Microsoft Teams: SBC Certification Program to Interop between Microsoft Phone System Direct Routing Interface and Certified Session Border Controllers

Version : 1.3

October 2018

Microsoft Corporation Technical Documentation License Agreement (Standard)

READ THIS! THIS IS A LEGAL AGREEMENT BETWEEN MICROSOFT CORPORATION ("MICROSOFT") AND THE RECIPIENT OF THESE MATERIALS, WHETHER AN INDIVIDUAL OR AN ENTITY ("YOU"). IF YOU HAVE ACCESSED THIS AGREEMENT IN THE PROCESS OF DOWNLOADING MATERIALS ("MATERIALS") FROM A MICROSOFT WEB SITE, BY CLICKING "I ACCEPT", DOWNLOADING, USING OR PROVIDING FEEDBACK ON THE MATERIALS, YOU AGREE TO THESE TERMS. IF THIS AGREEMENT IS ATTACHED TO MATERIALS, BY ACCESSING, USING OR PROVIDING FEEDBACK ON THE ATTACHED MATERIALS, YOU AGREE TO THESE TERMS.

1. For good and valuable consideration, the receipt and sufficiency of which are acknowledged, You and Microsoft agree as follows:

(a) If You are an authorized representative of the corporation or other entity designated below ("**Company**"), and such Company has executed a Microsoft Corporation Non-Disclosure Agreement that is not limited to a specific subject matter or event ("**Microsoft NDA**"), You represent that You have authority to act on behalf of Company and agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that Company will treat the Confidential Information accordingly;

(b) If You are an individual, and have executed a Microsoft NDA, You agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that You will treat the Confidential Information accordingly; or

I If a Microsoft NDA has not been executed, You (if You are an individual), or Company (if You are an authorized representative of Company), as applicable, agrees: (a) to refrain from disclosing or distributing the Confidential Information to any third party for five (5) years from the date of disclosure of the Confidential Information by Microsoft to Company/You; (b) to refrain from reproducing or summarizing the Confidential Information; and (c) to take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, but no less than reasonable care, to keep confidential the Confidential Information. You/Company, however, may disclose Confidential Information in accordance with a judicial or other governmental order, provided You/Company either (i) gives Microsoft reasonable notice prior to such disclosure and to allow Microsoft a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. Confidential Information shall not include any information, however designated, that: (i) is or subsequently becomes publicly available without Your/Company's breach of any obligation owed to Microsoft; (ii) became known to You/Company prior to Microsoft's disclosure of such information to You/Company pursuant to the terms of this Agreement; (iii) became known to You/Company from a source other than Microsoft other than by the breach of an obligation of confidentiality owed to Microsoft; or (iv) is independently developed by You/Company. For purposes of this paragraph, "Confidential Information" means nonpublic information that Microsoft designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential by Recipient". "Confidential Information" includes, without limitation, information in tangible or intangible form relating to and/or including released or unreleased Microsoft software or hardware products, the marketing or promotion of any Microsoft product, Microsoft business policies or practices, and information received from others that Microsoft is obligated to treat as confidential.

2. You may review these Materials only (a) as a reference to assist You in planning and designing Your product, service or technology" ("Product") to interface with a Microsoft Product as described in these Materials; and (b) to provide feedback on these Materials to Microsoft. All other rights are retained by Microsoft; this agreement does not give You rights under any Microsoft patents. You may not (i) duplicate any part of these Materials, (ii) remove this agreement or any notices from these Materials, or (iii) give any part of these Materials, or assign or otherwise provide Your rights under this agreement, to anyone else.

3. These Materials may contain preliminary information or inaccuracies, and may not correctly represent any associated Microsoft Product as commercially released. All Materials are provided entirely "AS IS." To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

4. If You are an entity and (a) merge into another entity or (b) a controlling ownership interest in You changes, Your right to use these Materials automatically terminates and You must destroy them.

5. You have no obligation to give Microsoft any suggestions, comments or other feedback“ ("Feedback") relating to these Materials. However, any Feedback you voluntarily provide may be used in Microsoft Products and related specifications or other documentation (collectively“, "Microsoft Offerings") which in turn may be relied upon by other third parties to develop their own Products. Accordingly, if You do give Microsoft Feedback on any version of these Materials or the Microsoft Offerings to which they apply, You agree: (a) Microsoft may freely use, reproduce, license, distribute, and otherwise commercialize Your Feedback in any Microsoft Offering; (b) You also grant third parties, without charge, only those patent rights necessary to enable other Products to use or interface with any specific parts of a Microsoft Product that incorporate Your Feedback; and (c) You will not give Microsoft any Feedback (i) that You have reason to believe is subject to any patent, copyright or other intellectual property claim or right of any third party; or (ii) subject to license terms which seek to require any Microsoft Offering incorporating or derived from such Feedback, or other Microsoft intellectual property, to be licensed to or otherwise shared with any third party.

6. Microsoft has no obligation to maintain confidentiality of any Microsoft Offering, but otherwise the confidentiality of Your Feedback, including Your identity as the source of such Feedback, is governed by Your NDA.

7. This agreement is governed by the laws of the State of Washington. Any dispute involving it must be brought in the federal or state superior courts located in King County, Washington, and You waive any defenses allowing the dispute to be litigated elsewhere. If there is litigation, the losing party must pay the other party’s reasonable attorneys’ fees, costs and other expenses. If any part of this agreement is unenforceable, it will be considered modified to the extent necessary to make it enforceable, and the remainder shall continue in effect. This agreement is the entire agreement between You and Microsoft concerning these Materials; it may be changed only by a written document signed by both You and Microsoft.

Table of Contents

1.0 Revision History 7

2.0 Introduction to Microsoft Teams Direct Routing SBC Certification Program 8

2.1 Terminology 8

2.2 Prerequisites to becoming a Partner 8

2.3 Certification and Re-testing timelines 9

2.3.1 Delivery of updated solution 9

2.4 Overview of the Certification Process 10

2.5 Product samples 10

2.6 Qualification Testing 11

2.6.1 Definition of same platform 11

2.6.2 Qualification testing by an approved independent test lab 11

2.6.3 Self -testing process 12

2.7 Updating certification for new versions of SBCs firmware 12

2.8 Product support and live-site operations 12

2.8.1 Support benefit options 13

2.8.2 Support integration requirements 14

3.0 Data reporting 15

4.0 Publishing your certification 15

4.1 Contacting Microsoft 15

5.0 Product Specifications 16

5.1 Scope of Certification 16

6.0 Qualification tests 17

6.1 End to End Scenarios 18

6.1.1 Definitions 18

6.1.2 Simple Inbound/Outbound PSTN Calls and Call Handling 18

6.1.3 Hold (Music On Hold Disabled) 20

6.1.4 Call Disconnect 24

6.1.5 Early media 27

6.1.6 Transfers 28

6.1.7 Call forward and Simultaneous Ring and Call forking 35

6.1.8 1:1 to Group Call Escalation 39

6.1.9 Auto Attendant (Required for V2) 41

6.1.10 Call Queues (required for V2) ... 42
6.2 Codec support ... 42
6.2.1 SILK codec support ... 42
6.2.2 SILK Codec Transcoding (Required to be supported by Dec 2018) ... 44
6.3 Media Requirements ... 45
6.3.1 Media Bypass: ICE Lite and MS Turn support ... 45
6.3.2 SRTP ... 49
6.3.3 DTMF support ... 53
6.3.4 Comfort Noise Passthrough and Generation ... 55
6.3.5 RTCP ... 59
6.4 Security Requirements ... 64
6.4.1 TLS v1.2 ... 64
6.5 Support for OPTIONS and Failover ... 64
6.5.1 Device responds to OPTIONS messages sent by the Teams SIP Proxy ... 64
6.5.2 Device sends SIP OPTIONS message to all three datacenters ... 64
6.5.3 Device tries the secondary datacenter when there is no response from the primary datacenter (cannot establish TLS/TCP connection) ... 65
6.5.4 Device tries the secondary datacenter when there is no response from the primary datacenter (no response to invite) ... 65
6.5.5 Device honors the retry-after timer in the 503 message received for the INVITE ... 66
7.0 Appendix 1. Direct Routing SIP Protocol description ... 66
7.1 Introduction ... 66
7.2 Processing the incoming request ... 67
7.2.1 Detailed requirements for Contact Header and Request-URI ... 67
7.3 Contact and Record-Route headers ... 70
7.3.1 Use of FQDN Name in Contact or Record-Route ... 70
7.4 Size of SDP Considerations ... 71
7.5 Call transfer ... 71
7.5.1 Methods for transferring the calls ... 71
7.5.2 Refer method ... 71
7.5.3 Basic Refer implementation ... 72
7.6 SBC connection to Direct Routing and Failover mechanism ... 74
7.7 Retry-After ... 75

7.8 ICE Restart: Media Bypass call transferred to an endpoint which does not support Media Bypass 75

8.0 Appendix 2. Media and Encryption requirements ... 79

8.1 Media Bypass. ICE Lite requirements ... 80

8.2 Encryption cipher and MKI requirements ... 80

8.3 SDES support Requirements ... 81

8.4 Format for Offer from SBC in BYPASS (Offer must contain SDES and can contain DTLS Optional in the following format) ... 81

8.5 Format for Answer containing SDES to SBC ... 81

8.6 Format for Offer from Teams to SBC ... 82

8.6.1 Format for SDES only offer to SBC ... 82

8.6.2 SILK Codec implementation recommendations ... 82

9.0 Appendix 3. Requirements to the Domain Names registered in Office 365 Administrator Center 82

9.1 SBC hosting scenario ... 83

8.0 Test cases matrix ... 83

10.0 Joint support process requirements ... 83

1.0 Revision History

Revision	Date	Description
1.0	July 2018	First version
1.1	August 2018	Added requirements and description of transferring a call in Media Bypass mode to a SfB participant (insert MP)
1.2	October 2018	Removed DTLS requirements, revised tests cases, marked cases that are not available in production
1.3	October 2018	Fixed minor issues with formatting, added requirement to support Microsoft TURN, added test case for Microsoft Turn, some cases that were marked before as not supported yet are marked as supported now (mostly early Media in Media Bypass mode)

2.0 Introduction to Microsoft Teams Direct Routing SBC Certification Program

Microsoft Teams partner solution certification programs are designed to help partners bring premium communication experiences to the market. The *Direct Routing SBC certification* shall also be referred to as the *certification program* in this document. Microsoft Teams customers trust the certification as an assurance that the partner solutions have been tested to provide the quality, compatibility, and reliability that ensures the best communication experience, and that the partner solutions are backed by best in class product support.

Solutions which pass the technical and process requirements outlined in this specification are eligible to:

- Use the certification logo and associated Microsoft related branding as outlined in the certification contract;
- Be listed on Microsoft sites including Microsoft product documentation as certified devices;
- Participate in integrated support with Microsoft

2.1 Terminology

Recommended – not required, but simplifies the troubleshooting if configured as in following examples if referred to technical parameters of SBCs. When referred to the program terms and conditions it is a non-mandatory program condition but recommended;

Must – strict requirement, the system does not work as expected without the configuration of the parameters as described in this document if referred to technical parameters of SBCs. When referred to program terms and conditions it is a non-negotiable program parameter;

SIP Hub – internet facing component of Microsoft Phone Direct Routing. Handles SIP (TLS) connection between SBCs and Direct Routing;

Media Processors - internet facing component of Microsoft Phone Direct Routing. Handles media traffic. Uses SRTP and SRTCP protocols.

2.2 Prerequisites to becoming a Partner

To qualify for the program a partner must have:

- A long-term interest in developing product lines for the Microsoft Teams or Skype for Business platform;
- A proven record of developing and marketing enterprise grade communication solutions;
- Established enterprise sales channels;

- Established high-quality customer support network capable to handle cases on 24 by 7 basis;
- Commitment to acquire a one of support options listed in this document;
- Microsoft Partner Network (MPN) program membership at the minimum level as described on the following link https://partner.microsoft.com/en-us/membership/core-benefits. Join at a level that aligns with your business strategies.

  Note: the MPN programs evolves over time. The evolution might include but not limited changes to program requirements, certification level names. If such change occur, partner expected to maintain at least minimum level in the program.

2.3 Certification and Re-testing timelines

Partner solutions must comply with the latest published specification at the time of development. Microsoft committed to keep technical parameters for interoperability with SBC as described in this specification unchanged. However, based on the customer feedback or if product evolution requires changes in SIP Hub and Media Processors, Microsoft might issue a new specification. After specification published, partner must re-certify the device.

We define two terms:

- **Enforcement Period** – this is the time from when a specification is published until all newly submitted products must meet the new specification.
- **Recertification Period** – this is the time by which any existing certified products must be updated and retested against a new specification or newer versions of the Microsoft UC solution.

Category	Enforcement period	Recertification period
Shipped product	6 months	9 months

Recertification for partner operated service requires compliance against any new requirements and may include targeted retesting against previous requirements.

Though all efforts are made to ensure that the specification is final at the time of publication, and to allow partners a reasonable time to accommodate new changes, it is possible that urgent changes may need to be made outside of the normal enforcement and recertification periods. Microsoft will communicate directly with partners to coordinate any such hotfixes.

2.3.1 Delivery of updated solution

Once a solution is certified against the latest specification, or if an interim update is required due to either a hotfix or update in any Microsoft SDK components, partners are expected to facilitate and encourage customers to update.

2.4 Overview of the Certification Process

Certification entails more than simply testing a product against a test plan. It also includes a variety of process alignments between Microsoft and the partner (e.g., for support) as well as structured customer feedback. The following steps must be completed to achieve and maintain a certification:

Action	Owner
Complete legal contracts: NDA, Certification Program Brand Licensing Agreement	Partner
Notify the certification program team at Microsoft if the candidate product has any unique features or if there is any question about which certification category applies to the product.	Partner
Develop product to meet requirements (including self-testing)	Partner
Develop hooks for test automation, synthetic transactions and telemetry (as applicable for program and solution delivery method).	Partner
Perform certification testing (at Partner expense)	Lab
If failures are identified by lab testing, fix and resubmit to lab (additional fees may apply)	Partner
Review final lab test results (identify resolution plan)	Microsoft
Support process alignment (including training, drills, and sample product)	Partner/Microsoft
Draft detailed product documentation, configuration guidance & marketing content	Partner
Review product documentation & marketing content for compliance with program scope	Microsoft
Approve certification	Microsoft
Prepare and conduct training for Microsoft support organization on how to pair the SBC and troubleshooting methodology	Partner
Publish certification on Microsoft websites	Microsoft
Perform post-certification requirements (e.g., Noc-Noc or support drills, telemetry and business metric reviews, fix temporary waivers, customer education / training sessions, recertification)	Partner/Microsoft

2.5 Product samples

Partner must provide product samples to Microsoft and independent lab for purposes of testing, and other evaluation purposes

Microsoft adds all devices that are being certified in the engineering development lab. The devices are used for making test calls in production and pre-production environment. Microsoft releases new versions of SIP Hub every week and Media Processors every other week at the moment of publication the specification. The test devices provided by partner are vital part of the release process. Microsoft will not release new version unless all SBCs in Microsoft lab pass the tests with a release candidate.

The samples provided to Microsoft will not be returned, however samples provided to independent labs may be reclaimed after certification test cycle completion. The sample must be GA versions, unless otherwise agreed. The product samples must be supported by the partner.

Deliver to	Number of samples
Microsoft	As agreed with Microsoft. At least two per each certified platform. If several SBC share the platform only one SBC is required.
Test Lab*	As described in the Test Topology section

*Partner can request lab to complete relevant NDA before delivery

2.6 Qualification Testing

The qualification testing results in publishing device as Certified for Teams Direct Routing. To pass certification SBC must pass all tests, listed in section 6.0 Qualification Tests

There are two options for qualification testing:

- Qualification testing by an approved independent test lab;
- Qualification testing by SBC vendor (self-testing)

Partner can use self-testing only if:

- SBC which are self-certified have the same platform AND
- At least one SBC from the same platform qualified via the approved lab;

.

2.6.1 Definition of same platform

- The SBCs should have the same firmware code;
- DSP type of the SBCs is the same across models;
- SBCs have the same CPU family;
- SBCs Perform transcoding in the same manner;
- SBCs handle voice in the same fashion

2.6.2 Qualification testing by an approved independent test lab

Qualification testing normally is conducted at an approved independent test lab that is trained by Microsoft.

The certification partner is responsible for:

- Scheduling the lab testing;

- Providing samples and all necessary product documentation to the lab;
- Paying testing fees directly to the lab (and any re-test fees if necessary)

The independent lab is responsible for:

- Committing a schedule for test completing and fulfilling the schedule commitment unless delays are due to product defects or lack of product documentation or other collateral.
- Providing a standardized test report to Microsoft indicating the candidate solution's performance relative to the specification.

2.6.3 Self -testing process

If the SBC eligible for self-testing, the SBC vendor is responsible for:

- Running all tests listed in section 6 "Qualification tests" of this document;
- Sending the results to Microsoft using the email address drsbccertification@microsoft.com

Microsoft Direct Routing Certification team is responsible for:

- Reviewing the test results within one week after submission;
- Adding the SBC as certified device on the Direct Routing certification program page;

2.7 Updating certification for new versions of SBCs firmware

Every new major version of SBC requires re-certification.

Major version includes a version with protocol level changes. If any protocol level changes, are expected in the minor version of SBCs firmware the minor version also should be certified.

If SBC vendor want to renew the minor version of the SBC on Microsoft site, the description of the changes must be sent to drsbccertification@microsoft.com. Microsoft can renew the certification status per partner request if no protocol version introduced in the new minor version of the code.

Any re-test requires paying a fee to selected CTCs.

2.8 Product support and live-site operations

All certification partners are required to maintain first-tier quality of support for their certified products, which means a support level that meets or exceeds the support provided for the company's non-certified products and is among the best across peers in the solution category.

To support first-tier support, partners are required to have a Microsoft support contract as described in 2.8.1 "Support benefit options".

All post-certification in-market cases must be routed through this support channel rather than through the Microsoft certification program team.

2.8.1 Support benefit options

All partners must have a support plan which provides at least the minimum benefits as indicated below. The support contract required when incidents are raised with Microsoft on behalf of customers. Support engineers will not handle the cases if partner doesn't have a contract. Incidents raised between two engineering organizations (Microsoft and Partner) during the development process can be raised directly as described in the "Teams Direct Routing Joint Support" documentation.

In addition, if partners are at risk of consuming the maximum incident count provided by their benefit, they must proactively purchase a higher support plan.

Support offerings may change, and partner should update their offering as necessary to meet these minimum requirements for the duration that their product remains certified and in market. Current offerings can be found here https://partner.microsoft.com/en-us/support/partnersupport.

Support features	Minimum requirement
Microsoft Products & Services Supported	As appropriate for certified product
Support Delivery Method	Remote
Submit Support Tickets On Behalf of End Customer	Required
24x7 Technical Support	Required
Case Severity & Target Initial Response Times	• Severity A: 2 hours • Severity B: 4 hours • Severity C: 8 hour
24x7 Critical Situation Support	Optional*
Support Account Management	Optional unless partner has high volume of support tickets

** See expectation in "Teams Direct Routing Joint Support Process Requirements". Partner expected to make a decision about need of "24x7 Critical Situation Support" based on the requirements listed in the document "Teams Direct Routing Joint Support Process Requirements".*

The document provided separately.

.

Based on the number of anticipated cases, the partner needs to pick one of the options below. The detailed comparison of the offers available on the following link https://partner.microsoft.com/en-us/support/partnersupport.

Support Option	Considerations
MPN Support benefit	Provides a set number of support tickets per year along with other MPN benefits, but also requires company achieve certain competencies (vary by solution type). More about competencies: https://partner.microsoft.com/en-US/membership/core-benefits
Microsoft Advanced Support for Partners	Lower cost than Premier support and with higher priority response queues than MPN. Ideal for partners that expect higher support volume than MPN allows, and who need faster response
Premier Support	Most comprehensive support option, but also most expensive. Premier support contracts are offered at different levels depending on the anticipated support volume.

2.8.2 Support integration requirements

2.8.2.1 Support Training

Partners are required to develop training content and a step-by step troubleshooting guide which will be delivered to Microsoft support organization's regional trainers. The training is typically 1-2 hours of content delivered as a presentation with leave-behind collateral. Partners are expected to deliver updated training after recertification if there are major changes to the product. The objective of this training is to educate the Microsoft support organization on the product to the degree that they can speak generally about the product, perform basic troubleshooting and collect enough information to efficiently initiate a support hand-off to the partner. Training must also include information for how to configure specific features supported by the SBC in order to integrate with the Microsoft cloud service.

2.8.2.2 Customer facing documentation

Partners are required to provide and maintain step-by step configuration guides to the customers by publishing them on the partners web site. Partners are required to update documentation if Microsoft adds new functionality which requires changes in partner interconnection instructions.

2.8.2.3 Live-site support (NOC to NOC support)

SBC partners are required to have additional support requirements as described below:

- 24hr Global Support Process – Partner has to have a support center staffed at all times able to take calls and get domain experts on phone bridges in short order to solve customer high priority, high severity incidents.
- NOC to NOC Support – Partner must provide NOC-NOC support process documentation prior to certification that describes:
    - Process for Microsoft to contact partner support in case if a Sev 1 / Major incident;
    - Commands that need to be executed to reproduce an issue;
    - Steps to be carried out to collect logs from a customer's SBC

A sev1 incident involving a certified SBC is an outage impacting several users, such that users are unable to place to or from Teams via their Direct Routing certified SBC. The partner is expected to acknowledge the incident within 15 minutes and get on each other's Sev 1 incident bridge within 30 min of contact initiation to provide short term resolution, root cause analysis and a longer-term resolution plan, if applicable.

Noc-Noc drill – in order to practice the support engagement process for high priority issues that require real-time investigation by Microsoft dev-ops team, Microsoft and the partner will conduct drills before certification and at a regular cadence (no less than once a quarter) after the service is live. Microsoft and Partners are expected to acknowledge the incident within 15 minutes and get on each other's, Sev 1 incident bridge within 30 minutes. The drills conducted every 6 months.

3.0 Data reporting

Partners have to provide on quarterly basis bugs reported by Direct Routing customers across the various SBC models certified, which were not escalated to Microsoft

4.0 Publishing your certification

On receiving formal approval from certification program team, the partner must work with Microsoft marketing to provide device images, company logo and marketing content for posting to Microsoft websites.

Partner and Microsoft will periodically review the list of qualified products to be removed from the active **the partner solutions catalog** listing because of end of life, field issues, or replacement by newer models. Additionally, Microsoft will remove any product that fails to maintain certification status for any reason.

4.1 Contacting Microsoft

For any questions regarding requirements or certification process, please contact the certification program team at drsbccertification@microsoft.com

5.0 Product Specifications

5.1 Scope of Certification

A Session Border Controller deployed on the customer's network can interface with the Sip Proxy in Microsoft Teams service in the cloud, allowing the customer to terminate PSTN traffic to and from their Teams client using the customer's own SIP trunk provider or to 3rd party PSTN equipment connected to the SBC. This Service is known as Direct Routing. More information about direct routing is available here. This document describes the main requirements for a Session Border Controller (SBC) to be certified with Direct Routing interface. Although this specification cover many technical interop requirements, in case if any interop questions are not clear, please contact drsbccertification@microsoft.com for clarifications.

Direct Routing built to comply with RFC standards. The standards are listed below. Unless otherwise specified, partners supposed to use RFC standards. However, there is one case which implemented by Microsoft but not documented in RFC standards. The case covered in Appendix 2. Media Encryption Offer / Answer Requirement for SBC in BYPASS Mode.

Direct Routing has strict requirements to Contact header of the SIP messages. Details are listed in Appendix 1. Direct Routing SIP Protocol description;

The SBC connected to the Direct Routing must comply with the following RFC (or their successors):

- RFC 3261 SIP: Session Initiation Protocol;
- RFC 5245 Interactive Connectivity Establishment (ICE) for Media Bypass. The SBC MUST support:
  - ICE Lite, the Teams clients are full ICE clients;
  - ICE Restart (https://tools.ietf.org/html/rfc5245#section-9.1.1.1). See more on ICE restart use case and examples Appendix 1. 7.9 ICE Restart: Media Bypass call transferred to an endpoint which does not support Media Bypass
- RFC 3515 The Session Initiation Protocol (SIP) Refer method. Note the Direct Routing interface sends Refer messages on call transfers. There are some specifics to the size of the Refer message and when Direct Routing decides if Refer should or should not be sent. Please consult section 6.7 "Refer method" of Appendix 1. Direct Routing SIP Protocol description for more information;
- RFC 3325 Private Extension to the Session Initiation Protocol for asserted identity within Trusted Networks. Sections about handling P-Asserted-Identity header. Direct Routing if configured can send P-Asserted-Identity with Privacy ID headers.
- RFC 4244 "An extension to Session Initiation Protocol (SIP) for requires History Information". Please consult section 6.8 "History-Info and Referred By methods" of Appendix 1. Direct Routing SIP Protocol description for more information;

- RFC 3892 "The Session Initiation Protocol Referred By mechanism." Please consult section 6.8 "History-Info and Referred By methods" of Appendix 1. Direct Routing SIP Protocol description for more information;
- Protect RTP traffic using SRTP. SBC must be able to establish keys using SDES (RFC 3711 and RFC 4771) method. Please consult Appendix 2. Media Encryption Offer / Answer Requirement for SBC in BYPASS Mode for more information;
- RFC 8035 Session Description Protocol (SDP) Offer/Answer Clarifications for RTP/RTCP Multiplexing;
- Support of MS-Turn Relay as described in https://interoperability.blob.core.windows.net/files/MS-TURN/[MS-TURN].pdf The MS Turn Relay is used in Media Bypass cases
- Ability to either:
    - ✓ Recommended: transcode SILK OR
    - ✓ Supported for certification: Support SILK Passthrough mode[1]
- Support of the following codecs – SILK, G729, G711, optionally OPUS;
- Support of adding Certificates from the 3rd party Certification authorities to protect connection between the SBC and the Direct Routing interface. The list of Certification authorities supported by Direct Routing interface is available in documentation for Direct Routing

[1] *Even though Microsoft supports SILK passthrough, Microsoft will not recommend SBC that use only SILK passthrough to the customers if SIP trunk, connected to the SBC does not support SILK codec. Reason: from our telemetry and customer feedback we see that using G.711 or G729 over internet is not optimal from end user experience point of view. G.711 is not susceptible to internet conditions (no QoS end to end, potential delays of the packets) and, therefore, we observer issues with voice quality. On the other side, SILK was designed by Microsoft to work over the internet and compensate potential issues with network conditions. The difference in terms of end user experience between using G.711 and SILK is notable with SILK providing much better voice quality if traffic flows via internet. If SBC only supports SILK pass through, the only case where Microsoft will recommend using SBC with SILK passthrough is when SIP trunk behind the SBC supports SILK codec.*

Detailed requirements for Media and Sip protocol described in:

- Appendix 1. Direct Routing SIP Protocol description;
- Appendix 2. Media Encryption Offer / Answer Requirement for SBC in BYPASS Mode

If any portion of the document is not clear or you have feedback on the specification, please consult with drsbccertification@microsoft.com

6.0 Qualification tests

6.1 End to End Scenarios

The section below outlines the details tests cases required to pass during the certification process. The certification test performed by TekVizion lab.

The tests performed with Teams and Skype for Business (once supported) Windows Clients unless the case description indicate s use of a different client

6.1.1 Definitions

- **Outbound call.** Call from a Teams or SfB client to a PSTN Number (Teams/SfB Cleint-> Direct Routing -> SBC -> SIP/TDM Trunk);
- **Inbound call**. Call from a PSTN number to a Teams or SfB user (SIP/TDM Trunk -> SBC -> Direct Routing -> Teams/SfB Client)

6.1.2 Simple Inbound/Outbound PSTN Calls and Call Handling

6.1.2.1 Device supports ptime of 20 ms for an inbound call to Teams user

ID	43920
Priority	1
Summary	[Objective] Device must be able to establish a call with the configured ptime == 20 ms. [Pre-condition] - Configure Device to have ptime value of 20ms.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams/SfB user	Direct Routing interface receives INVITE from Device. The INVITE's SDP ptime value is set to 20ms.
2	Teams/SfB user picks up the call	Call is connected with bi-directional audio, vcoie is clear, no echo
3	PSTN user hangs up	Call is disconnected

6.1.2.2 Device sends its own FQDN in the contact header

ID	43922
Priority	1
Summary	[Objective] Device sends its own FQDN in contact header s described in "Appendix 1 Direct Routing SIP protocol Description" in all requests and responses for a call from Teams/SB user to PSTN user. [Pre-Condition]

	- SBC's FQDN is set during the setup - SBC's FQDN should match the FQDN found in SBC's certificate Subject Name/SAN
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams/SfB user calls PSTN user	Call is connected with bi-directional audio and the Contact headers in all request messages sent from the Device have Device's FQDN
2	Teams/SfB user hangs up	Call is disconnected

6.1.2.3 Device is capable to perform manipulation of phone number on outbound call according to the trunk provider requirements

ID	47275
Priority	1
Summary	[Objective] Validate that the device is capable of manipulating number in the Request URI number according to the trunk provider requirements. [Pre-Condition] - Device is configured to manipulate phone numbers on outgoing calls
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams/SfB user calls PSTN user	1. Device receives INVITE from Direct Routing with number in Request URI and To fields, which doesn't match the trunk provider requirements. 2. Devices performs manipulation of the number according to the trunk provides requirements
2	PSTN user picks up	Call is connected with bi-directional audio
3	Teams/SfB user hangs up	Call is disconnected

6.1.2.4 Device is capable to perform manipulation of phone number on inbound call according to Direct Routing interface requirements

ID	47276
Priority	1
Summary	[Objective] Validate the ability of the device to manipulate phone number on inbound call. [Pre-Condition] - Teams/SfB user configured with E.164 number as the DID; - Incoming call from trunk send to a non-E.164 number, which must be converted to E.164 phone number

Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**		**Expected Result**
1	A PSTN user calls Teams/SfB user		Device receives INVITE with no-E.164 number in the FROM URI. Dive manipulates the number and converts it to E.164 number before sending to Direct Routing interface
2	Teams/SfB user picks up the call		Call is established with bi-directional audio
3	Teams/SfB user hangs up		Call is disconnected

6.1.2.5 Device accepts call from Teams user where the user's calling line identity is set to anonymous

ID	49028		
Priority	1		
Summary	[Objective] Device accepts call from Teams user where the user's calling line identity is set to anonymous and process the call towards PSTN/customer SIP Trunk. [Pre-Condition] - Set the Teams user's calling line identity as anonymous. 1. Create a new calling line identity using New-CsCallingLineIdentity command. *New-CsCallingLineIdentity -Identity Anonymous -Description "Anonymous policy" -CallingIDSubstitute Anonymous -EnableUserOverride $false* 2. Assign the new calling line identity policy to the Teams user using the below command. *Grant-CsCallingLineIdentity -Identity "amos.marble@contoso.com" -PolicyName Anonymous*		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**		**Expected Result**
1	Teams/SfB user calls a PSTN user		PSTN user rings and displays the caller ID as 'Anonymous' for the ringing call
2	PSTN user picks up the call		Call is connected with bi-directional audio
3	Teams user hangs up		Call is disconnected

6.1.3 Hold (Music On Hold Disabled)

6.1.3.1 Teams user places inbound call from PSTN on hold and then resumes

ID	43924
Priority	1
Summary	[Objective] Device is able to process Hold-Resume initiated by Teams/SfB user for an inbound call from PSTN End Point.

Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Call is connected with bi-directional audio	
2	Teams/SfB user initiates call hold	1.Call goes on hold with no way audio 2. Direct Routing sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK 3. Device should send SRTCP packets during hold	
3	Teams/SfB user resumes the call	Call is resumed with bi-directional audio	
4	PSTN user hangs up	Call is disconnected	

6.1.3.2 Teams/SfB user places outbound call to PSTN on hold and then resumes

ID	[43925]	
Priority	1	
Summary	[Objective] Device is able to process Hold-Resume initiated by Teams/SfB user in a outbound call to PSTN user.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams/SfB user calls PSTN user	Call is connected with bi-directional audio
2	Teams/SfB user initiates call hold	1.Call goes on hold with no way audio 2. Teams SIP Proxy sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK 3. Device should send SRTCP packets during hold
3	Teams/SfB user resumes the call	Call is resumed with bi-directional audio
4	Teams/SfB user hangs up	Call is disconnected

6.1.3.3 Teams/SfB user places outbound call to PSTN on hold for over 15 minutes and then resumes

ID	[43926]	
Priority	1	
Summary	[Objective] Audio is re-established when Teams user resumes a call after placing it on hold for 15 minutes.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams/SfB user calls PSTN user	Call is established with bi-directional audio

2	Teams/SfB user places the call on hold for 15 minutes	1. Call goes on hold with no way audio 2. Teams SIP Proxy sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK 3. Device should send SRTCP packets during hold
3	Teams/SfB user resumes the call after 15 minutes	Call is resumed with bi-directional audio successfully
4	Teams/SfB user hangs up	Call is disconnected

6.1.3.4 Teams/SfB user places an inbound call from PSTN on hold for over 15 minutes and then resumes

ID	43927	
Priority	1	
Summary	[Objective] Audio is re-established when Teams/SfB Client resumes a call after placing it on hold for 15 minutes.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams/SfB user	Call is established with bi-directional audio
2	Teams/SfB user places the call on hold for 15 minutes	1.Call goes on hold with no way audio 2. Teams SIP Proxy sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK 3. Device should send SRTCP packets during hold
3	Teams/SfB user resumes the call after 15 minutes	Call is resumed with bi-directional audio successfully
4	PSTN user hangs up	Call is disconnected

6.1.3.5 Teams/SfB user places outbound call to PSTN on hold after 30 minutes and then resumes

ID	43928	
Priority	1	
Summary	[Objective] When an outbound call has been active for 30 minutes, audio can be re-established if Teams user places call on hold and then resumes.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams/SfB user calls PSTN user	Call is established with bi-directional audio
2	Call is kept up with active talk path in both directions	SRTP packets are continuously streamed in both directions and two-way audio is still present

3	Teams/SfB user places the call on hold after 30 minutes	1. No audio is present while call is on hold 2. Device sends and receives SRTCP packets while call is on hold and call does not drop
4	Teams/SfB user resumes the call	Bi-directional audio is established
5	Teams/SfB user hangs up	Call is disconnected

6.1.3.6 Teams/SfB user places inbound call from PSTN on hold after 30 minutes and then resumes

ID	43929
Priority	1
Summary	[Objective] When an inbound call has been active for 30 minutes, audio can be re-established if Teams user places call on hold and then resumes.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN End Point calls Teams/SfB Client	Call is established with bi-directional audio
2	Call is kept up with active talk path in both directions	SRTP packets are continuously streamed in both directions and two way audio is still present
3	Teams/SfB Client places the call on hold after 30 minutes	1. No audio is present while call is on hold 2. Device sends and receives SRTCP packets while call is on hold and call does not drop
4	Teams/SfB Client resumes the call	Bi-directional audio is established
5	PSTN End Point hangs up	Call is disconnected

6.1.3.7 Teams/SfB user places outbound call on hold and then disconnects during hold

ID	49672
Priority	1
Summary	[Objective] Device is able to handle the termination made by Teams user when the call is on hold.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams/SfB user calls PSTN user	Call is connected with bi-directional audio
2	Teams/SfB user initiates call hold	Call goes on hold with no way audio
3	Teams/SfB user hangs up during the hold	Call is disconnected

6.1.3.8 Teams/SfB user places inbound call on hold and then disconnects during hold

ID	49673
Priority	1

Summary	[Objective] Device is able to handle the termination made by Teams user when the call is on hold.		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams/SfB user	Call is connected with bi-directional audio	
2	Teams/SfB user initiates call hold	Call goes on hold with no way audio	
3	PSTN user hangs up during the hold	Call is disconnected	

6.1.4 Call Disconnect

6.1.4.1 PSTN user disconnects inbound call to Teams/SfB user before it is answered

ID	[43940]	
Priority	1	
Summary	[Objective] Device is able to CANCEL the call before it gets connected.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams/SfB user	Teams user rings and ringing is heard on PSTN user
2	PSTN user hangs up the call while Teams/SfB user is ringing	1. Teams/SfB user stops ringing and call is disconnected on PSTN user 2. Device sends CANCEL to Direct Routing and receives 200 OK for the CANCEL 3. Device receives and processes 487 Request Terminated from Teams SIP Proxy 4. Device responds with ACK to the 487 Request Terminated

6.1.4.2 Teams/SfB user disconnects outbound call to PSTN user before it is answered

ID	[43941]	
Priority	1	
Summary	[Objective] Device handles CANCEL sent by Teams SIP Proxy before the call gets connected.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**

1	Teams/SfB user calls PSTN user	PSTN End Point rings and ringing is heard on Teams Client
2	Teams/SfB user hangs up the call while PSTN user is ringing	1. Device receives, and processes CANCEL from Direct Routing 2. Device responds to the CANCEL with 200 OK 3. Device sends 487 Request Terminated to the Direct Routing

6.1.4.3 PSTN user disconnects an inbound connected call

ID	43942	
Priority	1	
Summary	[Objective] Device should handle the disconnect from PSTN End Point for an inbound connected call.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams/SfB user	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

6.1.4.4 PSTN user disconnects an outbound connected call

ID	43943	
Priority	1	
Summary	[Objective] Device should handle the disconnect from PSTN End Point for an outbound connected call.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams/SfB user calls PSTN user	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

6.1.4.5 Teams/SfB user disconnects an inbound connected call

ID	43944	
Priority	1	
Summary	[Objective] Device should handle the disconnect from Teams user for an inbound connected call.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams/SfB user	Call is connected with bi-directional audio
2	Teams/SfB user hangs up	Call is disconnected

6.1.4.6 Teams/SfB user disconnects an outbound connected call

ID	43945		
Priority	1		
Summary	[Objective] Device should handle the disconnect from Teams user for an outbound connected call. [Pre-Condition]-		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	Teams/SfB user calls PSTN user	Call is connected with bi-directional audio	
2	Teams/SfB user hangs up	Call is disconnected	

6.1.4.7 Device can disconnect a call forked to Teams/SfB users set to “Do not disturb”

ID	43946		
Priority	1		
Summary	[Objective] Device can disconnect a forked call when all Teams users are set to 'Do not Disturb'. [Pre-Condition] - Teams/SfB user logged into multiple locations - Status is set to 'Do not Disturb' in Teams Client		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams/SfB user	Direct Routing forks the call to each End Point as the Teams user is logged into multiple locations	
2	Direct Routing sends local 183 Session Progress with SDP first and then sends 480 Temporarily Unavailable to the Device	Device processes the 480 Temporarily Unavailable message and disconnects the call	

6.1.4.8 Device responds with 488 Not Acceptable for outbound call

ID	43948
Priority	1
Summary	[Objective] Validate that the device can handle properly misconfigured requests (for example, codec misconfiguration). Proper response on misconfigured requests - respond with 488 Not Acceptable for an outbound call [Pre-Condition] - SRTP disabled on Device.

Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	Teams/SfB user calls PSTN user	Device receives an INVITE from Teams SIP Proxy including SRTP support	
2	Devices sends “488 Not Acceptable”	Direct Routing receives the “488 Not Acceptable” from device and disconnects the call	

6.1.5 Early media

6.1.5.1 Device supports reliable Early Media for a call from Teams/SfB to PSTN

ID	43950	
Priority	1	
Summary	[Objective] Device supports Early media towards Direct Routing for a call from Teams/SfB to PSTN. [Pre-Condition] - Configure device to support Early media towards Direct Routing	
Applicable	Non-Media Bypass (Early Media is not supported in Media Bypass mode)	
Step	**Action**	**Expected Result**
1	Teams/SfB user calls PSTN user	PSTN user rings
2	Device receives INVITE from Direct Routing with SDP	Device sends 18x provisional response with SDP as a part of Early media negotiation
3	PSTN user answers the call	Verify if the call is established with two-way audio and there is no audio clipping
4	Teams/SfB user hangs up	Verify if the call is disconnected

6.1.5.2 PSTN user calls Teams/SfB user that is set to simultaneously ring an IVR number and IVR responds

ID	43953	
Priority	1	
Summary	[Objective] Device should be able to support the simultaneous ring functionality set on Teams/SfB Client. [Pre-Condition] - Configure Teams user simultaneously ring to IVR number on a PSTN endpoint	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Teams/SfB user rings and the IVR number also rings simultaneously
2	Device receives the INVITE for IVR number from Teams SIP Proxy	Device process the simultaneous call towards PSTN

3	Allow the IVR endpoint to answer the call	Device receives 200 OK from PSTN side for the IVR number call and forwards the same to Direct Routing in the second call leg
4	Call gets established between the PSTN user and IVR endpoint	Verify if the PSTN end point is able to hear the IVR menu played after 200 OK
5	PSTN user hangs up	Call is disconnected

6.1.6 Transfers

Device must be able to handle **REFER** based transfers and the **Referred-by** header which carries information of the referrer or the transferring party in a call transfer to PSTN scenario.

Please read section 6.7 “Refer method” of Appendix 1. Direct Routing SIP Protocol Description

6.1.6.1 Blind Transfer with REFER

6.1.6.1.1 Inbound PSTN Call to Teams blind transferred to Skype For Business user

ID	43955	
Priority	1	
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams/SfB user	Teams/SfB user answers the call and call is connected with bidirectional audio
2	Teams/SfB user transfers the call to Skype for Business user	Device processes the REFER sent by Teams SIP Proxy and responds with 202 Accepted
3	Device sends a new INVITE containing "Replaces" and "Referred-By" headers to Teams SIP Proxy	Call is connected with bidirectional audio between PSTN user and Skype for Business user
4	PSTN user hangs up	Call is disconnected

6.1.6.1.2 Inbound PSTN Call to Teams blind transferred to Teams User

ID	43956
Priority	1
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user 1	Teams user 1 answers the call and call is connected with bidirectional audio
2	Teams user 1 transfers the call to Teams user 2	Device processes the REFER sent by Teams SIP Proxy and responds with 202 Accepted
3	Device sends a new INVITE containing "Replaces" and "Referred-By" headers to Teams SIP Proxy	Call is connected with bidirectional audio between PSTN user and Teams user 2
4	PSTN user hangs up	Call is disconnected

6.1.6.1.3 Inbound PSTN Call to Teams blind transferred to another PSTN User

ID	43957
Priority	1
Summary	[Objective] Device handles the REFER for a blind transfer call initiated by the Teams user to a PSTN user [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is connected with bi-directional audio
2	Teams user blind transfers the call to PSTN user 2	Device accepts the REFER and responds with 202 Accepted
3	PSTN user 2 picks up	Bi-directional audio is established between PSTN user 1 and PSTN user 2
4	PSTN user 1 hangs up	Call is disconnected

6.1.6.1.4 Outbound PSTN call from Teams user blind transferred to Skype for Business User

ID	43958
Priority	1
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is established with bi-directional audio

2	Teams user transfers the call to Skype for Business user	Device processes the REFER sent by Teams SIP Proxy and responds with 202 Accepted
3	Device sends a new INVITE containing "Replaces" and "Referred-By" headers to Teams SIP Proxy	Call is connected with bidirectional audio between PSTN user and Skype for Business user
4	PSTN user hangs up	Call is disconnected

6.1.6.1.5 Outbound PSTN call from Teams user blind transferred to Teams User

ID	43959	
Priority	1	
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams user 1 calls PSTN user	Call is connected with bi-directional audio
2	Teams user 1 transfers the call to Teams user 2	Device processes the REFER sent by Teams SIP Proxy and responds with 202 Accepted
3	Device sends a new INVITE containing "Replaces" and "Referred-By" headers to Teams SIP Proxy	Call is connected with bidirectional audio between PSTN user and Teams user 2
4	PSTN user hangs up	Call is disconnected

6.1.6.1.6 Outbound PSTN call from Teams user blind transferred to PSTN User

ID	43960	
Priority	1	
Summary	[Objective] Device handles the REFER for a blind transfer call initiated by the Teams user to a PSTN user [Pre-Condition] - REFER support enabled on Device	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user 1	Call is connected with bi-directional audio
2	Teams user blind transfers the call to PSTN user 2	Device accepts the REFER and responds with 202 Accepted
3	PSTN user 2 picks up	Bi-directional audio is established between PSTN user 1 and PSTN user 2
4	PSTN user 1 hangs up	Call is disconnected

6.1.6.1.7 Inbound call to Teams user transferred to Teams pure online user that has call forward to PSTN (Microsoft calling plan)

ID	43962
Priority	1
Summary	[Objective] Device handles REFER for a transferred call [Pre-Condition] - Two Teams users: User 1 configured for Direct Routing and User 2 configured with Microsoft Calling Plan
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user 1	Call is established with bi-directional audio
2	Teams user transfers the call to Teams user 2	Teams user 2 rings
3	Teams user 2 picks up	Call is established with bi-directional audio between PSTN user and Teams user 2
4	PSTN user hangs up	Call is disconnected

6.1.6.1.8 Device maintains the original session when the blind transferred call (with REFER) fails

ID	49220
Priority	1
Summary	[Objective] Device maintains the original session when a blind transferred call (with REFER) fails. [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Device receives INVITE and call is connected with bi-directional audio
2	Teams user transfers the call to an invalid number, Teams SIP Proxy sends a INVITE (hold) to Device	Device responds with 200 OK for the hold INVITE
3	Teams SIP Proxy sends a REFER to Device	Device processes the REFER and responds with 202 Accepted
4	Device forwards the appropriate cause received from PSTN user for dialog 2 to Teams SIP Proxy	Dialog 2 is disconnected and dialog 1 with PSTN user 1 is in hold state
5	Teams user resumes dialog 1	Call is connected with bi-directional audio
6	PSTN user hangs up	Call is disconnected

6.1.6.2 Consultative Transfer

6.1.6.2.1 *Inbound PSTN Call to Teams consultative transferred to Skype for Business user*

ID	43969
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user makes a consultation call to Skype for Business user	PSTN user goes on hold and Skype for business user rings
3	Skype for Business user picks up	Call is established between Skype for Business user and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user to Skype for Business user	Device accepts the REFER with Refer-to header from Teams SIP Proxy and call is established between PSTN user and Skype for Business user with bi-directional audio
5	PSTN user hangs up	Call is disconnected

6.1.6.2.2 *Inbound PSTN Call to Teams consultative transferred to Teams User*

ID	43970
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user 1	Call is connected with bi-directional audio
2	Teams user 1 makes a consultation call to Teams user 2	PSTN user goes on hold and Teams user 2 rings
3	Teams user 2 picks up	Call is established between Teams user 2 and Teams user 1 with bi-directional audio
4	Teams user 1 transfers the call with PSTN user to Teams user 2	Device accepts the REFER with Refer-to header from Teams SIP Proxy and call is established between PSTN user and Teams user 2 with bi-directional audio
5	PSTN user hangs up	Call is disconnected

6.1.6.2.3 *Inbound PSTN Call to Teams consultative transferred to another PSTN User*

ID	43971

Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is connected with bi-directional audio
2	Teams user makes a consultation call to PSTN user 2	PSTN user 1 goes on hold and PSTN user 2 rings
3	PSTN user 2 picks up	Call is established between PSTN user 2 and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user 1 to PSTN user 2	Device accepts the REFER with Refer-to header from Teams SIP Proxy and call is established between PSTN user 1 and PSTN user 2 with bi-directional audio
5	PSTN user 1 hangs up	Call is disconnected

6.1.6.2.4 Outbound PSTN call from Teams user consultative transferred to Skype for Business User

ID	43972
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user makes a consultation call to Skype for Business user	PSTN user goes on hold and Skype for business user rings
3	Skype for Business user picks up	Call is established between Skype for Business user and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user to Skype for Business user	Device accepts the REFER with Refer-to header from Teams SIP Proxy and call is established between PSTN user and Skype for Business user with bi-directional audio
5	PSTN user hangs up	Call is disconnected

6.1.6.2.5 Outbound PSTN call from Teams user consultative transferred to Teams User

ID	43973
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side

	[Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user 1 calls PSTN user	Call is connected with bi-directional audio
2	Teams user 1 makes a consultation call to Teams user 2	PSTN user goes on hold and Teams user 2 rings
3	Teams user 2 picks up	Call is established between Teams user 2 and Teams user 1 with bi-directional audio
4	Teams user 1 transfers the call with PSTN user to Teams user 2	Device accepts the REFER with Refer-to header from Teams SIP Proxy and call is established between PSTN user and Teams user 2 with bi-directional audio
5	PSTN user hangs up	Call is disconnected

6.1.6.2.6 Outbound PSTN call from Teams user consultative transferred to PSTN User

ID	43974
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Call is connected with bi-directional audio
2	Teams user makes a consultation call to PSTN user 2	PSTN user 1 goes on hold and PSTN user 2 rings
3	PSTN user 2 picks up	Call is established between PSTN user 2 and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user 1 to PSTN user 2	Device accepts the REFER with Refer-to header from Teams SIP Proxy and call is established between PSTN user 1 and PSTN user 2 with bi-directional audio
5	PSTN user 1 hangs up	Call is disconnected

6.1.6.2.7 Device maintains the original session when the consultation call fails

ID	49255
Priority	1
Summary	[Objective] Device is able to handle the consultative transfer performed on Teams side

	[Pre-Condition] - REFER support enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Device receives INVITE and call is connected with bi-directional audio
2	Teams user initiates a consultation call to invalid PSTN number 2, Teams SIP Proxy sends a INVITE (hold) to Device	Device responds with 200 OK for the hold INVITE
3	Teams SIP Proxy sends a REFER to Device	Device processes the REFER and responds with 202 Accepted
4	Device forwards the appropriate cause received from PSTN user for the second call to Teams SIP Proxy	Second call is disconnected and first call with PSTN user 1 is in hold state
5	Teams user resumes first call	Call is connected with bi-directional audio
6	PSTN user hangs up	Call is disconnected

6.1.7 Call forward and Simultaneous Ring and Call forking

6.1.7.1 PSTN User calls a Teams user that has forwarded calls to Delegates

ID	43981
Priority	1
Summary	[Objective] Device can handle an inbound call to Teams user forwarded to its delegates. [Pre-Condition] - Set call forward to 'Delegates' in Teams client
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Delegates starts ringing and ring back is heard
2	One of the delegates picks up	Other delegates stop ringing and call is connected with bi-directional audio
3	PSTN user hangs up	Call is disconnected

6.1.7.2 Inbound call to Teams that is forwarded to voicemail after no response and voicemail is left (Azure VM)

ID	43983
Priority	1
Summary	[Objective] Device handles an inbound call from PSTN to Teams user which is forwarded to

	Azure Voicemail. [Pre-Condition] - Teams user with Azure Voicemail enabled		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Teams user rings	
2	Teams user does not answer the call	Call is forwarded to Azure Voicemail due to no response timeout	
3	PSTN user leaves voicemail	Voicemail is successfully deposited	
4	Use DTMF to navigate the voicemail system	DTMF tones are recognized by the voicemail system	

6.1.7.3 Inbound call to Teams that is forwarded to voicemail after no response and disconnected without leaving voicemail

ID	43984	
Priority	1	
Summary	[Objective] Device is able to handle an inbound call to Teams user forwarded to voicemail after no response. [Pre-Condition] - Unanswered calls forward to voicemail is set in Teams Client settings	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Teams user starts ringing
2	Teams user does not answer the call	Call gets forwarded to voicemail
3	PSTN End Point disconnects the call without leaving voicemail	Call is disconnected

6.1.7.4 PSTN user calls Teams user that simultaneously rings another PSTN user and PSTN user answers

ID	43985	
Priority	1	
Summary	[Objective] Device is able to support the simultaneous ring functionality. [Pre-Condition] - Configure Teams user to simultaneous ring at another PSTN user 2 - Enable Forward Call History and PAI on Teams tenant trunk configuration	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user 1 calls Teams user	Both the Teams user and PSTN user 2 ring and ringback is heard on PSTN user 1
2	PSTN user 2 picks up	PSTN user 2 and PSTN user 1 are connected with bi-directional audio
3	PSTN user 1 hangs	Call is disconnected

6.1.7.5 PSTN user calls Teams user that simultaneously rings another PSTN user and Teams user answers

ID	43986
Priority	1
Summary	[Objective] Device is able to support the simultaneous ring functionality. [Pre-Condition] - Configure Teams Client to simultaneous ring at another PSTN End Point 2 - Enable Forward Call History and PAI on Teams tenant trunk configuration
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Both the Teams user and PSTN user 2 ring and ringback is heard on PSTN user 1
2	Teams user picks up	Teams user and PSTN user 1 are connected with bi-directional audio
3	Device processes the CANCEL received for the call to PSTN user 2	Call to PSTN user 2 is terminated successfully
4	PSTN user 1 hangs up	Call is disconnected

6.1.7.6 PSTN user calls Teams user that simultaneously rings delegates and PSTN user hangs up due to no response

ID	43987
Priority	1
Summary	[Objective] Device should handle an inbound call to Teams user who is set to simultaneous ring on delegates. [Pre-Condition] - Teams user set to simultaneous ring on delegates
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN End Point calls Teams user	Teams user and its delegates ring simultaneously
2	Teams user and its delegates does not pick up	Call is still ringing
3	PSTN user hangs up	Call is cancelled successfully

6.1.7.7 PSTN user calls Teams user that simultaneously rings delegates and one of the delegates responds

ID	43988
Priority	1
Summary	[Objective] Device should handle an inbound call to Teams user who is set to simultaneous ring on delegates and one of delegate answers. [Pre-Condition] - Teams user set to simultaneous ring on delegates

Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Teams user and its delegates ring simultaneously	
2	One of the delegates picks up	Call is connected with bi-directional audio	
3	PSTN user hangs up	Call is disconnected	

6.1.7.8 PSTN user calls Teams user that is logged into two different clients (eg desktop and mobile) and Teams user responds from one machine

ID	43989	
Priority	1	
Summary	[Objective] Device should handle an inbound call to Teams user logged in different devices and answered at any one device. [Pre-Condition] - Login Teams user in different devices (example: Teams Client, Teams Mobile App and Web Browser)	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Teams user starts ringing in all the devices wherever logged in
2	Teams user in any one of the device answers	Call is connected with bi-directional audio
3	PSTN user hangs up	Call is disconnected

6.1.7.9 PSTN user calls Teams user that is forwarded to second PSTN user

ID	47070	
Priority	1	
Summary	[Objective] Device is able to handle the forwarded call by Teams user to second PSTN user. [Pre-Condition] - Teams user is set call forward unconditional to PSTN number - Enable Forward Call History and PAI on Teams tenant trunk configuration	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user 1 calls Teams user	PSTN user 2 rings
2	PSTN user 2 picks up	Call is established with bi-directional audio between PSTN user 1 and PSTN user 2
3	PSTN user 1 hangs up	Call is disconnected

6.1.8 1:1 to Group Call Escalation

6.1.8.1 Teams user calls another Teams user and then adds another PSTN user and participants mutes and unmute themselves

ID	44001
Priority	1
Summary	
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user 1 calls Teams user 2	Teams user 1 and Teams user 2 are connected with bi-directional audio
2	Teams user 1 escalates the ongoing call to a group call by adding a PSTN user	PSTN user rings
3	PSTN user picks up	PSTN user joins the group call successfully
4	Teams user 1 mutes himself	Other participants can still hear each other but not Teams user 1. Teams user 1 can hear both participants
5	Teams user 1 unmutes himself	All participants can hear each other
6	Repeat steps 5 & 6 with Teams user 2	
7	Teams user 1 removes the PSTN user	PSTN user leaves group call and PSTN call is disconnected. Teams users can still hear each other

6.1.8.2 Teams user calls PSTN user and then adds another PSTN user and participants mute and unmute the PSTN users

ID	44002
Priority	1
Summary	
Applicable	Future case, not yet supported (will be applicable to Non-Media Bypass and Media Bypass calls)

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Call is connected with bi-directional call
2	Teams user escalates the ongoing call to a group call by adding PSTN user 2	PSTN user 2 rings
3	PSTN user 2 picks up	PSTN user 2 joins the group call successfully and all participants can hear each other
4	Teams user mutes PSTN user1	Participants can hear each other but nobody can hear PSTN user1. PSTN user 1 can hear both participants
5	Teams user removes the PSTN user 2 from the group call	PSTN user 2 leaves group call
6	PSTN user 1 disconnects	PSTN user 1 leaves group call

6.1.8.3 PSTN user calls Teams user who escalates the call to group call by adding another PSTN user

ID	44003
Priority	1
Summary	
Applicable	Future case, not yet supported (will be applicable to Non-Media Bypass and Media Bypass calls)

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is connected with bi-directional audio
2	Teams user escalates the ongoing call to group call by adding PSTN user 2	PSTN user 2 rings
3	PSTN user 2 picks up	PSTN user 2 joins the group call successfully
4	PSTN user 1 and 2 disconnects	PSTN user 1 and 2 leaves group call

6.1.8.4 Teams user calls PSTN user and then adds another Teams user

ID	49222
Priority	1
Summary	[Objective] Teams user calls PSTN user and then adds another teams user by escalating the call to group call
Applicable	Future case, not yet supported (will be applicable to Non-Media Bypass and Media Bypass calls)

Step	Action	Expected Result
1	Teams user 1 calls PSTN user	Call is connected with bi-directional audio
2	Teams user 1 escalates the call to group call by adding Teams user 2 to the call	All three users are connected
3	Teams user 1 removes Teams user 2 from the group call	Teams user 2 gets disconnected
4	Remaining users disconnect their respective calls	Users are disconnected

6.1.8.5 PSTN user calls Teams user and then adds another Teams user

ID	49380
Priority	1
Summary	[Objective] PSTN user calls Teams user and then adds another teams user by escalating the call to group call
Applicable	Future case, not yet supported (will be applicable to Non-Media Bypass and Media Bypass calls)

Step	Action	Expected Result
1	PSTN user calls Teams user 1	Call is connected with bi-directional audio
2	Teams user 1 escalates the call to group call by adding Teams user 2 to the call	All three users are connected

3	Teams user 1 removes Teams user 2 from the group call	Teams user 2 gets disconnected
4	Remaining users disconnect their respective calls	Teams user 2 gets disconnected

6.1.9 Auto Attendant (Required for V2)

6.1.9.1 Inbound call to a Teams auto attendant transferred to a Teams user after menu option selection

ID	44006	
Priority	1	
Summary	[Objective] Device is able to handle an inbound call from PSTN to Teams auto attendant number [Pre-Condition] - Auto Attendant configured on Teams side	
Applicable	Future case, not yet supported (will be applicable to Non-Media Bypass and Media Bypass calls)	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams Auto Attendant number	Call is connected with Auto Attendant
2	PSTN user navigates the menu to select the transfer to user option and inputs the Teams user identity	Call is transferred to Teams user
3	Teams user answers the call	Teams user and PSTN user are connected with bi-directional audio
4	PSTN user hangs up	Call is disconnected

6.1.9.2 Inbound call to Teams user transferred to a Skype for Business auto attendant number after menu option selection

ID	44007	
Priority	1	
Summary	[Objective] Device is able to handle a transfer initiated by Teams to Skype for Business user's auto attendant number [Pre-Condition] - Auto attendant is configured on Skype for Business user side	
Applicable	Future case, not yet supported (will be applicable to Non-Media Bypass and Media Bypass calls)	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Call is connected with bi-directional audio

2	Teams user blind transfers the call to Skype for Business auto attendant number	Call is transferred successfully and PSTN user hears the auto attendant menu
3	PSTN user navigates the menu and requests for a transfer to Skype for Business user	Skype for Business user rings
4	Skype for Business user picks kup	Call is connected with bi-directional audio between PSTN user and Skype for Business user
5	PSTN user hangs up	Call is disconnected

6.1.10 Call Queues (required for V2)

6.1.10.1Inbound calls to a Teams call queue plays music on hold and then rings the teams call agents assigned to that queue

ID	44008
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to Teams call queue number [Pre-Condition] - Call queue is configured on Teams side with a PSTN number assigned - Teams users are assigned to the Call queue as agents
Applicable	Non-Media Bypass and Media Bypass calls

Step	**Action**	**Expected Result**
1	PSTN user calls Teams Call queue	PSTN user hears MOH/greeting configured for the call queue and the teams call agents rings
2	One of agent picks up	Call is connected with bi-directional audio between the PSTN user and Teams call agent
3	PSTN user hangs up	Call is disconnected

6.2 Codec support

Device must support SILK, G711, G729 codecs

6.2.1 SILK codec support

6.2.1.1 Teams User Calls PSTN User with SILK and other Codecs enabled at tenant and all the same codecs offered by the customer's SIP Trunk

ID	44009
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user to PSTN user with SILK codecs present in the offer SDP

	[Pre-Condition] - SILK Codec enabled on Teams side - SILK Codec enabled on Device side - SILK codec Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	The INVITE from Teams has SILK and other Codecs enabled at tenant
2	PSTN user rings	Call is connected with bi-directional audio
3	Teams user hangs up	Call is disconnected

6.2.1.2 PSTN User calls Teams user with SILK and other Codecs offered by customer's trunk and the same codecs enabled at the tenant

ID	44010
Priority	1
Summary	[Objective] Device should be able to accept and handle the codecs from PSTN side and towards Teams SIP Proxy [Pre-Condition] - Configure device to use SILK codecs and other codecs towards Teams SIP proxy - Configure device to use the supported codecs on PSTN side - SILK codec Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is answered and established with bi-directional audio
2	Device sends INVITE to Teams SIP Proxy with SILK codecs included in the SDP	The SDP part contains SILK codecs along with the other supported codecs
3	PSTN user hangs up	Call is disconnected

6.2.1.3 Device must not offer SILK and other codecs in final offer unless it supports transcoding to and from SILK codec

ID	44011
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user to PSTN user with SILK codecs present in the offer SDP [Pre-Condition] - SILK Codec enabled on Teams side - SILK Codec enabled on Device side - SILK codec Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio

2	Device does not offer SILK codec in its final offer	SILK codec is not negotiated
3		Codec negotiated and used is other than SILK codec
4	Teams user hangs up	Call is disconnected

6.2.2 SILK Codec Transcoding (Required to be supported by Dec 2018)

6.2.2.1 PSTN User calls Teams user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer's SIP trunk

ID	49026	
Priority	1	
Summary	[Objective] Device is able to handle an inbound call from PSTN user to Teams user when only SILK codec is enabled on the trunk towards Teams but not on the trunk towards customer's SIP Trunk [Pre-Condition] - SILK Codec enabled on Device towards Teams - SILK Codec disabled on Device towards customer SIP Trunk - Transcoding enabled on Device	
Applicable	Only applicable to devices which support transcoding Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Device offers only SILK codec towards Teams SIP Proxy	Call is established with SILK codec between Device and Teams SIP Proxy
3	Device does not respond with SILK codec towards customer's SIP trunk	Call is established with any codec other than SILK between Device and customer's SIP trunk
4	PSTN user hangs up	Call is disconnected

6.2.2.2 Teams user calls PSTN user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer's SIP trunk

ID	49027
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user to PSTN user when only SILK codec is enabled on the trunk towards Teams but not on the trunk towards customer's SIP Trunk

	[Pre-Condition] - SILK Codec enabled on Device towards Teams - SILK Codec disabled on Device towards customer SIP Trunk - Transcoding enabled on Device
Applicable	Only applicable to devices which support transcoding Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device does not offer SILK codec towards customer's SIP trunk	Call is established with any codec other than SILK between Device and customer's SIP trunk
3	Device responds with only SILK codec towards Teams SIP Proxy	Call is established with SILK codec between Device and Teams SIP Proxy
4	Teams user hangs up	Call is disconnected

6.3 Media Requirements

6.3.1 Media Bypass: ICE Lite and MS Turn support

Please read the section 7.1 "Ice Lite Requirements" in Appendix 2. Media and Encryption Requirements

6.3.1.1 Device can establish a direct media connection with Teams client for an outbound all to IVR

ID	44026
Priority	1
Summary	[Objective] Device must be able to accept Icelite candidates and accept direct media connection with Teams client [Pre-condition] - Ensure the Teams client is behind the firewall, in the same network as the Device
Applicable	Media Bypass only

Step	Action	Expected Result
1	Teams client calls PSTN endpoint	Device responds with Ice candidates in the 183 SDP
2		Teams user can hear early media from the IVR
3		Teams user can navigate IVR menu using DTMF
4	Call is established	Call is connected with bi-directional audio
5		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
6	Teams client hangs up the call	Call is disconnected

6.3.1.2 Device can establish a direct media connection with Teams client for an inbound call

ID	[44027]
Priority	1
Summary	[Objective] Device must be able to accept Icelite candidates and accept direct media connection with Teams client [Pre-condition] - Ensure the Teams client is behind the firewall, in the same network as the Device
Applicable	Media Bypass only

Step	Action	Expected Result
1	PSTN user calls Teams user	Device offers ICE candidates in the INVITE SDP, teams user rings and ring back is heard on PSTN side
2		Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
4	PSTN user hangs up the call	Call is disconnected

6.3.1.3 Device can establish media connection with Teams client behind a firewall in a different network (eg home) for outbound call to IVR

ID	[44030]
Priority	1
Summary	[Objective] Device can establish media connection with Teams client behind a firewall in a different network (eg: home network) for outbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network)
Applicable	Media Bypass only (only for SBCs which support ICE Lite with NAT)

Step	Action	Expected Result
1	Teams user calls PSTN user	Device responds with Ice candidates in the 183 SDP
2		Teams user can hear early media from the IVR
3		Teams user can navigate IVR menu using DTMF
4	Call is established	Call is connected with bi-directional audio
5		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
6	Teams client hangs up the call	Call is disconnected

6.3.1.4 Device can establish media connection with Teams client behind a firewall in a different network (eg home) for inbound call

ID	44031
Priority	1
Summary	[Objective] Device can establish media connection with Teams client behind a NAT in a different network (eg: home network) for inbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network)
Applicable	Media Bypass only (only for SBCs which support ICE Lite with NAT)

Step	Action	Expected Result
1	PSTN user calls Teams user	Device offers ICE candidates in the INVITE SDP, teams user rings and ring back is heard on PSTN side
2		Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
4	PSTN user hangs up the call	Call is disconnected

6.3.1.5 Device can establish media connection with Teams client behind a firewall in a different network via relay server for outbound call to IVR

ID	49008
Priority	1
Summary	[Objective] Device can establish media connection with Teams client behind a NAT in a different network (eg: home network) for outbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network) and block the reflexive IP of the Teams client from being able to access the Device IP
Applicable	Media Bypass only

Step	Action	Expected Result
1	Teams user calls PSTN user (sends relay candidates with higher priority)	Device responds with Ice candidates in the 183 SDP
2		Teams user can hear early media from the IVR which is established via the relay server
3		Teams user can navigate IVR menu using DTMF
4	Call is established	Call is connected with bi-directional audio
5		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
6	Teams client hangs up the call	Call is disconnected

6.3.1.6 Device can establish media connection with Teams client behind a NAT in a different network via relay server for inbound call

ID	[49009](#)		
Priority	1		
Summary	[Objective] Device can establish media connection with Teams client behind a NAT in a different network (eg: home network) for inbound call or if a device doesn't support NAT validate routing of media via Microsoft TURN servers [Pre-condition] - Ensure the Teams user is in a different network (eg: home network) and block the reflexive IP of the Teams client from being able to access the Device IP		
Applicable	Media Bypass only		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Device offers ICE candidates in the INVITE SDP, teams user rings and ring back is heard on PSTN side	
2		Call is connected with bi-directional audio	
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media via the relay server	
4	PSTN user hangs up the call	Call is disconnected	

6.3.1.7 Device can route calls from Teams user in Tenant-A to Teams user in Tenant-B

ID	[49671](#)	
Priority	1	
Summary	[Objective] Device can route the calls from a Teams user in Tenant-A to Teams user in Tenant-B when the Teams user is called using DID. [Pre-Condition] - Device is paired with Tenant-A and Tenant-B - Device is configured with internal call routing for calls between two tenants using DID	
Applicable	Media Bypass only	
Step	**Action**	**Expected Result**
1	Teams user (Tenant-A) calls Teams user (Tenant-B)	Call is connected with bi-directional audio
2		Call is routed Via the SBC without going to the PSTN, call escalated from Media Bypass to non-Bypass mode
3	Teams user (Tenant-A) hangs up	Call is disconnected

ID	[49672](#)
Priority	1
Summary	[Objective] Device can work with MS Turn relay [Pre-Condition] - Device is paired , voice routing configured

	- Device is whitelisted only to receive media from Office 365 IP range (https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges) - Client is in external network (the client IP is not whitelisted on SBC)
Applicable	Media Bypass only

Step	Action	Expected Result
1	Client makes a call	Call is connected with bi-directional audio In SDP there is indication of using MS Turn Server in 200 OK message

6.3.2 SRTP

Please refer to 7.2 "Encryption cipher and MKI requirements" in Appendix 2. "Media and Encryption Requirements"

6.3.2.1 Device sends crypto attributes in SDP for call from PSTN End Point to Teams Client

ID	43905
Priority	1
Summary	[Objective] Device is able to send crypto attributes in SDP for a TLS-SRTP call [Pre-Condition] - SRTP enabled on Device - SRTP enabled on Teams side - Media Bypass OFF on Teams side
Applicable	Non-Media Bypass only

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends crypto attributes in the INVITE's SDP sent to Teams SIP Proxy representing SDES or SDES with DTLS Optional media security method
2	Teams user picks up	Call is established with bi-directional audio
3	PSTN user hangs up	Call is disconnected

6.3.2.2 Device sends crypto attributes in SDP for call from Teams Client to PSTN End Point

ID	43906
Priority	1
Summary	[Objective] Device is able to send crypto attributes in SDP for a TLS-SRTP call [Pre-Condition] - SRTP enabled on Device - SRTP enabled on Teams side - Media Bypass OFF on Teams side

Applicable	Non-Media Bypass only

Step	Action	Expected Result
1	Teams user calls PSTN user	Device sends crypto attributes in the response message (18x, 200) SDP sent to Teams SIP Proxy
2	PSTN user picks up	Call is established with bi-directional audio
3	Teams user hangs up	Call is disconnected

6.3.2.3 Teams users make outgoing calls via web browser (Microsoft Edge)

ID	47915
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Microsoft Edge)
Applicable	Non-Media Bypass (scenario will be supported for Media Bypass in future)

Step	Action	Expected Result
1	Teams user from web browser calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

6.3.2.4 Teams users receives inbound calls via web browser (Microsoft Edge)

ID	47916
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Microsoft Edge)
Applicable	Non-Media Bypass (scenario will be supported for Media Bypass in future)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

6.3.2.5 Teams users make outgoing calls via web browser (Mozilla Firefox) -future case, until notice Microsoft doesn't support Firefox

ID	47917
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user

	[Pre-Condition] - Teams user logged in using web browser (Mozilla Firefox)
Applicable	Non-Media Bypass (scenario will be supported for Media Bypass in future)

Step	Action	Expected Result
1	Teams user from web browser calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

6.3.2.6 Teams users receives inbound calls via web browser (Mozilla Firefox) -future case, until notice Microsoft doesn't support Firefox

ID	47918
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Mozilla Firefox)
Applicable	Non-Media Bypass (scenario will be supported for Media Bypass in future)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

6.3.2.7 Teams users make outgoing calls via web browser (Chrome)

ID	47919
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Chrome)
Applicable	Non-Media Bypass (scenario will be supported for Media Bypass in future)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

6.3.2.8 Teams users receives inbound calls via web browser (Chrome)

ID	47920
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in

	via web browser [Pre-Condition] - Teams user logged in using web browser (Chrome)
Applicable	Non-Media Bypass (scenario will be supported for Media Bypass in future)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

6.3.2.9 Device does not change the SSRC of an established inbound secure RTP session

ID	49010
Priority	1
Summary	[Objective] During an inbound call, the SSRC field in the secure RTP packets is not changed. The SSRC value remains unchanged from the time the secure RTP session was established to the end of the session.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTP packet
4	PSTN user hangs up	Call is disconnected

6.3.2.10 Device does not change the SSRC of an established inbound secure RTCP session

ID	49011
Priority	1
Summary	[Objective] During an inbound call, the SSRC field in the secure RTCP packets is not changed. The SSRC value remains unchanged from the time the secure RTCP packets being sent by Device till the end of the session.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTCP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTCP packet
4	PSTN user hangs up	Call is disconnected

6.3.2.11 Device does not change the SSRC of an established outbound secure RTP session

ID	49012
Priority	1
Summary	[Objective] During an outbound call, the SSRC field in the secure RTP packets is not changed. The SSRC value remains unchanged from the time the secure RTP session was established to the end of the session.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTP packet
4	Teams user hangs up	Call is disconnected

6.3.2.12 Device does not change the SSRC of an established outbound secure RTCP session

ID	49013
Priority	1
Summary	[Objective] During an outbound call, the SSRC field in the secure RTCP packets is not changed. The SSRC value remains unchanged from the time the secure RTCP packets being sent by Device till the end of the session.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTCP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTCP packet
4	Teams user hangs up	Call is disconnected

6.3.3 DTMF support

6.3.3.1 Device offers DTMF payload type in the range of 96-127 to Teams SIP Proxy

ID	43907
Priority	1
Summary	[Objective] Device must offer DTMF payload type in the range of 96-127 and must indicate support for telephony events. [Pre-condition] - Set the DTMF transport type on the Device to support RFC 2833.

Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Teams SIP Proxy receives INVITE from Device	
2		The INVITE's SDP contains the DTMF payload type in the range of 96-127	
3		Events parameter associated with the telephone-event media type is included and indicates support for events 0-15 or 0-16	
4		Call is established with bi-directional audio	
5	Teams user hangs up	Call is disconnected	

6.3.3.2 Teams user calls an IVR number and navigates through the IVR menu after call connection

ID	43908	
Priority	1	
Summary	[Objective] Teams user is able to navigate through the Interactive Voice Response Menu and Device is able to process the DTMF digits received from Teams. The digits are sent to Device after 200 OK is received and RTP stream established.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams user calls an IVR number	IVR menu is played after 200 OK is received from Device
2	Navigate through the IVR menu (ANY LEVEL of the IVRMENU)	Call is not dropped and digits are recognized by the remote system
3	Teams user hangs up	Call is disconnected

6.3.3.3 Teams user calls an IVR number and navigates through the IVR menu before call connection

ID	43909	
Priority	1	
Summary	[Objective] Teams user is able to navigate the Interactive Voice Response Menu and Device processes the DTMF digits received from Teams.	
Applicable	Non-Media Bypass and Media Bypass	
Step	**Action**	**Expected Result**
1	Teams user calls IVR number	IVR menu is played before 200 OK is received from Device
2	Navigate through the IVR menu (ANY LEVEL of the IVRMENU)	Call is not dropped and digits entered by the Teams user are recognized by the remote system
3	Teams user hangs up	Call is disconnected

6.3.3.4 Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR

ID	43910		
Priority	1		
Summary	[Objective] This Test case aims to verify Rapid DTMF Digit Handling by the Device when user pastes a string of digits such as a Conference ID into Teams Client.		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	Teams user calls IVR number for joining a conference by ID (external conference such as Webex)	Call is connected, 200 OK is received from Device	
2	Join the conference by pasting a conference ID from the client.	Call is not dropped and digits pasted by the Teams Client are recognized by the DUT and IVR.	
3	Teams user hangs up	Call is disconnected	

6.3.4 Comfort Noise Passthrough and Generation

6.3.4.1 Device offers comfort noise payload in the INVITE's SDP to SIP Proxy even when not offered by the carrier

ID	43911	
Priority	1	
Summary	[Objective] Device should offer/negotiate comfort noise payload in the SDP to SIP Proxy even when the carrier does not offer them. [Pre-condition] - Comfort Noise enabled on Device.	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user.	Device sends INVITE to Teams SIP Proxy. The SDP contains the Comfort Noise payload type 13.
2	Teams user answers the call.	Call is established with bi-directional audio.
3	PSTN user hangs up.	Call is disconnected.

6.3.4.2 Device sends comfort noise packets to Teams when PSTN user mutes an outbound call

ID	43912
Priority	1
Summary	[Objective] After Comfort Noise negotiation, Device sends Comfort Noise packets when PSTN

	user mutes the call. [Pre-condition] - Comfort Noise enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Mute the call on the PSTN user for 3 minutes	Verify Comfort Noise packets are sent from the Device to Teams SIP Proxy
3		Unidirectional audio from Teams user to the PSTN user
4		Call stays connected on mute for 3 minutes
5	Teams user hangs up	Call is disconnected

6.3.4.3 Device sends comfort noise packets to Teams when PSTN user mutes an inbound call

ID	43913
Priority	1
Summary	[Objective] After Comfort Noise negotiation, Device sends Comfort Noise packets when PSTN user mutes the call. [Pre-condition] - Comfort Noise enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Mute the call on the PSTN user for 3 minutes	Verify that Comfort Noise packets are sent from the Device to Teams SIP Proxy
3		Unidirectional audio from Teams user to the PSTN user
4		Call stays connected on mute for 3 minutes
5	PSTN user hangs up	Call is disconnected

6.3.4.4 Teams user mutes an Inbound call from PSTN and then unmutes

ID	43936
Priority	1
Summary	[Objective] Device is able to handle an inbound call muted on Teams user and is able to keep the call connected on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN End Point calls Teams client	Call is connected with bi-directional audio
2	Teams Client mutes the call for 3 minutes	Media capture indicates Comfort Noise packets are received from Teams SIP Proxy

3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 3 minutes
5	PSTN user hangs up	Call is disconnected

6.3.4.5 Teams user mutes an Outbound call to PSTN and then unmutes

ID	43937	
Priority	1	
Summary	[Objective] Device is able to handle an outbound call muted on Teams user and is able to keep the call connected on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user mutes the call for 3 minutes	Media capture indicates Comfort Noise packets are received from Teams SIP Proxy
3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 3 minutes
5	Teams user hangs up	Call is disconnected

6.3.4.6 Teams user mutes outbound call to PSTN for over 30 minutes and then unmutes

ID	43938	
Priority	1	
Summary	[Objective] Device is able to handle an outbound call muted by Teams user and is able to keep the call connected for 30 minutes on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are received from Teams SIP Proxy
3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 30 minutes
5	Teams user hangs up	Call is disconnected

6.3.4.7 Teams user mutes inbound call from PSTN for over 30 minutes and then unmutes

ID	[43939](43939)		
Priority	1		
Summary	[Objective] Device is able to handle an inbound call muted by Teams user and is able to keep the call connected for 30 minutes on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Call is connected with bi-directional audio	
2	Teams user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are received from Teams SIP Proxy	
3		Unidirectional audio is present from PSTN user to Teams user	
4		Call stays connected on mute for 30 minutes	
5	PSTN user hangs up	Call is disconnected	

6.3.4.8 PSTN user mutes outbound call to PSTN for over 30 minutes and then unmutes

ID	[47927](47927)		
Priority	1		
Summary	[Objective] Device can handle an outbound call muted on PSTN side and is able to keep the call connected for 30 minutes on sending comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	Teams user calls PSTN user	Call is connected with bi-directional audio	
2	PSTN user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are sent by device	
3		Unidirectional audio is present from Teams user to PSTN user	
4		Call stays connected on mute for 30 minutes	
5	Unmute the call	Two-way audio is present	
6	Teams user hangs up	Call is disconnected	

6.3.4.9 PSTN user mutes inbound call to Teams user for over 30 minutes and then unmutes

ID	[47928](47928)

Priority	1
Summary	[Objective] Device can handle an inbound call muted on PSTN side and is able to keep the call connected for 30 minutes on sending comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN End Point calls Teams client	Call is connected with bi-directional audio
2	PSTN user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are sent by device
3		Unidirectional audio is present from Teams user to PSTN user
4		Call stays connected on mute for 30 minutes
5	Unmute the call	Two-way audio is present
6	PSTN user hangs up	Call is disconnected

6.3.5 RTCP

6.3.5.1 RTCP Generation

6.3.5.1.1 Device must provide RTCP received from the far end for a transcoded inbound call when service provider or gateway sends RTCP

ID	44016
Priority	1
Summary	[Objective] Device is able to passthrough RTCP packets offered by service provider or the PSTN gateway to Teams [Pre-Condition] - RTCP passthrough enabled on Device - Transcoding enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected
2	Device involves in transcoding	Two was audio is present
3	Device passthrough the RTCP packets received from Service provider or the PSTN gateway to Teams SIP Proxy	Teams SIP Proxy receives RTCP packets during the call
4	PSTN user hangs up	Call is disconnected

6.3.5.1.2 Device must provide RTCP received from the far end for a transcoded outbound call when service provider or gateway sends RTCP

ID	44017
Priority	1
Summary	[Objective] Device is able to passthrough RTCP packets offered by service provider or the PSTN gateway to Teams [Pre-Condition] - RTCP passthrough enabled on Device - Transcoding enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected
2	Device involves in transcoding	Two was audio is present
3	Device passthrough the RTCP packets received from Service provider or the PSTN gateway to Teams SIP Proxy	Teams SIP Proxy receives RTCP packets during the call
4	Teams user hangs up	Call is disconnected

6.3.5.1.3 Device must provide RTCP received from the far end for an inbound call that doesn't involve transcoding when service provider or gateway sends RTCP

ID	44018
Priority	1
Summary	[Objective] Device is able to passthrough RTCP packets offered by service provider or the PSTN gateway to Teams [Pre-Condition] - RTCP passthrough enabled on Device - Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Device passthrough the RTCP packets received from Service provider or the PSTN gateway to Teams SIP Proxy	Teams SIP Proxy receives RTCP packets during the call
3	PSTN user hangs up	Call is disconnected

6.3.5.1.4 Device must provide RTCP received from the far end for an outbound call that doesn't involve transcoding when service provider or gateway sends RTCP

ID	44019
Priority	1

Summary	[Objective] Device is able to passthrough RTCP packets offered by service provider or the PSTN gateway to Teams [Pre-Condition] - RTCP passthrough enabled on Device - Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device passthrough the RTCP packets received from Service provider or the PSTN gateway to Teams SIP Proxy	Teams SIP Proxy receives RTCP packets during the call
3	Teams user hangs up	Call is disconnected

6.3.5.1.5 Device must provide RTCP for a transcoded inbound call when service provider or gateway does not send RTCP

ID	44020
Priority	1
Summary	[Objective] Device is able to generate RTCP packets towards Teams when the service provider or PSTN gateway does not provide RTCP [Pre-Condition] - RTCP enabled on Device - Transcoding enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected
2	Device involves in transcoding	Two was audio is present
3	Device generates RTCP packets towards Teams when Service provider or PSTN gateway does not provide RTCP	Teams SIP Proxy receives RTCP packets during the call
4	PSTN user hangs up	Call is disconnected

6.3.5.1.6 Device must provide RTCP for a transcoded outbound call when service provider or gateway does not send RTCP

ID	44021
Priority	1
Summary	[Objective] Device is able to generate RTCP packets towards Teams when the service provider or PSTN gateway does not provide RTCP [Pre-Condition] - RTCP enabled on Device - Transcoding enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected
2	Device involves in transcoding	Two was audio is present
3	Device generates RTCP packets towards Teams when Service provider or PSTN gateway does not provide RTCP	Teams SIP Proxy receives RTCP packets during the call
4	Teams user hangs up	Call is disconnected

6.3.5.1.7 Device must provide RTCP for an inbound call that doesn't involve transcoding when service provider or gateway does not send RTCP

ID	44022
Priority	1
Summary	[Objective] Device is able to generate RTCP packets towards Teams when the service provider or PSTN gateway does not provide RTCP [Pre-Condition] - RTCP enabled on Device - Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Device generates RTCP packets towards Teams when Service provider or PSTN gateway does not provide RTCP	Teams SIP Proxy receives RTCP packets during the call
3	PSTN user hangs up	Call is disconnected

6.3.5.1.8 Device must provide RTCP for an outbound call that doesn't involve transcoding when service provider or gateway does not send RTCP

ID	44023
Priority	1
Summary	[Objective] Device is able to generate RTCP packets towards Teams when the service provider or PSTN gateway does not provide RTCP [Pre-Condition] - RTCP enabled on Device - Transcoding disabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device generates RTCP packets towards Teams when Service provider or PSTN gateway does not provide RTCP	Teams SIP Proxy receives RTCP packets during the call
3	Teams user hangs up	Call is disconnected

6.3.5.2 RTCP Multiplexing (RFC 8035)

6.3.5.2.1 Device must indicate support for RTCP multiplexing by including the a=rtcp-mux attribute in the offer.

ID	44024
Priority	1
Summary	[Objective] Device must indicate support for RTCP multiplexing by including the a=rtcp-mux attribute in the offer SDP for an inbound call to Teams [Pre-Condition] - RTCP multiplexing enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends a=rtcp-mux attribute in the offer SDP indicating support for RTCP multiplexing
2	Device receives response from Teams SIP Proxy with a=rtcp-mux attribute	Call is connected with bi-directional audio
3	Device accepts RTCP packets sent by Teams SIP proxy	RTCP packets are received on the RTP port itself
4	PSTN user hangs up	Call is disconnected

6.3.5.2.2 Device must respond with a=rtcp-mux attribute in the SDP response if the offer contained it.

ID	44025
Priority	1
Summary	[Objective] Device must indicate support for RTCP multiplexing by including the a=rtcp-mux attribute in the answer SDP for an outbound call from Teams [Pre-Condition] - RTCP multiplexing enabled on Device
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Device receives a=rtcp-mux attribute in the offer SDP
2	Device sends a=rtcp-mux attribute in the answer SDP indicating support for RTCP multiplexing	Call is connected with bi-directional audio
3	Device sends RTCP packets to Teams SIP Proxy	RTCP packets are sent on the RTP port itself
4	Teams user hangs up	Call is disconnected

6.4 Security Requirements

6.4.1 TLS v1.2

6.4.1.1 Device must support TLS v1.2

ID	44033
Priority	2
Summary	[Objective] Device must support TLS version 1.2 or higher. [Pre-Condition] - Configure TLS version 1.2 on the Device and disable TLS 1.0, TLS 1.1 support
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	Device involves in TLS Handshake messages with Teams SIP Proxy	TLS version is mentioned by the Device
2	PSTN user calls Teams user	Call is connected with bi-directional audio
3	PSTN user hangs up	Call is disconnected

6.5 Support for OPTIONS and Failover

Please refer to 6.9 "SIP Options and Failover Mechanism" and 6.10 "Retry-After" in Appendix 1. Direct Routing SIP Protocol description

6.5.1 Device responds to OPTIONS messages sent by the Teams SIP Proxy

ID	33882
Priority	1
Summary	[Objective] Device responds to SIP OPTIONS message sent by Teams SIP Proxy.
Applicable	Only Options messages

Step	Action	Expected Result
1	Teams SIP Proxy sends OPTIONS message after Device has sent OPTIONS	Device responds to the OPTIONS with 200 OK indicating that Device's SIP signaling is up
2	Check this over a period of 7 minutes	Device responds to each of the OPTIONS messages received

6.5.2 Device sends SIP OPTIONS message to all three datacenters

ID	33883
Priority	1
Summary	[Objective] Device sends periodic OPTIONS message to all datacenters – primary, secondary and tertiary datacenter. But does not load balance calls. [Pre-Condition] - Device is configured to send SIP OPTIONS every 60 seconds to all three datacenter FQDNs
Applicable	Only Options messages

Step	Action	Expected Result
1	Device sends SIP OPTIONS to ping to all datacenters every 60 seconds	Device receives OPTIONS response from Teams SIP Proxy and marks the SIP Peer is up
2		Verify if the FROM and CONTACT header in the OPTIONS message sent by Device has its own FQDN

6.5.3 Device tries the secondary datacenter when there is no response from the primary datacenter (cannot establish TLS/TCP connection)

ID	47815
Priority	1
Summary	[Objective] Device when not able to establish TLS/TCP connection with primary datacenter, will try the secondary datacenter, due to ACL blocking outbound connection to the Teams SIP Proxy [Pre-Condition] - Device is configured to failover between three datacenters.
Applicable	Non-Media Bypass and Media Bypass calls

Step	Action	Expected Result
1	PSTN user calls Teams user	Device tries primary datacenter and fails to establish TLS/TCP connection
2	Device failover the call to secondary datacenter	Device can establish TLS/TCP connection successfully
3	Teams user answers the call	Call is established with two way audio
4	PSTN user hangs up	Call is disconnected

6.5.4 Device tries the secondary datacenter when there is no response from the primary datacenter (no response to invite)

ID	47817
Priority	1

Summary	[Objective] Device sends INVITE and tries the secondary datacenter when there is no response for the INVITE from the primary datacenter [Pre-Condition] - Device is configured to failover between three datacenters.		
Applicable	Non-Media Bypass and Media Bypass calls		
Step	**Action**	**Expected Result**	
1	PSTN user calls Teams user	Device sends INVITE to primary datacenter	
2	Device tries secondary datacenter when there is no response for the INVITE	Device sends INVITE to secondary datacenter	
3	Teams user answers the call	Call is established with two way audio	
4	PSTN user hangs up	Call is disconnected	

6.5.5 Device honors the retry-after timer in the 503 message received for the INVITE

ID	49024	
Priority	1	
Summary	[Objective] Device honors the retry-after timer in the 503 message received for the INVITE if present. Device clears the connection on receiving 503 and retries the same FQDN after the retry-after timer value. Eg Retry-After: 1	
Applicable	Non-Media Bypass and Media Bypass calls	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Device sends the INVITE to primary datacenter FQDN (sip.pstnhub.microsoft.com)
2	Teams SIP Proxy returns 503 Service Unavailable with retry-after header	Device clears the connection upon receiving 503. Device re-resolves the FQDN and initiates a new connection with the same FQDN after the timer value present in retry-after header expires.

7.0 Appendix 1. Direct Routing SIP Protocol description

7.1 Introduction

This portion of the document covers specific requirements to SIP Headers, size of SDP considerations and requirements to the domain names in Office 365 tenant.

The SIP Hub component of Microsoft Direct Routing uses SIP protocol, based on RFC 3261. To properly route traffic from SBC to and from the SIP Hub some SIP parameters MUST have specific values. The document covers mandatory parameters when configuring connection between SBCs and Microsoft Direct Routing. The document also has detailed examples of flow where the described parameters used.

The audience for the document is SBC vendors or SBC administrators who configure the connection between the SBC and the SIP Hub service.

7.2 Processing the incoming request

Example of the SIP Invite message:

Parameter name	Example of the value
Request-URI	INVITE sip:+18338006777@sip.pstnhub.microsoft.com SIP /2.0
Via Header	Via: SIP/2.0/TLS sbc1.adatum.biz:5058;alias;branch=z9hG4bKac2121518978
Max-Forwards header	Max-Forwards:68
From Header	From: <sip:7168712781@sbc1.adatum.biz;transport=udp;tag=1c747237679
To Header	To: sip:+183338006777@sbc1.adatum.biz
CSeq header	CSeq: 1 INVITE
Contact Header	Contact: <sip: 68712781@sbc1.adatum.biz;transport=tls>

During the connection the Microsoft SIP Hub uses two fields Request-URI and Contact header to:

- Check that the FQDN part of the Contact header matches the Common Name or Subject Alternative name of the presented certificate (sbc1.adatum.biz in the example);
- Validate the FQDN part of the Contact header with list of paired in Office 365 SBCs FQDNs;
- Perform the lookup of the user number in the Request-URI within a specific tenant and convert it to the SIP URI of the user;
- Find and apply specific parameters for this SBC as configured by the administrator during the call (for example if P-Asserted-Identity field should be send)

It is not supported to have a 3rd party SIP Proxy or User Agent Server between the Microsoft SIP Hub and the paired SBC, which might modify the Request URI, created by the paired SBC

7.2.1 Detailed requirements for Contact Header and Request-URI

7.2.1.1 Contact header

For all incoming calls to Microsoft SIP Hub, the Contact Header MUST have the paired SBC FQDN in URI hostname:

*Syntax: Contact: <sip:phone or sip address@**FQDN of the SBC;transport=tls>***

This name also MUST be in Common Name or Subject Alternative name field (s) of the presented certificate.

It is supported using wildcard values of the name (s) in the Common Name or Subject Alternative Name fields of the certificate.

The support of wildcard according to the https://tools.ietf.org/html/rfc2818#section-3.1 , specifically

*"Names may contain the wildcard character * which is considered to match any single domain name component or component fragment. E.g., *.a.com matches foo.a.com but not bar.foo.a.com. f*.com matches foo.com but not bar.com.".*

If more than one value in the Contact header presented in a SIP message sent by SBC, only the FQDN portion of the first value of the Contact header used.

7.2.1.2 Request-URI

For all incoming calls, the Request-URI used to match the phone number to a user.

The phone number MUST contain "+" sign.

Correct value:

- INVITE sip:+18338006777@sip.pstnhub.microsoft.com SIP /2.0

Incorrect value:

- INVITE sip:18338006777@sip.pstnhub.microsoft.com SIP /2.0

7.2.1.3 Detailed traffic flow description

Step 1. Checking the certificate. On the initial connection, the Direct Routing takes the FQDN name presented in the Contact header and matches it to the Common Name or Subject Alternative name of the presented certificate. The SBC name MUST match either option below:

- ***Option 1.*** The full FQDN name presented in the Contact header matches the Common Name/Subject Alternative name of the presented certificate OR
- ***Option 2.*** Domain portion of the FQDN name presented in the Contact header (for example adatum.biz of the FQDN name sbc1.adatum.biz) MUST matches the wildcard value in Common Name/Subject Alternative Name (for example *.adatum.biz)

Step 2. Try to find a tenant using full FQDN name presented in Contact. Check if the FQDN name from the Contact header is registered as a DNS name in any Office 365 tenant. Goal to allow only the connections that are originating from an SBC from a valid (registered in any Office 365 tenant) FQDN.

Step 3. Take the phone number presented in the Request-URI and perform the reverse number lookup. Match the presented phone number to a user SIP URI withing the tenant found on the previous step.

Step 4. Apply trunk settings. Find the parameters set by tenant admin for this SBC.

Example:

On incoming Invite an SBC presents two headers:

- Request-URI: INVITE sip:+18338006777@sip.pstnhub.microsoft.com SIP /2.0
- Contact: <sip: 68712781@sbc1.adatum.biz;transport=tls>

Step 1. Checking the certificate. Certificate check using the FQDN name of the SBC from the Contact header. To complete the check for the example above, the certificate MUST have one of the options below:

- Option 1. Common name = sbc1. adatum.biz OR
- Option 2. Subject Alternative name = sbc1.adatum.biz OR
- Option 3. Common or Subject Alternative name = *.adatum.biz

If presented certificate matches, traffic allowed, if not request rejected;

Step 2. Try to find a tenant using full FQDN name presented in Contact. Find and note which tenant in Office 365 has sbc1.adatum.biz registered as a domain name. If the tenant found, proceed to Step 4, if tenant with domain name sbc1.adatum.biz does not exist, proceed to Step 3;
Step 2a (only if 2 not successful). Try to find a tenant using domain portion of FQDN name, presented in Contact if Step 2 unsuccessful. Remove the host portion from the SBC FQDN. Result adatum.biz Find and note which tenant in Office 365 has adatum.biz registered as a domain name. If the tenant found, proceed to Step 4, if such tenant does not exist, reject the request;
Step 3. Match of the number to SIP address of the user. Perform reverse number lookup of the number +18338006777 to a user in the tenant found in either Step 2 or Step 3;
Step 4. Apply trunk settings. For example, trunk sbc1.adatum.biz has media bypass enabled, process call with media bypass.

The requirements for two lookups, one for sbc1.adatum.biz and the second adatum.biz is for the scenario where one SBC interconnected to many tenants (carrier scenario) and covered later in the document.
Note, If the tenant found in Step 2, the Step 3 skipped.

7.3 Contact and Record-Route headers

The SIP Hub needs to calculate the next hop FQDN in new in-dialog client transactions (for example Bye or Re-Invite), and when replying to SIP Options. Either Contact or Record-Route used.

According to the RFC 3261 is it mandatory to use Contact header in any request which can result in the establishing a new dialog. The Record-Route only required if a proxy wants to stay on the path of future requests in a dialog.

Microsoft recommends using only Contact header and ever present Record-Route to SIP Hub.

The reasons explained below.

1. Per RFC 3261, the Record -Route is used if a proxy wants to stay on the path of future requests in a dialog, which is not essential as all traffic goes between the Microsoft SIP Hub and the paired SBC. There is no need for an intermediate proxy server between the SBC and Microsoft SIP Hub.
2. The other factor, the Microsoft SIP Hub uses only Contact header (and not Record-Route) to determine the next hop when sending outbound ping Options (and not Record-Route). Configuring only one parameter (Contact) instead of two (Contact and Record-Route) simplifies the administration.

To calculate the next hop the SIP Hub uses:

- Priority 1. Top-level Record-Route. If the top-level Record-Route contains the FQDN name or IP, the FQDN name or IP used to make outbound in-dialog connection;
- Priority 2. Contact header. If Record-Route does not exist, the SIP hub will look up the value of the Contact header to make the outbound connection (recommended configuration)

If both Contact and Record-Route used the SBC administrator must keep their values identical which can be an administrative overhead.

7.3.1 Use of FQDN Name in Contact or Record-Route

Use of IP address is not supported in either Record-Route or Contact. The only supported option is an FQDN Name, which also MUST match either Common Name or Subject Alternative Name of the SBC certificate (wildcard values in the certificate supported).

If an IP address presented in the Record-route or Contact, the certificate check fails and calling experience breaks.

If FQDN does not match the value of the Common or Subject Alternative Name in the presented certificate, the call also fails.

7.4 Size of SDP Considerations

The Direct Routing interface might send a SIP message exceeding 1,500 bytes. The size of SDP primarily causes this. However, if there is a UDP trunk behind the SBC, it might reject such message if forwarded from Microsoft SIP Hub to the Trunk unmodified. We do recommend stripping some values in SDP on SBC when sending the message to the UDP trunks. For example, the ICE candidates or unused codecs can be removed.

7.5 Call transfer

7.5.1 Methods for transferring the calls

Direct Routing supports two methods for call transfer:

- On receiving the transfer, sending a Refer to connecting SBC;
- Handle transfer on Direct Routing. In this case Direct Routing in case of call transfer will send a new Invite

Choosing the method depends on capabilities of the SBC.

If the SBC indicates in SIP messages that it supports Refer than Direct Routing interface will use Refer method for call transfers.

Example of SBC sending the indication of Refer method being supported:

```
ALLOW: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
```

If the SBC doesn't include the Refer as a supported method, Direct Routing will use Basic Refer call flow as described in 7.1 of https://www.ietf.org/rfc/rfc3892.txt

Example of SBC indicating that Refer method is not supported:

```
ALLOW: INVITE,ACK,CANCEL,BYE,INFO,NOTIFY,PRACK,UPDATE,OPTIONS
```

7.5.2 Refer method

The Direct Routing always prefer sending Refer message in case of transferring the calls. The supported SBC MUST be able to handle Refer messages locally. However if Refer is missing in Allow header (please consult page 165 in RFC 3261 to learn more about Allow header and read the section above) the Direct Routing will handle transfer on its own without Refer header. Note Direct Routing will not be able to handle transfer without Refer if Media Bypass configured.

The size of the Refer header can be more than 1000 symbols, The SBC must support handling Refer messages with size more than 1000 symbols.

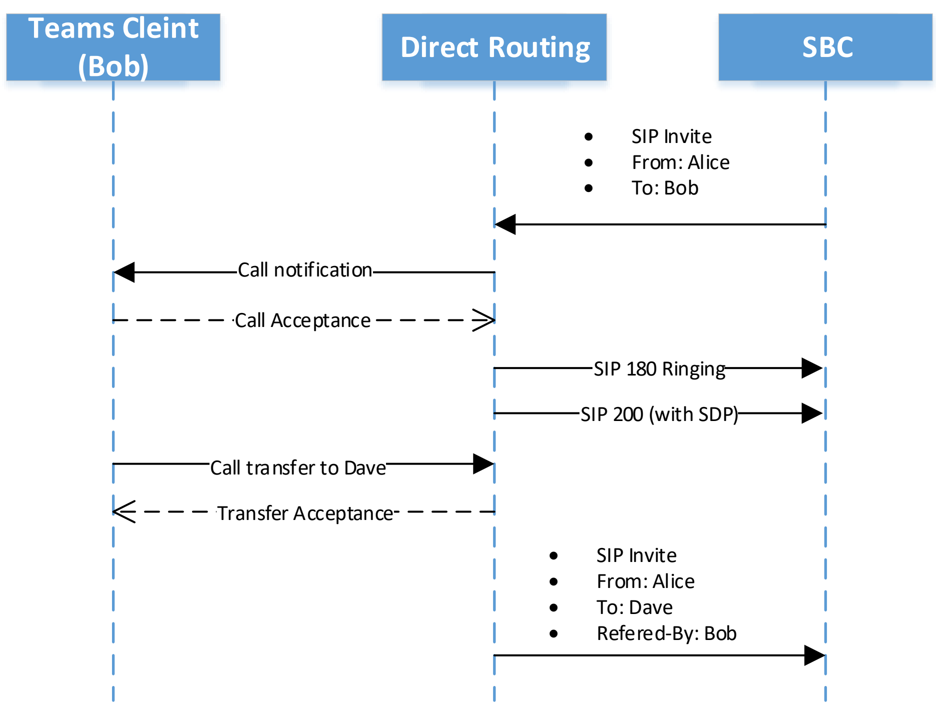
Example of refer message, send by Direct Routing interface:

REFERRED-BY: *sip:sip.pstnhub-ppe.skype.net:5061;x-m=8:orgid:610b9123-1cd9-406d-ad88-8a1173213440;x-t=8bd26852-6bec-4491-8527-29ee61dd6aa3;x-a=Asy/aMh9Bz9bZJnmorltTcJhn6iMd3ChCPlJIYILM50O99TjiC0WWVg37hGHR4JXdRDjqCuZOaLSJP4OzrW4T8zAOdduZemwh2pN8Gcig9Z9EuTMQ5TYGpQA6a900qOIrWhH7avf30lQx4vNq+EG9cCKOLE9ocP1QIveGOCsLMEa+eY//MiA9aTl2ggyUP8KhNoNZWHvw9UzmHH5LjLOefzZqhUyG714SbZoU1oRrmPQnzNea6bWOK/LfJ1BaFAl+1K/ZealfYuZe+U5qeODefSJFW5NeERDyYVkIam2Yl7ZdPjnHNqHQb4xqQu/pz6l/FEkTr2aAQkjrUUlDS3lCm1zrcj47QE8dz/lFBrgsM6cCwgsKMSXyOk9NGjwYaVXfjXwfld5qPPNyOSboVCpkN0Ty68txe93VN+aeSod2KEdYfF9NqKX68Mwya7qj61MOXr34dE7sfRdPS55WjIHiaWqHDdfV43d9DaNex6DaD5zn9IkwjjBvS9RlDK4KV615zxWnh/Star+v4XrLDGdy7yLxxxnvRImC2pMp+26wj/RxlSSCodt+MwH9gidO08XqYbi5+9qrQcADbD05ag/ObeNsj4HVNaVY7dGh1Nl/iTt6cuTnpM/aMejy9mk7Il5hZHxBunHbVEZDq36LKW88FFtZg7LWbrC/A+H7+jWVRdy77GAC6Bg6BQqSbBw8sueGkrmiJbCF/Q9, msgLen = 1517.296 06262018 212053.429509:1.01.00.36030.Info .SIPCM: SipFeSocketRecvMsg - msg = DsyilhWO73iMWlxySc+bej3UoONPkSI4E4cGi6Y6qyze4j6InzHR*

7.5.3 Basic Refer implementation

If the SBC indicated that Refer method is not supported, the Direct Routing will act as a Referee and generate new invites according to the Basic Refer description in 7.1 of https://www.ietf.org/rfc/rfc3892.txt

Call Flow.



7.5.3.1 History-Info and Referred By Headers

History-Info. The History-Info header is used for retargeting SIP requests and "provide(s) a standard mechanism for capturing the request history information to enable a wide variety of services for networks and end-users" (RFC 4244 – Section 1.1, http://www.ietf.org/rfc/rfc4244.txt). For the Microsoft Phone System this is used in Simulring and Call Forwarding scenarios.

If sending the History-Info is enabled:

- The SIP Proxy will insert a parameter containing the associated phone number in individual History-Info entries that comprise the History-Info header sent to the PSTN Controller. Using only entries that have the phone number parameter, the PSTN Controller will rebuild a new History-Info header, and pass it on to the SIP trunk provider via SIP Proxy;
- History-Info header will be added for ***simultaneous ring*** and ***call forwarding*** cases;
- History-Info header will not be added for call transfer cases;
- Note that an individual history entry in the reconstructed History-Info header will have the phone number parameter provided combined with the Direct Routing FQDN (sip.pstnhub.microsoft.com) set as the host part of the URI; a parameter of 'user=phone' will be added as part of the SIP URI. Any other parameters associated with the original History-Info header, except for phone context parameters, will be passed thru in the re-constructed History-Info header. Note that entries that are private (as determined via the mechanisms defined in Section 3.3 of RFC 4244) will be forwarded as-is since the SIP trunk provider is a trusted peer;
- Inbound History-Info is ignored;

  Format of History-info header sent by SIP Proxy:

<sip:UserB@
sip.pstnhub.microsoft.com?Privacy=history&Reason=SIP%3B\cause%3D486>;index=1.2,
If call was redirected several times, information about every redirect included with appropriate reason in chronological order.

Header Example:

History-info:
<sip:+14257123456@sip.pstnhub.microsoft.com;user=phone?Reason=SIP;cause=302;text="Move Temporarily">;index=1
<sip:+14257123457@sip.pstnhub.microsoft.com;user=phone?Reason=SIP;cause=496;text="User Busy">;index=1.1

The History-Info is protected by mandatory TLS mechanism.

Referred-By. The Referred-By header is used for retargeting SIP requests, specifically for Call Transfer scenarios with regards to the Microsoft Phone System. In a call transfer scenario it may be necessary to provide the refer target with specific information about the referrer and the refer request itself. In the case of SIP trunks the Referred-By header carries information (referrer's identity) which is typically used for authentication and billing purposes by the SIP trunk provider.

Note SIP Proxy doesn't protect Referred-By by S/MIME as recommended in RFC 3892 as both Microsoft Phone System and paired SBC considered as trusted entities and traffic is always encrypted between the two entities. The tenant administrator might configure additional protection or stripping the header on SBC when call is forwarded to public PSTN.

When Referred-By enabled:

- The SIP Proxy will provide the SIP URI containing the phone number in a referrer-phone header;
- Inbound Referred-By is ignored;
- Referred –By outbound shall support the following format:

SIP URI - E.164; Example: sip:+14257123456@ sip.pstnhub.microsoft.com;user=phone

Header Example:

Referred-By: sip:+ 14257123456@sip.pstnhub.microsoft.com;user=phone

Microsoft Direct Connect interface does not include any privacy headers with the History-Info or Referred-By headers. By default, they are disabled and it is responsibility of the tenant administrator to decide what to do with the headers when send outside the SBC. It is assumed what the administrator fully understands the privacy requirements when enables the headers.

7.6 SBC connection to Direct Routing and Failover mechanism

The connection point for Direct Connect are three FQDNs:

- **sip.pstnhub.microsoft.com** – Global FQDN, must be tried first. When SBC sends request to resolve this name, the Microsoft Azure DNS servers returns an IP address pointing to the primary Azure datacenter assigned to the SBC. The assignment is based on performance metrics of the datacenters and geographical proximity to the SBC. The IP address returned corresponds to the primary FQDN
- **sip2.pstnhub.microsoft.com** – Secondary FQDN, geographically maps to the second priority region;
- **sip3.pstnhub.microsoft.com** – Tertiary FQDN, geographically maps to the third priority region

Placing these three FQDNs in order above required to Provide the failover when connection from an SBC is established to a datacenter which is experiencing a temporary issue. See description below
SBC must send Options to all three datacenters.

Failover Mechanism

The SBC makes DNS query to resolve sip.pstnhub.microsoft.com. Based on geographical proximity and the datacenters performance metrics the primary datacenter is selected. If during the connection the primary datacenter experiences an issue, the SBC will try the sip2.pstnhub.microsoft.com which resolves to the second assigned datacenter, and in rare case if datacenters in two regions are not available the SBC retries the last FQDN (sip3.pstnhub.microsoft.com) which provides the tertiary datacenter IP.

The table below summarizes the relationships between primary, secondary and tertiary datacenters:

If SBC is located in	EMEA	NOAM	ASIA
The secondary datacenter (sip2.pstnhub.microsoft.com)	US	EU	US
The tertiary datacenter (sip3.pstnhub.microsoft.com)	ASIA	ASIA	EU

7.7 Retry-After

In cases if a Direct Routing datacenter is busy, the interface can send to the SBC Retry-After message with interval 1 second.

When the SBC receives a 503 with a Retry-After header in response to an INVITE the SBC must terminate that connection, perform a new DNS request (for the next datacenter, for example secondary if primary replied with retry-after) and try placing a call via a new datacenter

7.8 ICE Restart: Media Bypass call transferred to an endpoint which does not support Media Bypass

Please read carefully, we saw issues in this scenario with the SBCs.

SBC MUST support ICE restart as described in https://tools.ietf.org/html/rfc5245#section-9.1.1.1

The restart in Direct Routing implemented according to this paragraph of RFC:

```
To restart ICE, an agent MUST change both the ice-pwd and the ice-
ufrag for the media stream in an offer.  Note that it is permissible
to use a session-level attribute in one offer, but to provide the
same ice-pwd or ice-ufrag as a media-level attribute in a subsequent
offer.  This is not a change in password, just a change in its
```

representation, and does not cause an ICE restart.

An agent sets the rest of the fields in the SDP for this media stream as it would in an initial offer of this media stream (see Section 4.3). Consequently, the set of candidates MAY include some, none, or all of the previous candidates for that stream and MAY include a totally new set of candidates gathered as described in Section 4.1.1.

In case if call initially was established with Media Bypass and the call transferred to a SfB client Direct Routing need to insert a Media Processor as it is not supported to use Direct Routing with SfB client with Media Bypass. Direct Routing starts ICE restart process by changing the ice-pwd and ice-ufrag and offering new media candidates in a reinvite.

Example of call flow.

Initial invite from a supported SBC to Direct Routing:

```
INVITE sip:+37225001020@sbc.adatum.biz SIP/2.0
Via: SIP/2.0/TLS sbc.adatum.biz:5061;alias;branch=z9hG4bKac1696703830
Max-Forwards: 68
From: <sip:+37281000527@pstnbotrm.eastus.cloudapp.azure.com>;tag=1c1789452806
To: <sip:+37225001020@sbc.adatum.biz>
Call-ID: 1009424558782018113512@sbc.adatum.biz
CSeq: 1 INVITE
Contact: <sip:+37281000527@sbc.adatum.biz:5061;transport=tls>
Supported: norefersub,100rel,timer,replaces,sdp-anat
Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE, OPTIONS
Session-Expires: 1800
Min-SE: 90
User-Agent: A supported SBC
Content-Type: application/sdp
Content-Length: 674
v=0
o=- 489700321 271447286 IN IP4 40.115.115.41
s=pjmedia
b=AS:84
t=0 0
a=X-nat:0
a=ice-lite
m=audio 10925 RTP/SAVP 0 101
c=IN IP4 40.115.115.41
b=TIAS:64000
a=rtcp:10926 IN IP4 40.115.115.41
a=sendrecv
```

a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ice-ufrag:XFeYuizJ59QFDSAC
a=ice-pwd:iBYEjPuiS4JKSgaFukv4wUi+
a=candidate:1126159041 1 udp 2130706431 40.115.115.41 10925 typ host
a=candidate:1126159040 2 udp 2130706431 40.115.115.41 10926 ty
2018-08-07T11:06:19.719237+00:00 10.0.0.8 [S=5629616]: [SID=b04af8:14:632376] p host
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:t79MCw3WCKtGfkqeSBZylWaAgdqLzTxGTrb6unQM|2^31
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:K4FDB/K/PHwPrZdPh0V5UmPsa+u9Pg2OcNEnw4YF|2^31

Reply from Direct Routing Interface with local candidates of the client (media bypass call). Note the Direct routing sent the local IP of the client as trunk configured for Media Bypass

SIP/2.0 200 OK
FROM: <sip:+37281000527@pstnbotrm.eastus.cloudapp.azure.com>;tag=1c1789452806
TO: <sip:+37225001020@sbc.adatum.biz>;tag=47de5befe60c45a09476402edd77e2e2
CSEQ: 1 INVITE
CALL-ID: 1009424558782018113512@sbc.adatum.biz
VIA: SIP/2.0/TLS sbc.adatum.biz:5061;branch=z9hG4bKac1696703830
RECORD-ROUTE: <sip:sip-du-a-eu.pstnhub-ppe.skype.net:5061;transport=tls;lr>
CONTACT: <sip:api-du-a-euno.pstnhub-ppe.skype.net:8000;transport=tls;x-i=9fd825d7-ca71-4af2-bfab-b68eb08fabec;x-c=/v1/ngc/call/00fa72acd5d746cdb74c25a3e6865808/s/1/12603f8cc38b40cab9ffe4b4c8a89308>
CONTENT-LENGTH: 654
CONTENT-TYPE: application/sdp
ALLOW: INVITE
ALLOW: ACK
ALLOW: OPTIONS
ALLOW: CANCEL
ALLOW: BYE
ALLOW: NOTIFY
SERVER: Microsoft.PSTNHub.SIPProxy v.2018.8.7.3 i.EUNO.2
v=0
o=- 78 0 IN IP4 10.0.0.5
s=session
c=IN IP4 10.0.0.5
b=CT:10000000
t=0 0
m=audio 31440 RTP/SAVP 0 101

c=IN IP4 10.0.0.5
a=rtcp:31441
a=ice-ufrag:A64M
a=ice-pwd:t3Qd3sg6Aozs7eVhw6+2LBzO
a=candidate:1 1 UDP 2130706431 10.0.0.5 31440 typ host
a=candidate:1 2 UDP 2130705918 10.0.0.5 31441 typ host
a=candidate:2 1 tcp-act 1684798975 10.0.0.5 31440 typ srflx raddr 10.0.0.5 rport 31440
a=candid
2018-08-07T11:06:23.884455+00:00 10.0.0.8 [S=5629678]: [SID=b04af8:14:632376] ate:2 2 tcp-act 1684798462 10.0.0.5 31440 typ srflx raddr 10.0.0.5 rport 31440
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:n6xzN8M1WogTnZ+wbA9ONdvurElDIkUuW0r2WuVu|2^31
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16,36

After some time, the Teams client decided to transfer the call to a user with SfB endpoint and sends a reinvite. Note in the reinvite we provide the media candidates from a MP and a new ice-ufrag and ice-pwd

INVITE sip:+37281000527@sbc.adatum.biz:5061;transport=tls SIP/2.0
FROM: <sip:+37225001020@sbc.adatum.biz>;tag=47de5befe60c45a09476402edd77e2e2
TO: <sip:+37281000527@pstnbotrm.eastus.cloudapp.azure.com>;tag=1c1789452806
CSEQ: 1 INVITE
CALL-ID: 1009424558782018113512@sbc.adatum.biz
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.114.76.79:5061;branch=z9hG4bKc95ed1e
CONTACT: <sip:api-du-a-euno.pstnhub-ppe.skype.net:8000;transport=tls;x-i=9fd825d7-ca71-4af2-bfab-b68eb08fabec;x-c=/v1/ngc/call/00fa72acd5d746cdb74c25a3e6865808/s/1/12603f8cc38b40cab9ffe4b4c8a89308>
CONTENT-LENGTH: 1203
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2018.8.7.3 i.EUNO.0
CONTENT-TYPE: application/sdp
ALLOW: INVITE
ALLOW: ACK
ALLOW: OPTIONS
ALLOW: CANCEL
ALLOW: BYE
ALLOW: NOTIFY
v=0
o=- 3360 0 IN IP4 127.0.0.1
s=session
c=IN IP4 52.115.56.195

```
b=CT:10000000
t=0 0
m=audio 50200 RTP/SAVP 104 117 9 103 111 18 0 8 97 101 13 118
c=IN IP4 52.115.56.195
a=rtcp:50201
a=ice-ufrag:ts9g
a=ice-pwd:xuzNWB1yjadHrcWtdnQsNWSH
a=rtcp-mux
a=candidate:1 1 UDP 2130706431 52.115.56.195 50200 typ srflx raddr 10.0.0.6 rport 50200
a=candidate:1 2 UDP 2130705918 52.115.56.195 50201 typ srflx raddr 10.0
2018-08-07T11:07:40.406884+00:00 10.0.0.8 [S=5630153]: [SID=b04af8:14:632376] .0.6 rport
50201
a=candidate:2 1 tcp-act 1684798975 52.115.56.195 50200 typ srflx raddr 10.0.0.6 rport 50200
a=candidate:2 2 tcp-act 1684798462 52.115.56.195 50200 typ srflx raddr 10.0.0.6 rport 50200
a=label:main-audio
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:k6TLDsIJ1X+oe1M+snYfEdZVnIeIuy71FyhEZxMG|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:grIE/52bQUtjFTUb6sEJojGd1R9M9srMq7+d8Qt0|2^31
a=sendrecv
a=rtpmap:104 SILK/16000
a=rtpmap:117 G722/8000/2
a=rtpmap:9 G722/8000
a=rtpmap:103 SILK/8000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000
a=ptime:20
```

The SBC MUST correctly handle this scenario.

8.0 Appendix 2. Media and Encryption requirements

An SBC can function in two modes:

- Without Media Bypass. In this case all RTP traffic flows Teams Client <-> Media Processors <-> SBC.
- With Media Bypass. In this case RTP media flows between the Teams endpoints and SBC (Teams <-> SBC).

Note SIP traffic always goes via SIP proxy

The section below describes specific requirements to media and encryption with and without media bypass.

The section does not substitute RFCs but aims to help SBC vendors to clarify the requirements.

SBC vendors, unless stated otherwise, MUST use RFCs mentioned below for detailed technical reference.

8.1 Media Bypass. ICE Lite requirements

Direct Routing supports media bypass with SBC enabled for ICE Lite as described in [RFC 5245](RFC 5245).

The SBCs must respond to connectivity checks and include only host candidates for any media stream.

Teams client, which is full ICE client, performs aggressive nomination. SBC MUST use the highest priority candidate pair for which checks are received for media flow, before end of connectivity checks.

At the end of connectivity checks, SBC will receive Re-Invite with the final local and remote candidates selected by connectivity checks. Device must validate and respond to STUN binding requests and periodic keepalives (STUN binding requests).
The credentials will be sent via SIP for every session (short-term credential mechanism)

- a=ice-pwd:<password>
- a=ice-ufrag:<ufrag>

One Teams user might have multiple endpoints, SBC MUST be able to handle multiple ICE connectivity checks with own ICE credentials.

The SBC, after receiving the provisional answer with the callee's candidates, MUST begin the connectivity checks. A single initial offer can result in multiple provisional answers being received as a result of forking. The Interactive Connectivity Establishment (ICE) processing MUST be carried out independently for each provisional answer.

8.2 Encryption cipher and MKI requirements

The SBC MUST support SRTP encryption cipher AES_CM_128_HMAC_SHA1_80 for offer and answer.

MKI:

- SDES – non-zero MKI is used per RFC;
- DTLS – Not supported

Example of crypto attribute in SDP offer from the SBC:

a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:V/Lr6Lsvhad/crSB9kCQ28jrYDxR2Yfk5bXryH5V|2^31

When the SBC is configured with SRTP as the Media Security mode and SDES as the Media Security method, the SDP of offer/answer from device MUST follow the example below:

m=audio 52884 RTP/SAVP 111 103 104 9 0 8 106 13 110 112 113 126
a=crypto:0 AES_CM_128_HMAC_SHA1_32 inline:Hr4D2cgUu9+Uza5Igz/JkVx59DAxDbaxJg862ibQ|2^31
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:JPEaIxHegfuv53ykBPZk8hV0GO8kTiiqRMfHimEE|2^31
a=rtcp:52884
a=rtcp-mux

8.3 SDES support Requirements

The Device must be able to offer SDES in the format as described below. Microsoft Media Processors always prefer SDES. In case of non-Media Bypass even if a client only supports DTLS the Media Processors will convert to SDES.

In case of Media Bypass, if a client is DTLS only (future Google Chrome state) the Direct Routing will insert MP in the path. Between the SBC and media Processor component of Direct Routing SDES is always used.

At the moment of writing this specification there were no Teams client which only offer DTLS, however Google announced that at some point of time they will stop supporting SDES.

8.4 Format for Offer from SBC in BYPASS (Offer must contain SDES and can contain DTLS Optional in the following format)

m=audio 54056 UDP/TLS/RTP/SAVP 0 8 76 77 18 9 101 13
a=rtcp:54056
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:krXco0QRglwErMqtbMs2zSw29tBdmdgXpEYZhQmp|2^31
a=fingerprint:sha-256
AE:24:07:15:5C:B7:45:1A:E4:45:60:C1:1E:68:0E:CC:8D:A6:78:3B:76:65:BB:B0:77:88:07:F8:98:18:62
:34
a=setup:actpass
a=rtcp-mux

8.5 Format for Answer containing SDES to SBC

m=audio 54056 RTP/SAVP 111 103 104 9 0 8 description 106 13 110 112 113 126
a=rtcp:54056
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:fBc61ikv1kMy0sF85DblNqTzVAbFa7hJQ9GKb6Yj|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80
inline:O1qT9tWbs/NwJVwhfrgF5tCrbNOxnVDqkIqTx4rz|2^31
a=rtcp-mux

8.6 Format for Offer from Teams to SBC

8.6.1 Format for SDES only offer to SBC

m=audio 52884 RTP/SAVP 111 103 104 9 0 8 106 13 110 112 113 126
a=crypto:0 AES_CM_128_HMAC_SHA1_32
inline:Hr4D2cgUu9+Uza5Igz/JkVx59DAxDbaxJg862ibQ|2^31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:JPEaIxHegfuv53ykBPZk8hV0GO8kTiiqRMfHimEE|2^31
a=rtcp:52884
a=rtcp-mux

8.6.2 SILK Codec implementation recommendations

If an SBC doesn't support SILK it is expected that vendor will implement the SILK codec. The description of the codec is available on request.

Recommended parameters:

- SILK NB with High Complexity, recommended target bitrate 13 kbit/sec;
- SILK WB with High Complexity, recommended target rate 36 kbit/sec

9.0 Appendix 3. Requirements to the Domain Names registered in Office 365 Administrator Center

The Microsoft Phone System Hybrid Connection uses the domain name registered in Office 365 administrator center to validate if an SBC can be paired with this tenant.

To pair an SBC tenant administrator needs to connect to Office 365 PowerShell (description how to connect to Office 365 PowerShell), run a command New-CSOnlinePSTNGateway command and specify the FQDN of the SBC which is being paired.

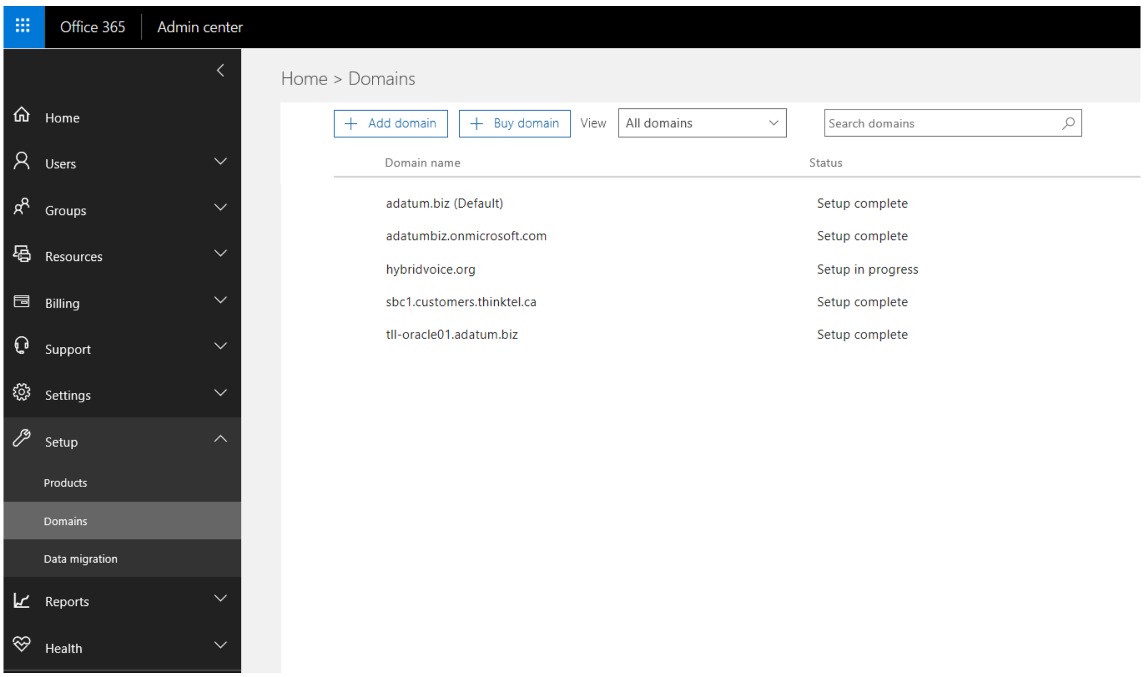
During connection to Office 365 PowerShell the tenant administrator provides the credentials, so the session established only for a specific tenant.

When command run, it checks if the FQDN name of SBC belongs to one of the domain names registered in tenant for which New-CSOnlinePSTNGateway command run.

The FQDN portion of the SBC name can be from any domain registered, except the domain names *.onmicrosoft.com and with status "Setup Complete" in the Office 365 administrator center.

Once FQDN name for SBC chosen and the SBC paired, it can serve users with any SIP addresses valid for this tenant.

For example, the picture below shows that there are five domains registered in Office 365 tenant.



9.1 SBC hosting scenario

The configuration of the SBC hosting scenario described here https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-sbc-multiple-tenants

8.0 Test cases matrix

The Matrix is the summary of cases listed in 5.2 End to end scenarios and provided as an additional document. If you did not receive the matrix or have questions, please send an email to drsbccertification@microsoft.com

10.0 Joint support process requirements

The Joint support process requirements are documented in a separate document. If you did not receive the document or have questions, please send an email to drsbccertification@microsoft.com