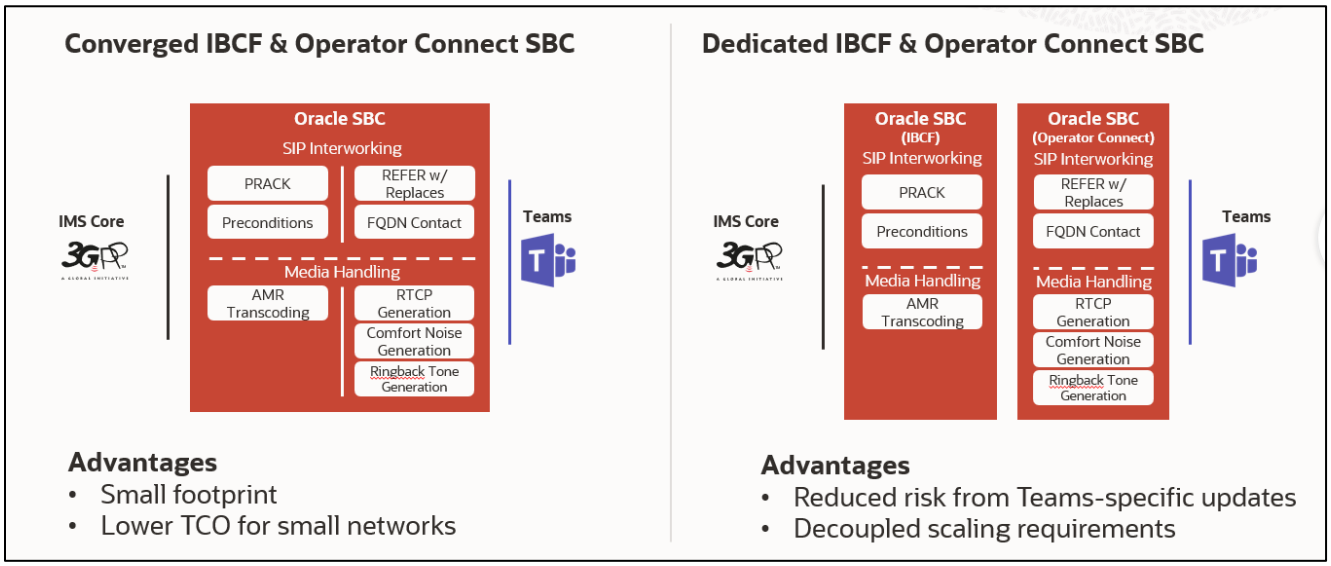
## 6.1 Signalling Interworking Requirements:

- **100rel/PRACK Interworking** – Where IMS uses PRACK exclusively, Microsoft Teams does not, and this must be interworked at the IMS border. While OC-SBC is capable of performing PRACK interworking we are doing the PRACK interworking on P-CSCF in the test bed to support merge-early-dialogs.
- **Preconditions** – IMS networks MAY choose to implement Preconditions, which is not supported by Microsoft Teams. When this is used, Preconditions Interworking must be used at the border.
- **REFER termination and Replaces interworking** – Microsoft Teams has specific requirements for Call Transfers which require interworking at the border. In normal scenarios REFER will be handled by IMS Network's TAS but OC-SBC is also capable of handling REFERs. OC-SBC is also REFERs in the test bed.
- **Encryption Interworking** – Where an IMS core can be unencrypted, Microsoft Teams can optionally be encrypted to elevate security (although this is not a requirement of Operator Connect). When needed, encryption services are applied at the border. OC-SBC can perform the interoperability between an encrypted and unencrypted network for both signaling as well as Media.

- **Teams-specific Contact** – Microsoft Teams requires the Contact header be formatted with an FQDN as opposed to IP, which is not the case within 3GPP networks. OC-SBC converts the IP Address to FQDN of the Contact Header.
- **Local Media Playback** – Oracle SBC performs can perform Local Media Playback when required for generating ringback tones and during early media scenarios.
- SBC Interworking for handling SDP offer in a-line (call hold/waiting) – During call hold scenarios Oracle SBC performs the conversion of SDP a line from Caller towards Microsoft to convert the attribute to inactive.
- Media Requirements
- **Transcoding of unsupported codecs** – Where IMS cores use both AMR-WB and AMR, Microsoft Teams only supports AMR-WB, so calls delivered using AMR must be transcoded.
- **RTCP** – While IMS calls may support end to end RTCP, Microsoft Teams requires it, so selective RTCP Generation at the border is required to ensure service continuity.
- **Comfort Noise** – IMS does not implicitly require Comfort Noise (CN) packets, whereas Microsoft Teams prefers this. Comfort Noise generation at the border provides a smoother experience.

# 7 SBC Deployment options

## 7.1 Converged vs Dedicated SBC Options

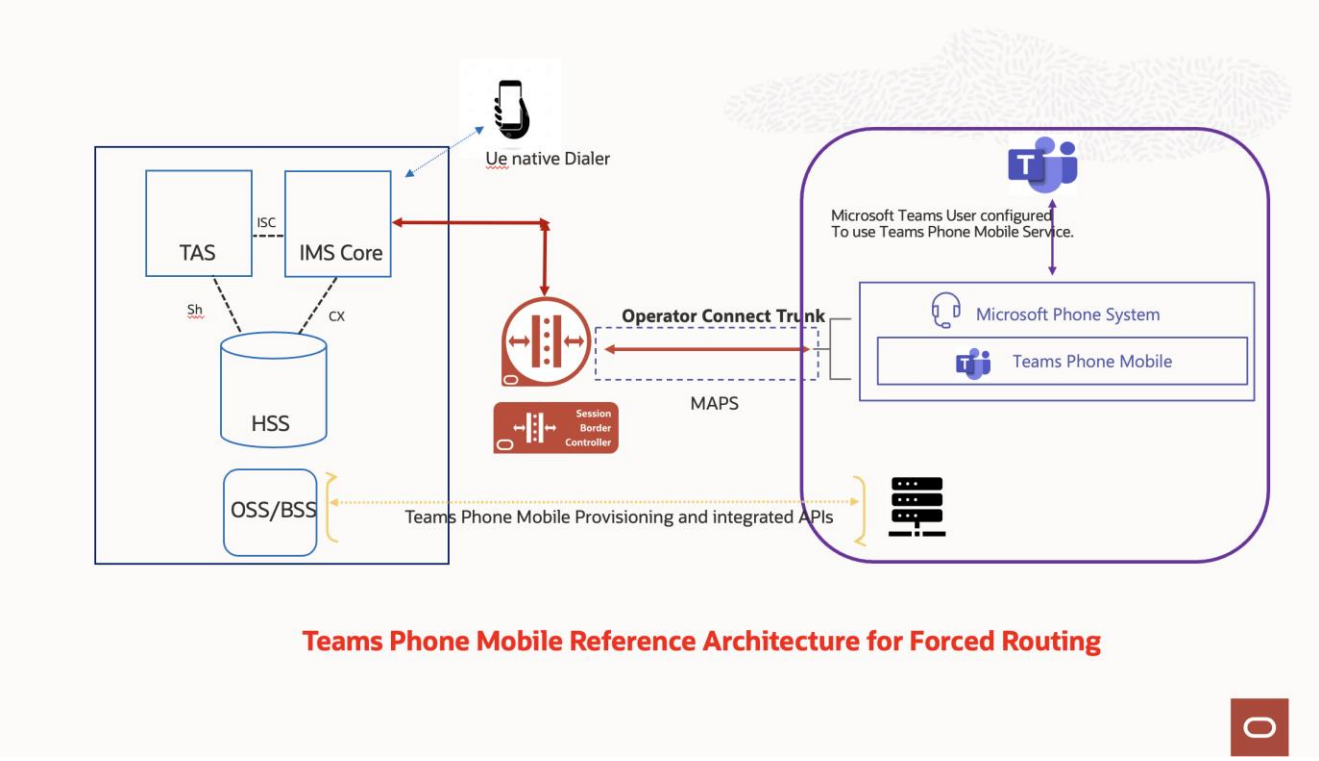



When integrating an Oracle SBC with your IMS core for Microsoft Teams Phone Mobile, you have two options:

- Converged SBC: Configure your Oracle SBC to handle both IBCF and Operator Connect SBC functionalities.
- Dedicated SBC: Introduce a separate SBC dedicated to interworking with Teams Phone Mobile.

We recommend the Dedicated SBC approach for integrating an SBC with your IMS core to support Microsoft Teams Phone Mobile. This involves introducing a separate SBC to handle all required functionality. While a Converged SBC option using the Oracle SBC is also possible, we've focused on testing and documenting the Dedicated SBC approach for this application note.

# 8 Network topology




# 9 Oracle SBC Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Microsoft Teams Phone Mobile.

Note :- In the running configuration you will find configuration related to PSTN connectivity because in the current setup PSTN breakout is also terminated onto OC-SBC.While the configuration is shown in the ACLI output and the ACLI running configuration,it is not highlighted as part of the Application Note.

This guide assumes the OC-SBC has been installed, management interface has been configured, product selected and entitlements have been assigned.
If you require more information on how to install your SBC platform, please refer to the ACLI configuration guide.

To access the ACLI on your OC-SBC, ssh to the management IP address or access via SBC console port:

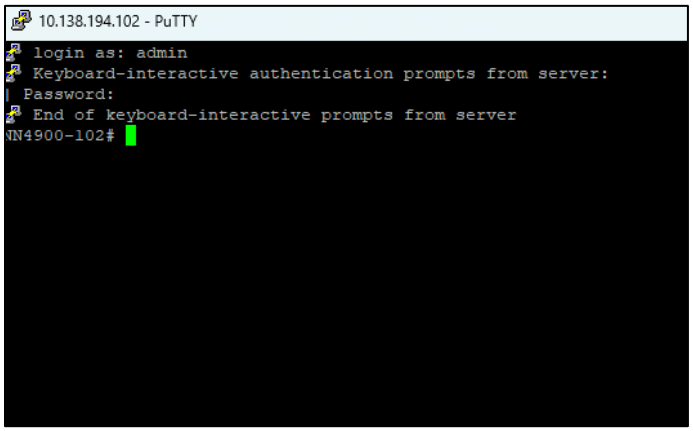
Console Settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

When the login screen appears, enter the username and password to access the OC-SBC.

*Any configuration parameter not specifically listed below can remain at the OC-SBC default value and does not require a change for the connection to Microsoft Teams Phone Mobile to function properly.*

*Note: the configuration examples below were captured from a system running the latest GA software, 9.2.0*




## 9.1 System-Config

To enable system level functionality for the OC-SBC, you must first enable the 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)

To configure system-config from ACLI –

ACLI Path: config t→system→system-config

```
system-config
      hostname                  oraclesbc.com
      description               SBC connecting IMS to Teams Phone Mobile
      location                  Burlington, MA
      transcoding-cores         1
```

### 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.

To configure NTP from ACLI –

ACLI Path: config t→system→ntp-sync

```
ntp-config
      server                    216.239.35.0
```

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

## 9.2 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 Microsoft Teams Phone Mobile, the other to connect to an IMS Network.

*The slots and ports used in this example may be different from your network setup*.

### 9.2.1 Physical Interfaces

- Use the following table as a configuration example:

| Config Parameter | Teams Phone Mobile | IMS |
|---|---|---|
| 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*

To configure Physical Interfaces from ACLI –

ACLI Path: config t→system→phy-interface

```
phy-interface
      name                    s0p0
      operation-type            Media
phy-interface
      name                    s1p0
      operation-type            Media
      slot                    1
```

### 9.2.2 Network Interfaces

- Use the following table as a configuration example:

| Configuration Parameter | Teams Phone Mobile | IMS |
|---|---|---|
| Name | S0p0 | S1p0 |
| IP Address | 10.0.2.10 | 10.0.3.10 |
| Netmask | 255.255.255.0 | 255.255.255.0 |
| Gateway | 10.1.2.1 | 10.1.3.1 |
| DNS Primary IP | 8.8.8.8 | |
| DNS Domain | cloudsbc.cgbusolutionslab.com | |

To configure Network Interfaces from ACLI –
ACLI Path: config t→system→network-interface

```
network-interface
      name                    s1p0
      ip-address               10.0.3.10
      netmask                  255.255.255.0
      gateway                  10.1.3.1
network-interface
      name                    s0p0
      ip-address               10.0.2.10
      netmask                  255.255.255.0
      gateway                  10.1.2.1
      dns-ip-primary             8.8.8.8
      dns-ip-backup1             8.8.4.4
      dns-ip-backup2             9.9.9.9
      dns-domain               Cloudsbc.cgbusolutionslab.com
```

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

## 9.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Microsoft Teams Phone Mobile.

Note: Teams Phone Mobile Trunk can also use TCP/RTP Protocol. Use of MAPS (Microsoft Azure Peering Service ) Transport is a MUST for Network to Network Connection between the Oracle SBC and Operator Connect Teams Phone Mobile. Traffic sent through 3rd Part Internet is not supported. For the purpose of the Application Note we have provided TLS/SRTP method of connectivity between Oracle SBC and Microsoft Teams Phone Mobile.

When Using TLS/SRTP Microsoft Teams Phone Mobile recommends 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 **Microsoft Trusted Root Certificate Program**. A list of currently supported Certificate Authrities can be found at: **Public trusted certificate for the SBC.** These are the same CA's supported by Teams Direct Routing Interface.

### 9.3.1 Certificate Records

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

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

GUI Path: security/certificate-record

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

- SBC Certificate (end-entity certificate)
- DigiCert RootCA Cert (Root CA used to sign the SBC's end entity certificate)
- DigiCert Global Root G2 (Microsoft Presents the SBC a certficate 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.*

#### 9.3.1.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Microsoft to secure the connection. The are two requirements when configuring this certificate.

1. Common name must contain the SBC's FQDN

2. extened-key-usage-list must contain both serverAuth and clientAuth.

In this example our common name will be **cloudsbc.cgbusolutionslab.com.** You must also give the certificate record a name and set the extended-key-usage-list to support both client and servier authentication. All other fields are optional, and can remain at default values.

To Configure the certificate record from ACLI:

ACLI Path: config t→security→certificate-record

```
certificate-record
      name                        SBCCertificateforTPM
      state                     California
      locality                   Redwood City
      organization                 Oracle Corporation
      unit                      Oracle CGBU-LABS BOSTON
      common-name                     cloudsbc.cgbusolutionslab.com
      key-usage-list                digitalSignature
                                    keyEncipherment
      extended-key-usage-list         clientAuth
                                      serverAuth
```

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

### 9.3.1.2 Root CA and Intermediate Certificates

#### 9.3.1.2.1 DigiCert Root 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.

#### 9.3.1.2.2 Digicert Global Root G2

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: https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem

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

| Config Parameter | DigiCert Global Root G2 | DigiCert Root CA |
|---|---|---|
| Common Name | DigiCert Global Root G2 | DigiCert Global Root CA |
| Key Size | 2048 | 2048 |
| Key-Usage-List | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment |
| Extended Key Usage List | serverAuth | serverAuth |
| Key algor | rsa | rsa |
| Digest-algor | Sha256 | Sha256 |

```
certificate-record
      name                    DigiCertGlobalRootG2
      common-name                   DigiCert Global Root G2
certificate-record
      name                    DigiCertRoot
      common-name                   DigiCert Global Root CA
```

#### 9.3.1.3 Save and Activate

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.

```
NN4900-102# save-config
checking configuration
-------------------------------------------------------------------
Results of config verification:
   3 configuration errors
   2 configuration warnings
Run 'verify-config' for more details
-------------------------------------------------------------------
Save-Config received, processing.
save-config waiting 120000 ms 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'.
NN4900-102# activate-config
Activate-Config received, processing.
activate-config waiting 120000 ms for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
NN4900-102#
```

#### 9.3.1.4 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**.

To perform the Steps From ACLI use the below command –

```
NN4900-102# generate-certificate-request SBCCertificateforTPM

--This Step generates a text on Screen as shown below --

-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQ
QH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAr3AmjF15PcIcWiB/kFExUGNHQHIbkJi28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLlBsLfem43tbKq5jz/jrvaUzyhlCvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNYbKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZIhvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQE
L
BQADggEBADD5Y+u08LxmTMIsJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNlG276i7pFN1vCIjEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTlQ5P4IgyVJqSBkdI29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMcIOawgDecZ8UjHpJ
lznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----
```

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.

#### 9.3.1.5 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.
After all certificates have been imported, issue a third **save/activate** to complete the configuration of certificates on the Oracle SBC.

To import the certificate from ACLI follow below procedure -

```
NN4900-102# import-certificate try-all SBCCertificateforTeams

The System will show a prompt as below -


IMPORTANT:
      Please enter the certificate in the PEM format.
      Terminate the certificate with ";" to exit.....

Enter the Signed Certificate text as shown below-

-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQ
QH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAr3AmjF15PcIcWiB/kFExUGNHQHIbkJi28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLlBsLfem43tbKq5jz/jrvaUzyhlCvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNYbKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZIhvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQE
L
BQADggEBADD5Y+u08LxmTMIsJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNlG276i7pFN1vCIjEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTlQ5P4IgyVJqSBkdI29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMcIOawgDecZ8UjHpJ
lznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----;
```

**save and activate** your configuration.

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

### 9.3.2 TLS Profile

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

To configure system-config from ACLI –
ACLI Path: config t→security→tls-profile

```
tls-profile
      name                        TeamsTLSProfile
      end-entity-certificate          SBCCertificateforTPM
      trusted-ca-certificates         DigiCertGlobalRootG2
                                  DigiCertRoot
      mutual-authenticate              enabled
      tls-version                   tlsv12
```

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

#### 9.3.3 Media Security

This section outlines how to configure support for media security between the OC-SBC and Microsoft Teams Phone Mobile.

##### 9.3.3.1 SDES-Profile

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

To configure system-config from ACLI –

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

```
sdes-profile
      name                        TeamsSRTP
      crypto-list                  AES_CM_128_HMAC_SHA1_80
      srtp-auth                   enabled
      srtp-encrypt                  enabled
      srtcp-encrypt                 enabled
      mki                         disabled
      egress-offer-format               same-as-ingress
      use-ingress-session-params
      options
      key
      salt
      srtp-rekey-on-re-invite           disabled
      lifetime                    31
```

#### 9.3.3.2 Media Security Policy

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

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 IMS Core.

To configure media security from ACLI.

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

```
media-sec-policy
      name                          IMSNonSecure
      pass-through                  disabled
      options
      inbound
            profile
            mode                    rtp
            protocol                none
            hide-egress-media-update          disabled
      outbound
            profile
            mode                    rtp
            protocol                none
media-sec-policy
      name                          TeamsMediaSecurity
      pass-through                  disabled
      options
      inbound
            profile                 TeamsSRTP
            mode                    srtp
            protocol                sdes
            hide-egress-media-update          disabled
      outbound
            profile                 TeamsSRTP
            mode                    srtp
            protocol                sdes
```

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

## 9.4 Transcoding Configuration

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

### 9.4.1 Media Profiles

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

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

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

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 |
|---|---|---|---|
| Surname | narrowband | wideband | wideband |
| Payload-Type | 103 | 104 | 118 |
| Clock-rate | 8000 | 16000 | 0 |

To configure system-config from ACLI –

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

```
media-profile
      name                  CN
      subname                 wideband
      payload-type              118
media-profile
      name                  SILK
      subname                 narrowband
      payload-type              103
      clock-rate               8000
media-profile
```

```
        name                    SILK
        subname                  wideband
        payload-type              104
        clock-rate               16000
```

### 9.4.2 Codec Policies

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

While transcoding media codecs is optional, Microsoft does require the SBC generate Comfort Noise and RTCP packets towards Teams if the connection on the other side of the SBC does not support either.
Microsoft does not support AMR narrowband (AMR) but does support AMR:WB so AMR narrowband must be stripped from the IMS offer towards Microsoft.

To satisfy this requirement, the SBC uses transcoding resources to generate those packets, which does require a codec policy be configured and assigned.

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

```
codec-policy
        name                    TPMCodecPolicy
         allow-codecs             * AMR:no
         add-codecs-on-egress       CN
        order-codecs
        packetization-time        20
```

If you have chosen to configure the media profiles 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:

```
codec-policy
        name                    TPMCodecPolicy
        allow-codecs             *
        add-codecs-on-egress       CN::wideband SILK::wideband
        order-codecs
        packetization-time        20
```

Lastly, since some IMS networks may have issues with the codecs being offered by Teams Teams Phone Mobile, you can create another codec policy to remove unwanted or unsupported codecs from the request/responses to your Sip Trunk provider.

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

```
codec-policy
      name                          IMSCoreCodecs
      allow-codecs                      PCMU G729 telephone-event AMR
      add-codecs-on-egress              PCMU AMR
```

### 9.4.3 RTCP Policy

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

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.

To configure system-config from ACLI –

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

```
rtcp-policy
      name                          rtcpGen
      rtcp-generate                   all-calls
      hide-cname                      disabled
```

## 9.5 Media Configuration

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

### 9.5.1 Media Manager

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

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

- 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.

To configure system-config from ACLI –

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

```
media-manager
      state                    enabled
options                        audio-allow-asymmetric-pt
                                 xcode-gratuitous-rtcp-report-generation
```

### 9.5.2 Realm Config

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

.

- Use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

| Config Parameter | Teams Phone Mobile Realm | IMS Realm |
|---|---|---|
| Identifier | Teams | ims |
| Network Interface | s0p0:0 | s1p0:0 |
| Mm in realm | enabled | enabled |
| Media Sec policy | TeamsSecurityPolicy | PSTNNonSecure |
| Teams-FQDN | cloudsbc.cgbusolutionslab.com | |
| Teams-fqdn-in-uri | enabled | |
| Sdp-inactive-only | enabled | |
| RTCP mux | enabled | |
| | | |
| Codec policy | TPMCodecPolicy | IMSCoreCodecs |
| RTCP policy | rtcpGen | |
| Access-control-trust-level | HIGH | HIGH |
| ringback-trigger | | 183 |
| ringback-file | | US_Ringback_tone.raw |
| merge-early-dialogs | | enabled |
| hide-egress-media-update | | enabled |

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

- Network Interface

- Media Security Policy
- Codec Policy (optional on the PSTN Realm)
- RTCP Policy
- Ringback trigger,ringback-file, merge-early-dialogs and hide-egress-media-update are required on IMS Ream and are explained in Section of the doc.

To configure realm-config from ACLI –

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

```
realm-config
      identifier                    Teams
      description                    Realm Facing Teams Direct Routing
      network-interfaces                s0p0:0.4
      mm-in-realm                     enabled
      qos-enable                     enabled
      media-sec-policy                  sdesPolicy
      rtcp-mux                      enabled
      teams-fqdn                     cloudsbc.cgbusolutionslab.com
      teams-fqdn-in-uri                enabled
      sdp-inactive-only                enabled
      access-control-trust-level          high
      codec-policy                   TPMCodecPolicy
      rtcp-policy                   rtcpGen
realm-config
      identifier                    ims
      network-interfaces                s1p0:0.4
      media-sec-policy                 RTP
      access-control-trust-level          high
      options                       merge-early-dialogs enable
      codec-policy                    IMSCoreCodecs
      hide-egress-media-update             enabled
      ringback-trigger                 183
      ringback-file                   US_Ringback_tone.raw
      merge-early-dialogs                enabled
```

### 9.5.3 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the OC-SBC. 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

- Click Add, and use the below examples to configure steering-pool.

To configure steering pool from ACLI

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

```
steering-pool
      ip-address          10.0.2.10
      start-port          20000
      end-port            40000
      realm-id            Teams
steering-pool
      ip-address          10.0.3.10
      start-port          20000
      end-port            40000
      realm-id            ims
```

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

### 9.6 Sip Configuration

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

#### 9.6.1 Sip-Config

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

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 sip 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).
- **inmanip-before-validate** (optional) allows the header rules in a sip-manipulation to apply before the message is parsed.
- **sip-message-len** has been increased in the setup to 65535 to allow large sip packets from the Network.
- **multiple-dialogs-enhancement** applied on the sip-config to enable multiple early dialog support. To Allows the merging of early dialogs within forking scenarios, "merge-early-dialogs" should be enabled on the caller side realm-config.
- dialog-transparency is disabled to support merge-early-dialogs feature as explained in Section 12.2.3 of the document.

To configure sip config from ACLI.

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

```
sip-config
      dialog-transparency          disabled
      home-realm-id                Teams
      options                      inmanip-before-validate
                                   max-udp-length=0
                                   multiple-dialogs-enhancement
      sip-message-len              65535
      extra-method-stats           enabled
      npli-upon-register           disabled
```

### 9.6.2 Replaces Header Support

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

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

To configure support for Replaces, we configure the following:

#### 9.6.2.1 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.

To configure sip feature from ACLI

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

```
sip-feature
      name                          replaces
      realm                         Teams
      require-mode-inbound                Pass
     require-mode-outbound                Pass
```

#### 9.6.2.2 Sip Profile

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

To configure sip profile from ACLI

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

```
sip-profile
      name                          forreplaces
      replace-dialogs                  enabled
```

### 9.6.3 Sip Manipulation

#### 9.6.3.1 Sip-manipulation for Teams Phone Mobile call routing logic -

MS Teams uses custom header for identifying/signaling originating/terminating session case: The header name is **X-MS-FMC,** which plays a crucial role in streamlining mobile call handling within the Microsoft Teams Phone Mobile environment.

Possible values for this header are:

| Value | Description | Teams Generated | Teams Received | Correlated Header |
|---|---|---|---|---|
| MO | Mobile Originated | YES | YES | **Anonymous:** P-Asserted-Identity*<br>**Non-Anonymous:** From |
| MT | Mobile Terminated | YES | YES | Request-URI |
| APP | Call from APP | YES | NO | N/A |

Microsoft requires that all requests from the Oracle SBC contain this header with the proper identification, MO or MT. We do this by matching on the information we receive from the IMS core in the P-Server-User header and use sip manipulation to add the correct value for proper call handling within the Teams Phone Mobile environment.

To configure the sip manipulation via ACLI:

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

```
sip-manipulation
    name                    TPMlogic
    header-rule
        name                matchterm
        header-name         P-Served-User
        action              manipulate
        msg-type            request
        methods             INVITE
        element-rule
            name            matchtermval
            parameter-name  sescase
            type            header-param
            action          store
            comparison-type boolean
            match-value     term
        element-rule
            name            matchorigval
            parameter-name  sescase
            type            header-param
            action          store
            comparison-type boolean
            match-value     orig
    header-rule
        name                addmsftheader
        header-name         X-MS-FMC
        action              add
        comparison-type     boolean
        msg-type            request
        methods             INVITE
        match-value         $matchterm.$matchtermval
        new-value           MT
    header-rule
        name                addmsftheader2
        header-name         X-MS-FMC
        action              add
        comparison-type     boolean
        msg-type            request
        methods             INVITE
        match-value         $matchterm.$matchorigval
        new-value           MO
```

While the above manipulation acts as the logic for adding the required Microsoft headers when sending calls towards Microsoft, we have additional header rules into the HMR which may or may not be required in your implementation. These rules are provided for reference –

Removesupported – Removes supported header when sending the Sip Invite towards Microsoft.

ModPAI – Modifies the P-Asserted-Identity to format it as per Microsoft requirements.
removePVNI, RemoveUserAgent, removePSU – Remove the P-VisitedNetwork ID, User Agent and P-Served User when sending the Invite towards Microsoft.
StoreHost – Formats the To header as per the request-URI parameters.

```
header-rule
        name                    removesupported
        header-name               Supported
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    ModPAI
        header-name               P-Asserted-Identity
        action                  manipulate
        msg-type                  request
        methods                   INVITE
        element-rule
            name                      ModUserPAI
            type                    uri-host
            action                    replace
            comparison-type               pattern-rule
            new-value                   $FROM_HOST.$0
    header-rule
        name                    removePVNI
        header-name               P-Visited-Network-ID
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    RemoveUserAgent
        header-name               User-Agent
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    removePSU
        header-name               P-Served-User
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    StoreHost
        header-name               request-uri
        action                  store
        comparison-type             pattern-rule
```

```
        msg-type                    out-of-dialog
        methods                     INVITE
        element-rule
            name                        storeurihost
            type                        uri-host
            action                      store
    header-rule
        name                        CopyHost
        header-name                 To
        action                      manipulate
        methods                     INVITE
        element-rule
            name                        replacehost
            type                        uri-host
            action                      replace
            comparison-type                 boolean
            match-value                 $StoreHost.$storeurihost
            new-value                   $StoreHost.$storeurihost.$0
```

The above sip-manipulation is applied as out-manipulationid on the Teams facing sip-interface.

#### 9.6.3.2 Sip-manipulation to change error 487 to 603

Striprouteheader – Sip-manipulation named Striprouteheader is applied as in-manipulationid on the IMS's sip-interface.

The header rules - striproute1, striproute0 strip the IMS added route headers towards Microsoft.
ChangeCLine – is a requirement for the test bed and can be ignored.
Header rule - check487 converts 487 Request terminated Error response to 603 Decline. As per Microsoft requirement When a TPM user rejects the call via their default mobile dialer with a SIP error response of 487, the operator network must send towards Teams network a 603, so that the call can be redirected to the User's voicemail as well as stop ringing any registered Teams endpoints.

```
sip-manipulation
    name                    striprouteheader
    header-rule
        name                    striproute1
        header-name                 Route[1]
        action                  delete
        msg-type                    request
        methods                 INVITE
    header-rule
        name                    striproute0
        header-name                 Route[0]
        action                  delete
```

```
        msg-type                    request
        methods                     INVITE
    mime-sdp-rule
        name                        ChangeCLine
        msg-type                    request
        methods                     INVITE
        action                      manipulate
        sdp-session-rule
            name                        Cline
            action                      manipulate
            sdp-line-rule
                name                        modcline
                type                        c
                action                      replace
                comparison-type                 pattern-rule
                match-value                 IN IP4 129.158.200.139
                new-value                   "IN IP4 10.0.3.10"
    header-rule
        name                        check487
        header-name                 @status-line
        action                      manipulate
        msg-type                    reply
        methods                     INVITE
        element-rule
            name                        Is487
            type                        status-code
            action                      store
            match-value                 487
    header-rule
        name                        mod487
        header-name                 @status-line
        action                      manipulate
        msg-type                    reply
        methods                     INVITE
        element-rule
            name                        make603
            type                        status-code
            action                      replace
            comparison-type                 boolean
            match-value                 $check487.$Is487
            new-value                   603
        element-rule
            name                        changeReason
            type                        reason-phrase
            action                      replace
            comparison-type                 boolean
```

```
            match-value                 $check487.$Is487
            new-value                   "Decline"
```

#### 9.6.3.3 Sip-Manipulation for P-Early-media header.

Sip-manipulation named E164 which is applied as out-manipulationid on the IMS sip-interface serves below purpose –

Header-rule addPlus formats the Number to E.164 format.
Header-rule PEMAdd calls a sip-manipulation Add_PEM_to_183 which calls another sip-manipulation Ins_PEM183 is created to add P-early Media header with a value of “send only" on the 183 Message from Microsoft towards IMS.

The requirement for this sip-manipulation is explained in Section 12.2 of the document.

```
sip-manipulation
      name                        E164
      header-rule
            name                      addPlus
            header-name                 Request-URI
            action                    manipulate
            comparison-type             pattern-rule
            msg-type                  request
            methods                   INVITE
            element-rule
                  name                  tendigits
                  type                uri-user
                  action              replace
                  comparison-type           pattern-rule
                  match-value             ^[0-9]{10}$
                  new-value               \+1+$ORIGINAL
            element-rule
                  name                  elevendigits
                  type                uri-user
                  action              replace
                  comparison-type           pattern-rule
                  match-value             ^[0-9]{11}$
                  new-value               \++$ORIGINAL
      header-rule
            name                      PEMAdd
            header-name                 FROM
            action                    sip-manip
            msg-type                  reply
            methods                   INVITE
            new-value                 Add_PEM_to_183
```

```
pri-tpm-sbc# sh ru sip-manipulation Add_PEM_to_183 short
sip-manipulation
        name                            Add_PEM_to_183
        header-rule
                name                            Detect_183
                header-name                         @status-line
                action                          manipulate
                comparison-type                     pattern-rule
                element-rule
                        name                            detect183
                        type                            status-code
                        action                          sip-manip
                        comparison-type                     pattern-rule
                        match-value                     183
                        new-value                       Ins_PEM183
pri-tpm-sbc# sh ru sip-manipulation Ins_PEM183 short
sip-manipulation
        name                            Ins_PEM183
        header-rule
                name                            Ins_PEM_Field
                header-name                     P-Early-Media
                action                          add
                new-value                       sendonly
```

#### 9.6.4 Sip Interface

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

Configure two sip interfaces, one associated with IMS Realm, and the other for Teams Phone Mobile.

Use the table below as an example to configure:

| Config Parameter | IMS | Teams |
|---|---|---|
| Realm ID | ims | Teams |
| Sip-Profile | | forreplaces |
| out-manipulationid | striprouteheader | TPMlogic |
| in-manipulationid | E164 | |
| **Sip Port Config Parameter** | **IMS** | **Teams** |
| Address | 10.0.3.10 | 10.0.2.10 |
| Port | 5060 | 5061 |
| Transport protocol | TCP | TLS |
| TLS profile | | TeamsTLSProfile |
| Allow anonymous | agents-only | all |

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

To configure sip interface from ACLI

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

```
sip-interface
      realm-id                    Teams
      sip-port
            address                   10.0.2.10
            port                    5061
            transport-protocol            TLS
            tls-profile               tlsteams
            allow-anonymous               all
      spl-options
HeaderNatPublicSipIfIp=129.80.211.181,HeaderNatPrivateSipIfIp=10.0.2.10
      out-manipulationid            TPMlogic
      sip-profile                 forreplaces
sip-interface
      realm-id                    ims
      sip-port
            address                   10.0.3.10
            allow-anonymous               agents-only
      sip-port
            address                   10.0.3.10
            transport-protocol            TCP
            allow-anonymous               agents-only
      spl-options
HeaderNatPublicSipIfIp=129.158.200.139,HeaderNatPrivateSipIfIp=10.0.3.10
      in-manipulationid           striprouteheader
      out-manipulationid            E164
```

### 9.6.5 Session Agents

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

Microsoft provides four (4) regional FQDN's for PSTN Hub (NOAM, EMEA, APAC, OCEA), These FQDNs must be configured as Session-Agents in the order of the served market. For e.g. If SBC primarily serves NOAM market(s) you MUST configure their environment to target the NOAM FQDN first.

Following 4 FQDNs must be configured as Session-Agents on Oracle SBC.

**NOAM:** sip-us.gcs.pstnhub.microsoft.com

**EMEA:** sip-eu.gcs.pstnhub.microsoft.com

**APAC:** sip-as.gcs.pstnhub.microsoft.com

**OCEA**: sip-au.gcs.pstnhub.microsoft.com

Use the table below to configure Session Agents:

| Config parameter | Session Agent 1 | Session Agent 2 | Session Agent 3 | Session Agent 3 |
|---|---|---|---|---|
| Hostname | sip-us.gcs.pstnhub.microsoft.com | sip-eu.gcs.pstnhub.microsoft.com | sip-as.gcs.pstnhub.microsoft.com | sip-au.gcs.pstnhub.microsoft.com |
| Port | 5061 | 5061 | 5061 | 5061 |
| Transport method | StaticTLS | StaticTLS | StaticTLS | StaticTLS |
| Realm ID | Teams | Teams | Teams | Teams |
| Ping Method | OPTIONS | OPTIONS | OPTIONS | OPTIONS |
| Ping Interval | 60 | 60 | 60 | 60 |

| | | | | |
|---|---|---|---|---|
| Refer Call Transfer | enabled | enabled | enabled | enabled |
| Ping Response | enabled | enabled | enabled | enabled |

Note: In the test setup OC-SBC is handling REFERs for call transfers hence the Refer Call Transfer parameter is enabled on the Session-Agents. This will not be required if the REFER messages for call transfers are handled by the IMS Network.

We'll also configure a session agent for the IMS Core.

To configure session agents from ACLI

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

```
session-agent
      hostname                sip-as.gcs.pstnhub.microsoft.com
      port                  5061
      transport-method          StaticTLS
      realm-id                Teams
      ping-method               OPTIONS
      ping-interval             60
      ping-response             enabled
      refer-call-transfer       enabled
session-agent
      hostname                sip-au.gcs.pstnhub.microsoft.com
      port                  5061
      transport-method          StaticTLS
      realm-id                Teams
      ping-method               OPTIONS
      ping-interval             60
      ping-response             enabled
      refer-call-transfer       enabled
session-agent
      hostname                sip-eu.gcs.pstnhub.microsoft.com
      port                  5061
      transport-method          StaticTLS
      realm-id                Teams
      ping-method               OPTIONS
      ping-interval             60
      ping-response             enabled
```

```
        refer-call-transfer             enabled
session-agent
        hostname                        sip-us.gcs.pstnhub.microsoft.com
        port                        5061
        transport-method                StaticTLS
        realm-id                    Teams
        ping-method                     OPTIONS
        ping-interval                   60
        ping-response                   enabled
        refer-call-transfer             enabled
```

We have defined Session Agents SCSCF and PCSCF for IMS Core as per the requirement of the Test bed. You may have to define additional IMS components based on your network setup and requirements.

```
session-agent
        hostname                    129.213.187.4
        transport-method                StaticTCP
        realm-id                    ims
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
        refer-call-transfer             enabled

session-agent
        hostname                    volte.oraclecgbupoc.co.uk
        port                        5063
        realm-id                    ims
```

### 9.6.6 Session Group

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

All four 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.

- Use the following as an example to configure:

To configure session group from ACLI

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

```
session-group
      group-name                    TeamsPhoneMobile
      dest                      sip-us.gcs.pstnhub.microsoft.com
                                 sip-eu.gcs.pstnhub.microsoft.com
                                 sip-as.gcs.pstnhub.microsoft.com
                                 sip-au.gcs.pstnhub.microsoft.com
```

### 9.7 Routing Configuration

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

**Local Policy for Calls**

We have configured below local-policies on the OC-SBC to route the call From IMS network to Microsoft and from Microsoft to IMS.Please adjust local policies according to your network requirements.

To configure local policy from ACLI:

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

```
local-policy
      from-address                  *
      to-address                  *
      source-realm                  Teams
      policy-attribute
            next-hop                    129.213.187.4
            realm                     ims
local-policy
      from-address                  *
      to-address                  volte.oraclecgbupoc.co.uk
      source-realm                  Teams
      policy-attribute
            next-hop                    sag:ocsag
            realm                     Teams
            action                    replace-uri
            terminate-recursion             enabled
local-policy
```

```
    from-address                *
    to-address                *
    source-realm                ims
    policy-attribute
        next-hop                    sag:ocsag
        realm                   Teams
        action                  replace-uri
```

As we are handling Transfers on OC-SBC an additional Local Policy is created for call transfers towards Microsoft TPM users which routes back the REFERs to a TPM user towards Microsoft. This policy is not required if REFERs are handed in the IMS Network.

```
local-policy
    from-address                *
    to-address                sip.gcs.pstnhub.microsoft.com
    source-realm                Teams
    policy-attribute
        next-hop                    sag:ocsag
        realm                   Teams
        action                  replace-uri
```

### 9.8 SIP Access Controls

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

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

https://docs.oracle.com/en/industries/communications/session-border-controller/9.2.0/security/security-guide.pdf

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

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high

2. Set the access control trust level on public facing realms to HIGH

Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.
Use this example to create ACL's for all Microsoft Teams subnets. This example can be followed for any of the public facing interfaces, i.e., Sip Trunk, etc…

To configure access control from ACLI

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

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

```
access-control
      realm-id                  ims
      source-address              129.213.136.120
      application-protocol          SIP
      trust-level               high
access-control
      realm-id                  ims
      source-address              129.213.187.4
      application-protocol          SIP
      trust-level               high
access-control
      realm-id                  ims
      source-address              158.101.98.101
      application-protocol          SIP
      trust-level               high
access-control
      realm-id                  Teams
      source-address              52.112.0.0/14
      application-protocol          SIP
      trust-level               high
access-control
      realm-id                  Teams
      source-address              52.120.0.0/14
      application-protocol          SIP
      trust-level               high
```

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone Mobile.

You'll need to **save and activate** your configuration!

# 10 Verify Connectivity

## 10.1 Oracle SBC Options Pings

While in the Oracle SBC ACLI, Utilize the "show sipd options" command to check for OPTIONS to and from the SBC.

```
NN4900-102# show sipd options
OPTIONS (22:17:05-116)
                    --------- Server --------   --------- Client --------
Message/Event       Recent      Total  PerMax   Recent      Total  PerMax
                    ------  ---------  ------   ------  ---------  ------
OPTIONS Requests        10      80976      10        7      59979       9
Retransmissions          0          0       0        0          0       0
200 OK                  10      80928      10        7      59979       9
403 Forbidden            0         48       4        0          0       0
Transaction Timeouts     -          -       -        0          0       0
Locally Throttled        -          -       -        0          0       0

Avg Latency=0.001 for 7
Max Latency=0.002
NN4900-102#
```

Looking at both the **Server Recent** and **Client Recent**, verify the counters are showing OPTIONS Requests and 200OK responses.

# 11 Syntax Requirements for SIP Invite and SIP Options:

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.

Microsoft includes two customer headers **X-MS-TenantId and X-MS-FMC**: that contains the specific customer's O365 Tenant ID and type of call which can be MO,MT or App (Call orginated from Teams Client)

Note: The information is masked in the below example for security purpose.

## 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 and Final Responses.

Contact Header-Invite and Final Response

- Must have the FQDN sub-domain of the Oracle SBC.
- **Syntax: Contact: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>**

**Picture 1** Example of an Outbound INVITE from OC-SBC to Microsoft Teams when the call is originated from the native dialer.

```
INVITE sip:+918130313388@sip-
us.gcs.pstnhub.microsoft.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS
129.80.211.181:5061;branch=z9hG4bKjqnuho20dgioci186hl0.1
Max-Forwards: 67
Contact: <sip:+17812032798-
kb6trde2tmaa5@cloudsbc.cgbusolutionslab.com:5061;transport=tls>;sip
.ice
To: <sip:+918130313388@sip-us.gcs.pstnhub.microsoft.com:5061>
From:
"+17812032798"<sip:+17812032798@cloudsbc.cgbusolutionslab.com>;tag=
SDlg3q102-866d834c
Call-ID: SDlg3q102-771ef03cf155a9bd75752f0bc82ee477-a002h90020
CSeq: 1 INVITE
Allow: OPTIONS, SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER,
INFO
Content-Type: application/sdp
Content-Length: 448
P-Asserted-Identity:
<sip:+17812032798@cloudsbc.cgbusolutionslab.com>
P-Asserted-Identity: <tel:+17812032798>
X-MS-SBC: Oracle/VM/9.2.0p2
X-MS-FMC: MO
```

**Picture 2** Example of an Outbound INVITE from OC-SBC to Microsoft Teams and 200OK Response for the Terminating User.

```
INVITE sip:+17812032798@sip-
us.gcs.pstnhub.microsoft.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS
129.80.211.181:5061;branch=z9hG4bKnkshuo20301q7koprou0.1
From:
<sip:+918130313388@cloudsbc.cgbusolutionslab.com;user=phone>;tag=SD
rsipd02-1737061874-
To: "ORACLESOLLAB ."<sip:+17812032798@sip-
us.gcs.pstnhub.microsoft.com:5061;user=phone>
Call-ID: SDrsipd02-1413f8d3430bbb0ac3067ec9d9fff725-a004050050
CSeq: 1067923422 INVITE
Contact:
<sip:+918130313388@cloudsbc.cgbusolutionslab.com:5061;transport=tls
>;sip.ice
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Recv-Info: x-broadworks-client-session-info
Accept:
application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 63
Content-Type: application/sdp
Content-Length: 560
X-MS-SBC: Oracle/VM/9.2.0p2
X-MS-FMC: MT
```

```
SIP/2.0 200 OK
FROM:
<sip:+918130313388@cloudsbc.cgbusolutionslab.com;user=phone>;tag=SD
rsipd02-1737061874-1707237863355-
TO: "ORACLESOLLAB ."<sip:+17812032798@sip-
us.gcs.pstnhub.microsoft.com:5061;user=phone>;tag=288cffdf7f444a5c8
00b8f753bb4e021
CSEQ: 1067923422 INVITE
CALL-ID: SDrsipd02-1413f8d3430bbb0ac3067ec9d9fff725-a004050050
VIA: SIP/2.0/TLS
10.0.2.10:5061;branch=z9hG4bKnkshuo20301q7koprou0.1
RECORD-ROUTE: <sip:sip-
us.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-a-usea.pstnhub.microsoft.com:443;x-i=46df673f-
486e-49b7-8907-3c0a88093814;x-
c=964a4f5cbcb2547b83f6834244cada37/s/1/36913655622a42f6a7d5ce82008b
0d32>
CONTENT-LENGTH: 463
SUPPORTED: timer
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
SESSION-EXPIRES: 3600;refresher=uas
SERVER: Microsoft.PSTNHub.SIPProxy v.2024.2.6.5 i.USEA.1
```

```
X-MS-TenantId: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

**Picture 3** Example of an Inbound INVITE from Microsoft Teams and 200OK response from OC-SBC when call is originated from Teams App.

```
INVITE
sip:+918130313388@cloudsbc.cgbusolutionslab.com:5061;user=phone;tra
nsport=tls SIP/2.0
FROM:”A"<sip:+17812032798@sip.gcs.pstnhub.microsoft.com:5061;user=p
hone>;tag=f5f2eadf00eb4c1dabf
TO:
<sip:+918130313388@cloudsbc.cgbusolutionslab.com:5061;user=phone>
CSEQ: 1 INVITE
CALL-ID: 0eda2c078d475cc49fb25c60c062b4df
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.121.152.238:5061;branch=z9hG4bKa1f450a5
RECORD-ROUTE: <sip:sip-
as.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-a-jawe.pstnhub.microsoft.com:443;x-i=042391f0-
2eaa-40b2-b9ca-6b4bff7549ae;x-
c=0eda2c078d475cc49fb25c60c062b4df/d/10/b52aac267e60436ab5e2b41076e
c2e31>
CONTENT-LENGTH: 740
MIN-SE: 300
SUPPORTED: histinfo,timer
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2024.2.6.5 i.JAEA.4
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
P-ASSERTED-IDENTITY: <tel:+17812032798>
P-ASSERTED-IDENTITY: <sip:testing@solutionslab.cgbubedford.com>
PRIVACY: id
SESSION-EXPIRES: 1800
X-MS-FMC: APP
X-MS-TenantId: xxxxxxxxxxxxxxxxxxxxxxx
```

```
SIP/2.0 200 OK
FROM:
<sip:+918130313388@cloudsbc.cgbusolutionslab.com:5060;user=phone>;t
ag=1f3d2cf80a
TO:
<sip:+17814437243@20.110.144.248:5060;user=phone>;tag=c428e41bfffff
fff441c10fdf29ff1d1
CSEQ: 2 INVITE
CALL-ID: 1-1f3d2cf80a020100.4e254b4f@68.68.117.67
VIA: SIP/2.0/TLS 10.1.4.4:5061;branch=z9hG4bKbv84u130a0ploamklum0.1
RECORD-ROUTE: <sip:sip-
us.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-a-usea.pstnhub.microsoft.com:443;x-i=5b91f474-
e551-4193-aafd-3402ebf9515a;x-
c=460859ece4ce5d59b176f00581a1415c/s/1/853ad12525314f64ae4677a23afd
c208>
CONTENT-LENGTH: 1285
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
SERVER: Microsoft.PSTNHub.SIPProxy v.2022.2.14.2 i.USEA.4
X-MS-TenantId: xxxxxxxxxxxxxxxxxxxxxxx
```

### 11.3 Requirements for SIP Options.

Below are the Microsoft requirements for SIP Options Message.

- The SBC MUST support the SIP OPTIONS method and respond to an incoming SIP OPTIONS request based on RFC 3261.
- The SBC MUST NOT respond with SIP/2.0 405 Method Not Supported or 215 SIP/2.0 501 Not Implemented.
- The OPTIONS pings from SBC MUST NOT exceed a frequency of one transaction every 60 seconds for each configured trunk and MUST NOT be more less frequent than one 229 transaction every 180 seconds for each configured trunk.
- Microsoft will not initiate OPTIONS pings to SBC until it receives OPTIONS pings from the SBC.
- The CONTACT header MUST contain the FQDN of the trunk and MUST specify both the port and protocol (e.g., 5061 and TLS)
- **Syntax: Contact: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>**
- Microsoft will not include the ACCEPT header and will ignore any body text in the response.

**Picture 3** - Example of SIP OPTIONS message from Oracle SBC to Microsoft.

```
OPTIONS sip:sip-us.gcs.pstnhub.microsoft.com:5061;transport=tls
SIP/2.0
Via: SIP/2.0/TLS
20.65.42.129:5061;branch=z9hG4bKdik4l8206025aqb9v510
Call-ID: c75cbb319998591b44c2c7e20e8f717b0000g30@10.1.4.4
To: sip:ping@sip-us.gcs.pstnhub.microsoft.com
From:
sip:ping@cloudsbc.cgbusolutionslab.com;tag=bba52bd57d6bd688fde828d0
5f2a71830000g30
Max-Forwards: 70
CSeq: 7 OPTIONS
Contact: sip:ping@
cloudsbc.cgbusolutionslab.com:5061;transport=tls;sip.ice
Expires: 60
Route: sip:52.115.54.0:5061;transport=tls;lr
X-MS-SBC: Oracle/VM/9.2.0p2
Content-Length: 0
```

**Picture 4** - Example of SIP OPTIONS message from Microsoft to Oracle SBC.

```
OPTIONS sip:ping@cloudsbc.cgbusolutionslab.com:5061;transport=tls
SIP/2.0
FROM: <sip:sip-us.gcs.pstnhub.microsoft.com:5061>;tag=89a53e30-
276b-4596-a761-0ac7c919a859
TO: <sip:ping@cloudsbc.cgbusolutionslab.com>
CSEQ: 1 OPTIONS
CALL-ID: 92542534-cad5-4501-a418-b9f6304bf45b
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.115.54.0:5061;branch=z9hG4bK728aa3f0
CONTACT: <sip:sip-us.gcs.pstnhub.microsoft.com:5061>
CONTENT-LENGTH: 0
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2022.2.14.2 i.USEA.3
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
```

# 12 Appendix A

## 12.1 Oracle SBC deployed behind NAT

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

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

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

- The private IP address must be the same IP as configured on both the SIP Interface and Steering Pool
- The public IP address must be the public IP address of the NAT device

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

The SPL is applied to the Teams side SIP interface.

HeaderNatPublicSipIfIp= 129.80.211.18,HeaderNatPrivateSipIfIp=10.0.2.10

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.

To configure header  NAT SPL from ACLI

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

Choose the sip interface on which the header NAT SPL needs to be applied. Under spl-options add the entry as per example shared below.

```
spl-options
HeaderNatPublicSipIfIp=129.80.211.18,HeaderNatPrivateSipIfIp=10.0.2.10
```

- Perform a **save and activate** configuration for changes to take effect.

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

### 12.2 Early Media handling, Local Media Playback and Merge Dialogs -

For certain call flows with early Media Microsoft expects OC-SBC to merge early dialogs sent by Teams and generates a PEM header towards the IMS Core and play Ringback Tone Locally. Microsoft also requires OC-SBC to merge multiple 183 Session Progress Messages from Teams backend and make it a single fork.

We have achieved this by configuring some additional parameters onto the SBC and through sip-manipulations.

#### 12.2.1 Early Media handling

For the requirement of OC-SBC generates a PEM header towards the IMS Core and play Ring back Tone Locally. We have created the sip-manipulation explained in section 9.6.3

The HMR works as below on the 183 Session progress Message from Microsoft.

Inbound 183 Session Progress from Microsoft towards Oracle SBC.

```
SIP/2.0 183 Session Progress
FROM:
<sip:+918130313388@cloudsbc.cgbusolutionslab.com;user=phone>;tag=SD
4dthf02-861130111-1706516226676-
TO: "ORACLESOLLAB ."<sip:+17812032798@sip-
us.gcs.pstnhub.microsoft.com:5061;user=phone>;tag=1c370fd74fa848f18
0e1cdb5e1b03172
CSEQ: 707105083 INVITE
CALL-ID: SD4dthf02-66926c0021824938f6f2de24181dbaf4-a004050
VIA: SIP/2.0/TLS
10.0.2.10:5061;branch=z9hG4bKijge4u00c81tudqgtau0.1
RECORD-ROUTE: <sip:sip-
us.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-b-usea.pstnhub.microsoft.com:443;x-i=38d12233-
f46d-4215-adb9-c5d52b97b0f5;x-
c=b6721950dcf157ae9168ba217afeb25a/s/1/bbef7d3473084ab6b4d4687af54d
063b>
CONTENT-LENGTH: 465
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
SERVER: Microsoft.PSTNHub.SIPProxy v.2024.1.22.1 i.USEA.1
X-MS-TenantId: XXXXXXXXXX
```

Outbound 183 Session progress from SBC towards IMS

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/TCP
10.0.17.20:5060;received=129.213.187.4;branch=z9hG4bK9pi2kq20e8fli1
1lqan0.1
Via: SIP/2.0/UDP
10.0.17.22:5060;branch=z9hG4bKjva37b20agt0hpru2910.1
Via: SIP/2.0/UDP
129.158.200.139:5060;branch=z9hG4bKh3ad2l00cok0vf8848r0.1
From: <sip:+918130313388@63.77.76.250;user=phone>;tag=SD4dthf01-
861130111-1706516226676-
To: "ORACLESOLLAB
."<sip:+17812032798@141.146.36.101:5061;user=phone>;tag=SD4dthf99-
1c370fd74fa848f180e1cdb5e1b03172
Call-ID: SD4dthf01-66926c0021824938f6f2de24181dbaf4-a004050
CSeq: 707105083 INVITE
```

```
Record-Route: <sip:SDgdc09+fpebnfmuvif67u3p5p8fr1ubf-
gl5p7bvvoeuctgh5p7b10ocud5@129.213.187.4:5060;lr;transport=udp>
Contact: <sip:129.158.200.139:5060;x-i=38d12233-f46d-4215-adb9-
c5d52b97b0f5;x-
c=b6721950dcf157ae9168ba217afeb25a/s/1/bbef7d3473084ab6b4d4687af54d
063b;transport=tcp>
CONTENT-LENGTH: 345
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
SERVER: Microsoft.PSTNHub.SIPProxy v.2024.1.22.1 i.USEA.1
X-MS-TenantId: XXXXXXXXXX
P-Early-Media: sendonly
```

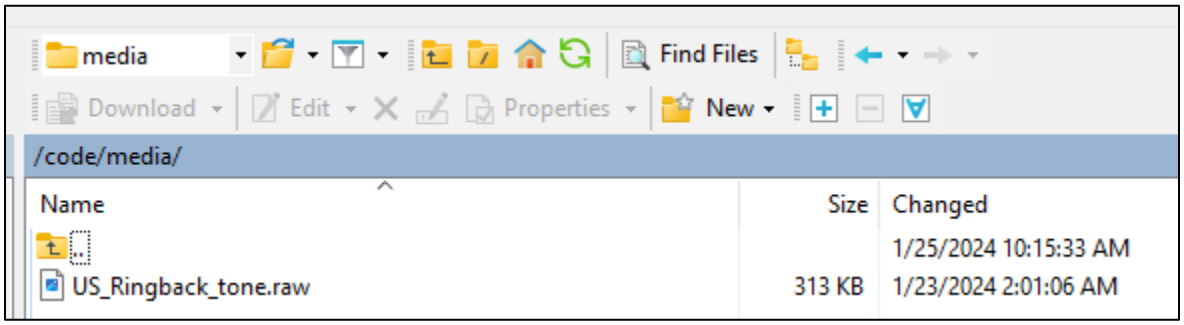
### 12.2.2 Oracle SBC Local Media Playback

Oracle SBC has the capability of playing local media on certain triggers.For this case we are playing the Local Media on the 183 Session progress from the Microsoft towards the Caller.

#### 12.2.2.1 Media Files

Media files of ring back 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, load the file to the /code/media directory on the Oracle SBC. SFTP to the SBC management IP address to securely transfer the file into this directory. In this example, we're using a common SFTP client, WinSCP.




Lastly, we'll assign this file to the realm facing the IMS Core and set the trigger for the SBC to generate local ring back.

#### 12.2.2.2 Local Media Playback Config

To assign the ring back file on the realm through ACLI, navigate to below path and provide the name of the ring back file at the ringback-file config object.

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

```
realm-config
      identifier                    ims
      network-interfaces              s1p0:0.4
      media-sec-policy                RTP
      access-control-trust-level        high
      ringback-trigger                183
      ringback-file                   US_Ringback_tone.raw
```

- Perform a **save and activate** configuration for changes to take effect.

### 12.2.3 Merge Early Dialogs

Microsoft requires OC-SBC to merge multiple 183 Session Progress Messages from Teams backend and make it a single fork. To handle this requirement, we are creating below configuration on the SBC.

```
sip-config
      dialog-transparency             disabled
      home-realm-id                   Teams
      registrar-domain                *
      registrar-host                  *
      registrar-port                  5060
      options                         inmanip-before-validate
                                    max-udp-length=0
                                    multiple-dialogs-enhancement
realm-config
      identifier                    ims
      network-interfaces              s1p0:0.4
      media-sec-policy                RTP
      access-control-trust-level        high
      options                       merge-early-dialogs enable
      hide-egress-media-update          enabled
      ringback-trigger                183
      ringback-file                   US_Ringback_tone.raw
      merge-early-dialogs               enabled
```

Please follow Oracle SBC documentation Section Merge Function within Early Dialog Support on Page 647 for detailed understanding on Merge-early-dialogs feature.

Note Merge-early-dialogs does not work with –

- Offerless call
- Preconditions interworking
- SRVCC • multiple audio or video m-line
- p-early-media-header with 'add' and 'modify' options.

- You should configure HMU to maintain RTP consistency. •
- Dialog transparency should be disabled.

# 13 Appendix B

## 13.1 Test Cases

This version of Application Note is created as per below conducted tests-

| S no. | Case | Status |
|---|---|---|
| 1 | Intra Tenant Call | PASSED |
| 3 | TPM Origination Call to Non-Teams user | PASSED |
| 4 | MT Call to TPM User | PASSED |
| 5 | SBC Sip and Media Interworking towards Teams User | PASSED |
| 6 | SBC Interworking Offer in a-line | PASSED |
| 7 | Cold Transfer to TPM Enabled User | PASSED |
| 8 | Call Transfer to External PSTN | PASSED |
| 10 | Consultative Transfer to TPM Enabled User | PASSED |
| 11 | Call Uplift via Teams App for the Teams Native Dialer in Call | PASSED |
| 13 | User not Assigned in TPM | PASSED |
| 14 | Call Forking and Local Reject (Orig PSTN or Volte User) | PASSED |
| 15 | Local User Rejects incoming call needs to route to TPM VM (global reject SIP Error) | PASSED |
| 16 | Call Forking and Cancel | PASSED |

# 14 ACLI Running Configuration

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

```
pri-tpm-sbc#
pri-tpm-sbc# sh ru short
access-control
        realm-id                        ims
        source-address                    129.213.136.120
        application-protocol                SIP
        trust-level                     high
access-control
        realm-id                        ims
        source-address                    129.213.187.4
        application-protocol                SIP
        trust-level                     high
access-control
        realm-id                        siptrunk
        source-address                    141.146.36.88
        application-protocol                SIP
        trust-level                     high
access-control
        realm-id                        ims
        source-address                    158.101.98.101
        application-protocol                SIP
        trust-level                     high
access-control
        realm-id                        Teams
        source-address                    52.112.0.0/14
        application-protocol                SIP
        trust-level                     high
access-control
        realm-id                        Teams
        source-address                    52.120.0.0/14
        application-protocol                SIP
        trust-level                     high
certificate-record
        name                            BaltimoreRoot
        common-name                         Baltimore CyberTrust Root
certificate-record
        name                            DigiCertGlobalRootG2
        organization                      DigiCert
        unit                            www.digicert.com
        common-name                         DigiCert Global Root G2
certificate-record
        name                            DigiCertRoot
        common-name                         DigiCert Global Root CA
certificate-record
        name                            SBCCertificateforTPM
        common-name                         cloudsbc.cgbusolutionslab.com
```

```
        extended-key-usage-list              clientAuth
                                    serverAuth
codec-policy
        name                        IMSCoreCodecs
        allow-codecs                   PCMU G729 telephone-event AMR
        add-codecs-on-egress              PCMU AMR
codec-policy
        name                        TPMCodecPolicy
        allow-codecs                   * AMR:no
        add-codecs-on-egress              CN
http-server
        name                        web
ice-profile
        name                        ice
        stun-conn-timeout                 0
        stun-keep-alive-interval          0
local-policy
        from-address                   *
        to-address                    *
        source-realm                   Teams
        policy-attribute
                next-hop                  129.213.187.4
                realm                     ims
local-policy
        from-address                   *
        to-address                    sip.gcs.pstnhub.microsoft.com
        source-realm                   Teams
        policy-attribute
                next-hop                  sag:ocsag
                realm                     Teams
                action                    replace-uri
local-policy
        from-address                   *
        to-address                    volte.oraclecgbupoc.co.uk
        source-realm                   Teams
        policy-attribute
                next-hop                  sag:ocsag
                realm                     Teams
                action                    replace-uri
                terminate-recursion             enabled
local-policy
        from-address                   *
        to-address                    *
        source-realm                   ims
        policy-attribute
                next-hop                  sag:ocsag
```

```
            realm                   Teams
            action                  replace-uri
local-policy
      from-address                  *
      to-address                    pstn.com
      source-realm                  ims
      policy-attribute
            next-hop                141.146.36.88
            realm                   siptrunk
local-policy
      from-address                  *
      to-address                    *
      source-realm                  siptrunk
      policy-attribute
            next-hop                158.101.98.101
            realm                   ims
media-manager
      options                       audio-allow-asymmetric-pt
                                    xcode-gratuitous-rtcp-report-generation
media-profile
      name                          CN
      subname                       wideband
      payload-type                  118
      clock-rate                    16000
media-profile
      name                          SILK
      subname                       narrowband
      payload-type                  103
      clock-rate                    8000
media-profile
      name                          SILK
      subname                       wideband
      payload-type                  104
      clock-rate                    16000
media-sec-policy
      name                          IMSNonSecure
media-sec-policy
      name                          TeamsMediaSecurity
      inbound
            profile                 SDES
            mode                    srtp
            protocol                sdes
      outbound
            profile                 SDES
            mode                    srtp
            protocol                sdes
```

```
network-interface
        name                    s0p0
        hostname                cloudsbc.cgbusolutionslab.com
        ip-address              10.0.2.10
        netmask                 255.255.255.0
        gateway                 10.0.2.1
        dns-ip-primary          8.8.8.8
        dns-domain              cloudsbc.cgbusolutionslab.com
network-interface
        name                    s0p1
        ip-address              10.0.4.10
        netmask                 255.255.255.0
        gateway                 10.0.4.1
network-interface
        name                    s1p0
        ip-address              10.0.3.10
        netmask                 255.255.255.0
        gateway                 10.0.3.1
ntp-config
        server                  216.239.35.0
phy-interface
        name                    s0p0
        operation-type          Media
phy-interface
        name                    s0p1
        operation-type          Media
        port                    1
phy-interface
        name                    s1p0
        operation-type          Media
        slot                    1
realm-config
        identifier              Teams
        description             Realm Facing Teams Direct Routing
        network-interfaces      s0p0:0.4
        mm-in-realm             enabled
        qos-enable              enabled
        media-sec-policy        sdesPolicy
        rtcp-mux                enabled
        ice-profile             ice
        teams-fqdn              cloudsbc.cgbusolutionslab.com
        teams-fqdn-in-uri       enabled
        sdp-inactive-only       enabled
        access-control-trust-level  high
        codec-policy            TPMCodecPolicy
        rtcp-policy             rtcpGen
```

```
realm-config
        identifier                      ims
        network-interfaces                s1p0:0.4
        media-sec-policy                RTP
        access-control-trust-level        high
        options                         merge-early-dialogs enable
        codec-policy                    IMSCoreCodecs
        hide-egress-media-update            enabled
        ringback-trigger                183
        ringback-file                   US_Ringback_tone.raw
        merge-early-dialogs               enabled
realm-config
        identifier                      siptrunk
        network-interfaces                s0p1:0.4
        media-sec-policy                RTP
        options                         merge-early-dialogs enable
        hide-egress-media-update            enabled
        merge-early-dialogs             enabled
response-map
        name                            reject
        entries
                recv-code                   487
                xmit-code                   603
                reason                  Decline
rtcp-policy
        name                            rtcpGen
        rtcp-generate                   all-calls
sdes-profile
        name                            TeamsSRTP
        lifetime                        31
session-agent
        hostname                      129.213.187.4
        transport-method                StaticTCP
        realm-id                      ims
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
        refer-call-transfer             enabled
session-agent
        hostname                      141.146.36.88
        realm-id                      siptrunk
        ping-interval                   30
        ping-response                   enabled
session-agent
        hostname                      158.101.98.101
        ip-address                    158.101.98.101
```

```
        realm-id                ims
session-agent
        hostname                sip-as.gcs.pstnhub.microsoft.com
        port                    5061
        transport-method        StaticTLS
        realm-id                Teams
        ping-method             OPTIONS
        ping-interval           30
        ping-response           enabled
        refer-call-transfer     enabled
session-agent
        hostname                sip-au.gcs.pstnhub.microsoft.com
        port                    5061
        transport-method        StaticTLS
        realm-id                Teams
        ping-method             OPTIONS
        ping-interval           30
        ping-response           enabled
        refer-call-transfer     enabled
session-agent
        hostname                sip-eu.gcs.pstnhub.microsoft.com
        port                    5061
        transport-method        StaticTLS
        realm-id                Teams
        ping-method             OPTIONS
        ping-interval           30
        ping-response           enabled
        refer-call-transfer     enabled
session-agent
        hostname                sip-us.gcs.pstnhub.microsoft.com
        port                    5061
        transport-method        StaticTLS
        realm-id                Teams
        ping-method             OPTIONS
        ping-interval           30
        ping-response           enabled
        refer-call-transfer     enabled
session-agent
        hostname                volte.oraclecgbupoc.co.uk
        port                    5063
        realm-id                ims
session-group
        group-name              ocsag
        dest                    sip-us.gcs.pstnhub.microsoft.com
                                sip-eu.gcs.pstnhub.microsoft.com
                                sip-au.gcs.pstnhub.microsoft.com
```

```
                                    sip-as.gcs.pstnhub.microsoft.com
session-timer-profile
      name                          ToTeams
      force-reinvite                enabled
      request-refresher             uas
session-translation
      id                            toPSTN
sip-config
      dialog-transparency           disabled
      home-realm-id                 Teams
      registrar-port                5060
      options                       inmanip-before-validate
                                    max-udp-length=0
                                    multiple-dialogs-enhancement
      sip-message-len               65535
      extra-method-stats            enabled
      allow-pani-for-trusted-only   disabled
      add-ue-location-in-pani       disabled
      npli-upon-register            disabled
sip-feature
      name                          replaces
      realm                         Teams
      require-mode-inbound          Pass
      require-mode-outbound         Pass
sip-interface
      realm-id                      Teams
      sip-port
            address                 10.0.2.10
            port                    5061
            transport-protocol      TLS
            tls-profile             tlsteams
            allow-anonymous         all
      spl-options
HeaderNatPublicSipIfIp=129.80.211.181,HeaderNatPrivateSipIfIp=10.0.2.10
      out-manipulationid            TPMlogic
      sip-profile                   forreplaces
sip-interface
      realm-id                      ims
      sip-port
            address                 10.0.3.10
            allow-anonymous         agents-only
      sip-port
            address                 10.0.3.10
            transport-protocol      TCP
            allow-anonymous         agents-only
```

```
        spl-options
HeaderNatPublicSipIfIp=129.158.200.139,HeaderNatPrivateSipIfIp=10.0.3.10
        in-manipulationid                striprouteheader
        out-manipulationid               E164
sip-interface
        realm-id                         siptrunk
        sip-port
                address                  10.0.4.10
                allow-anonymous                  agents-only
        spl-options
HeaderNatPublicSipIfIp=129.80.186.157,HeaderNatPrivateSipIfIp=10.0.4.10
sip-manipulation
        name                             AddPAcmePlayback
        header-rule
                name                     CheckForSDPInactive
                header-name                  Content-Type
                action                   store
                comparison-type                  pattern-rule
                methods                  INVITE
                element-rule
                        name                     Inactive
                        parameter-name                   application/SDP
                        type                     mime
                        action                   store
                        match-value                  a=inactive
        header-rule
                name                     StartMoH
                header-name                  P-Acme-Playback
                action                   add
                comparison-type                  boolean
                methods                  INVITE
                match-value                  $CheckForSDPInactive.$Inactive
                new-value                    "start;duration=continuous;direction=both;stop-on-final-
resp=false"
sip-manipulation
        name                             AddReftertoAllow
        header-rule
                name                     AllowRefer
                header-name                  Allow
                action                   manipulate
                methods                  Invite
                new-value                    $ORIGINAL+",REFER"
sip-manipulation
        name                             Add_PEM_to_183
        header-rule
                name                     Detect_183
```

```
            header-name                     @status-line
            action                        manipulate
            comparison-type                 pattern-rule
            element-rule
                name                         detect183
                type                        status-code
                action                       sip-manip
                comparison-type                pattern-rule
                match-value                    183
                new-value                     Ins_PEM183
sip-manipulation
      name                          DeleteSDP
      header-rule
            name                      Store180
            header-name                 @status-line
            action                    store
            msg-type                    reply
            methods                     Invite
            element-rule
                name                       store180
                type                      status-code
                action                     store
                match-value                  180
      mime-sdp-rule
            name                      sdpStrip
            msg-type                    reply
            methods                     Invite
            action                    delete
            comparison-type               boolean
            match-value                 $Store180.$store180
sip-manipulation
      name                          E164
      header-rule
            name                      addPlus
            header-name                 Request-URI
            action                    manipulate
            comparison-type               pattern-rule
            msg-type                    request
            methods                     INVITE
            element-rule
                name                       tendigits
                type                      uri-user
                action                     replace
                comparison-type              pattern-rule
                match-value                  ^[0-9]{10}$
                new-value                    \+1+$ORIGINAL
```

```
        element-rule
            name                    elevendigits
            type                    uri-user
            action                  replace
            comparison-type             pattern-rule
            match-value                 ^[0-9]{11}$
            new-value                   \++$ORIGINAL
    header-rule
        name                    PEMAdd
        header-name                 FROM
        action                  sip-manip
        msg-type                reply
        methods                 INVITE
        new-value                   Add_PEM_to_183
sip-manipulation
    name                    Ins_PEM183
    header-rule
        name                    Ins_PEM_Field
        header-name                 P-Early-Media
        action                  add
        new-value                   sendonly
sip-manipulation
    name                    Mod480
    header-rule
        name                    check480
        header-name                 @status-line
        action                  manipulate
        msg-type                reply
        methods                 INVITE
        element-rule
            name                    Is480
            type                    status-code
            action                  store
            match-value                 480
    header-rule
        name                    mod480
        header-name                 @status-line
        action                  manipulate
        msg-type                reply
        methods                 INVITE
        element-rule
            name                    make603
            type                    status-code
            action                  replace
            comparison-type             boolean
            match-value                 $check480.$Is480
```

```
            new-value                   603
        element-rule
            name                        changeReason
            type                        reason-phrase
            action                      replace
            comparison-type             boolean
            match-value                 $check480.$Is480
            new-value                   "Decline"
sip-manipulation
    name                        RemoveAttribute
    mime-sdp-rule
        name                    RemoveXAttribute
        msg-type                request
        methods                 Invite
        action                  manipulate
        sdp-media-rule
            name                RemoveX
            media-type          audio
            action              manipulate
            sdp-line-rule
                name            RemoveA
                type            a
                action          delete
                comparison-type     pattern-rule
                match-value         x-candidate-info
    header-rule
        name                    AcmeNATFrom
        header-name             From
        action                  manipulate
        msg-type                request
        methods                 Invite
        element-rule
            name                FromHost
            type                uri-host
            action              replace
            new-value           $LOCAL_IP
        element-rule
            name                FromPort
            type                uri-port
            action              replace
            new-value           $LOCAL_PORT
    header-rule
        name                    AcmeNatTo
        header-name             To
        action                  manipulate
        msg-type                request
```

```
        methods                 Invite
        element-rule
            name                ToHost
            type                uri-host
            action              replace
            new-value           $REMOTE_IP
        element-rule
            name                ToPort
            type                uri-port
            action              replace
            new-value           $REMOTE_PORT
    header-rule
        name                    RemovePrivacy
        header-name             Privacy
        action                  delete
        msg-type                request
        methods                 Invite
    header-rule
        name                    DeletePAI
        header-name             P-Asserted-Identity[1]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    DeletePAI0
        header-name             P-Asserted-Identity[0]
        action                  delete
        msg-type                request
        methods                 INVITE
sip-manipulation
    name                    TPMlogic
    header-rule
        name                    matchterm
        header-name             P-Served-User
        action                  manipulate
        msg-type                request
        methods                 INVITE
        element-rule
            name                matchtermval
            parameter-name      sescase
            type                header-param
            action              store
            comparison-type     boolean
            match-value         term
        element-rule
            name                matchorigval
```

```
            parameter-name              sescase
            type                      header-param
            action                     store
            comparison-type                boolean
            match-value                 orig
    header-rule
        name                        addmsftheader
        header-name                   X-MS-FMC
        action                      add
        comparison-type               boolean
        msg-type                    request
        methods                     INVITE
        match-value                   $matchterm.$matchtermval
        new-value                   MT
    header-rule
        name                        addmsftheader2
        header-name                   X-MS-FMC
        action                      add
        comparison-type               boolean
        msg-type                    request
        methods                     INVITE
        match-value                   $matchterm.$matchorigval
        new-value                   MO
    header-rule
        name                        removesupported
        header-name                   Supported
        action                      delete
        msg-type                    request
        methods                     INVITE
    header-rule
        name                        ModPAI
        header-name                   P-Asserted-Identity
        action                      manipulate
        msg-type                    request
        methods                     INVITE
        element-rule
            name                      ModUserPAI
            type                    uri-host
            action                    replace
            comparison-type                pattern-rule
            new-value                   $FROM_HOST.$0
    header-rule
        name                        removePVNI
        header-name                   P-Visited-Network-ID
        action                      delete
        msg-type                    request
```

```
        methods                 INVITE
    header-rule
        name                    RemoveUserAgent
        header-name             User-Agent
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    removePSU
        header-name             P-Served-User
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    StoreHost
        header-name             request-uri
        action                  store
        comparison-type         pattern-rule
        msg-type                out-of-dialog
        methods                 INVITE
        element-rule
            name                storeurihost
            type                uri-host
            action              store
    header-rule
        name                    CopyHost
        header-name             To
        action                  manipulate
        methods                 INVITE
        element-rule
            name                replacehost
            type                uri-host
            action              replace
            comparison-type     boolean
            match-value         $StoreHost.$storeurihost
            new-value           $StoreHost.$storeurihost.$0
sip-manipulation
    name                    ZoomE164
    header-rule
        name                addplus
        header-name         Request-URI
        action              manipulate
        msg-type            request
        methods             Invite
        element-rule
            name            TenDigits
```

```
                type                    uri-user
                action                  replace
                comparison-type             pattern-rule
                match-value             ^[0-9]{10}$
                new-value               \+1+$ORIGINAL
            element-rule
                name                    ElevenDigits
                type                    uri-user
                action                  replace
                comparison-type             pattern-rule
                match-value             ^[0-9]{11}$
                new-value               \++$ORIGINAL
        header-rule
            name                    AddContactOptions
            header-name                 Contact
            action                  add
            msg-type                request
            methods                 OPTIONS
            new-value               "<sip:ping@"+141.146.36.68+":5061>"
sip-manipulation
        name                    add100reltosupported
        header-rule
            name                    add100rel
            header-name                 Supported
            action                  manipulate
            comparison-type             pattern-rule
            msg-type                request
            methods                 INVITE
            new-value               100rel
sip-manipulation
        name                    striprouteheader
        header-rule
            name                    striproute1
            header-name                 Route[1]
            action                  delete
            msg-type                request
            methods                 INVITE
        header-rule
            name                    striproute0
            header-name                 Route[0]
            action                  delete
            msg-type                request
            methods                 INVITE
        mime-sdp-rule
            name                    ChangeCLine
            msg-type                request
```

```
        methods                         INVITE
        action                        manipulate
        sdp-session-rule
            name                         Cline
            action                      manipulate
            sdp-line-rule
                name                        modcline
                type                       c
                action                      replace
                comparison-type                pattern-rule
                match-value                   IN IP4 129.158.200.139
                new-value                    "IN IP4 10.0.3.10"
    header-rule
        name                          check487
        header-name                     @status-line
        action                        manipulate
        msg-type                       reply
        methods                        INVITE
        element-rule
            name                         Is487
            type                       status-code
            action                      store
            match-value                   487
    header-rule
        name                          mod487
        header-name                     @status-line
        action                        manipulate
        msg-type                       reply
        methods                        INVITE
        element-rule
            name                         make603
            type                       status-code
            action                      replace
            comparison-type                boolean
            match-value                   $check487.$Is487
            new-value                    603
        element-rule
            name                         changeReason
            type                       reason-phrase
            action                      replace
            comparison-type                boolean
            match-value                   $check487.$Is487
            new-value                    "Decline"
sip-manipulation
    name                        test
    header-rule
```

```
            name                          addxfmc
            header-name                      X-MS-FMC
            action                        add
            msg-type                       request
            methods                       INVITE
            new-value                      MT
sip-monitoring
      match-any-filter                 enabled
      monitoring-filters               *
sip-profile
      name                           forreplaces
      replace-dialogs                  enabled
ssh-key
      name                           admin
      type                           authorized-key
      size                           2048
steering-pool
      ip-address                      10.0.2.10
      start-port                     20000
      end-port                       40000
      realm-id                       Teams
steering-pool
      ip-address                      10.0.3.10
      start-port                     20000
      end-port                       40000
      realm-id                       ims
steering-pool
      ip-address                      10.0.4.10
      start-port                     20000
      end-port                       40000
      realm-id                       siptrunk
system-config
      hostname                        oraclesbc.com
      description                     SBC connecting IMS to Teams Phone Mobile
      dos-cores                      1
      transcoding-cores                1
tls-global
      session-caching                enabled
      diffie-hellman-key-size           DH_KeySize_2048
tls-profile
      name                           TeamsTLSProfile
      end-entity-certificate           SBCCertificateforTPM
      trusted-ca-certificates          DigiCertGlobalRootG2
                                    DigiCertRoot
      mutual-authenticate              enabled
      tls-version                    tlsv12
```

```
pri-tpm-sbc#
```

**Oracle Corporation, World Headquarters**
2300 Cloud Way
Austin, TX 78741, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/Oracle/


twitter.com/Oracle


oracle.com

Integrated Cloud Applications & Platform Services