Application Note

Public

Direct Routing for Microsoft Phone System with Cisco Unified Border Element (CUBE)

22 September, 2021

Contents

Introduction

Customers using Microsoft Phone System have the option of connecting to the public telephony network (PSTN) using a certified Session Border Controller (SBC), such as the Cisco Unified Border Element (CUBE).

This application note describes a tested CUBE configuration for connecting Microsoft Phone System to the PSTN using Verizon's IP Trunking service. CUBE can be configured to connect with many service providers offering SIP trunking services. Please refer to your service provider documentation and the content provided at https://www.cisco.com/c/en/us/solutions/enterprise/interoperability-portal/networking_solutions_products_genericcontent0900aecd805bd13d.html for guidance on how to adjust this tested configuration to meet the specific requirements of your trunking service.

This document assumes the reader is knowledgeable with the terminology and configuration of Direct Routing for Microsoft Phone System. Only CUBE configurations required for this tested solution are presented. Feature configuration and most importantly the dial plan, are customer specific so must be customized accordingly.

- This application note describes how to configure Direct Routing for Microsoft Phone System to the PSTN (Verizon) via CUBE. Minimum required CUBE releases are:
  - CUBE v12.8.0 or later [IOS-XE – 17.2.1r] (**with Media bypass disabled**)
  - CUBE v14.1 or later [IOS-XE – 17.3.3] (**with Media bypass enabled**)
- **Configuration shown in this application note is based on IOS-XE 17.6.1a or later, which is recommended for all CUBE deployments with Direct Routing for Microsoft Phone System. Other IOS-XE releases requiring a different CUBE configuration may also be used, but the reader should check for any pending software defects and deploy a modified configuration as needed.**
- Testing was performed in accordance with Direct Routing for Microsoft Phone System test methodology and among features verified were – basic calls, DTMF transport, blind transfer, consultative transfer, call forward, ad-hoc conference and hold/resume.
- The CUBE configuration detailed in this document is based on a lab environment that has been used to detail the important settings required for successful interoperability with a simple dial plan. Microsoft guidance for the configuration of call routing and policy in Phone System must be followed to ensure calls compete as expected.

Network Topology

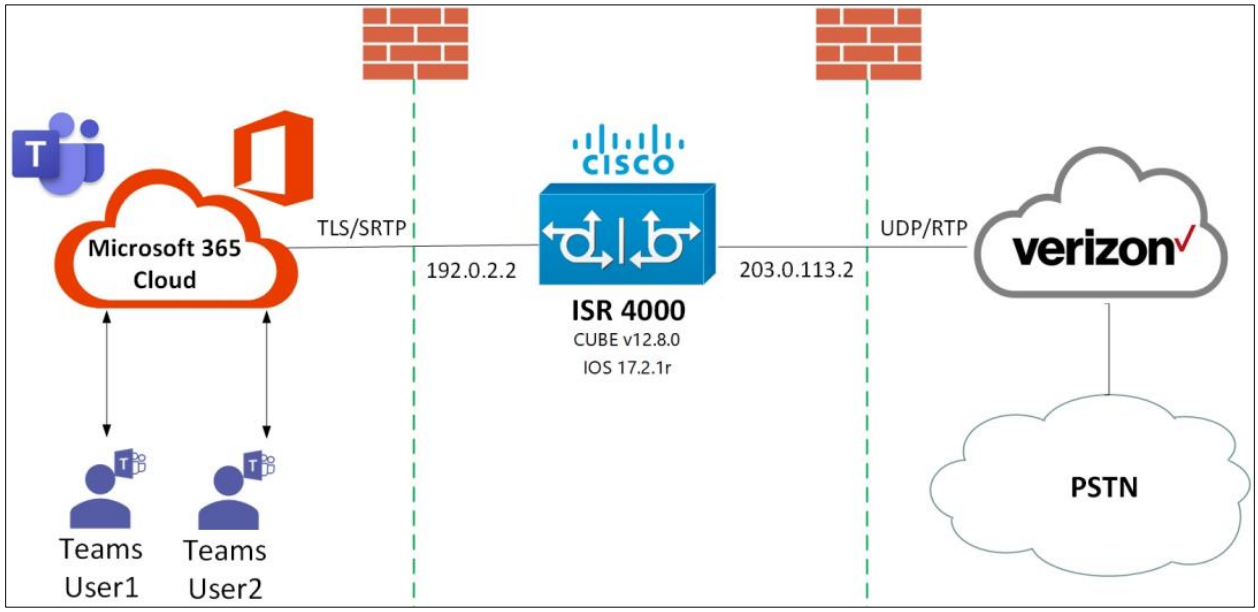


Figure 1 Network Topology

- The network topology includes the Microsoft Phone System, Teams client and CUBE. Microsoft 365 admin center is used to configure a gateway trunk associated with CUBE's public FQDN. Verizon was used as the service provider with a SIP trunk to CUBE using its public IP Address.
- SIP signaling used between CUBE and Microsoft Phone System Direct routing is over TLS and to Verizon is over UDP transport.

Direct Routing for Microsoft Phone System and CUBE Settings

Setting	Value
Transport from CUBE to MS Phone System	TLS with SRTP
Transport from CUBE to Verizon	UDP with RTP
Session Refresh	YES

Tested System Components

The following components were used in the testing of this solution. Please refer to product documentation for details of other supported options.

Hardware

- A Cisco ISR 4321 router was used for this tested solution. Any CUBE platform may be used though, (refer to https://www.cisco.com/go/cube) for more information.
- Microsoft Windows computer (to run Microsoft Teams client)

Software

- CUBE-Version: 14.4 [IOS-XE 17.6.1a or later]
- Microsoft Office 365 Tenant with Phone System license
- Microsoft Teams desktop client version 1.3.00.12058 (version 1.3.00.30866 for media bypass enabled)

Tested Features

Features Supported

- Incoming and outgoing off-net calls using G.711 u-law
- Ad-hoc Conference
- Call hold & Resume
- Blind and Consultative Call transfer
- Call forward (all and no answer)
- DTMF (RFC2833)
- Microsoft Teams Calling number privacy
- CUBE High Availability (for validated CUBE-HA configuration refer to Appendix A)

Features Not Supported

- RTCP multiplexing (RTCP-Mux)
- Comfort Noise generation
- RTCP generation when not provided by peer leg
- Fax (Not supported by Phone System)

Caveats

- Testing has been executed with both Media Bypass disabled (IOS-XE 17.2.1r) and Media Bypass enabled (IOS-XE 17.3.3) in Microsoft Phone System.
- For inbound calls towards Microsoft Phone System to work with ring back, 183 messages with SDP are blocked in CUBE.
- CUBE sends History-info header to PSTN in all basic calls instead of sending it only on Call forward and simultaneous ring calls.
- The Phone System tenant must be configured to generate ring back audio to the PSTN caller during blind transfer.
- CUBE does not support RTCP multiplexing (rtcp-mux).
- CUBE will forward, but not generate RTCP.
- CUBE does not generate comfort noise (CN) towards Phone System clients when PSTN mutes the call.
- In an inbound call to Microsoft Teams DND user, CUBE hunted to all Microsoft Phone system data centers when it received a 408 from Teams DND user and it does not pass that 408 from Teams to PSTN. However, if Teams sends 480 for DND as per test case expectation, then CUBE can pass that to PSTN.

Configuring Cisco Unified Border Element for Microsoft Phone System

This section details the aspects of CUBE configuration that are required to enable interworking with Microsoft Phone System. This guidance should be used to either create a new or adapt an existing configuration. A full configuration is also provided for reference.

The following formatting conventions are used in the remainder of this guide.

Cisco IOS Exec Commands

```
# show running-config
```

Cisco IOS Configuration Commands

```
hostname sbc1
```

Microsoft PowerShell commands

```
Get-CsOnlinePSTNGateway
```

Prerequisites

The following is required before adding CUBE as a Direct Routing Session Bordering Controller:

- Public, Internet routable IP address
- Fully Qualified Domain Name (FQDN) for CUBE from the same domain that is used by Phone System.
- Public certificate for the CUBE FQDN issued by one of the Certificate Authorities supported by Microsoft. Refer to Microsoft documentation for more information.

Licensing

Ensure that the appropriate licenses are enabled for using CUBE and TLS for the platform you are using. You will need to save your configuration and reload the platform when changing feature licenses.

For Cisco ISR 1000 Series and Cisco 4000 Series routers, use the following commands:

```
license boot level uck9
license boot level securityk9
```

For Cisco Cloud Services Router 1000 Series virtual routers using IOS-XE 17.3 or earlier, configure both the feature and required throughput levels. The following example uses 1Gbps throughput, select the appropriate level for the number of calls anticipated.

```
license boot level ax
platform hardware throughput level MB 1000
```

For Cisco ASR 1000 Series routers, use *either* the Advanced IP services or Advanced Enterprise services with one of the following commands:

```
license boot level advipservices
license boot level adventerprise
```

For Cisco Catalyst 8300 and 8200 Series Edge Platforms, use the DNA Network Essentials feature license, or better and the required throughput level. The following example uses 25Mbps bidirectional crypto throughput, select the appropriate level for the number of calls anticipated.

```
license boot level network-essentials
platform hardware throughput crypto 25M
```

For Cisco Catalyst 8000V Edge Software, use the DNA Network Essentials feature license, or better and the required throughput level. The following example uses 1Gbps throughput, select the appropriate level for the number of calls anticipated.

```
license boot level network-essentials
platform hardware throughput level MB 1000
```

IP Networking

Note: CUBE and service provider addresses used in this guide are fictional and provided for illustration purposes only.

```
interface GigabitEthernet0/0/0
 description towards Microsoft Phone System
 ip address 192.0.2.2 255.255.255.0
!
interface GigabitEthernet0/0/1
 description towards PSTN (Verizon)
 ip address 203.0.113.2 255.255.255.0
!
ip tcp synwait-time 5
```

Route To Phone System & Internet

```
ip route 0.0.0.0 0.0.0.0 192.0.2.1
```

Route To PSTN-Verizon

```
ip route 19.51.100.0 255.255.255.0 203.0.113.1
```

Domain Name

Use the same domain name for the router as used for the Microsoft 365 tenant.

```
ip domain name example.com
```

DNS Servers

DNS must be configured to resolve addresses for Microsoft Direct Routing servers.

```
ip name-server 208.67.222.222 208.67.220.220
```

NTP Servers

Configure a suitable NTP source to ensure that the correct time is used by the platform.

```
ntp server 192.0.2.1
```

Certificates

Microsoft Phone System Direct Routing allows only TLS connections from SBCs for SIP traffic with a certificate signed by one of the following trusted Certification Authorities. Certificate Authority choice may vary in GCC and DoD (gov) environments.

Certificates with a wildcard in the certificate Subject Alternate Name field conforming to RFC2818 are also supported. For more information, refer to the Microsoft documentation.

The following steps describe how to create and install a compatible certificate.

Generate RSA key

```
crypto key generate rsa general-keys label sbc exportable
The name for the keys will be: sbc
Choose the size of the key modulus in the range of 512 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [1024]: 2048
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
```

Create SBC Trustpoint

```
crypto pki trustpoint sbc
 enrollment terminal
 fqdn sbc.example.com
 subject-name cn=sbc.example.com
 subject-alt-name sbc.example.com
 revocation-check crl
 rsakeypair sbc
```

Generate Certificate Signing Request (CSR)

```
crypto pki enroll sbc
% Start certificate enrollment..

% The subject name in the certificate will include: cn=sbc.example.com
% The subject name in the certificate will include: sbc.example.com
Display Certificate Request to terminal? [yes/no]: yes
```

Use this CSR to request a certificate from one of the supported Certificate authorities.

Authenticate CA Certificate

Enter the following command, then paste the CA certificate that verifies the host certificate into the trust point (usually the intermediate certificate). Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted:

```
crypto pki authenticate sbc

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

Note: Refer the running configuration for the trust point of Root CA.

Import signed host certificate

Enter the following command then paste the host certificate into the trust point. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted:

```
crypto pki import sbc certificate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

Specify the default trust point and TLS version with SIP-UA defaults

```
sip-ua
 no remote-party-id
 retry invite 2
 transport tcp tls v1.2
 crypto signaling default trustpoint sbc
 handle-replaces
```

Trusted CA trust point for Baltimore

Create the CA certificate trust point used to validate Microsoft Phone System TLS messages:

```
crypto pki trustpoint baltimore
 enrollment terminal
 revocation-check crl
```

Enter the following command then paste the CA certificate (https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem) into the trust point. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted:

```
crypto pki authenticate baltimore

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

Global CUBE settings

To enable CUBE with settings required to interwork with Microsoft Phone System, the following commands must be entered:

```
voice service voip
 ip address trusted list           ! SIP messages allowed from these networks
  ipv4 52.112.0.0 255.252.0.0      ! Microsoft cloud services
  ipv4 52.120.0.0 255.252.0.0
  ipv4 19.51.100.0                 ! Service Provider trunk
 rtcp keepalive
 address-hiding
 mode border-element
 allow-connections sip to sip
 no supplementary-service sip refer
 supplementary-service media-renegotiate
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  session refresh
  header-passing
  error-passthru
  conn-reuse
  pass-thru headers 290
  sip-profiles inbound
```

Explanation

Command	Description
`ip address trusted list`	Allows traffic from Phone System and the PSTN. Refer to Microsoft documentation for address and port information to use for firewall configuration.
`allow-connections sip to sip`	Allow back to back user agent connections between two SIP call legs
`rtcp-keepalive`	Enables CUBE to send RTCP keepalive packets for the session keepalive
`handle-replaces`	Handles INVITEs with replaces. Required for Phone System

Call Admission Control

Call processing capacity for any CUBE instance will be influenced by several considerations, including software version, features configured and the platform itself.

To ensure that calls continue to be processed reliably, we suggest that you configure Call Admission Control as follows to reject calls when use of system resources exceeds 85%. Refer to the CUBE Configuration Guide for further details.

```
call threshold global cpu-avg low 75 high 85
call threshold global total-mem low 75 high 85
call treatment on
```

Message Handling Rules

The following SIP Profiles are required within the CUBE configuration to interop with Direct Routing. SIP Profiles are listed for an environment where CUBE is configured with a routable public IP address and also where CUBE is deployed behind NAT. When CUBE is configured with a private IP address behind a NAT router/firewall, it requires SIP message manipulation to translate between private (internal) and public (external) embedded IP addresses. The NAT-based alterations shown here assume a static 1:1 NAT.

In a NAT deployment the DNS FQDN used to reach CUBE must resolve to the public NAT address. The CUBE host certificate must use this same FQDN.

Additional SIP Profile rules may be required to cover all headers/SDP lines in the SIP messages where the IP address will have to be modified.

SIP Profile 100: Manipulations for outbound messages to PSTN trunk

Message manipulations should be configured as required for the PSTN service being used. The following rule was required specifically for the Verizon trunk used in this case:

1. [**Rule 10**] Use SDP `inactive` instead of `sendonly`.

```
voice class sip-profiles 100
 rule 10 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
```

SIP Profile 200: Manipulations for outbound messages to Phone System

The following sip profile is required to:

1. [**Rules 10 and 20**] Replace CUBE IP address with Fully qualified domain names (FQDN) in the 'Contact' header of INVITE messages.
2. [**Rule 30**] Set "user=phone" in all requests.
3. [**Rules 40 and 50**] Add the "X-MS-SBC" header containing SBC version details in all request and response. Specify your router model as defined in the table below.
4. [**Rule 60**] Set the audio SDP attribute to inactive instead of sendonly for calls on hold.
5. **[Rule 70]** Ensure that routable IP address is used for media
6. **[Rules 71-74]** Replace embedded private IP addresses with the external NAT address.
7. [**Rules 80 and 90**] Set crypto life-time as 2^31 in all SDP sent from CUBE.
8. [**Rules 100 and 110 – only required for Media Bypass disabled**]
   Remove ICE candidate headers when Media Bypass is disabled in Phone System.
9. **[Rules 130-180]** Replace embedded private IP addresses in SDP with the external NAT address.
10. **[Rule 260]** Adjust cause code returned by Phone System for Busy on Busy calls to ensure that caller hears busy tone.

CUBE configured with a public IP address

```
voice class sip-profiles 200
 rule 10 request ANY sip-header Contact modify "@.*:" "@sbc.example.com:"
 rule 20 response ANY sip-header Contact modify "@.*:" "@sbc.example.com:"
 rule 30 request ANY sip-header SIP-Req-URI modify "sip:(.*):5061 (.*)"
"sip:\1:5061;user=phone \2"
 rule 40 request ANY sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 50 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 60 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 70 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "192.0.2.2"
 rule 80 request ANY sdp-header Audio-Attribute modify
"(a=crypto:.*inline:[A-Za-z0-9+/=]+)" "\1|2^31"
 rule 90 response ANY sdp-header Audio-Attribute modify
"(a=crypto:.*inline:[A-Za-z0-9+/=]+)" "\1|2^31"
rule 100 request ANY sdp-header Audio-Attribute modify "a=candidate.*"
"a=label:main-audio"
 rule 110 response ANY sdp-header Audio-Attribute modify "a=candidate.*"
"a=label:main-audio"
 rule 260 response 486 sip-header Reason modify "cause=34;" "cause=17;"
```

CUBE behind NAT

```
voice class sip-profiles 200
 rule 10 request ANY sip-header Contact modify "@.*:" "@sbc.example.com:"
 rule 20 response ANY sip-header Contact modify "@.*:" "@sbc.example.com:"
```

```
 rule 30 request ANY sip-header SIP-Req-URI modify "sip:(.*):5061 (.*)"
"sip:\1:5061;user=phone \2"
 rule 40 request ANY sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 50 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 60 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 70 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "nat-ext-ip"
 rule 71 response ANY sdp-header Connection-Info modify "IN IP4 cube-priv-ip" "IN IP4
nat-ext-ip"
 rule 72 response ANY sdp-header Audio-Connection-Info modify "IN IP4 cube-priv-ip"
"IN IP4 nat-ext-ip"
 rule 73 request ANY sdp-header Connection-Info modify "IN IP4 cube-priv-ip" "IN IP4
nat-ext-ip"
 rule 74 request ANY sdp-header Audio-Connection-Info modify "IN IP4 cube-priv-ip"
"IN IP4 nat-ext-ip"
 rule 80 request ANY sdp-header Audio-Attribute modify
"(a=crypto:.*inline:[A-Za-z0-9+/=]+)" "\1|2^31"
 rule 90 response ANY sdp-header Audio-Attribute modify
"(a=crypto:.*inline:[A-Za-z0-9+/=]+)" "\1|2^31"
rule 100 request ANY sdp-header Audio-Attribute modify "a=candidate.*"
"a=label:main-audio"
 rule 110 response ANY sdp-header Audio-Attribute modify "a=candidate.*"
"a=label:main-audio"
rule 130 response ANY sdp-header Audio-Attribute modify "a=rtcp:(.) IN IP4 cube-priv-
ip " "a=rtcp:\1 IN IP4 nat-ext-ip "
 rule 140 request ANY sdp-header Audio-Attribute modify "a=rtcp:(.) IN IP4 cube-priv-
ip " "a=rtcp:\1 IN IP4 nat-ext-ip "
 rule 150 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.) cube-
priv-ip (.) " "a=candidate:1 1\1 nat-ext-ip \2"
 rule 160 request ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.) cube-
priv-ip (.) " "a=candidate:1 1\1 nat-ext-ip \2"
 rule 170 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.) cube-
priv-ip (.) " "a=candidate:1 2\1 nat-ext-ip \2"
 rule 180 request ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.) cube-
priv-ip (.) " "a=candidate:1 2\1 nat-ext-ip \2
 rule 260 response 486 sip-header Reason modify "cause=34;" "cause=17;"
```

To aid with support, Microsoft require the specific SBC model to be included in SIP messages. Select the appropriate replacement string from the following options when configuring rules 40 and 50:

Platform	Profile string
ISR1100 (any)	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR1100**/\1"
ISR4321	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4321**/\1"
ISR4331	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4331**/\1"

ISR4351	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4351**/\1"
ISR4431	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4431**/\1"
ISR4451-X	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4451**/\1"
ISR4461	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4461**/\1"
Catalyst 8000V	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**C8000V**/\1"
Catalyst 8200	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**C8200**/\1"
Catalyst 8300	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**C8300**/\1"
ASR1001-X	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1001X**/\1"
ASR1002-X	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1002X**/\1"
ASR1004	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1004**/\1"
ASR1006/RP2	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1000RP2**/\1"
ASR1006/RP3	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1000RP3**/\1"

SIP Profile 290: Manipulations for inbound messages from Phone System

The following sip profile is required to:

1. [**Rule 10 and 15**] Handle REFER and ensure that the subsequent INVITE is sent to the correct Phone System proxy.
2. [**Rules 20 and 30**] Add a routing prefix to the user part of REFER To header to direct the subsequent INVITE to the correct Microsoft Phone System proxy.
3. [**Rule 40**] Ensure that the correct platform ID is used, as described above.
4. [**Rules 50 and 60 – only required for Media Bypass disabled**]
   Remove "ice-candidates" in SDP request and response, which are not required when Media Bypass is disabled.
5. [Rules 70-170] Convert embedded public and private addresses for request and response messages.

CUBE configured with a public IP address

```
voice class sip-profiles 290
 rule 10 request REFER sip-header From copy "@(.*com)" u05
 rule 15 request REFER sip-header From copy "sip:(sip.*com)" u05
 rule 20 request REFER sip-header Refer-To modify "sip:\+(.*)@.*:5061"
"sip:+AAA\1@\u05:5061"
 rule 30 request REFER sip-header Refer-To modify "<sip:sip.*:5061"
"<sip:+AAA@\u05:5061"
 rule 40 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 50 request ANY sdp-header Audio-Attribute modify "a=ice-.*"
"a=label:main-audio"
 rule 60 request ANY sdp-header Attribute modify "a=ice-.*" "a=label:main-audio"
```

CUBE behind NAT

```
voice class sip-profiles 290
 rule 10 request REFER sip-header From copy "@(.*com)" u05
 rule 15 request REFER sip-header From copy "sip:(sip.*com)" u05
 rule 20 request REFER sip-header Refer-To modify "sip:\+(.*)@.*:5061"
"sip:+AAA\1@\u05:5061"
 rule 30 request REFER sip-header Refer-To modify "<sip:sip.*:5061"
"<sip:+AAA@\u05:5061"
 rule 40 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 50 request ANY sdp-header Audio-Attribute modify "a=ice-.*"
"a=label:main-audio"
 rule 60 request ANY sdp-header Attribute modify "a=ice-.*" "a=label:main-audio"
 rule 70 response ANY sdp-header Audio-Attribute modify "IN IP4 cube-priv-ip" "IN IP4
nat-ext-ip"
 rule 80 request ANY sdp-header Connection-Info modify "IN IP4 nat-ext-ip" "IN IP4
cube-priv-ip"
 rule 90 response ANY sdp-header Audio-Attribute modify "IN IP4 nat-ext-ip" "IN IP4
cube-priv-ip"
```

```
 rule 100 response ANY sdp-header Connection-Info modify "IN IP4 nat-ext-ip" "IN IP4
cube-priv-ip"
 rule 110 request ANY sdp-header mline-index 1 c= modify "IN IP4 nat-ext-ip" "IN IP4
cube-priv-ip"
 rule 120 response ANY sdp-header mline-index 1 c= modify "IN IP4 nat-ext-ip" "IN IP4
cube-priv-ip"
 rule 130 request ANY sdp-header Audio-Attribute modify "a=candidate:1 1 (.*) nat-
ext-ip" "a=candidate:1 1 \1 cube-priv-ip"
 rule 140 request ANY sdp-header Audio-Attribute modify "a=candidate:1 2 (.*) nat-
ext-ip" "a=candidate:1 2 \1 cube-priv-ip"
 rule 150 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1 (.*) nat-
ext-ip" "a=candidate:1 1 \1 cube-priv-ip"
 rule 160 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2 (.*) nat-
ext-ip" "a=candidate:1 2 \1 cube-priv-ip"
 rule 170 request ANY sdp-header Audio-Attribute modify "IN IP4 cube-priv-ip" "IN IP4
nat-ext-ip"
```

SIP Profile 280: Message Manipulations for REFER INVITE to Phone System

With the above REFER-TO user part modification, the dial-peer 280 will be matched and the INVITE sent to Phone System after removing the user part routing prefix.

The following sip profile is required to:

1. [**Rules 10 and 20**] Add the "X-MS-SBC" header containing SBC version details in all request and response.
2. **[Rules 30, 110 and 120]** Ensures that the outbound To header uses the same FQDN as the Request URI.
3. **[Rules 70 – 120]** Removes the +AAA REFER steering pattern from all headers.
4. **[Rules 130 and 140]** Replace host details in contact headers with that provided in the FROM header.
5. **[Rules 160 and 170]** Update audio connection IP address.
6. **[Rules 180 -250]** Convert embedded public and private addresses for request and response messages.
7. **[Rule 260]** Adjust cause code returned by Phone System for Busy on Busy calls to ensure that caller hears busy tone.

CUBE configured with a public IP address

```
voice class sip-profiles 280
 rule 10 request ANY sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 20 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 30 request INVITE sip-header SIP-Req-URI copy "@(.*:5061)" u01
 rule 40 request INVITE sip-header From copy "@(.*)>" u02
 rule 71 request INVITE sip-header SIP-Req-URI modify ""sip:\+AAA@" "sip:"
 rule 80 request INVITE sip-header SIP-Req-URI modify "sip:\+AAA" "sip:+"
 rule 90 request INVITE sip-header History-Info modify "<sip:\+AAA@" "<sip:"
 rule 100 request INVITE sip-header History-Info modify "<sip:\+AAA" "<sip:+"
 rule 110 request INVITE sip-header To modify "<sip:\+AAA@(.*)>" "<sip:\u01>"
 rule 120 request INVITE sip-header To modify "<sip:\+AAA(.*)@.*>" "<sip:+\1@\u01>"
 rule 130 request ANY sip-header Contact modify "@.*:" "@\u02:"
 rule 140 response ANY sip-header Contact modify "@.*:" "@\u02:"
 rule 150 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 160 response 200 sdp-header Session-Owner copy "IN IP4 (.*)" u04
 rule 170 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "\u04"
 rule 260 response 486 sip-header Reason modify "cause=34;" "cause=17;"
```

CUBE behind NAT

```
voice class sip-profiles 280
 rule 10 request ANY sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 20 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 30 request INVITE sip-header SIP-Req-URI copy "@(.*:5061)" u01
 rule 40 request INVITE sip-header From copy "@(.*)>" u02
 rule 71 request INVITE sip-header SIP-Req-URI modify ""sip:\+AAA@" "sip:"
 rule 80 request INVITE sip-header SIP-Req-URI modify "sip:\+AAA" "sip:+"
 rule 90 request INVITE sip-header History-Info modify "<sip:\+AAA@" "<sip:"
 rule 100 request INVITE sip-header History-Info modify "<sip:\+AAA" "<sip:+"
 rule 110 request INVITE sip-header To modify "<sip:\+AAA@(.*)>" "<sip:\u01>"
 rule 120 request INVITE sip-header To modify "<sip:\+AAA(.*)@.*>" "<sip:+\1@\u01>"
 rule 130 request ANY sip-header Contact modify "@.*:" "@\u02:"
 rule 140 response ANY sip-header Contact modify "@.*:" "@\u02:"
 rule 150 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 160 response 200 sdp-header Session-Owner copy "IN IP4 (.*)" u04
 rule 170 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "\u04"
 rule 180 request ANY sip-header Via modify "SIP(.*) cube-priv-ip(.*)" "SIP\1 nat-
ext-ip\2"
 rule 190 request INVITE sip-header Requested-By modify "sip:cube-priv-ip>" "sip:nat-
ext-ip>"
```

```
 rule 200 request ANY sdp-header Audio-Connection-Info modify "cube-priv-ip" "nat-
ext-ip"
 rule 210 request ANY sdp-header Connection-Info modify "cube-priv-ip" "nat-ext-ip"
 rule 220 request ANY sdp-header Session-Owner modify "cube-priv-ip" "nat-ext-ip"
 rule 230 response ANY sdp-header Audio-Connection-Info modify "cube-priv-ip" "nat-
ext-ip"
 rule 240 response ANY sdp-header Connection-Info modify "cube-priv-ip" "nat-ext-ip"
 rule 250 response ANY sdp-header Session-Owner modify "cube-priv-ip" "nat-ext-ip"
 rule 260 response 486 sip-header Reason modify "cause=34;" "cause=17;"
```

SIP header Pass-through list

Pass-through Referred-By header to be used in the REFER INVITE send to Phone System.

```
voice class sip-hdr-passthrulist 290
 passthru-hdr Referred-By
```

Options Keepalive

To ensure that Contact and From headers include the SBC fully qualified domain name, the following profile is used. Ensure that the appropriate platform ID is used, as described above.

CUBE configured with a public IP address

```
voice class sip-profiles 299
 rule 10 request OPTIONS sip-header From modify "<sip:.*:5061"
"<sip:sbc.example.com:5061"
 rule 20 request OPTIONS sip-header Contact modify "<sip:.*:5061"
"<sip:sbc.example.com:5061"
 rule 30 request OPTIONS sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
!
voice class sip-options-keepalive 200
 sip-profiles 299
 transport tcp tls
```

CUBE behind NAT

```
voice class sip-profiles 299
 rule 9 request ANY sip-header Via modify "SIP(.*) cube-priv-ip(.*)" "SIP\1 nat-ext-
ip\2"
 rule 10 request OPTIONS sip-header From modify "<sip:cube-priv-ip"
"<sip:sbc.example.com"
 rule 20 request OPTIONS sip-header Contact modify "<sip:cube-priv-ip"
"<sip:sbc.example.com"
 rule 30 request OPTIONS sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
rule 40 response ANY sdp-header Connection-Info modify "IN IP4 cube-priv-ip" "IN IP4
nat-ext-ip"
 rule 50 response ANY sdp-header Audio-Connection-Info modify "IN IP4 cube-priv-ip"
"IN IP4 nat-ext-ip"
!
voice class sip-options-keepalive 200
 sip-profiles 299
 transport tcp tls
```

SRTP Crypto

Used to set the crypto cipher for the Microsoft Phone System trunk.

```
voice class srtp-crypto 1
 crypto 1 AES_CM_128_HMAC_SHA1_80
```

STUN ICE-Lite (For Media Bypass enabled only)

Used to enable STUN with ICE-Lite for Media bypass enabled in Microsoft Phone System trunk.

```
voice class stun-usage 1
 stun usage ice lite
```

Phone System Tenant

Defines parameters for the trunk towards Phone System

```
voice class tenant 200
  srtp-crypto 1
  localhost dns:sbc.example.com
  session transport tcp tls
  no referto-passing
  bind all source-interface GigabitEthernet0/0/0
  pass-thru headers 290
  no pass-thru content custom-sdp
  sip-profiles 200
  sip-profiles 290 inbound
  early-offer forced
  block 183 sdp present
```

PSTN Trunk Tenant

Defines parameters for the trunk towards the PSTN. Configure in accordance with service provider requirements.

```
voice class tenant 100
  options-ping 60
  session transport udp
  bind all source-interface GigabitEthernet0/0/1
  no pass-thru content custom-sdp
  sip-profiles 100
  early-offer forced
```

Number translation rules

The following translation rules ensure that numbers presented to Microsoft Phone System are in +E164 format. Translation rules used for the PSTN trunk should format numbers in accordance with the service provider requirements.

From PSTN translation rule with non +E164

```
voice translation-rule 100
 rule 1 /^\([2-9].........\)/ /+1\1/
!
voice translation-profile 100
 translate calling 100
 translate called 100
```

From Phone System translation rule with +E164

```
voice translation-rule 200
 rule 1 /^\+1\(.*\)/ /\1/
!
voice translation-profile 200
 translate calling 200
 translate called 200
```

Codecs

Only the G711ulaw codec has been used for this tested configuration. Ensure that only codecs supported by both PSTN and Microsoft Phone System are included in this configuration.

```
voice class codec 1
 codec preference 1 g711ulaw
```

Dial peers

Outbound Dial-peer to the PSTN using UDP with RTP

The following is an example configuration. Use the settings appropriate for your SIP trunk service.

```
dial-peer voice 100 voip
 description outbound to PSTN
 destination-pattern +1[2-9]..[2-9]......$
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target ipv4:19.51.100.0:5088
 voice-class codec 1
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
```

Inbound Dial-peer from the PSTN using UDP with RTP

The following is an example configuration. Use the settings appropriate for your SIP trunk service.

```
voice class uri 190 sip
 host ipv4:19.51.100.0
!
dial-peer voice 190 voip
 description inbound from PSTN
 translation-profile incoming 100
 rtp payload-type comfort-noise 13
 session protocol sipv2
 incoming uri via 190
 voice-class codec 1
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
```

Outbound Dial-peers to Phone System using TLS with SRTP

To ensure the correct failover order, the following prioritized dial peers are used. To simplify configuration, a common E164 pattern map defining all numbers and prefixes used by Phone System is used for all 3 dial peers. Use patterns that match the number ranges used for calls placed to Phone System. The configuration for all three dial peers is the same, with the exception of preference and Phone System proxy FQDN.

```
voice class e164-pattern-map 200
  e164 +17199T
 !
!
dial-peer voice 200 voip
 description towards Phone System Proxy 1
 preference 1
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip.pstnhub.microsoft.com:5061
 destination e164-pattern-map 200
 voice-class codec 1
 voice class stun-usage 1 ! Include for Media Bypass enabled only
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
!
dial-peer voice 201 voip
 description towards Phone System Proxy 2
 preference 2
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip2.pstnhub.microsoft.com:5061
 destination e164-pattern-map 200
 voice-class codec 1
 voice class stun-usage 1 ! Include for Media Bypass enabled only
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
!
dial-peer voice 202 voip
```

```
description towards Phone System Proxy 3
huntstop
preference 3
rtp payload-type comfort-noise 13
session protocol sipv2
session target dns:sip3.pstnhub.microsoft.com:5061
destination e164-pattern-map 200
voice-class codec 1
voice class stun-usage 1 ! Include for Media Bypass enabled only
voice-class sip tenant 200
voice-class sip options-keepalive profile 200
dtmf-relay rtp-nte
srtp
fax protocol none
no vad
```

Inbound Dial-peer from Phone System using TLS with SRTP

The inbound dial-peer from Phone System is selected using the SBC FQDN as presented in the incoming TO: header.

```
voice class uri 290 sip
 host sbc.example.com
!
dial-peer voice 290 voip
 description inbound from Microsoft Phone System
 translation-profile incoming 200
 rtp payload-type comfort-noise 13
 session protocol sipv2
 incoming uri to 290
 voice-class codec 1
 voice class stun-usage 1 ! Include for Media Bypass enabled only
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound Dial-peer to Phone System for REFER using TLS with SRTP

To correctly handle call transfers, INVITEs following a REFER from Phone System, must be directed back to Phone System. Inbound REFER messages are processed by dial peer 290 and the associated SIP profile adds a routing prefix (AAA) to the refer-to header. The subsequent INVITE is therefore routed to Phone System through the following dial peer after the routing prefix is removed.

```
dial-peer voice 280 voip
 description Phone System REFER routing
 destination-pattern +AAAT
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target sip-uri
 voice-class codec 1
 voice-class sip profiles 280
 voice class stun-usage 1 ! Include for Media Bypass enabled only
 voice-class sip tenant 200
 voice-class sip requri-passing
 dtmf-relay rtp-nte
 srtp
 no vad
```

Privacy Headers

Phone System can be configured to send privacy headers if required, using the following the command.

```
Set-CsOnlinePSTNGateway -Identity sbc1.be4000portal.com -ForwardPai $True
```

To forward the P-Asserted-Identity and Privacy headers sent from Phone System to the PSTN, add the following configuration.

```
dial-peer voice 100 voip
 voice-class sip asserted-id pai
 voice-class sip privacy-policy passthru
```

This will reformat the P-Asserted-Identity header to use a sip:, rather than tel: URI on the PSTN leg and include the Privacy header as provider from Phone System. In this case, the From header will be anonymized, as follows:

From: <sip:anonymous@anonymous.invalid>;tag=1E5FC8C-1642

If your service provider requires the same format, but with the original caller details from Phone System in place, consider the following alternative configuration:

```
dial-peer voice 100 voip
 voice-class sip asserted-id pai
!
voice class sip-profiles 100
 rule 40 request INVITE sip-header P-Asserted-Identity modify "(<.*>)"
"\1\x0D\x0APrivacy: id"
```

Configuration example

The following configuration contains a sample configuration of CUBE (non-NAT) with all parameters detailed above.

```
version 17.6
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname sbc
!
boot-start-marker
boot system flash isr4300-universalk9.17.06.01a.SPA.bin
boot-end-marker
!
logging buffered 10000000
!
ip name-server 208.67.222.222 208.67.220.220
ip domain name example.com
!
crypto pki trustpoint sbc
 enrollment terminal
 fqdn sbc.example.com
 subject-name cn=sbc.example.com
 subject-alt-name sbc.example.com
 revocation-check crl
 rsakeypair sbc
!
crypto pki trustpoint ROOT
 enrollment terminal
 revocation-check none
!
crypto pki trustpoint baltimore
 enrollment terminal
 revocation-check crl
!
crypto pki trustpoint SLA-TrustPoint
 enrollment terminal
 revocation-check crl
!
crypto pki certificate chain sbc
 certificate 64B02D3A6D5DD499
```

```
certificate ca 07
crypto pki certificate chain ROOT
 certificate ca 00
crypto pki certificate chain baltimore
 certificate ca 020000B9
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
!
voice service voip
 ip address trusted list
  ipv4 52.112.0.0 255.252.0.0
  ipv4 52.120.0.0 255.252.0.0
  ipv4 19.51.100.0
 rtcp keepalive
 address-hiding
 mode border-element
 allow-connections sip to sip
 no supplementary-service sip refer
 supplementary-service media-renegotiate
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  session refresh
  header-passing
  error-passthru
  conn-reuse
  pass-thru headers 290
  sip-profiles inbound
!
voice class uri 290 sip
 host sbc.example.com
!
voice class uri 190 sip
 host ipv4:19.51.100.0
!
voice class codec 1
 codec preference 1 g711ulaw
!
voice class sip-profiles 100
 rule 10 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
!
voice class sip-profiles 200
 rule 10 request ANY sip-header Contact modify "@.*:" "@sbc.example.com:"
 rule 20 response ANY sip-header Contact modify "@.*:" "@sbc.example.com:"
```

```
 rule 30 request ANY sip-header SIP-Req-URI modify "sip:(.*):5061 (.*)"
"sip:\1:5061;user=phone \2"
 rule 40 request ANY sip-header User-Agent modify "(IOS.*)" "\1\x0D\x0AX MS SBC:
Cisco UBE/ISR4321/\1"
 rule 50 response ANY sip-header Server modify "(IOS.*)" "\1\x0D\x0AX MS SBC: Cisco
UBE/ISR4321/\1"
 rule 60 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 70 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "192.0.2.2"
 rule 80 request ANY sdp-header Audio-Attribute modify "(a=crypto:.*inline:[A Za z0
9+/=]+)" "\1|2^31"
 rule 90 response ANY sdp-header Audio-Attribute modify "(a=crypto:.*inline:[A Za z0
9+/=]+)" "\1|2^31"
!!!!! – rules 100 and 110 For Media Bypass disabled only – !!!!!
 rule 100 request ANY sdp-header Audio-Attribute modify "a=candidate.*" "a=label:main
audio"
 rule 110 response ANY sdp-header Audio-Attribute modify "a=candidate.*"
"a=label:main audio"
 rule 260 response 486 sip-header Reason modify "cause=34;" "cause=17;"
!
voice class sip-profiles 280
 rule 10 request ANY sip-header User-Agent modify "(IOS.*)" "\1\x0D\x0AX MS SBC:
Cisco UBE/ISR4321/\1"
 rule 20 response ANY sip-header Server modify "(IOS.*)" "\1\x0D\x0AX MS SBC: Cisco
UBE/ISR4321/\1"
 rule 30 request INVITE sip-header SIP-Req-URI copy "@(.*:5061)" u01
 rule 40 request INVITE sip-header From copy "@(.*)>" u02
 rule 71 request INVITE sip-header SIP-Req-URI modify ""sip:\+AAA@" "sip:"
 rule 80 request INVITE sip-header SIP-Req-URI modify "sip:\+AAA" "sip:+"
 rule 90 request INVITE sip-header History-Info modify "<sip:\+AAA@" "<sip:"
 rule 100 request INVITE sip-header History-Info modify "<sip:\+AAA" "<sip:+"
 rule 110 request INVITE sip-header To modify "<sip:\+AAA@(.*)>" "<sip:\u01>"
 rule 120 request INVITE sip-header To modify "<sip:\+AAA(.*)@.*>" "<sip:+\1@\u01>"
 rule 130 request ANY sip-header Contact modify "@.*:" "@\u02:"
 rule 140 response ANY sip-header Contact modify "@.*:" "@\u02:"
 rule 150 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 160 response 200 sdp-header Session-Owner copy "IN IP4 (.*)" u04
 rule 170 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "\u04"
 rule 260 response 486 sip-header Reason modify "cause=34;" "cause=17;"
!
```

```
voice class sip-profiles 290
 rule 10 request REFER sip-header From copy "@(.*com)" u05
 rule 15 request REFER sip-header From copy "sip:(sip.*com)" u05
 rule 20 request REFER sip-header Refer-To modify "sip:\+(.*)@.*:5061"
"sip:+AAA\1@\u05:5061"
 rule 30 request REFER sip-header Refer-To modify "<sip:sip.*:5061"
"<sip:+AAA@\u05:5061"
 rule 40 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
!!!!! – rules 50 and 60 For Media Bypass disabled only – !!!!!
 rule 50 request ANY sdp-header Audio-Attribute modify "a=ice-.*"
"a=label:main-audio"
 rule 60 request ANY sdp-header Attribute modify "a=ice-.*" "a=label:main-audio"
!
voice class sip-profiles 299
 rule 10 request OPTIONS sip-header From modify "<sip:192.0.2.2"
"<sip:sbc.example.com"
 rule 20 request OPTIONS sip-header Contact modify "<sip:192.0.2.2"
"<sip:sbc.example.com"
 rule 30 request OPTIONS sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
!
voice class sip-hdr-passthrulist 290
 passthru-hdr Referred-By
!
voice class e164-pattern-map 200
  e164 +17199T
 !
!
voice class sip-options-keepalive 200
 sip-profiles 299
 transport tcp tls
!
voice class tenant 100
  options-ping 60
  session transport udp
  bind control source-interface GigabitEthernet0/0/1
  bind media source-interface GigabitEthernet0/0/1
  no pass-thru content custom-sdp
  sip-profiles 100
  early-offer forced
!
voice class tenant 200
  srtp-crypto 1
  localhost dns:sbc.example.com
```

```
  session transport tcp tls
  no referto-passing
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
  pass-thru headers 290
  no pass-thru content custom-sdp
  sip-profiles 200
  sip-profiles 290 inbound
  early-offer forced
  block 183 sdp present
!
voice class srtp-crypto 1
 crypto 1 AES_CM_128_HMAC_SHA1_80
!
voice class stun-usage 1
 stun usage ice lite
!
voice translation-rule 100
 rule 1 /^\([2-9].........\)/ /+1\1/
!
voice translation-rule 200
 rule 1 /^\+1\(.*\)/ /\1/
!
voice translation-profile 100
 translate calling 100
 translate called 100
!
voice translation-profile 200
 translate calling 200
 translate called 200
!
license accept end user agreement
license boot level uck9
license boot level securityk9
license smart transport smart
memory free low-watermark processor 67178
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 description towards Microsoft Phone System
 ip address 192.0.2.2 255.255.255.0
 negotiation auto
```

```
!
interface GigabitEthernet0/0/1
 description towards PSTN (Verizon)
 ip address 203.0.113.2 255.255.255.0
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface Service-Engine0/4/0
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
ip tcp synwait-time 5
ip route 0.0.0.0 0.0.0.0 192.0.2.1
ip route 19.51.100.0 255.255.255.0 203.0.113.1
!
dial-peer voice 100 voip
 description outbound to PSTN
 destination-pattern +1[2-9]..[2-9]......$
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target ipv4:19.51.100.0:5088
 voice-class codec 1
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 190 voip
 description inbound from PSTN
 translation-profile incoming 100
 rtp payload-type comfort-noise 13
 session protocol sipv2
 incoming uri via 190
 voice-class codec 1
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 200 voip
 description towards Phone System Proxy 1
```

```
 preference 1
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip.pstnhub.microsoft.com:5061
 destination e164-pattern-map 200
 voice-class codec 1

 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
!
dial-peer voice 201 voip
 description towards Phone System Proxy 2
 preference 2
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip2.pstnhub.microsoft.com:5061
 destination e164-pattern-map 200
 voice-class codec 1
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
!
dial-peer voice 202 voip
 description towards Phone System Proxy 3
 huntstop
 preference 3
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip3.pstnhub.microsoft.com:5061
 destination e164-pattern-map 200
 voice-class codec 1
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
```

```
 srtp
 fax protocol none
 no vad
!
dial-peer voice 280 voip
 description Phone System REFER routing
 destination-pattern +AAAT
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target sip-uri
 voice-class codec 1
 voice-class sip profiles 280
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip requri-passing
 dtmf-relay rtp-nte
 srtp
 no vad
!
dial-peer voice 290 voip
 description inbound from Microsoft Phone System
 translation-profile incoming 200
 rtp payload-type comfort-noise 13
 session protocol sipv2
 incoming uri to 290
 voice-class codec 1
 voice-class stun-usage 1
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
!
sip-ua
 no remote-party-id
 retry invite 2
 transport tcp tls v1.2
 crypto signaling default trustpoint sbc
 handle-replaces
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
```

```
line vty 0 4
 exec-timeout 60 0
 login
 transport preferred ssh
 transport input ssh
!
ntp server 192.0.2.1
!
end
```

Microsoft Phone System Direct Routing configuration

Create Users in Microsoft 365

The following steps illustrate how to create a user in the Microsoft 365 portal

Login into http://portal.office.com/ using your Microsoft 365 tenant administrator credentials

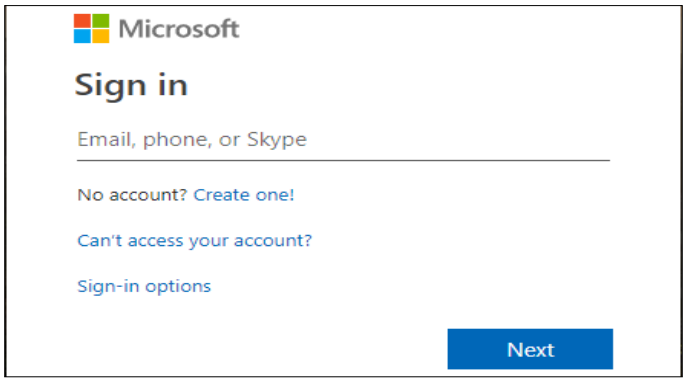


Figure 2 Office 365 Portal login

Select the Admin Icon in Office 365 to login Microsoft 365 Admin Center.

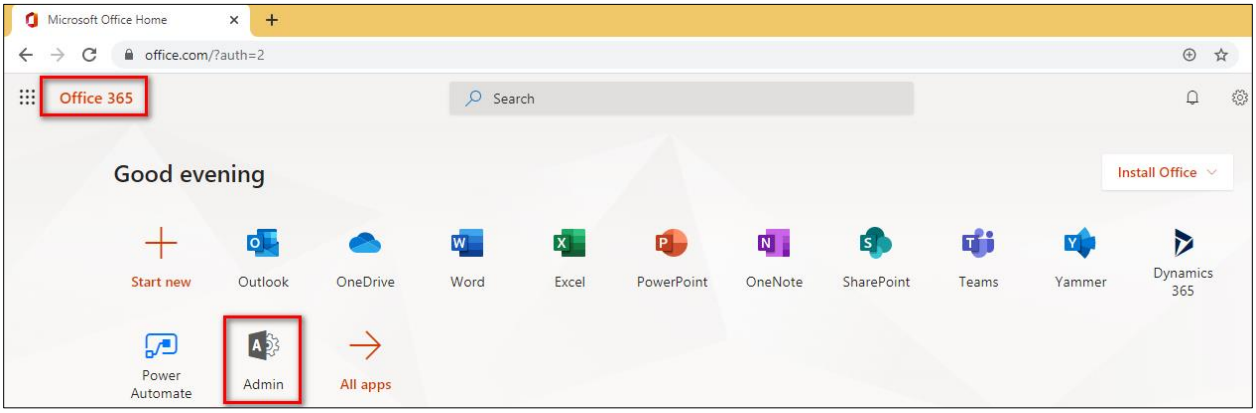


Figure 3 Navigating to Microsoft 365 Admin Center

Select “Add a user” from the Microsoft 365 Admin Center as shown below

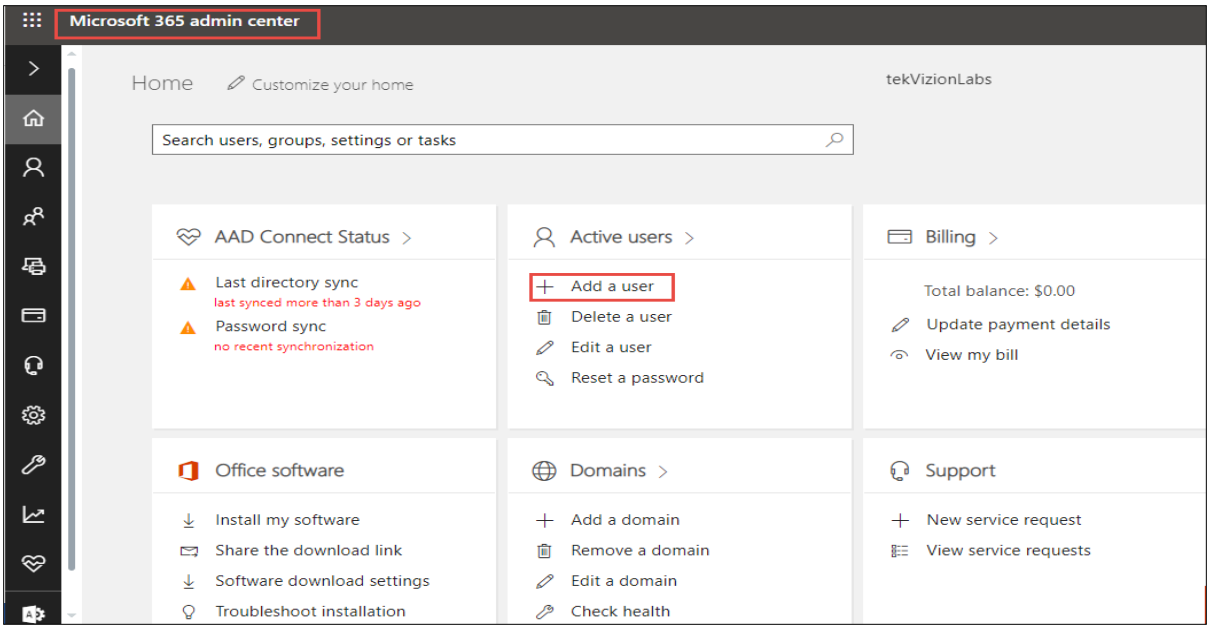


Figure 4 Microsoft 365 Admin Center

Enter the user details, password and assign required license to the users then Click Add

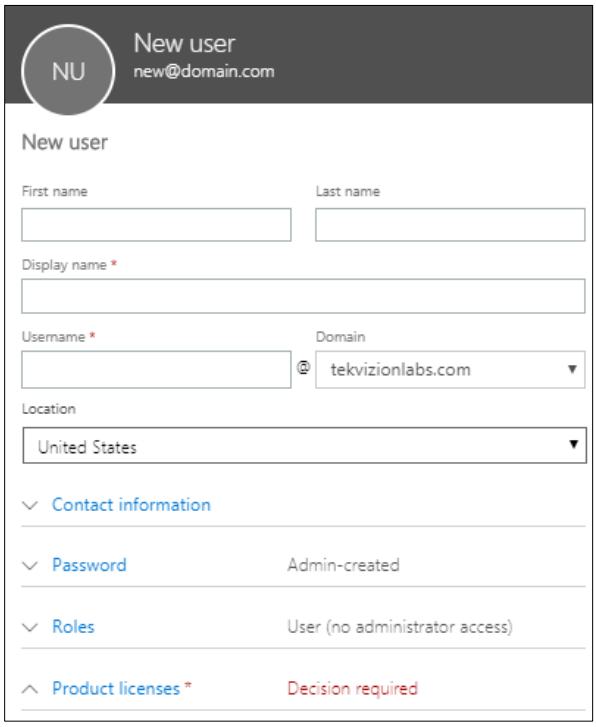


Figure 5 Teams user creation

Select the Admin icon from the Microsoft 365 Admin center home page and navigate to Microsoft Teams admin center as shown below

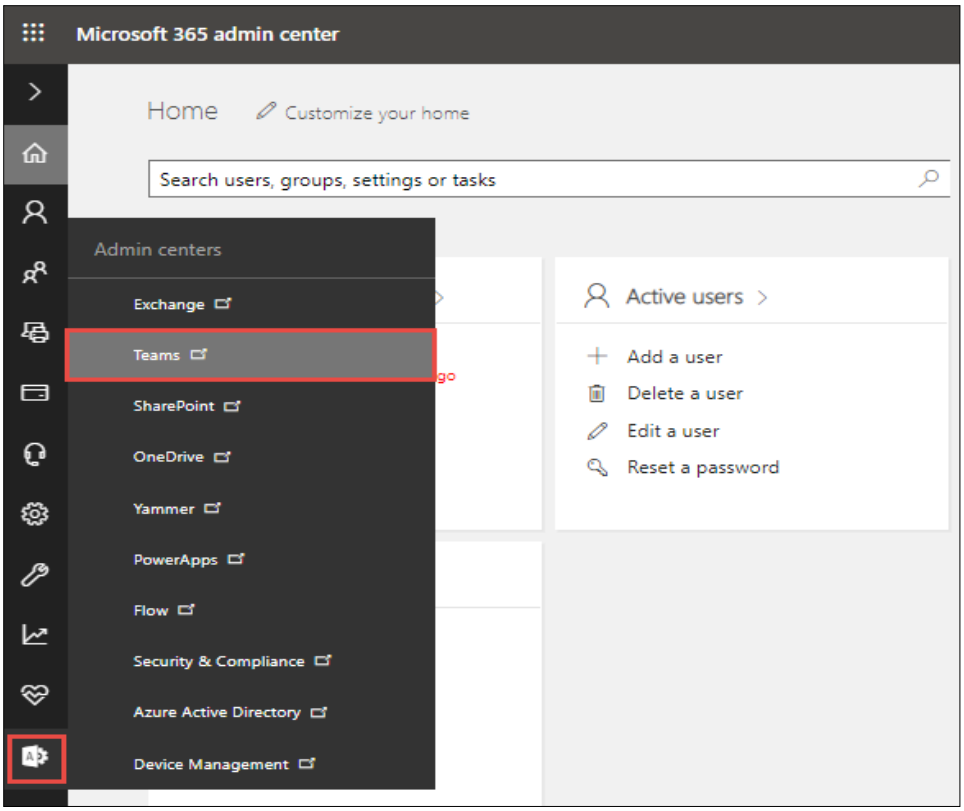


Figure 6 Microsoft 365 Admin Center to Teams Admin Center

Select Users from the Microsoft Teams Admin Center to view the list of available users

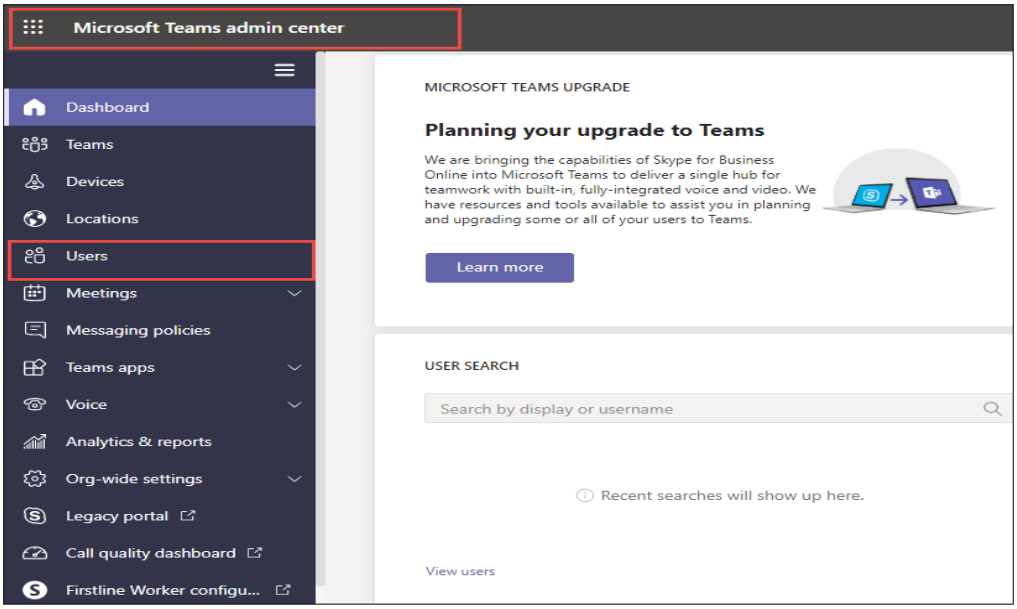


Figure 7 Users in Microsoft Teams Admin Center

Search for the user created and click on the user display name to view user properties as shown below

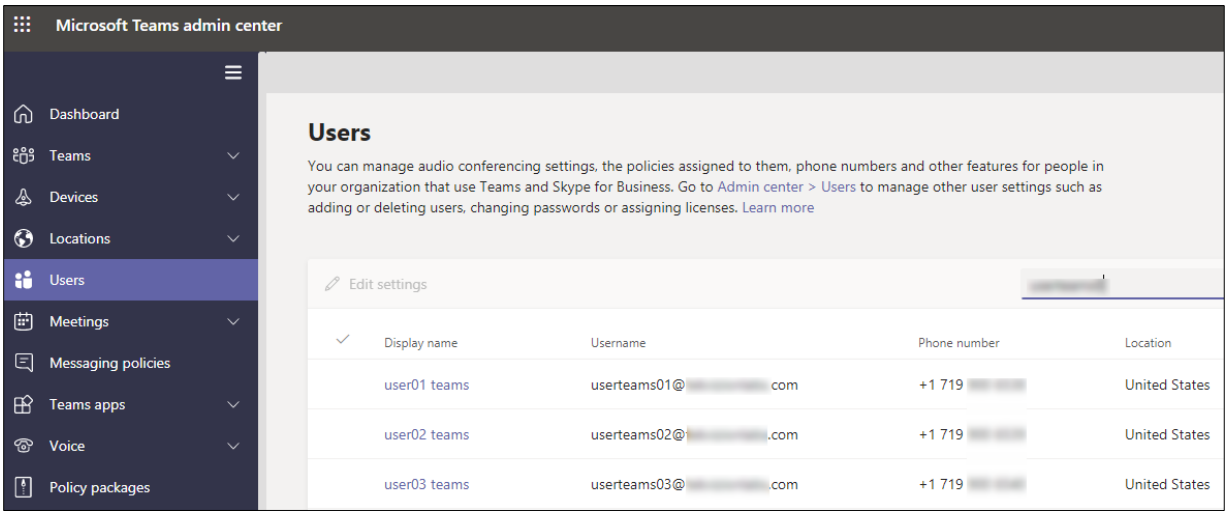


Figure 8 Users in Microsoft Teams Admin Center-cont.,

Under user properties, navigate to Accounts and set the Teams upgrade mode to Teams only

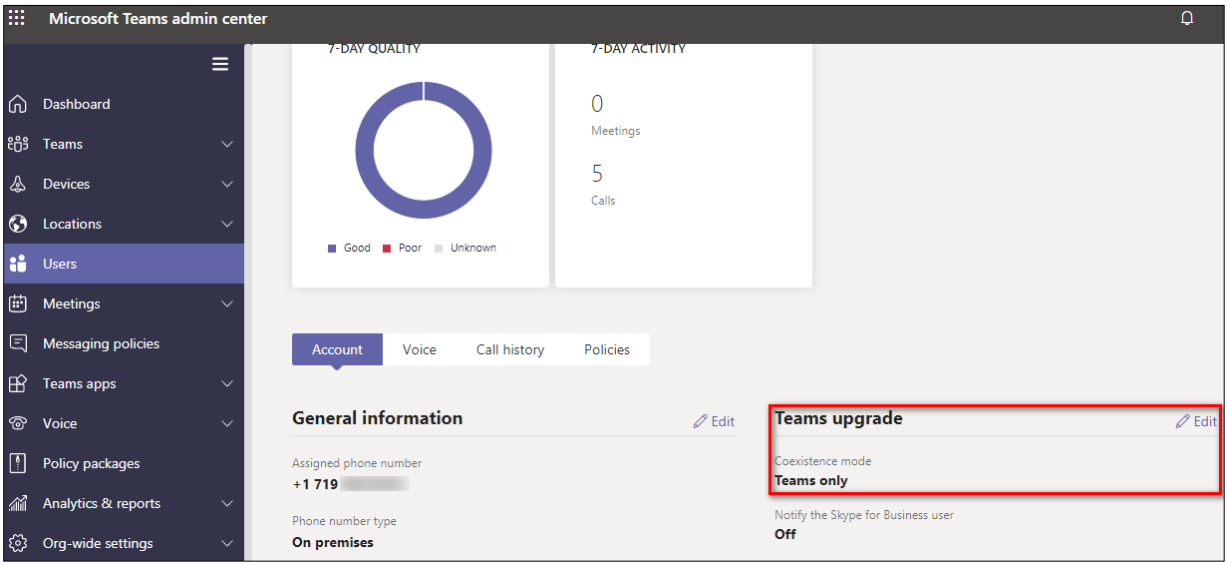


Figure 9 Upgrade Users to Teams only mode

Under user properties, navigate to Policies and set the Calling Policy as shown below. Here in the below example custom policy “Busy on Busy enabled” is assigned to user. Procedure to create custom policy is shown in the next section

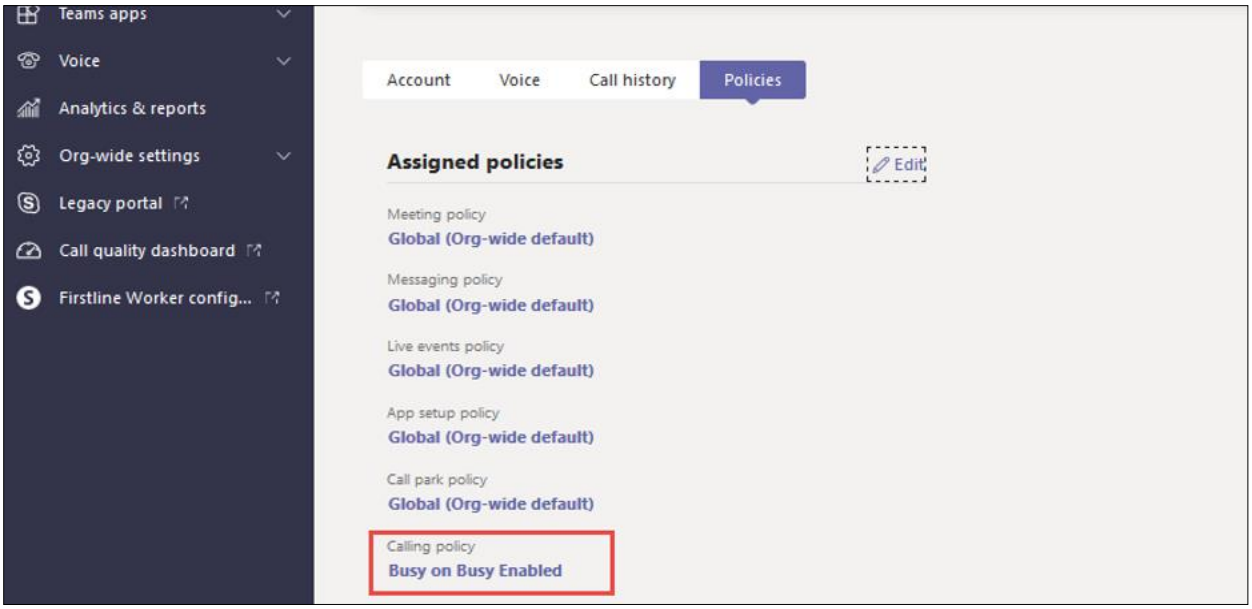


Figure 10 Assigning Calling Policies to Teams User

Under user properties, navigate to Policies and set the Caller ID Policy as shown below. In this example, caller ID policy "Anonymoustest" is assigned to user. The procedure to create a custom policy is shown in the next section

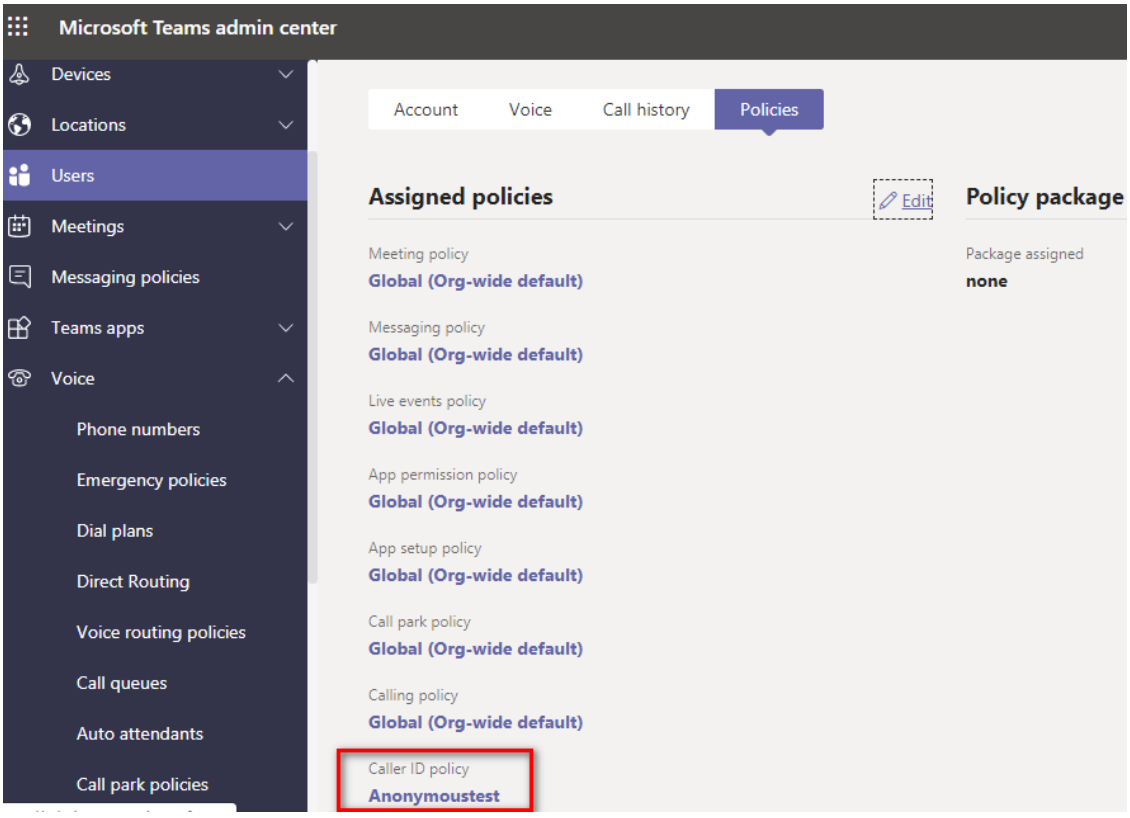


Figure 11 Assigning Caller ID policy to Teams User

Configure Calling policy in Microsoft Teams Admin Center.

To configure a custom policy, navigate to Microsoft Teams admin center > Voice > Calling Policies > New policy.

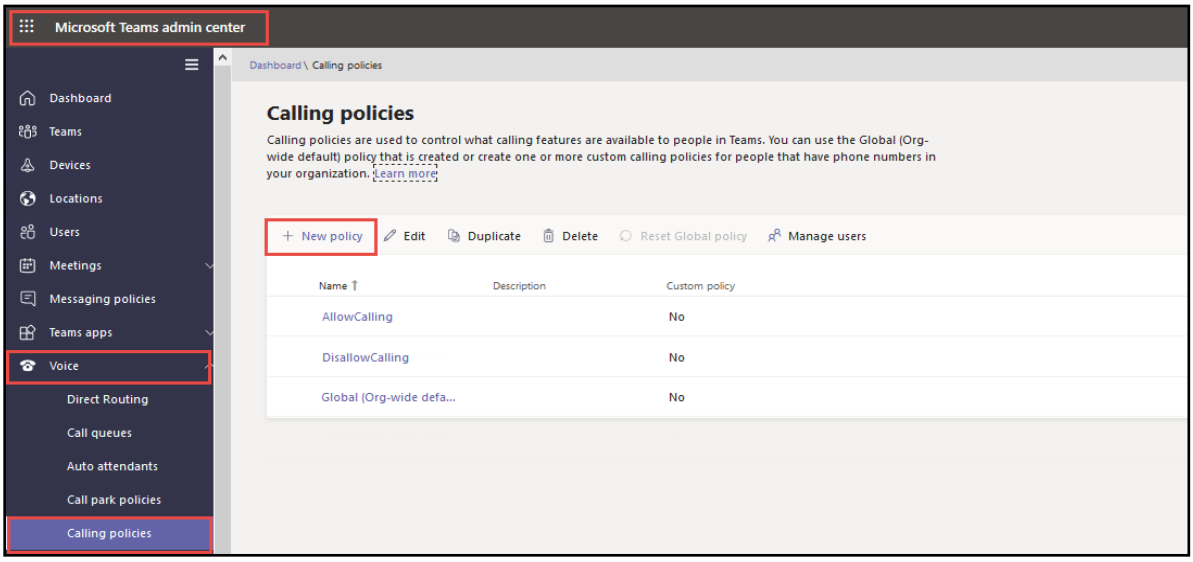


Figure 12 Calling Policies configuration

Create calling policy to turn on Busy on Busy. Click save to complete the configuration

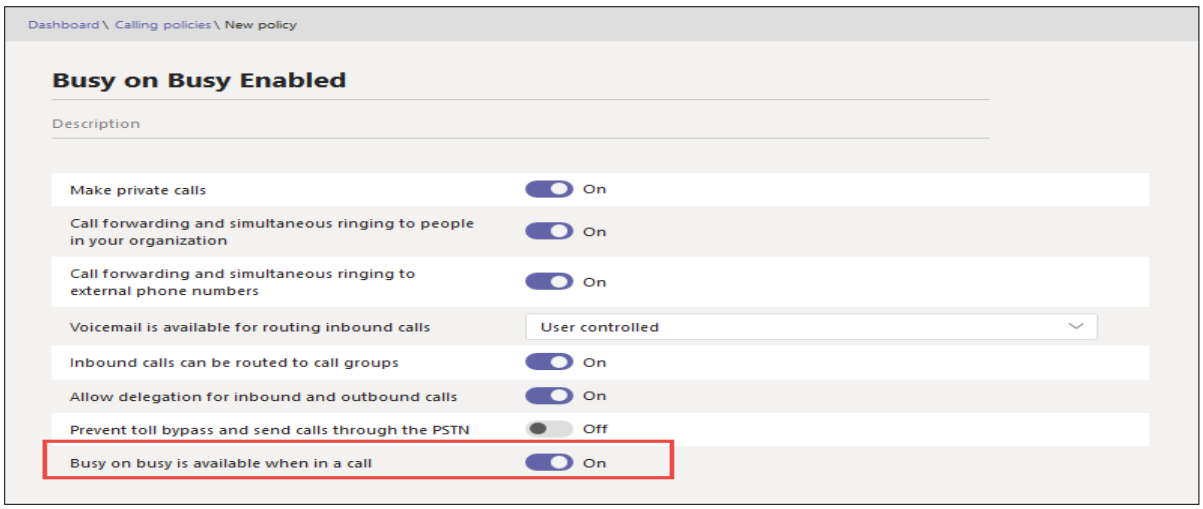


Figure 13 Enable Busy on Busy in Calling Policy

Configure Caller ID policy in Microsoft Teams Admin Center.

To configure a Caller ID policy, navigate to Microsoft Teams admin center > Voice > Caller ID Policies > Add

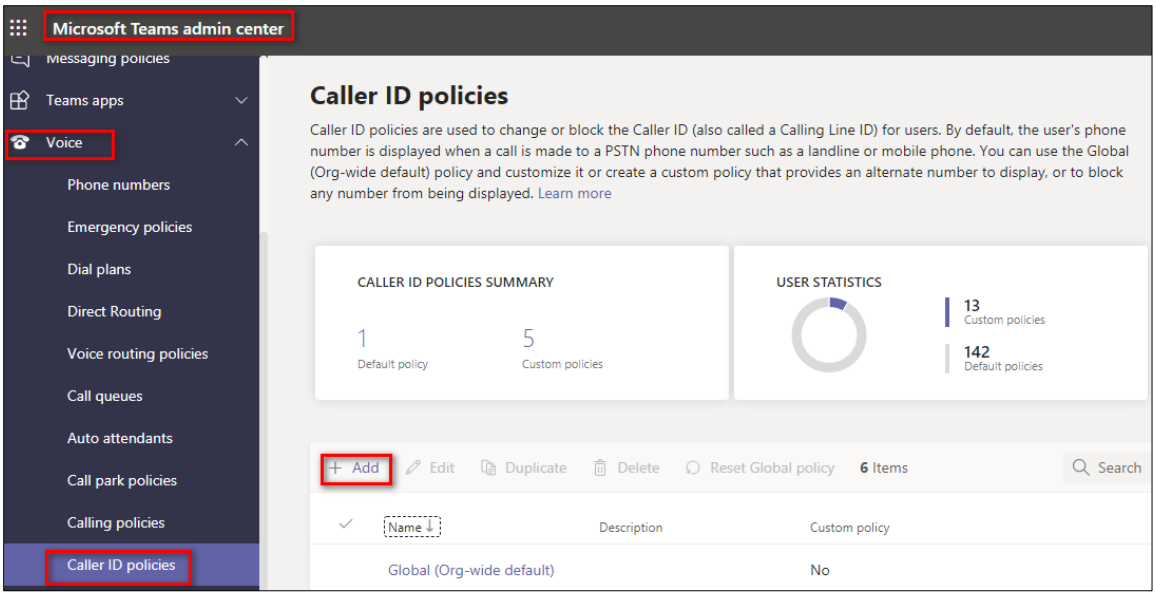


Figure 14 Caller ID Policies Configuration

Enter the caller ID policy Name and select the “Replace the Caller ID with Anonymous”. Click save to complete the configuration

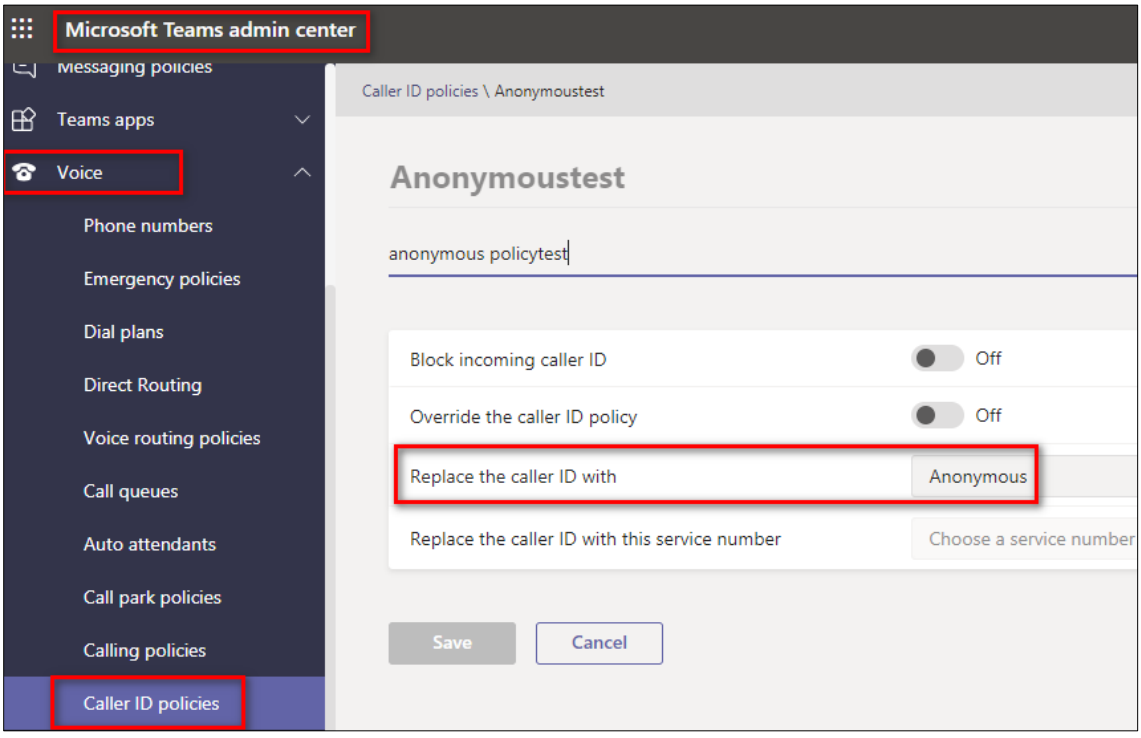


Figure 15 Select Anonymous for the Replace caller ID with

Configure User parameters using PowerShell.

Open Windows PowerShell installed with Azure Active Directory modules and connect to Microsoft 365 Tenant.

Note: The following actions may also be completed using Microsoft Teams admin center.

Use the following commands to set DID and enable Enterprise Voice, Hosted Voicemail and LineURI for Teams users.

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

Example:

```
Set-CsUser -Identity "user1@example.com" -EnterpriseVoiceEnabled $true -
HostedVoiceMail $true
-OnPremLineURI tel:12223331234
```

Create an Online PSTN Gateway

Using your administrator account, connect to the remote PowerShell of your Microsoft 365 tenant

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

After creating an Online PSTN Gateway use “Get-CsOnlinePstnGateway” command to view the online PSTN gateway details. Gateway Identity must be a valid FQDN for the Microsoft 365 tenant to reach CUBE.

For example:

```
New-CsOnlinePSTNGateway -Fqdn sbc.example.com -SipSignallingPort 5061
-ForwardCallHistory $False -ForwardPai $true -MaxConcurrentSessions 100 -Enabled
$true
```

Use the following command to view the settings for the new SBC.

```
PS C:\WINDOWS\system32> Get-CsOnlinePSTNGateway sbc.example.com
Identity                            : sbc.example.com
InboundTeamsNumberTranslationRules  : {}
InboundPstnNumberTranslationRules   : {}
OutboundTeamsNumberTranslationRules : {}
OutboundPstnNumberTranslationRules  : {}
Fqdn                                : sbc.example.com
SipSignalingPort                    : 5061
FailoverTimeSeconds                 : 10
ForwardCallHistory                  : False
ForwardPai                          : True
SendSipOptions                      : True
MaxConcurrentSessions               : 100
```

```
Enabled                             : True
MediaBypass                         : True
GatewaySiteId                       :
GatewaySiteLbrEnabled               : False
GatewayLbrEnabledUserOverride       : False
FailoverResponseCodes               : 408,503,504
GenerateRingingWhileLocatingUser    : True
PidfLoSupported                     : False
MediaRelayRoutingLocationOverride   :
ProxySbc                            :
BypassMode                          : None
```

Configure Online PSTN usage

Use the following command to add a new PSTN usage policy.

```
Set-CsOnlinePstnUsage -identity Global -Usage @{Add="<usage name>"}
```

For example:

```
Set-CsOnlinePstnUsage -identity Global -Usage @{Add="Unrestricted"}
```

The following command may be used to view the policy.

```
PS C:\WINDOWS\system32> Get-CsOnlinePstnUsage
Identity : Global
Usage    : {PSTN usage record Unrestricted}
```

Configure Voice Route

Use the following command to add a new Voice Route and associate it with an SBC and usage policy.

```
New-CsOnlineVoiceRoute -Identity "<Route name>" -NumberPattern ".*"
OnlinePstnGatewayList "<SBC FQDN>" -Priority 1 -OnlinePstnUsages "<PSTN usage name>"
```

For example:

```
New-CsOnlineVoiceRoute -Identity "USA" -NumberPattern "\+1.*" OnlinePstnGatewayList
"sbc.example.com" -Priority 1 -OnlinePstnUsages "Unrestricted"
```

After creating online voice route use the following command to view the online voice route details. Here we can see the association of PSTN usage with the PSTN gateway. Example is shown below

```
PS C:\WINDOWS\system32> Get-CsOnlineVoiceRoute -Identity USA
Identity              : USA
Priority              : 1
Description           :
NumberPattern         : \+1.*
OnlinePstnUsages      : {Unrestricted}
OnlinePstnGatewayList : {sbc1.cube-tme.com}
Name                  : USA
```

Configure Online Voice Routing Policy

Create a new online Voice Routing Policy using the following command

```
New-CsOnlineVoiceRoutingPolicy "<policy name>" -OnlinePstnUsages "<pstn usage name>"
```

For Example:

```
New-CsOnlineVoiceRoutingPolicy "VRPolicy" -OnlinePstnUsages "Unrestricted"
```

After creating a Voice Routing Policy use the following command to view its properties.

```
PS C:\WINDOWS\system32> Get-CsOnlineVoiceRoutingPolicy -Identity VRPolicy
Identity          : Tag:VRPolicy
OnlinePstnUsages  : {Unrestricted}
Description       :
RouteType         : BYOT
```

Associate Teams users with a voice routing policy using the following command.

```
Grant-CsOnlineVoiceRoutingPolicy -Identity "<User name>" -PolicyName "<policy name>"
```

For example:

```
Grant-CsOnlineVoiceRoutingPolicy -Identity "<User name>" -PolicyName "<policy name>"
```

Calling Line Identity Policy

Add a Calling Line Identity Policy which is used to present\restrict users Caller ID.

New-CsCallingLineIdentity -Identity anonymous_policy -Description "clid restricted" -CallingIDSubstitute Anonymoustest -EnableUserOverride $true

Use the command **Get-CsCallingLineIdentity** to view the Calling Line Identity policy created.

```
PS C:\Users\spandian> Get-CsCallingLineIdentity -Identity anonymoustest


Identity              : Tag:Anonymoustest
Description           : anonymous policytest
EnableUserOverride    : False
ServiceNumber         :
CallingIDSubstitute   : Anonymous
BlockIncomingPstnCallerID : False
```

Figure 16: Anonymous Test

Associate the newly created policy to the users using the following command.

Grant-CsCallingLineIdentity -Identity "<User name>" -PolicyName anonymoustest

User associated with the policy gets an additional Option as “Caller ID” in their Teams Client.

Navigate to Settings -> Calls -> Caller ID in users Teams client, Check “**Hide my phone number and profile information”** to restrict caller ID.

Appendix A – Configuring CUBE High Availability for Microsoft Phone System

This section details the aspects of CUBE High Availability (active/standby CUBEs for stateful failover of active calls) configuration that is required to enable interworking with Microsoft Phone System.

Note: Further in this section, CUBE HA will refer to CUBE High Availability (HA) Layer 2 Box-to-box (B2B) redundancy for stateful call preservation.

Network Topology

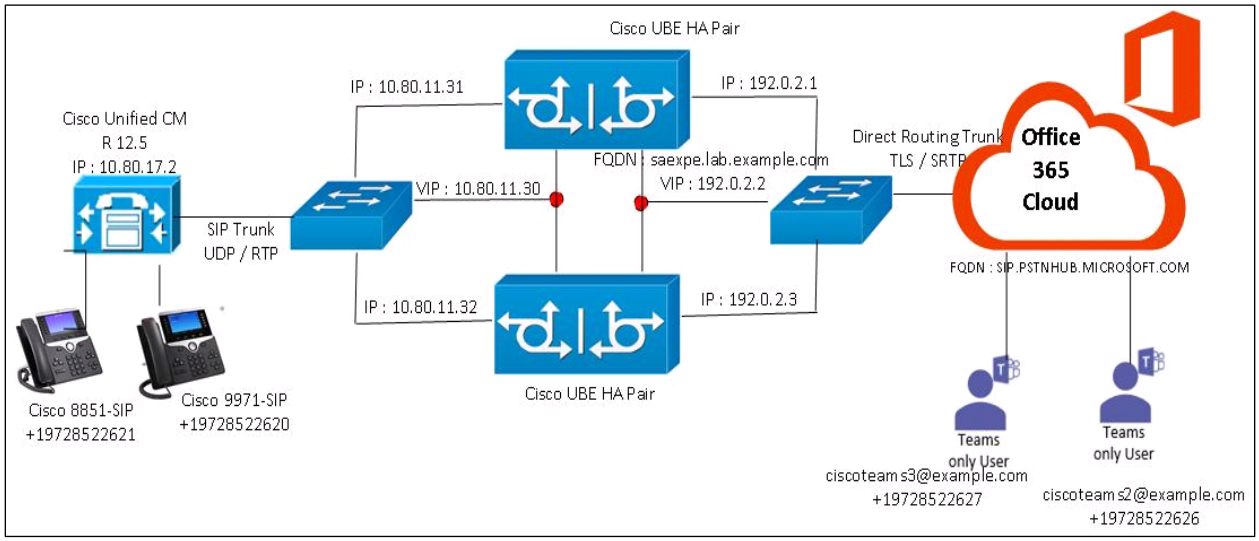


Figure 177 CUBE-HA Network Topology

- The network topology includes the Microsoft Phone System, Teams client, CUBE HA and CUCM. Microsoft 365 admin center is used to configure a gateway trunk associated with CUBE's public FQDN. CUCM 12.5.1 connects to CUBE HA using its LAN IP Address.

Direct Routing for Microsoft Phone System and CUBE HA Settings:

Setting	Value
Transport from CUBE HA to MS Phone System	TLS with SRTP
Transport from CUBE to CUCM	UDP with RTP

IP Networking

Note: CUBE HA IP addresses used in this guide are fictional and provided for illustration purposes only.

```
interface GigabitEthernet0/0/2
 description LAN/CUCM INTERFACE
 ip address 10.80.11.31 255.255.0.0
 negotiation auto
 redundancy rii 16
 redundancy group 1 ip 10.80.11.30 exclusive
!
interface GigabitEthernet0/0/3
 description WAN/Microsoft facing INTERFACE
 ip address 192.0.2.1 255.255.255.224
 negotiation auto
 redundancy rii 15
 redundancy group 1 ip 192.0.2.2 exclusive
```

Explanation

Command	**Description**
redundancy rii id	Redundant interface identifier to generate virtual MAC Same **rii id** to be used in CUBEs that has same virtual
redundancy group 1 ip x.x.x.x exclusive	Enable Redundancy group in physical interface with virtual IP towards Teams

Wildcard Certificate

This section displays the validated wildcard-based certificate option, which can be used for a CUBE-HA pair

Generate RSA key

```
crypto key generate rsa general-keys exportable label wildcard
The name for the keys will be: wildcard
Choose the size of the key modulus in the range of 512 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [1024]: 2048
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 0 seconds)
```

Create SBC Trustpoint

```
crypto pki trustpoint wildcard
 enrollment terminal
 subject-name cn=*.example.com
 rsakeypair wildcard
 revocation-check crl
 exit
```

Generate Certificate Signing Request (CSR)

```
crypto pki enroll wildcard
% Start certificate enrollment..

% Start certificate enrollment ..
% The subject name in the certificate will include: cn=*.example.com
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
```

Use this CSR to request a certificate from one of the supported Certificate authorities.

Import signed wildcard Certificate in CUBE

Enter the following command and then paste the CA and the device certificate into the trustpoint. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted:

```
crypto pki authenticate wildcard
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself



crypto pki import wildcard certificate
% The fully-qualified domain name will not be included in the certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
```

Exporting RSA key and certificate from CUBE 1

```
crypto pki export wildcard pkcs12 ftp://<username>:<password>@<x.x.x.x>/wildcard.pfx
password *******
Address or name of remote host [x.x.x.x]?
Destination filename [wildcard]?
Writing /wildcard Writing pkcs12 file to ftp://<username>@<x.x.x.x>/wildcard.pfx
!
CRYPTO_PKI: Exported PKCS12 file successfully.
```

Copy RSA key and certificate in CUBE 2

```
copy ftp://<username>:<password>@<x.x.x.x>/wildcard.pfx flash:
Destination filename [wildcard]?
Accessing ftp://*:*@<x.x.x.x>/wildcard.pfx...!
[OK - 4931/4096 bytes]

4931 bytes copied in 4.644 secs (1062 bytes/sec)
```

Import RSA key and certificate in CUBE 2

Using the below command, import the certificate to CUBE. This will automatically create the trustpoint “wildcard”

```
crypto pki import wildcard pkcs12 flash:wildcard.pfx password *******
% Importing pkcs12...
Source filename [wildcard.pfx]?
Reading file from bootflash:wildcard.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
```

Validation

Show crypto pki certificates can be used to display information about the certificate and the certificate of the CA.

CUBE 1:

```
MSTeams1#sh crypto pki certificates wildcard
Certificate
  Status: Available
  Certificate Serial Number (hex): 00D868B5A81343A259
  Certificate Usage: General Purpose
  Issuer:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    Name: *.example.com
    cn=*.example.com
    ou=Domain Control Validated
  CRL Distribution Points:
    http://crl.godaddy.com/gdig2s1-2592.crl
  Validity Date:
    start date: 22:36:28 UTC Jan 6 2021
    end   date: 22:36:28 UTC Jan 6 2022
  Associated Trustpoints: wildcard
  Storage: nvram:GoDaddySecur#A259.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 07
  Certificate Usage: Signature
  Issuer:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    cn=Go Daddy Secure Certificate Authority - G2
```

```
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  CRL Distribution Points:
    http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints: wildcard
  Storage: nvram:GoDaddyRootC#7CA.cer
```

CUBE 2

```
MSTeams2#sh crypto pki certificates wildcard
Certificate
  Status: Available
  Certificate Serial Number (hex): 00D868B5A81343A259
  Certificate Usage: General Purpose
  Issuer:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    Name: *.example.com
    cn=*.example.com
    ou=Domain Control Validated
  CRL Distribution Points:
    http://crl.godaddy.com/gdig2s1-2592.crl
  Validity Date:
    start date: 22:36:28 UTC Jan 6 2021
    end   date: 22:36:28 UTC Jan 6 2022
  Associated Trustpoints: wildcard
  Storage: nvram:GoDaddySecur#A259.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 07
```

```
  Certificate Usage: Signature
  Issuer:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  CRL Distribution Points:
    http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints: wildcard
  Storage: nvram:GoDaddyRootC#7CA.cer
```

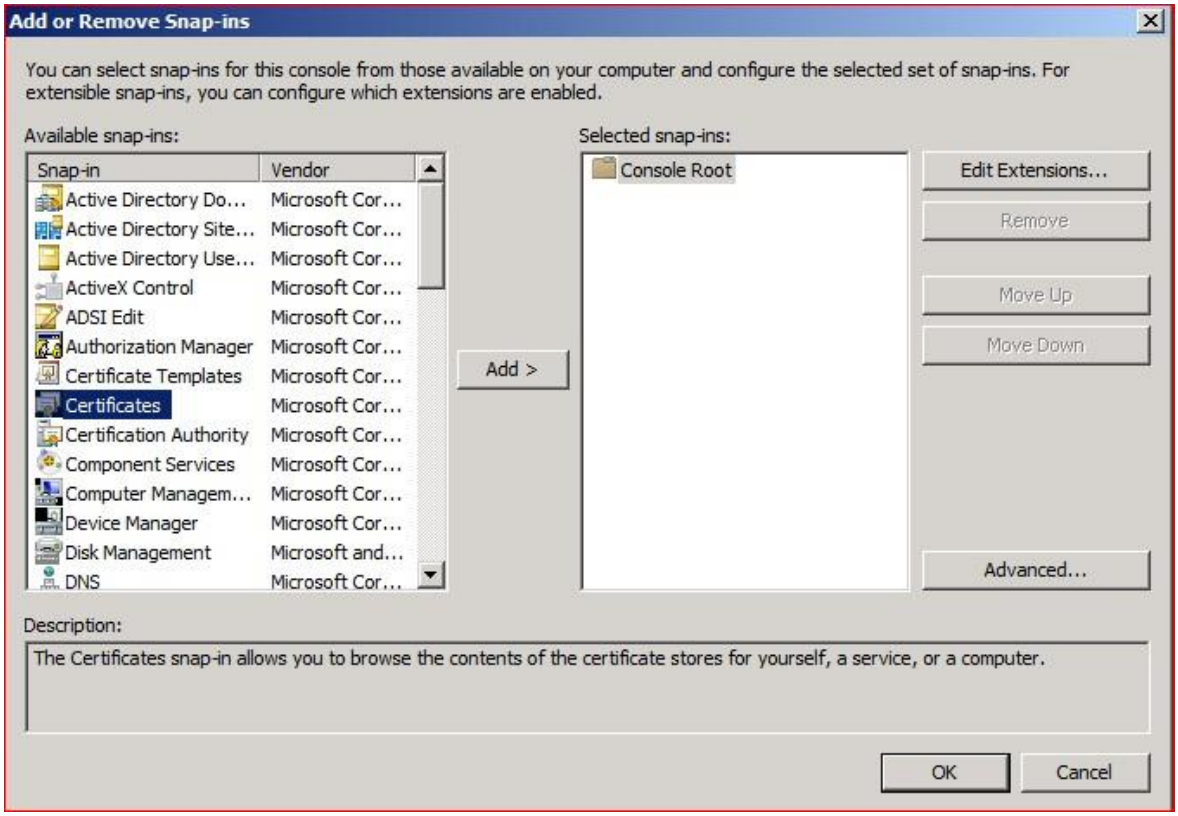
Hostname Certificate

This section displays the validated hostname-based certificate as an alternate option.

Generate External Server Certificate Signing Request

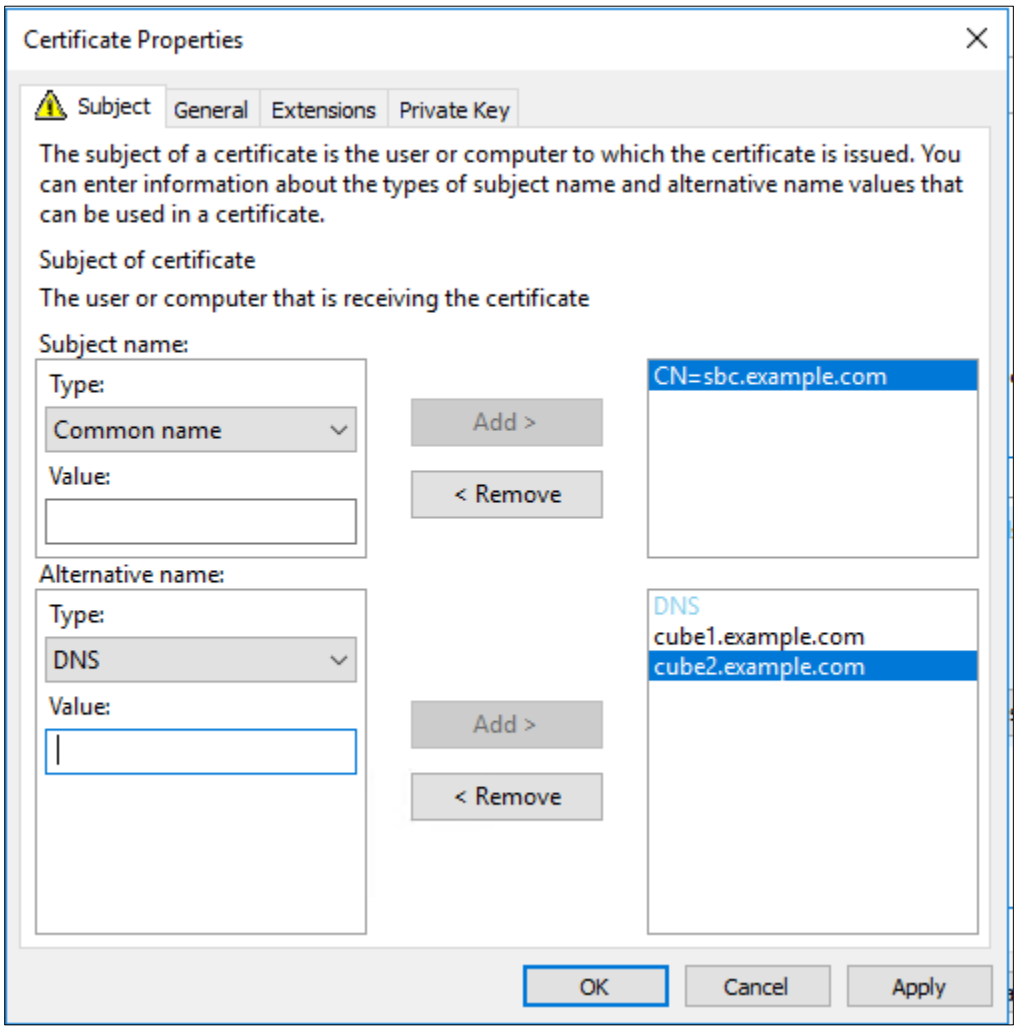
The Certificate Signing Request (CSR) is created by the SBC admin to represent an external server requesting a digital certificate. The process below outlines how a CSR is generated.

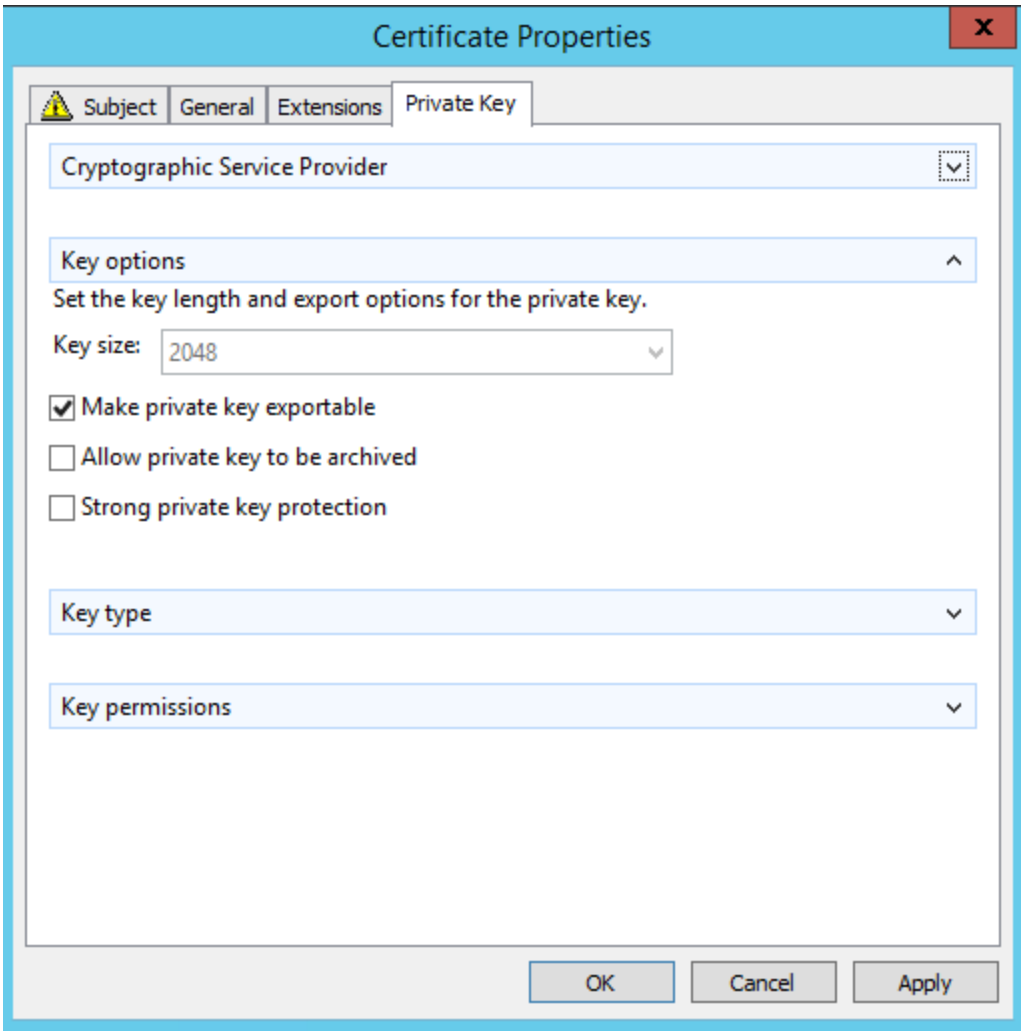
- Access the domain controller server and invoke the Microsoft Management Console (mmc) by typing “mmc” from the CA’s Start menu > “Search programs and files” window.
- “File” > “Add/Remove snap-in …” and move the “Certificates” available snap-in to the “Selected snap-ins” window by highlighting “Certificates” and clicking the “Add>” button.



- When added, the Certificates snap-in widow will appear. Select “Computer account” here.
- On the “Select Computer” window, select “Local computer:” and click “Finish” and then “OK” on the “Add or Remove Snap-ins” window.
- In the mmc “Console” window’s menu tree, expand “Certificates” and right-click on “Personal”. Select “All Tasks” > “Advanced Operations” > “Create Custom Request”.
- Hit “Next” in the Certificate Enrollment window and with “Active Directory Enrollment Policy” highlighted in the “Select Certificate Enrollment Policy” window, hit “Next”.
- In the “Certificate Enrollment” window’s “Template” pull-down menu, select “Web Server”. Ensure PKCS #10 is selected and hit the “Next” button.

- Under ‘Certificate information”, click on the “Details” double downward arrow icon on the right side of the window. Click on the “Properties” button.
- Certificate Properties window:
    - Subject Tab:
        - In the “Subject name” area, choose “Common name” from the “Type:” pull-down menu. In the “Value:” field, supply the FQDN of the server on whose behalf you are requesting a certificate. Then hit the “Add>” button. Click the “Apply” button.
        - In the “Alternate name” area, choose “Common name” from the “Type:” pull-down menu. In the “Value:” field, supply the FQDN of the server on whose behalf you are requesting a certificate. Then hit the “Add>” button. Click the “Apply” button.
    - General Tab: provide a friendly name.
    - Private Key Tab: hit the “Key options” double downward arrow icon and check the “Make private key exportable” box. Hit the “OK” button.





- Hit the “Next” button.
- Ensure the file format is “Base 64” and then hit the “Browse” button to provide the file name and path of where the offline CSR request will be saved. Be sure to add the .req filename extension in the “File name” window. Hit the “Save” button.

In the “Certificate Enrollment” window, select “Finish” to complete the CSR save process.

Import signed certificate

The CSR created in the above step should be used to get the certificate signed from a Microsoft approved Certificate Authority.

The public certificate imported to CUBE should be in .pfx format (certificate + private key).

Using the below command, import the certificate to CUBE. This will automatically create the trustpoint "saexpe"

```
crypto pki import saexpe pkcs12 tftp: password ********
% importing pkcs12...
Address or name of remote host []? X.x.x.x
Source filename [saexpe]? saexpe_new.pfx
Reading file from tftp://x.x.x.x/saexpe_new.pfx
Loading saexpe_new.pfx from x.x.x.x (via GigabitEthernet0/0/0): !
[OK - 5953 bytes]
% The CA cert is not self-signed.
% Do you also want to create trustpoints for CAs higher in
% the hierarchy? [Yes/no]: yes
CRYPTO_PKI: Imported PKCS12 file successfully.
```

Create SBC Trustpoint

```
crypto pki trustpoint saexpe
 enrollment terminal
 fqdn sbc.example.com
 subject-name cn=sbc.example.com
 subject-alt-name sbc.example.com
 revocation-check crl
 rsakeypair sbc
```

Validation

Show crypto pki certificates can be used to display information about the certificate and the certificate of the CA

Active CUBE output

```
MSTeams1#show crypto pki certificates saexpe
Certificate
  Status: Available
  Certificate Serial Number (hex): 009AAAAFC3E2FB1C35
  Certificate Usage: General Purpose
  Issuer:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
```

```
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    Name: sbc.example.com
    cn=sbc.example.com
    ou=Domain Control Validated
  CRL Distribution Points:
    http://crl.godaddy.com/gdig2s1-2214.crl
  Validity Date:
    start date: 13:36:19 UTC Aug 14 2020
    end   date: 22:33:00 UTC Oct 13 2021
  Associated Trustpoints: saexpe
  Storage: nvram:GoDaddySecur#1C35.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 07
  Certificate Usage: Signature
  Issuer:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  CRL Distribution Points:
    http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints: saexpe
  Storage: nvram:GoDaddyRootC#7CA.cer
```

Standby CUBE output

```
MSTeams2#show crypto pki certificates saexpe
Certificate
  Status: Available
  Certificate Serial Number (hex): 009AAAAFC3E2FB1C35
  Certificate Usage: General Purpose
  Issuer:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    Name: sbc.example.com
    cn=sbc.example.com
    ou=Domain Control Validated
  CRL Distribution Points:
    http://crl.godaddy.com/gdig2s1-2214.crl
  Validity Date:
    start date: 13:36:19 UTC Aug 14 2020
    end   date: 22:33:00 UTC Oct 13 2021
  Associated Trustpoints: saexpe
  Storage: nvram:GoDaddySecur#1C35.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 07
  Certificate Usage: Signature
  Issuer:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com
     Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com
     Inc.
    l=Scottsdale
```

```
    st=Arizona
    c=US
  CRL Distribution Points:
    http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints: saexpe
  Storage: nvram:GoDaddyRootC#7CA.cer
```

Global CUBE HA settings

To enable CUBE HA with settings required to interwork with Microsoft Phone System and Cisco UCM, the following additional commands must be entered:

```
voice service voip
 redundancy-group 1
```

Explanation

Command	Description
redundancy-group 1	Enable redundancy group globally

Configure Redundancy group

```
redundancy
 mode none
 application redundancy
  group 1
   priority 150 failover threshold 75
   timers delay 30 reload 60
   control GigabitEthernet0/0/0 protocol 1
   data GigabitEthernet0/0/0
```

Explanation

Command	Description
priority 150 failover threshold 75	Set priority weightage for CUBE 1 and CUBE 2. High priority CUBE turns Active and other StandBy
timers delay 30 reload 60	the amount of time to delay RG group's initialization and role negotiation after the interface comes up and reload
control GigabitEthernet0/0/0 protocol 1	interface used to exchange keepalive
data GigabitEthernet0/0/0	interface used for checkpointing of data traffic

Configure interface tracking for redundancy

```
track 1 interface GigabitEthernet0/0/2 line-protocol
track 2 interface GigabitEthernet0/0/3 line-protocol
!
redundancy
 mode none
 application redundancy
  group 1
   track 1 shutdown
   track 2 shutdown
```

Explanation

Command	Description
track 1 interface GigabitEthernet0/0/2 line-protocol	Allow to track the voice traffic interface state
track 2 interface GigabitEthernet0/0/3 line-protocol	Allow to track the voice traffic interface state
track 1 shutdown	Allow Active CUBE to initiate switchover after the traffic interface is down
track 2 shutdown	Allow Active CUBE to initiate switchover after the traffic interface is down

CUBE HA Validation commands

RG Infra Protocol

Show redundancy application group can be used to verify RG Infra protocol and CUBE HA status on the platform. Key output has been **highlighted**.

Active CUBE

```
MSTeams1#show redundancy application group all
Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:          0
                        Total # of down/up state changes due to faults: 2

RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.64.3.229, priority 150, intf Gi0/0/0
        Log counters:
                role change to active: 1
                role change to standby: 7
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 1, down 2, admin_down 1
                reload events: local request 0, peer request 6

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/0/0
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 319720, Bytes 19822640, HA Seq 0, Seq Number 319720, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
```

```
                Reload Peer: TX 8, RX 6
                Resign: TX 0, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 302651, Bytes 10290134, HA Seq 0, Seq Number 302659, Pkt Loss 0


Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT
```

Standby CUBE

```
MSTeams2#show redundancy application group all
Faults states Group 1 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           0
                        Total # of down/up state changes due to faults: 2

RG Protocol RG 1
------------------
        Role: Standby
        Negotiation: Enabled
        Priority: 150
        Protocol state: Standby-hot
        Ctrl Intf(s) state: Up
        Active Peer: address 10.64.3.228, priority 200, intf Gi0/0/0
        Standby Peer: Local
        Log counters:
                role change to active: 0
                role change to standby: 1
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 1, down 2, admin_down 1
                reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/0/0
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 302691, Bytes 18766842, HA Seq 0, Seq Number 302691, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 0, RX 0
        Active Peer: Present. Hold Timer: 10000
                Pkts 302683, Bytes 10291222, HA Seq 0, Seq Number 319753, Pkt Loss 0
```

```
Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
         RF state: STANDBY HOT
         Peer RF state: ACTIVE
```

show voice high-availability summary

Active CUBE

```
MSTeams1#show voice high-availability summary
========= HA CREATE|MODIFY Message Sizes =======
SCCPAPP Data Size:  448
SIPSPI  Data Size: 1144
H323SPI Data Size: 2212
RTPSPI  Data Size:  956
CCAPI   Data Size:  264
VOIPRTP Data Size:  372
DSP_MSP Data Size:   32
HA      Data Size:  100
  TOTAL DATA SIZE: 3396

========= HA APP_DATA Message Sizes =======
CCAPI_SYS     Data Size:    8
VOIP_STUN     Data Size:    8
SCCAPP_SYS    Data Size:   44
VOICE_RSC_VOL Data Size:  124
DCUBE_MBE     Data Size: 1040
    TOTAL SYS DATA SIZE:  512

======== Voice HA DB INFO ========
Number of call legs in HA DB: 0 (MAX:15360)
Number of call legs in HA sync pending DB: 0

----------------------------
First few entries in HA DB:
----------------------------

---------------------------------------
First few entries in Sync Pending DB:
---------------------------------------

---------------------------

======== Voice HA Process INFO ========
Redundancy is configured under 'voice service voip'

ACTIVE - process current tick:48805783,  index: 23
ACTIVE - process number of tick events pending: 0
ACTIVE - process number of tick events processed: 0
```

```
Breakdown per tick (TOTAL TICKS:128, 20ms/TICK, MAX EV/TICK:16)
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0
======== Voice HA RF INFO ========
FUNCTIONING RF DOMAIN: 0x2

-----
RF Domain: 0x0
Voice HA Client Name: VOIP RF CLIENT
Voice HA RF Client ID: 1345
Voice HA RF Client SEQ: 133
My current RF state ACTIVE (13)
Peer current RF state DISABLED (1)

Current VOIP HA state [LOCAL / PEER] :
        [ACTIVE (13) / DISABLED (1)]

VOIP HA RF CB Data:
        ENABLED:1
        flags: 0x6 [PEER_COMM_DOWN/PEER_PRESENCE_DOWN/IN-BOX HA]
        red_mode: 0

-----
RF Domain: 0x2 [RG: 1]
Voice HA Client Name: VOIP RG CLIENT
Voice HA RF Client ID: 4054
Voice HA RF Client SEQ: 481
My current RF state ACTIVE (13)
Peer current RF state STANDBY HOT (8)

Current VOIP HA state [LOCAL / PEER] :
        [ACTIVE (13) / STANDBY HOT (8)]

VOIP HA RF CB Data:
        ENABLED:1
        flags: 0x1 [PEER_COMM_UP/PEER_PRESENCE_UP/B2BHA]
        red_mode: 0
        rg_flags: 0x0
                ctrl [UP/NO SHUT]
```

```
                data [UP/NO SHUT]
                traffic (TOT:2; SH:0, DN:0) [UP/NO SHUT]

-----
Voice HA Active and Standby are in sync.
System has not experienced switchover.

======== Voice HA CF INFO ========
Voice HA Max Checkpoint Data Message Size: 15360
Voice HA CF for RG(1):
    local ip = 10.64.3.228; remote ip = 10.64.3.229
    local port = 56001; remote port = 56000
    CF setup done: TRUE
    Max CF RG Message Size : 15360
    CF RG Buffer Size      : 15360

    Role is Active. Client side stats:
        Received checkpointing requests: 15607
        Wrote to sockets: 15607
            Partial count: 1
            End count    : 15607
            Send event block      : 11
            Send event cleanup    : 0
            Send event error      : 0
        Checkpoint buffer in use: 0
        Pending transmit events: 0

======== Voice HA COUNTERS (non-clearable) ========
HA DB element pool overrun count    : 0
HA DB aux element pool overrun count: 0
HA DB insertion failure count       : 0
HA DB deletion failure count        : 0

ACTIVE
------
Max Media Up time since Call Create: 0 msecs
CF Checkpoint Received IPC Flow ON  : 0
CF Checkpoint Received IPC Flow OFF : 0

DB Entry Deleted - HA CREATE never checkpointed :0

Post CREATE Tick Event - move entry to sync pending db : 0
Post MODIFY Tick Event - move entry to sync pending db : 0
Post DELETE Tick Event - move entry to sync pending db : 0
```

```
Tick Event pool overrun - Malloc fail : 0
Tick Event Queue overrun              : 0
Tick Event Queue processing - No HA DB Entry : 0

CF Checkpoint Send Tick Event overflow (tick queue) : 0
CF Checkpoint Get Buffer failure             : 0
CF Checkpoint Message Send - ISSU xform fail : 0
CF Checkpoint Message Send - CF failed       : 0

STANDBY
-------
CF Standby Message Callback Invoked : 0
  Negotiation msg count : 0
  No msg header count   : 0
  ISSU xform fail count : 0
  Malloc fail count     : 0
  Enqueue fail count    : 0

======== Voice HA CALL COUNTERS ========

ACTIVE
------
Total number of CF checkpoint requests sent : 0
  Total CREATE sent  : 0
  Total MODIFY sent  : 0
  Total DELETE sent  : 0
  Total MDELETE sent :  0
    Added Element to MDELETE List:   0

STANDBY
-------
Total number of CF checkpoint requests received : 0
  Total CREATE received  : 0
  Total MODIFY received  : 0
  Total DELETE received  : 0
  Total MDELETE received : 0

======== Voice HA CALL ERROR COUNTERS ========

ACTIVE
------
Data Collect Abort count: 0

STANDBY
```

```
-------
Data Recreate failure count: 0 (CREATE:0, MODIFY:0)
Data Recreate DELETE count: 0

======== Voice HA APP_DATA COUNTERS ========

ACTIVE
------
Total number of CF APP_DATA requests sent : 16669
  Total APP_DATA sent                     : 16669
  Total APP_DATA received                 : 2

======== Voice HA APP_DATA ERROR COUNTERS ========

ACTIVE
------
APP DATA Collect Abort count: 0

STANDBY
-------
APP_DATA Recreate failure count: 0

======== Voice HA SWITCHOVER COUNTERS ========
Total number of reconciled HA DB entries      : 0
Total number of deleted HA DB entries (stale) : 0

======== Voice HA SWITCHOVER ERROR COUNTERS ========
Total number of HA DB entry delete failures (stale): 0
```

Standby CUBE

```
MSTeams2#show voice high-availability summary
========= HA CREATE|MODIFY Message Sizes =======
SCCPAPP Data Size:  448
SIPSPI  Data Size: 1144
H323SPI Data Size: 2212
RTPSPI  Data Size:  956
CCAPI   Data Size:  264
VOIPRTP Data Size:  372
DSP_MSP Data Size:   32
HA      Data Size:  100
  TOTAL DATA SIZE: 3396
```

```
========= HA APP_DATA Message Sizes =======
CCAPI_SYS     Data Size:    8
VOIP_STUN     Data Size:    8
SCCAPP_SYS    Data Size:   44
VOICE_RSC_VOL Data Size:  124
DCUBE_MBE     Data Size: 1040
    TOTAL SYS DATA SIZE:  512

======== Voice HA DB INFO ========
Number of call legs in HA DB: 0 (MAX:15360)
Number of call legs in HA sync pending DB: 0

----------------------------
First few entries in HA DB:
----------------------------

---------------------------------------
First few entries in Sync Pending DB:
---------------------------------------

---------------------------

======== Voice HA Process INFO ========
Redundancy is configured under 'voice service voip'

ACTIVE - process current tick:46224449,  index: 65
ACTIVE - process number of tick events pending: 0
ACTIVE - process number of tick events processed: 0
Breakdown per tick (TOTAL TICKS:128, 20ms/TICK, MAX EV/TICK:16)
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   0   0   0   0   0   0   0   0
======== Voice HA RF INFO ========
FUNCTIONING RF DOMAIN: 0x2

-----
RF Domain: 0x0
Voice HA Client Name: VOIP RF CLIENT
Voice HA RF Client ID: 1345
Voice HA RF Client SEQ: 133
```

```
My current RF state ACTIVE (13)
Peer current RF state DISABLED (1)

Current VOIP HA state [LOCAL / PEER] :
        [ACTIVE (13) / DISABLED (1)]

VOIP HA RF CB Data:
        ENABLED:1
        flags: 0x6 [PEER_COMM_DOWN/PEER_PRESENCE_DOWN/IN-BOX HA]
        red_mode: 0

-----
RF Domain: 0x2 [RG: 1]
Voice HA Client Name: VOIP RG CLIENT
Voice HA RF Client ID: 4054
Voice HA RF Client SEQ: 481
My current RF state STANDBY HOT (8)
Peer current RF state ACTIVE (13)

Current VOIP HA state [LOCAL / PEER] :
        [STANDBY HOT (8) / ACTIVE (13)]

VOIP HA RF CB Data:
        ENABLED:1
        flags: 0x1 [PEER_COMM_UP/PEER_PRESENCE_UP/B2BHA]
        red_mode: 0
        rg_flags: 0x0
                ctrl [UP/NO SHUT]
                data [UP/NO SHUT]
                traffic (TOT:2; SH:0, DN:0) [UP/NO SHUT]

-----
Voice HA Standby is not available.
System has not experienced switchover.

======== Voice HA CF INFO ========
Voice HA Max Checkpoint Data Message Size: 15360
Voice HA CF for RG(1):
    local ip = 10.64.3.229; remote ip = 10.64.3.228
    local port = 56000; remote port = 56001
    CF setup done: TRUE
    Max CF RG Message Size : 15360
    CF RG Buffer Size      : 15360
```

```
    Role is Standby. Server side stats:
        Received raw message: 15151
            Event incomplete message : 1
        Received checkpointing requests: 15612
        Invalid header counter: 0

======== Voice HA COUNTERS (non-clearable) ========
HA DB element pool overrun count    : 0
HA DB aux element pool overrun count: 0
HA DB insertion failure count       : 0
HA DB deletion failure count        : 0

ACTIVE
------
Max Media Up time since Call Create: 0 msecs
CF Checkpoint Received IPC Flow ON  : 0
CF Checkpoint Received IPC Flow OFF : 0

DB Entry Deleted - HA CREATE never checkpointed :0

Post CREATE Tick Event - move entry to sync pending db : 0
Post MODIFY Tick Event - move entry to sync pending db : 0
Post DELETE Tick Event - move entry to sync pending db : 0
Tick Event pool overrun - Malloc fail : 0
Tick Event Queue overrun              : 0
Tick Event Queue processing - No HA DB Entry : 0

CF Checkpoint Send Tick Event overflow (tick queue) : 0
CF Checkpoint Get Buffer failure             : 0
CF Checkpoint Message Send - ISSU xform fail : 0
CF Checkpoint Message Send - CF failed       : 0

STANDBY
-------
CF Standby Message Callback Invoked : 0
  Negotiation msg count : 0
  No msg header count   : 0
  ISSU xform fail count : 0
  Malloc fail count     : 0
  Enqueue fail count    : 0

======== Voice HA CALL COUNTERS ========

ACTIVE
```

```
------
Total number of CF checkpoint requests sent : 0
  Total CREATE sent  : 0
  Total MODIFY sent  : 0
  Total DELETE sent  : 0
  Total MDELETE sent :  0
    Added Element to MDELETE List:   0

STANDBY
-------
Total number of CF checkpoint requests received : 0
  Total CREATE received  : 0
  Total MODIFY received  : 0
  Total DELETE received  : 0
  Total MDELETE received : 0

======== Voice HA CALL ERROR COUNTERS ========

ACTIVE
------
Data Collect Abort count: 0

STANDBY
-------
Data Recreate failure count: 0 (CREATE:0, MODIFY:0)
Data Recreate DELETE count: 0

======== Voice HA APP_DATA COUNTERS ========

STANDBY
-------
Total number of CF APP_DATA requests received : 15612
  Total APP_DATA sent                         : 1
  Total APP_DATA received                     : 15612

======== Voice HA APP_DATA ERROR COUNTERS ========

ACTIVE
------
APP DATA Collect Abort count: 0

STANDBY
-------
APP_DATA Recreate failure count: 0
```

```
======== Voice HA SWITCHOVER COUNTERS ========
Total number of reconciled HA DB entries      : 0
Total number of deleted HA DB entries (stale) : 0

======== Voice HA SWITCHOVER ERROR COUNTERS ========
Total number of HA DB entry delete failures (stale): 0
```

Acronyms

Acronym	Definitions
CUBE	Cisco Unified Border Element
PSTN	Public Switched Telephone Network
CN	Comfort Noise
MS Teams	Microsoft Teams
SBC	Session Border Controller

Important Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. IN NO EVENT SHALL CISCOOR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCOOR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.