A logo of a company

Description automatically generated

**Microsoft Teams**

**Teams Phones Certification Program**

**Partner Requirements**

**V5.0**

Published: March 2023

Microsoft Confidential. © 2023 Microsoft Corporation. All rights reserved.  
  
These materials are confidential to and maintained as a trade secret by Microsoft Corporation. Information in these materials is restricted to Microsoft authorized recipients only. Any use, distribution, or public discussion of, and any feedback to, these materials are subject to the terms of the attached license. By providing any feedback on these materials to Microsoft, you agree to the terms of that license. The materials set forth in this document may be amended from time to time at the sole discretion of Microsoft.

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

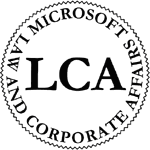
(c) If a Microsoft NDA has not been executed, You (if You are an individual), or Company (if You are an authorized representative of Company), as applicable, agrees: (a) to refrain from disclosing or distributing the Confidential Information to any third party for five (5) years from the date of disclosure 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 must 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's 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 must 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.



[Revision History 7](#_Toc128061807)

[Supporting Documentation 9](#_Toc128061808)

[1.0 Microsoft Teams Phones Certification Program 10](#_Toc128061809)

[1.1 Device category 10](#_Toc128061810)

[1.1.1 Audio only devices 10](#_Toc128061811)

[1.1.2 Video capable devices 10](#_Toc128061812)

[1.2 Delivery of certified solution 10](#_Toc128061813)

[1.3 Certification process overview 10](#_Toc128061814)

[1.4 Product samples 11](#_Toc128061815)

[1.5 Customer trials 11](#_Toc128061816)

[1.6 Certification testing 12](#_Toc128061817)

[1.6.1 Audio only devices 12](#_Toc128061818)

[1.6.2 Video capable devices 13](#_Toc128061819)

[1.7 Certification publication 14](#_Toc128061820)

[1.8 Customer Support and Live Site Operations 14](#_Toc128061821)

[1.9 Microsoft Support integration 14](#_Toc128061822)

[1.10 Data reporting 14](#_Toc128061823)

[2.0 Product requirements 15](#_Toc128061824)

[2.1 Product requirements: Audio only devices 15](#_Toc128061825)

[2.2 Product requirements: Video capable devices 15](#_Toc128061826)

[2.3 Kiosk Mode experience 15](#_Toc128061827)

[2.4 OOBE requirements 15](#_Toc128061828)

[2.4.1 Boot up sequence 15](#_Toc128061829)

[2.4.2 Requirements for multiple service providers 16](#_Toc128061830)

[2.5 Device encryption 17](#_Toc128061831)

[2.6 TLS 1.2 and Cipher suites support 17](#_Toc128061832)

[2.7 Android Intents support 17](#_Toc128061833)

[2.8 Idle Mode requirements 17](#_Toc128061834)

[2.9 LED requirements 17](#_Toc128061835)

[2.10 Dial Tone requirements 19](#_Toc128061836)

[2.11 Firmware to report additional device properties 20](#_Toc128061837)

[2.11.1 Report firmware version 20](#_Toc128061838)

[2.11.2 Report device type 20](#_Toc128061839)

[2.11.3 Report device capabilities 20](#_Toc128061840)

[2.12 Firmware release 21](#_Toc128061841)

[2.13 Device management 21](#_Toc128061842)

[2.14 Development and support tools 22](#_Toc128061843)

[2.14.1 Android Debug Bridge (ADB) 22](#_Toc128061844)

[2.14.2 FTP or Telnet 22](#_Toc128061845)

[2.14.3 Syslog 23](#_Toc128061846)

[2.15 User Messaging requirements 23](#_Toc128061847)

[2.16 OS level battery optimization requirements 23](#_Toc128061848)

[2.17 Hard Button Mapping requirements 23](#_Toc128061849)

[2.18 Audio Channel requirements 24](#_Toc128061850)

[2.18.1 High level requirements 24](#_Toc128061851)

[2.18.2 Audio Channel Switching 25](#_Toc128061852)

[2.18.3 Default Audio Channel when BT/USB Headset is connected 26](#_Toc128061853)

[2.19 Dialpad state intent 27](#_Toc128061854)

[2.20 Heads up notifications 27](#_Toc128061855)

[2.21 Teams button support 27](#_Toc128061856)

[3.0 Microsoft Teams Application requirements 27](#_Toc128061857)

[3.1 Feature support requirements 27](#_Toc128061858)

[3.2 Application support 29](#_Toc128061859)

[3.3 Emergency Call requirements 29](#_Toc128061860)

[3.3.1 Overall requirements 29](#_Toc128061861)

[3.3.2 Additional requirements 30](#_Toc128061862)

[3.4 LLDP (Link Layer Discovery Protocol) Requirements 30](#_Toc128061863)

[3.5 Accessibility requirements 31](#_Toc128061864)

[3.6 Microsoft Teams supported languages 32](#_Toc128061865)

[3.7 Persistent Device ID Requirements 32](#_Toc128061866)

[4.0 Partner Applications requirements 33](#_Toc128061867)

[4.1 Partner Applications requirements 33](#_Toc128061868)

[4.2 Partner Agent requirements 34](#_Toc128061869)

[4.3 Partner Device Settings requirements 34](#_Toc128061870)

[4.3.1 Personal Mode/ Host User: End User interface requirements 36](#_Toc128061871)

[4.3.2 Personal Mode/Host User:Admin user interface requirements 38](#_Toc128061872)

[4.3.3 Shared Mode: Conference Phone /CAP/Hot Desking User: End user interface requirements 38](#_Toc128061873)

[4.3.4 Shared Mode: Conference Phone /CAP/ Hot Desking User: Admin user interface requirements 39](#_Toc128061874)

Table of Contents

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Date | Description | Reviewers |
| 1.0 | April 2019 | Document created | Diana Vank |
|  | May 30, 2019 | Document published | Diana Vank |
| 2.0 | June 2020 | Yearly review process | Diana Vank  Ashish Mehta |
|  |  | Common document structure introduced across all device categories |  |
|  |  | Updated content for sections 1.2, 1.4, 2.3, 2.4, 4.1, 4.2 |  |
|  |  | Added new sections: 2.1, 2.2, 2.5, 2.6, 2.7, 2.11, 2.16, 2.17, 2.18, 2.19 |  |
| 3.0 | June 2020 | Merged into one certification program requirements document to cover audio only devices, video capable devices partner specs and certification program details  Updated version to v3.0 for continuity | Diana Vank |
|  | June 29, 2020 | Document published | Diana Vank |
| 4.0 | December 2021 | Section 1.2: Removed and replaced with updated statement in Section 1.3: Certification process overview | Diana Vank  Jyothi Peddi  Kruthika Ponnusamy |
|  |  | Section 1.3: Last row in the table updated to state: Maintain all certification requirements, including minimum Android OS version, as specified in the CPA |  |
|  |  | Section 2.4.1: Updated OOBE for device to fetch local time zone before signing |  |
|  |  | Section 2.4.2: Updated requirements for multiple service providers |  |
|  |  | Section 2.5: Updated encryption requirements to allow admin to query for encryption status |  |
|  |  | Section 2.10: Updated Dial tone requirements |  |
|  |  | Section 2.12: Updated Device Management |  |
|  |  | Section 2.14: Removed requirement for firmware to provide error messages to the user when the device has encountered network failures, this is now handled by the app and removed meaningful message if the app/OS crashes |  |
|  |  | Section 2.15: Removed Voice skills from Hardware Button Mapping Requirements |  |
|  |  | Section 2.17: Updated Dialpad state intent |  |
|  |  | Section 3.2.3: Removed section, internet non-available requirement, as it is now handled by the app |  |
|  |  | Section 3.2: New |  |
|  |  | Section 3.3.2: Added unsuccessful phone lock attempts will sign out device in additional requirements |  |
|  |  | Section 3.4: Added Talkback as a mandatory requirement for accessibility |  |
|  |  | Section 4.3.1: Updated Phone lock pin length to 6 digits |  |
|  |  | Section 4.3.4: Updated Phone lock pin length to 6 digits |  |
| 5.0 | March 2023 | Yearly Review | Jyothi Peddi  Kapil Khanna  Vinay Jagannatha Rao |
|  |  | Updated supporting documentation |  |
|  |  | Section 2.1 and 2.2 Updated phones product requirements spec version |  |
|  |  | Section 2.5 Updated Device Encryption with file-based requirements |  |
|  |  | Section 2.11 Added report device capabilities |  |
|  |  | Section 2.13 Updated device management |  |
|  |  | Section 2.13.4 Removed Teams license |  |
|  |  | Section 2.16 Added OS battery requirements |  |
|  |  | Section 3.4 Added LLDP requirements |  |
|  |  | Section 3.7 Added Persistent device id requirements |  |
|  |  | Section 4.3 Added two entries to access device settings |  |
|  |  | Section 4.3.2 Removed screen capture from personal mode admin settings |  |
|  |  | Section 4.3.4 Removed screen capture from shared mode admin settings |  |

# Supporting Documentation

|  |  |
| --- | --- |
| Section | Document Name |
| [1.7 Certification Testing](#_Certification_Testing) | Microsoft\_Teams\_VideoSpecifications\_5\_Final.pdf  Microsoft\_Teams\_AudioSpecifications\_5\_Final.pdf  Android MediaCodec Extension for Microsoft Teams\_Skype H.264 Hardware Video Offloading v1.pdf |
| [2.0 Product Requirements](#_Product_requirements_1) | Teams Phones Product Requirements v2.0.pdf |
| [4.1 Partner Application](#_Partner_Applications_requirements) | Microsoft Teams Guidelines for Partners.pdf |
| [4.2 Partner Agent requirements](#_Toc9054238) | Partner Agent Dev Design v3.pdf |

# Microsoft Teams Phones Certification Program

*Microsoft Teams Phones Certification Program is* designed to help partners bring premium communication experiences to the market. Microsoft Teams users 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
* Participate in integrated support with Microsoft

## Device category

Microsoft Teams certified devices must meet all the certification requirements as they apply to the assigned device category at the time a device enters the certification program.

### Audio only devices

Audio only capable devices are classified as Microsoft Teams *personal, common area* and/or *conferencing solutions,* where the target user would be using the device as a Microsoft Teams desk phone and common area phone for calling and collaboration scenarios, or conference phone for meeting scenarios.

### Video capable devices

Video capable devices are classified as Microsoft Teams *personal solution,* where the target user would be using the video phones as a Microsoft Teams desk phone for calling and collaboration scenarios.

## Delivery of certified solution

Once a solution is certified against the latest specification, or if an interim update is required due to a hotfix requirement, the partner must make the newly certified firmware available to Microsoft via delivery methods that are mutually agreed upon.

## Certification process overview

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 certification:

|  |  |
| --- | --- |
| Action | Owner |
| **Complete legal contracts: NDA, Certification Program Brand Licensing Agreement** | Microsoft/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 |
| **Conduct formal review of product ID and technical specifications** | Microsoft/Partner |
| **Develop product to meet requirements (including self-testing)** | Partner |
| **Plan and execute against agreed upon certification schedule** | Microsoft/Partner |
| **Plan and execute customer TAP** | Microsoft/Partner |
| **Perform certification testing at Microsoft approved 3rd party labs** | Partner |
| **Support process alignment (including training, drills, and sample product)** | Microsoft/Partner |
| **Deliver product documentation & marketing content (to be approved by Microsoft before publishing)** | Partner |
| **Review certification program qualifications and approve certification** | Microsoft |
| **Publish certification on Microsoft websites** | Microsoft |
| **Perform post-certification requirements**  **(e.g., telemetry reviews, fix temporary waivers, recertification)** | Microsoft/Partner |
| **Maintain all certification requirements, including minimum Android OS version, as specified in the CPA** | Partner |

## Product samples

Partner must provide product samples to Microsoft and/or independent lab for purposes of testing, and other evaluation purposes, as per the executed *Microsoft Teams Device Partner Framework Agreement* (aka Agreement) and/or any *Addendum* to the master Agreement, or the executed *Certification Program Agreement* (aka CPA).

These samples are in addition to those that may be shared with Microsoft field or marketing teams for marketing or sales training purposes. The total number of samples should include a mix of all models that the partner would submit for certification.

## Customer trials

The quality of certified products is made much more robust by incorporating real customer feedback prior to certification. Technology Adoption Programs (TAP) and/or Microsoft internal usage (known as MSIT Dogfood) are required for certification.

The exact TAP and/or MSIT Dogfood plans will be developed jointly by Microsoft and Partner as part of the certification program engagement.

For TAP, the following requirements apply.

|  |  |  |
| --- | --- | --- |
| TAP requirement | Typical conditions | Additional information |
| Customer recruitment | Microsoft and Partner joint effort | Microsoft will identify Teams customers interested in joining the TAP program for devices. |
| Number of customers | Minimum of 20 customers | Customer selection criteria to be agreed upon jointly based on product usage criteria (not marketing value) |
| TAP devices | Customer list with shipping addresses provided by Microsoft | Partner responsible for shipping devices, free of cost to customers, to mutually agreed TAP customer list. |
| TAP entrance criteria **(TAP Candidate)** | Microsoft and Partner joint effort | The product used during TAP is not yet certified but is expected to be at a high quality/stability bar to maximize usage and the ability to collect meaningful feedback |
| TAP duration | 6-10 weeks  1-2 product updates during TAP timeframe | Usage criteria to be defined by Microsoft ahead of TAP. TAP is concluded as soon as certification is approved. |
| TAP training content | Hardware and software how to documentation | Microsoft and Partner joint effort to ensure all necessary successful customer TAP readiness and meaningful feedback |
| TAP customers support | Daily review and response to customer feedback and creation of work items (as necessary) | Partner bears primary responsibility for OS/firmware updates and questions related to the hardware functionality.  Microsoft bears primary responsibility for Team, Company Portal, and device management support for the TAP program. |

## Certification testing

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

The 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.

### Audio only devices

* The following certification testing is required for all audio only devices pursuing certification under the *Microsoft Teams Phones Certification Program*.

|  |  |  |
| --- | --- | --- |
| * Certification Test | * Requirements | * Test Plan |
| * Audio certification | * Microsoft Teams Audio Specification v4 Final.pdf | * Test scenarios included in the Audio v4 spec. Microsoft approved 3rd party lab use approved tools and methodology to test devices and report results via Microsoft approved test results template |
| * Microsoft Teams phones | * This document, Microsoft Teams Phones Certification - Partner Requirements v4.pdf | * Microsoft released test plan. Microsoft approved 3rd party lab use approved tools and methodology to test devices and report results via Microsoft approved test results template |

### Video capable devices

* The following certification testing is required for all video capable devices pursuing certification under the *Microsoft Teams Phones Certification Program*.

|  |  |  |
| --- | --- | --- |
| * Certification Test | * Requirements | * Test Plan/Tool/Reporting |
| * Audio certification | * Microsoft Teams Audio Specification v4 Final.pdf | * Test scenarios included in the Audio v4 spec. Microsoft approved 3rd party lab use approved tools and methodology to test devices and report results via Microsoft approved test results template |
| * Video certification * (Hardware offloading) | * Android Video Hardware offloading Mediacodec extension API for Skype 0.31.pdf | * Test scenarios included in the MLVEC tool, a tool developed and made available to partners by Microsoft. Tool automatically generates results reports which need to be shared with Microsoft |
| * Video certification * (Video performance) | * MLVEC test passed | * Test scenarios included in the E2E Video Pipeline performance tool. Tool automatically generates reports that are made available to Microsoft |
| * Video certification | Microsoft\_Teams\_VideoSpecifications\_4\_Final.pdf | * Test scenarios included in the Video v4 spec Microsoft approved 3rd party lab use approved tools and methodology to test devices and report results via Microsoft approved test results template |
| * Microsoft Teams phones | * This document, Microsoft Teams phones Certification - Partner Requirements v5 | * Microsoft released test plan. Microsoft approved 3rd party lab use approved tools and methodology to test devices and report results via Microsoft approved test results template |

## Certification publication

Upon entering TAP program, the partner must work with Microsoft marketing to provide device images, company logo and marketing content for posting to Microsoft websites.

Once the certification team has approved a device for certification, a certification email is sent to the partner. At the same time, relevant Microsoft websites will be updated to list the certified partner device.

Partner and Microsoft will periodically review the list of certified products to be removed from active listing on Microsoft websites 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.

## Customer 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 Premier support contract, or a similar support benefit. All post-certification (in-market) support is expected to route through this support channel rather than through the Microsoft certification program team.

## Microsoft Support integration

Partners are required to develop training content 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.

## Data reporting

Partners must provide the quality and sales reporting for certified products to Microsoft in the standard template that will be made available to partners along with their agreements.

# Product requirements

## Product requirements: Audio only devices

Audio only device must meet all the product requirements as specified in the *Microsoft Teams Phones Product Requirements v2.0.pdf*, or the latest official version available at the time device enters the certification process.

## Product requirements: Video capable devices

Video capable device must meet all the product requirements as specified in the *Microsoft Teams Phones Product Requirements v2.0.pdf*, or the latest official version available at the time device enters the certification process.

## Kiosk Mode experience

Microsoft Teams certified devices enforce kiosk mode, where the end user’s interaction with the device is limited to the Microsoft Teams user interface for all desired actions.

* The operating system configuration must prevent users from accessing hardware or other touch screen options or gestures (e.g., swipe left/right, up/down) to exit the Microsoft Teams, Microsoft Company Portal, or Device Settings applications.
* The operating system configuration must prevent users from exiting the Microsoft Teams, Microsoft Company Portal, or Device Settings applications by using keyboard or hard key combinations.
* The operating system configuration must launch the Microsoft Teams application after power up by default and prevent access to the Android home screen.
* Device must support an operating system configuration that would allow the user to navigate the phone only via the Microsoft Teams application user interface.
* Device must not allow users to uninstall the Microsoft Teams application via the Android interface.
* Device must not allow users to exist the Microsoft Teams application via any of the available touch screen gestures.

## OOBE requirements

OOBE experience must meet all requirements as outlined in this section.

### Boot up sequence

Partners are responsible to ensure the following sequence and events are happening during initial boot up of the device.

**Boot Up screen**:

* Partners may display their logo on the boot up screen
* Partner must ensure all Microsoft Teams needed resources are initialized, including network and IP address acquisition
* Once initialization is complete, transition to next screen must happen without user intervention

**Language Selection screen**:

* Display list of supported languages (languages not supported by Microsoft Teams, see [Microsoft Teams Supported Languages](#_Microsoft_Teams_Supported_1) section below, must not be presented as an option)
* Users must be allowed to select a language.
* Once language selection is completed, transition to next screen must happen without user intervention.
* Device must fetch local time zone before signing in

**Loading Teams Application screen**:

* The next screen must be the Loading Teams Application screen without user intervention

### Requirements for multiple service providers

|  |  |  |
| --- | --- | --- |
| Feature | Requirement | Notes |
| Single Factory Image –  multiple service providers | SHALL NOT | The device shipping from factory shall not contain software from other service providers than Microsoft Teams. |
| Single Disti orderable SKU | REQUIRED | Must comply with branding guidelines  for the Certified for Microsoft Teams. |
| Customer orderable Teams SKU | REQUIRED | Required for mandatory Royalty tracking. |
| Device First-run Service picker | SHALL NOT |  |
| Account OOBE customizations | MAY | OOBE customizations should be aligned with Teams OOBE and require sign-off by Microsoft Teams. |
| Teams Image –  Reset to certified defaults | REQUIRED | Reset to default settings for Microsoft Teams shall not require user interaction. |
| Reset to Factory Image | MAY | The Reset to Factory Image shall use methods without UX on the device. |

## Device encryption

Devices must support Android-based encryption and must populate the right status for encryption using the appropriate Android API.

* Firmware must support Android-based device encryption (For Android 10 and above file-based encryption is required)  
  [File-Based Encryption | Android Open Source Project](https://source.android.com/security/encryption/file-based?hl=en)
* Firmware must populate the right status for encryption using the appropriate Android API

<https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#getStorageEncryptionStatus()>

* The encryption is enforced through Intune policy and Intune queries for getStorageEncryptionStatus() for encryption status, return values of ENCRYPTION\_STATUS\_PER\_USER (5) is recognized as active, fully configured encryption and satisfies Intune compliance
* Firmware must enable an admin to query the status of encryption.olson

## TLS 1.2 and Cipher suites support

Device must support TLS 1.2 and the Cipher Suites available at the time of certification. Partners to check with Microsoft on the most current list.

## Android Intents support

Device must support Android ‘intent’ inter-process communication mechanism.

Reference: <https://developer.android.com/reference/android/content/Intent.html>

## Idle Mode requirements

* For accurate presence information, the device needs to update user’s presence status to the Teams service. This will be achieved via broadcast intents that the firmware publishes to the Microsoft Teams application.
* Firmware must broadcast the ACTION\_DREAMING\_STARTED and ACTION\_DREAMING\_STOPPED intents when the device goes to idle mode either based on screen saver settings, device lock settings or office hour settings.
* When both the screen saver and device lock features are disabled by the user, the device must default to sending these events after a configurable idle timeout.
* When both the screen saver and device lock features are enabled, the device must enter idle mode based on the idle timeout setting that starts earliest.

## LED requirements

The Microsoft Teams application would provide updates via intents to the firmware when users interact on the touch screen interface during calls or meetings. This enables the firmware to update the available LED states on the phone. If multiple LED indicators are not available on the device to differentiate the various states listed below, the Mute state would take precedence over other states.

Firmware must listen to the intents that are broadcast and update the hardware indicators based on the information listed in the table below.

|  |  |  |
| --- | --- | --- |
| # | Scenario | Intent |
| 1 | Mute State: When user updates the mute state via the user interface, the Teams application will broadcast an intent. | ACTION: com.microsoft.skype.teams.ipphone.APP\_MUTE\_STATE  Data: MUTE\_STATE, 0 or 1  Where 0 represent Mute Off and 1 represents Mute On.  This data can be used to update the mute LED. |
| 2 | MWI: When the user has a new voicemail, the application will broadcast an intent. | ACTION: com.microsoft.skype.teams.ipphone.APP\_MISSEDVOICEMAIL\_STATE  Data: UNREAD\_VOICEMAIL, 0 or 1  Where 0 represent No Unread Voicemails and 1 represents New Voicemail Available.  This data can be used to update MWI indicator. |
| 3 | Missed Calls State: When the user has a new missed call, the application will broadcast an intent. | ACTION: com.microsoft.skype.teams.ipphone.APP\_MISSEDCALL\_STATE  Data: MISSED\_CALLS, 0 or 1  Where 0 represent No new missed calls and 1 represents New missed calls Available.  This data can be used to update MWI indicator. |
| 4 | Incoming Call State: When the user has a new incoming call, the application will broadcast an intent. | ACTION: com.microsoft.skype.teams.ipphone.APP\_INCOMINGCALL\_STATE  Data: INCOMING\_CALL, 0 or 1  Where 0 represent No new incoming call and 1 represents a new incoming call.  This data can be used to update MWI indicator and to play dial tone when user picks up the handset of presses speaker button. |
| 5 | In Call State: When the user is in a call or conference, the application will broadcast an intent. | ACTION: com.microsoft.skype.teams.ipphone.APP\_INCALL\_STATE  Data: IN\_CALL, 0 or 1  Where 0 represents call is in progress (no audio) and 1 represents a call in progress.  This data can be used by partners to reset the voice channel to the speaker for the next incoming call to ring.  This data can be used to update the speaker button LED. |
| 7 | Voicemail Playing State: When the user is playing voicemail audio, the app will send an intent | ACTION: com.microsoft.skype.teams.ipphone.APP\_VOICEMAILPLAYING\_STATE (Play/Pause button or Speed button on voicemail tab)  Data: PLAYING\_VOICEMAIL, 0 or 1  Where 0 represent that no voicemail audio is playing and 1 represents that the user has chosen to play the voicemail audio.  This data can be used to update the speaker button LED. |
| 8 | When user chooses audio output via touch screen UI during calls | ACTION: com.microsoft.skype.teams.ipphone.partner.APP\_AUDIO\_STATE  Data: HANDSETHOOK, 0 or 1 (similar to earpiece mode in mobile) SPEAKER, 0 or 1 HEADSETHOOK, 0 or 1 where 0 represents off and 1 represents on. |
| 9 | User SignIn State: When the user is signed into the Teams app, the application will broadcast an intent | ACTION: com.microsoft.skype.teams.ipphone.APP\_USER\_STATE  Data: SIGNED\_IN, 0 or 1  Where 1 represents user is signed in, 0 represents user is signed out |

## Dial Tone requirements

Firmware is responsible for playing the dial tone when the user picks up the handset or presses the speaker button to initiate an outgoing call. This might not apply for hardware that does not have handset or speaker buttons.

* Firmware must play a dial tone to the user via the user’s chosen audio channel (handset, headset or speaker) when an audio channel is activated (user-initiated) and all of the of the following intents are set to 0 by the Microsoft Teams Application.

(com.microsoft.skype.teams.ipphone.APP\_INCOMINGCALL\_STATE is set to 0) AND (com.microsoft.skype.teams.ipphone.APP\_INCALL\_STATE is set to 0) AND (com.microsoft.skype.teams.ipphone.APP\_VOICEMAILPLAYING\_STATE is set to 0)

If the speaker is the active audio channel, the Speaker LED must be ON when dial tone is playing.

* Firmware must stop playing a dial tone to the user via the user’s chosen audio channel (handset, headset or speaker) when one of the following states is set to 1 by the Microsoft Teams Application.

(com.microsoft.skype.teams.ipphone.APP\_INCOMINGCALL\_STATE is set to 1) OR (com.microsoft.skype.teams.ipphone.APP\_INCALL\_STATE is set to 1) OR (com.microsoft.skype.teams.ipphone.APP\_VOICEMAILPLAYING\_STATE is set to 1)

* Firmware must stop playing a dial tone to the user when user starts dialing number on dial pad.

Firmware must play dial tone again if the user clears phone number on dial pad.

## Firmware to report additional device properties

### Report firmware version

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Description | Partner Implementation | Teams App Query |
| **Report firmware version** | Firmware version info should be set as a System Property | Partner should be report this as a secure string, set as a system property with key "***build.firmware.version***". | System.getProperty("build.firmware.version") |

### Report device type

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Description | Partner Implementation | Teams App Query |
| **Report Device Type** | Firmware should send the device type to Teams to optimize its client experience based on the device type. | Partner should report this as a secure string, set as a system property with key "***teams\_device\_type***". | Settings.Secure.getString(application.getContentResolver(), "teams\_device\_type") |

The device type should be the following value:

* ***ipPhone***- This represents Teams phone device type

Eg: Settings.Secure.getString(application.getContentResolver(), "teams\_device\_type")

***Sample output:***  
ipPhone

### Report device capabilities

Firmware must implement *teams\_device\_capabilities* and report its capabilities as appropriate. Applicable values will be released by Microsoft via the one pager release process.

|  |  |  |
| --- | --- | --- |
| Description | Partner Implementation | Teams App Query |
| Firmware should send the device info to Teams to optimize its client experience based on the device capabilities. | Partner should report, as a secure string, set as a system property with key "***teams\_device\_capabilities***" from the FW side  **Note:** Multiple capabilities should be reported as a comma separate list of values. | Settings.Secure.getString(application.getContentResolver(), "teams\_device\_capabilities") |

## Firmware release

Firmware package must include the BIOS compatible with the specific hardware, the DSP and supporting drivers, and the operating system configuration as defined in this document. Firmware package must also include updateable Device Settings application, Partner Agent, Microsoft Admin Agent, Microsoft Company Portal, and the Microsoft Teams application.

It is the firmware package as described above that will be considered the certification firmware build and released officially for customers to download via TAC.

For each product release, the partner must provide 3 versions of the firmware bundle:

1. userdebug build: used by Microsoft Teams Engineering to develop and test new features on the specific firmware version
2. ‘dummy’ ADB enabled build: used by Microsoft QA teams for integration and feature testing
3. ADB disabled and release signed build: official build that will be released to customers, must be ‘released’ signed. Version must be higher than the ‘dummy’ build

Reference: [Signing Builds for Release](https://source.android.com/devices/tech/ota/sign_builds)

In addition, for each firmware bundle released to Microsoft as part of the regular product release cycle, the partner must provide the following:

* Release Notes
* Release build version information in the following format:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Manufacturer | Model(s) | Type | File Name | Version Code | Version Name | Build Type |
|  |  | Firmware |  |  |  | userdebug |
|  |  | Firmware |  |  |  | ADB enabled |
|  |  | Firmware |  |  |  | ADB disabled |

## Device management

Microsoft Teams certified devices are managed devices, management functions being provided via the Microsoft Teams Admin Center (TAC) solution.

TAC provides tenant administrators the ability to add new certified devices into their system, update these devices to the latest firmware, push application updates to these devices in a regular and reliable fashion and allow remote management of the devices.

TAC also provides tenant administrator access to phone-specific logs to debug failures scenarios including audio failures, connectivity issues, etc.

The device management agent is a software application/service which resides on the target device to allow for performance of the required device management activities. Implementation requirements for the device management agent are specified in [section 4.2](#_Partner_Agent_requirements) of this document.

* Device must support an agent running in the background to communicate and integrate with TAC.
* Device must apply all firmware, application and configuration updates received from TAC via intents.
* Device must retain application settings and device settings after application updates and/or firmware updates have been applied to the device.
* Device must not require factory resets after receiving updates through TAC
* Device may have an option to upgrade the firmware manually (via the web interface) when signed in as an administrator.
* TAC provides the tenant administrator access to device-specific logs to debug failures scenarios including audio failures, connectivity issues, etc.
* Device must allow Teams app to read ANR and tombstone logs for debugging purposes since the files downloaded from TAC don't contain logs from the OS.
  + Teams app should be able to read the /data/anr and /data/tombstone directories as well as be able to read the content of all trace files within the /data/anr and /data/tombstones directory.
  + Teams app will read all the files from these directories using standard Android IO APIs and attach to the log reported downloaded from TAC
* Device must upload logs without revealing PII data to the TAC solution.
* Device must report telemetry events to integrate reporting device status with the TAC solution.
* If the Microsoft Admin Agent terminates for any reason, firmware must restart the admin agent after a period of 15 minutes. The admin agent must be started as described in section 4.0 of this document.

## Development and support tools

### Android Debug Bridge (ADB)

* Firmware must provide ADB utility
* Partner must have the ability to provide firmware builds with ADB enabled, or disabled during certification process for engineering collaboration purposes
* The certified GA build must not have ADB enabled

### FTP or Telnet

* Partners can choose to have FTP and/or Telnet ports enabled during development phase
* The certified GA build must have FTP and Telnet disabled

### Syslog

* Partners can choose to have syslog enabled during development phase
* The certified GA build may have syslog enabled

## User Messaging requirements

* Device must provide message during updates of any of the Teams related applications running on the device
* The device must provide a visual indicator when the device is offline
* All user messages must be localized for all partner supported languages. See [Microsoft Teams Supported Languages](#_Microsoft_Teams_Supported) section of this document

## OS level battery optimization requirements

The OS level battery optimization must be turned OFF, regardless of whether the device uses battery or not. The operating system shouldn't start optimizing power by throttling network calls and/or reducing the thread priority of the Teams process.

## Hard Button Mapping requirements

For devices providing hard buttons, the Microsoft Teams Phones application will provide support for hardware buttons for call handling functions not limited to Redial, Mute/Unmute, Hold/Resume and Call Transfer.

Any hardware button on the device must be actionable by the user. See the table below for a list of actions that are supported by the Microsoft Teams application. Partners are encouraged to collaborate with Microsoft if they anticipate adding new hardware buttons outside of this list.

All hardware buttons on the device should be mapped to a [KeyEvent defined for Android](https://developer.android.com/reference/android/view/KeyEvent.html). Events that are not supported by Android should be mapped to the permitted custom Key Codes as defined in the Table below.

|  |  |  |
| --- | --- | --- |
| Item | Description | KeyEvent/Intent |
| Volume Control | User can control local devices’ volume via the up and down hardware buttons | [KEYCODE\_VOLUME\_UP](https://developer.android.com/reference/android/view/KeyEvent.html#KEYCODE_VOLUME_UP)  [KEYCODE\_VOLUME\_DOWN](https://developer.android.com/reference/android/view/KeyEvent#KEYCODE_VOLUME_DOWN) |
| Mute / Unmute | User can mute/unmute the local device microphone. If the device supports an LED for indication of mute state, it should indicate the MUTE state. | [KEYCODE\_MUTE](https://developer.android.com/reference/android/view/KeyEvent.html#KEYCODE_MUTE) |
| Standard dial pad | User can use buttons supported on dial pad, Phone keys 0 – 9, Phone key Star (\*), Phone Key Pound (#) | KEYCODE\_0 to KEYCODE\_9  KEYCODE\_STAR  KEYCODE\_POUND |
| ‘+’ in dial pad | Interpret ‘+’ from dialpad | LongPress on KEYCODE\_0 |
| DTMF support | Support for standard DTMF tones | KEYCODE\_0 to KEYCODE\_9  KEYCODE\_STAR  KEYCODE\_POUND |
| Contacts | User can launch Contact Search in the Microsoft Teams application by pressing the Contacts button | KEYCODE\_CONTACTS |
| Voice mail | A user can press a button to access their voicemail in the Microsoft Teams application on the device | KEYCODE 500 |
| Hold/Resume | A user can place a hold | KEYCODE 501 |
| Call Transfer | Ability to transfer a call to another user | KEYCODE 502 |
| Redial | User can redial the last called number. | KEYCODE 504 |
| Headset | User can press a button on the phone to switch the audio to a USB connected headset | KEYCODE 505 |
| Speaker | User can press a button on the phone to switch the audio to speakerphone. | KEYCODE 506 |
| Handset | User can pick up the handset on the phone to switch the audio to the handset. | KEYCODE 507 |
| Off hook support | User can initiate or accept an incoming call via the Microsoft Teams application on the device and audio is expected to come to the phone handset or headset. The firmware is responsible of managing audio through multiple output channels (headset, handset, or speakerphone). | The firmware must broadcast the intent below to inform the application about the audio channel that is currently active.  ACTION: com.microsoft.skype.teams.ipphone.partner.PHONE\_STATE\_UPDATED  Data: HANDSETHOOK, 0 or 1 SPEAKER, 0 or 1 HEADSETHOOK, 0 or 1 where 0 represents off and 1 represents on. |
| Video | User can initiate or accept an incoming video call via the Microsoft Teams application on the device. | KEYCODE 508 |

## Audio Channel requirements

### High level requirements

The user can initiate or accept an incoming call on the device through one of four options:

* Pick up Handset (if applicable)
* Press Speaker phone button
* Headset
* Touch Screen (Join/End Buttons) on the Microsoft Teams application

In all the cases listed above, audio is expected to play over one of the three possible output channels: Headset, Handset or Speakerphone.

Firmware is responsible for handling the audio flow through the user’s preferred channels and switching of the audio flow between these channels. For example, if the user chooses to pick up a call via the handset and transfer audio flow to the speaker phone, the firmware must route the audio channel from the handset to the speaker phone.

Firmware must play the audio via the channel chosen by the user and transfer the audio based on user behavior. If the audio channel is not switched during the call, the firmware must interpret a second action on the same hardware button press as ending the call.

### Audio Channel Switching

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initial State | Action | Expected State | Teams App to Firmware   (Audio Manger) | Firmware to App Intent |
| Audio Switching while in a call – Device Speaker | Speaker is selected | Speaker is lit.  Soft key shows the Speaker, and the audio is flowing through the speaker. | User selects the soft speaker button -> app updates AudioManager.setSpeakerphoneOn(true) -> | PHONE\_STATE\_UPDATED intent:  Speaker =1  Headset=0  Handset=0 |
| Audio Switching while in a call – USB Headset connected | Headset is selected | Headset button is lit on the device and the soft key shows headset connected. | AudioManager.setSpeakerphoneOn(false)  BT\_SCO is not initiated | PHONE\_STATE\_UPDATED intent:  Speaker =0  Headset=1  Handset=0 |
| Audio Switching while in a call – BT Connected | BT Soft Key is selected | Soft key show BT is connected. Audio should flow from the connected BT. | AudioManager.setSpeakerphoneOn(false)  BT\_SCO is initiated | PHONE\_STATE\_UPDATED intent:  Speaker =0  Headset=1  Handset=0 |
| Audio Switching while in a call - Handset |  |  | Teams will not send any intent. It would show handset icon. User cannot select the icon. | PHONE\_STATE\_UPDATED intent:   updated  Speaker =0  Headset=0  Handset=1 |

Note:

Whenever the user chooses to switch between the hard button on the device to the soft key on the app, the audio should flow through the selected channel. And the soft key should show the correct audio channel selected.

### Default Audio Channel when BT/USB Headset is connected

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initial State | Action | Expected State | Teams App to Firmware   (Audio Manger) | Firmware to App Intent |
| Incoming and Outgoing call default audio channel | only BT is connected | The default audio channel should the connected BT. | In this case we initialize the BT\_SCO connection and we call AudioManager.setSpeakerphoneOn(false) | PHONE\_STATE\_UPDATED intent:  Headset=1;  Speaker =0;  Handset=0 |
| Incoming and Outgoing call default audio channel | BT and USB headset both are connected | USB headset will be the default audio channel. | **Incoming call:**  Here, if the user accepts the call on the UI the default audio channel should be the USB headset.  BT\_SCO is not initiated.    **Outgoing Call:**  Here, if the user accepts the call on the UI the default audio channel should be the USB headset.  BT\_SCO is not initiated.    In this case we do not initialize the BT\_SCO connection and we call AudioManager.setSpeakerphoneOn(false) | PHONE\_STATE\_UPDATED intent:  Headset=1  Speaker =0  Handset=0    Firmware must prioritize the wired headset first |

Note: Default Audio: When the device has a BT or USB device connected, the default audio channel would be the USB Connected Headset.

## Dialpad state intent

|  |  |  |
| --- | --- | --- |
| Scenario |  | |
| **Dialpad state: when dial pad state changed, will broadcast an intent.** | ACTION:  com.microsoft.skype.teams.ipphone.DIALPAD\_STATE  Data:  DIALPAD\_STATE, can be 0,1,2  0 represents no dial pad show  1 represents dial pad is showing with no number.  2 represents dial pad is showing with number.    This intent can be used to change the audio channel and play dial tone.  When firmware receives 1 or 2, it must activate the audio channel. Teams will not send INCALL\_STATE when dial pad show. After INCALL\_STATE is sent and while call is in progress firmware should not respond to Dialpad state changes. Once the call is ended firmware should send PHONE\_STATE\_UPDATE with all audio source 0. |

## Heads up notifications

Device must support Android standard heads up notification as specified here: <https://developer.android.com/guide/topics/ui/notifiers/notifications#Heads-up>

## Teams button support

Firmware must listen to the intents that are broadcast and update the hardware indicators based on

the information listed in the table below.

|  |  |  |
| --- | --- | --- |
| Teams Feature | Firmware Dependency | Partner Action [Keycode/Intent] |
| Support Teams Button on the device | FW needs to send a new keycode when Teams App button is pressed on the device. | **KEYCODE\_503** |

# Microsoft Teams Application requirements

## Feature support requirements

Device must meet the following minimum feature requirements.

|  |  |
| --- | --- |
| Feature | Minimum requirements |
| Sign in | User must be able to sign in and sign out using their corporate account credentials |
| Presence | User should be able to see their status accurately reflected on the device  User should be able to manually change their status |
| Search | User should be able to search for a contact |
| Calls | User should be able to make an audio and/or video call, place an audio and/or video call on hold, mute and unmute an audio and/or video call  User should be able to transfer a call  User should be able to merge a call  User should be able to escalate a P2P call to a conference call  User should be able to call an IVR system and enter DTMF digits  Device should support multiple incoming calls |
| Meetings | User should be able to view their calendar and all meetings  User should be able to join and leave a meeting  User should be able to delete a meeting from the calendar  User should be able to see all meeting participants  User should be able to add and/or admit people into an existing meeting |
| Voicemail | User should be able to receive, play/pause and delete voicemail  User should be able to see a visual indicator when there is new voicemail |
| Call Park | User should be able to park and retrieve a parked call |
| Group call | User able to see an incoming group call notification  User able to accept, decline and/or join a group call |

Additionally, the device must support all Microsoft Teams features available at the time the device enters certification stage. For any features that require partners to make changes to either firmware or the partner apps, partner requirements will be provided via a one pager partner requirements document ahead of time.

For all certified devices, partners are also required to complete all work necessary to support a new Microsoft Teams application feature as communicated during the product release engagements.

## Application support

The following permissions must be granted by default to all Microsoft applications:

* Device admin privileges
* Admin access to overlay screen

## Emergency Call requirements

### Overall requirements

* Device must support 911 calls from the locked screen without requiring the user to unlock the device
* Emergency call icon / option must be available for the user, on the unlock code screen.

A screenshot of a phone number

Description automatically generated

* Clicking the emergency call icon/option must trigger an action from the firmware to publish an intent to the Microsoft Teams application. Once the intent is detected by the application, Microsoft Teams launches the 911 calling experience.
* Intent that the partner needs to publish:

com.microsoft.skype.teams.ipphone.partner.DIAL\_EMERGENCY\_NUMBER

* Teams App will share emergency data (from location policy or emergency call routing policy) to firmware after registration.

|  |  |
| --- | --- |
| *Intent:* | com.microsoft.skype.teams.ipphone.SHARE\_EMERGENCY\_INFO |
| *With Extras:* | String[] extra keyed with “EMERGENCY\_INFO” which will contain the emergency numbers.    String extra keyed with “CORRELATION\_ID” which will be used to uniquely identify the request |

The firmware will respond with intent:

|  |  |
| --- | --- |
| *Intent:* | com.microsoft.skype.teams.ipphone.partner.SHARE\_EMERGENCY\_INFO\_ACK |
| *With Extras:* | String extra correlationId keyed with “CORRELATION\_ID” that will be equal to the correlationId of the request |

* Firmware must confirm that they have received emergency call information.
* App will periodically refresh emergency calling information.
  + Nothing is expected from the firmware side. Teams application will periodically share the emergency data (via the same intent as above) if it changes.
* A new code change to support 911 from keypad on lock screen must be added.
* Every time the user presses 911 from keypad on lock screen, firmware must send an intent to app indicating the there is an ask for an emergency call.
* App must listen to the emergency dial intent from firmware and invoke dialing out 911.

* Firmware must have the following intent:

|  |  |
| --- | --- |
| *Intent:* | com.microsoft.skype.teams.ipphone.partner.DIRECT\_DIAL\_EMERGENCY\_NUMBER |
| *With Extras:* | String extra keyed with “EMERGENCY\_NUMBER” that contains the emergency number (not the mask) that was dialed.  e.g. user dials 911 OR 212 OR 768 OR 908 -> FW should return 911 |

* App must support auto-dial after user hits 911 or local emergency number.

### Additional requirements

* Firmware must validate PIN during PIN creation and update - we cannot support a PIN that starts with local emergency numbers.
* Screen should not be enforced unless the user is signed in.
* In CAP mode, screensaver should be disabled by default.
* Device must sign out after 5 unsuccessful attempts of phone lock pin.
* Device must provide a warning message on the number of attempts left to unlock the phone until it signs out.
* On user sign out, firmware should remove all emergency call information stored.

## LLDP (Link Layer Discovery Protocol) Requirements

Firmware must facilitate specific use cases and technical specifications needed to support LLDP- IEEE 802.1AB to resolve the devices dynamic location.

To make sure the device supports the Ethernet connection and report Chassis ID and Port ID attribute from the Device-based API, the specified attributes are to be sent to “Teams Calling” to resolve the Teams device dynamic location for Emergency calling Services (e.g. 911/E911 calling)

**LLDP API**

1. LLDP data will be shared by the firmware with Teams app after app reboot/boot or after LLDP

data changes.

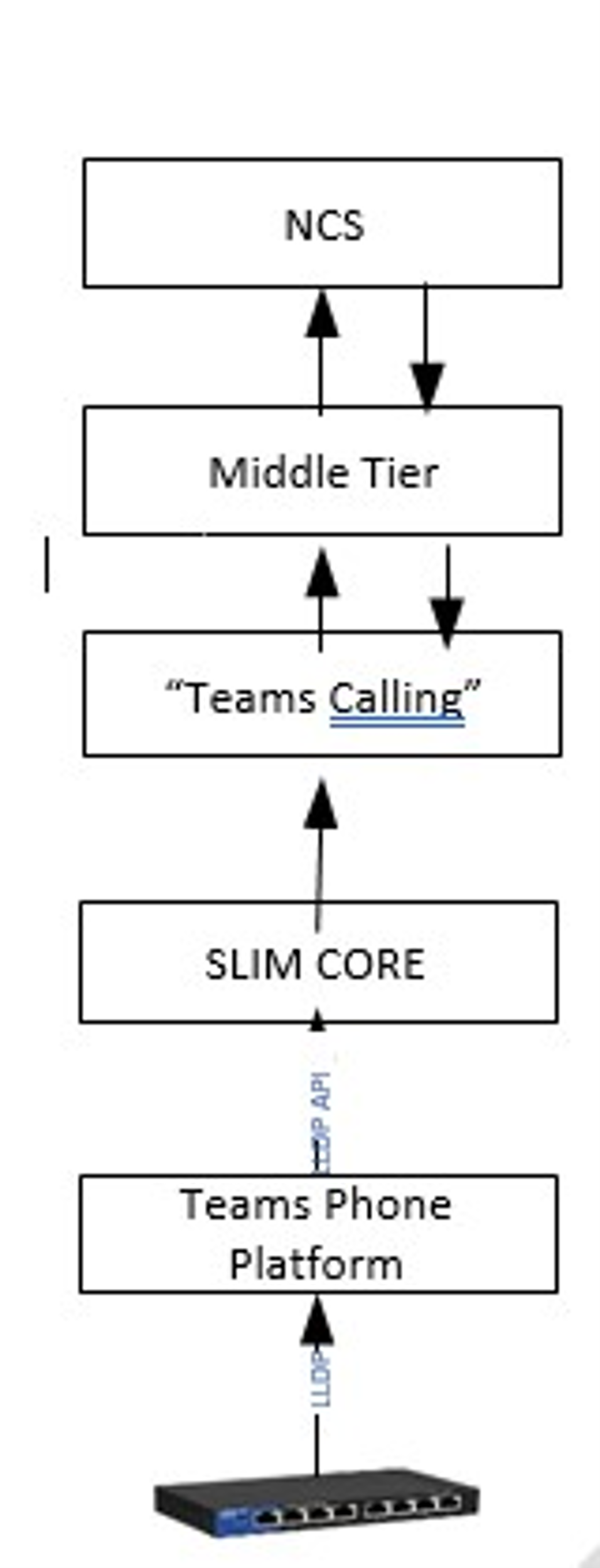
The firmware will send intent with info:

|  |  |
| --- | --- |
| Intent | com.microsoft.skype.teams.ipphone.partner.SHARE\_LLDP\_INFO |
| With Extras: | * Bytearray extra keyed with “CHASSIS\_ID ” This value is expected to be the raw value received from the switch as is. No formatting is expected to be done in FW. Formatting will be handled in Teams app. * Int extra keyed with “CHASSIS\_SUB\_TYPE ”. * Bytearray extra keyed with “PORT\_ID ” This value is expected to be the raw value received from the switch as is. No formatting is expected to be done in FW. Formatting will be handled in Teams app. * Int extra keyed with “PORT\_SUB\_TYPE”. * String extra keyed with “CORRELATION\_ID” which will be used to uniquely identify the request |

1. Firmware must resend LLDP information when some/any attribute changes.

**LLDP E2E Flow**

LLDP attributes in TLV format are fetched from by Teams Device 3rd party platform, as specified by IEEE 802.1AB. These attributes are consumed by the platform for its own needs. Slimcore is a Teams App media component that fetches LLDP Chassis ID and Port ID attributes from the device platform based on API that is specified in this document. These attributes, along with other network attributes are sent to “Teams Calling” and used to resolve Teams device dynamic location, as shown in the diagram below.



## Accessibility requirements

Partner applications deployed on the device must be compliant with accessibility requirements.

* Firmware must expose the settings below to support accessibility features on the device.
* The ability to enable/disable accessibility features should be one of the user settings under device settings. It should not be nested under other options. The accessibility setting should be disabled by default.

|  |  |  |
| --- | --- | --- |
| Feature | Priority | Description |
| Large Text | Mandatory | Provides users a UI experience with larger text size than normal |
| High Contrast Mode | Optional | Provides users a Teams experience with higher contrast on the screen |
| Color Correction | Mandatory | Provides users the ability to change color correction modes. |
| Talkback | Mandatory | As provided by Android OS |

## Microsoft Teams supported languages

Partner applications deployed on the device must be localized to any region supported by the partners. Microsoft Teams supported languages are listed for reference here:

<https://docs.microsoft.com/en-us/microsoftteams/audio-conferencing-supported-languages>

## Persistent Device ID Requirements

On Teams devices, we have many apps which may or may not be device owner apps and require access to the actual device hardware identifiers for multiple functionalities.

As mentioned in [this](https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html) article, from Android version 6 and greater, Android removes programmatic access to the device’s local hardware identifiers like MAC address for network adapters and serial number for apps using standard Android APIs. The WifiInfo.getMacAddress() and the BluetoothAdapter.getAddress() methods now return to a constant value of 02:00:00:00:00:00.

Moreover, from Android 10 release, according to [this](https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior), only device owner apps can access the actual device Wi-Fi MAC address.

**Requirements from Partners:**

* All Microsoft apps (Teams, Admin Agent, and Company Portal) present on Android Teams devices must be able to read MAC addresses of all ethernet, Wi-Fi and Bluetooth adapters present on the device.
* Teams, Admin Agent and Company Portal apps used on Android Teams devices must be able to read the device serial number.
* Partners should disable any randomized or dummy MAC addresses and serial numbers behavior. All Microsoft apps must be able to read the real addresses and serial numbers. See this for more details: [MAC Randomization Behavior  |  Android Open Source Project](https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior)
* MAC addresses and serial numbers must not be reset or changed on factory reset, OS or app update, or sign out. All hardware identifiers reported must always be the same.
* All Microsoft apps must be pre-granted all relevant permissions required by the OS to read the hardware identifiers.

**APIs used by Microsoft apps to read hardware identifiers:**

Microsoft apps leverage the following APIs to read the various device identifiers. These APIs must meet the requirements mentioned above:

* WifiInfo.getMacAddress()
* NetworkInterface.getHardwareAddress()
* BluetoothAdapter.getAddress()
* Build.getSerial()
* Build.SERIAL

**Permissions used by Microsoft apps to read hardware identifiers:**

Microsoft apps declare the following permissions in their AndroidManifest.xml:

READ\_PHONE\_STATE, READ\_PRIVILEGED\_PHONE\_STATE

We also expect that in future Android OS releases, Google will continue to evolve their OS and may introduce new restrictions which can prevent Microsoft apps from reading the MAC addresses. OEMs must relax those restrictions in all supported Android OS versions and allow Microsoft apps to read MAC addresses.

# Partner Applications requirements

Partner applications are Android applications that are developed and delivered by partners to users and phone administrators. These applications enable end users to customize the hardware experience of their phones and provide admins the ability to debug the phones for connectivity issues.

The term “partner applications” in this specification refers to the applications that are specified as mandatory in this section. The following terms and associated meaning will be used throughout this section.

M = Mandatory

O = Optional

Config Y/N = Controlled via TAC configuration settings

## Partner Applications requirements

* Partner applications must be available for users as part of the Out-of-the-Box experience.
* Partner applications must be invoked by the Microsoft Teams application and should not be accessible to the user directly via user interface or hardware buttons.
* Partners must write the required *Partner* *Settings* and *Admin Only* applications using the minimum Android OS version specified in the latest product requirements documents.
* Partner applications must be updated by the Microsoft Teams Admin Center through firmware updates.
* Partner applications must provide a user interface to exit the application.
  + The option for a user to exit the partner application and go back to the Microsoft Teams user interface can be via a back button or an exit button.
* Partner applications must use the same user interface theme as the Microsoft Teams application as defined in the following guidelines:
  + *Microsoft Teams Guidelines for Partners. pdf*
* Partner applications must use the same languages as the Microsoft Teams application. See supported languages section
* Partner applications should be delivered packaged with the firmware build
* The partner applications should provide support for deep linking.
  + See <https://developer.android.com/training/app-links/deep-linking.html>. This allows the partner to develop a single app for *Phone* *Settings* and *Admin Only* and allow the Microsoft Teams application to link to specific sections as needed.
    - //admin activity
    - android:scheme=”msteamspartner”
    - Android:host=”admin”
    - //setttings activity
    - android:scheme=”msteamspartner”
    - android:scheme=”settings”

## Partner Agent requirements

Partner must develop a partner agent to communicate with Microsoft Device Management solution as defined by the following:

* *Partner Agent Dev Design v3.pdf*

## Partner Device Settings requirements

Partners are required to implement a Device Settings application with two different interfaces:

* End User Interface
* Admin Interface – requires admin password to access advance menu options

There are two entries to access Device Settings application.

* On Sign in screen

A screenshot of a computer

Description automatically generated

* Under Settings

A screenshot of a phone

Description automatically generated

The Admin Interface must be available for all modes (personal, CAP, shared) and regardless of who is logged into the device in a Hotdesking scenario (host or user).

### Personal Mode/ Host User: End User interface requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Settings | Feature Type | Action | M/O | Default | Config Y/N |
| Language | List of Supported Languages | Ability for users to modify the language of the Microsoft Teams application on the device | M | To be set based on the region SKU | Yes |
| Time/Date Format\* | List of Date/Time Format options | Ability for users to modify the time/date format displayed on the devices | O | To be set based on the region SKU | Yes |
| Time Zone | Ability for users to select from standard Android time zone | M | To be set based on the region SKU | Yes |
| Display | List of Backlight / screen saver options | Ability for users to adjust backlight time out and screensaver wait time value | M | 30 mins | No |
| Phone Lock | Enable/Disable toggle button | Ability for users to enable/disable phone lock | M | Disabled | Yes |
| Timeout | Ability for users to modify idle time out after which phone is locked | M | 15 Minutes | Yes |
| PIN | When phone lock is enabled, ability for users to set a pin code - 6 digits, digits only, cannot start with emergency number of the number mask | M | N/A | Yes |
| Bluetooth\* | Bluetooth on/off | Ability for users to Enable and disable the Bluetooth discovery | M | Disabled | No |
| Scan/Discover | When Bluetooth is on, ability for users to scan/discover Bluetooth devices | M | Disabled | No |
| Wi-Fi\* | Wi-Fi Enable/Disable toggle | Ability for users to Enable/Disable Wi-Fi | M | Disabled | No |
|  | When Wi-Fi enabled, ability for users to select an available connection from the list and enter connection credentials | M | Disabled | No |
| Accessibility | High Contrast Mode | Ability for users to enable/disable high contrast mode. | M | Off | No |
| Large text | Ability for users to enable/disable large text | M | Off | No |
| Color correction | Ability for users to select Android standard color correction options | M | Off | No |
| Reboot | Reboot Phone | Ability to reboot the phone | M | N/A | N/A |
| About | Screen to display various device info | About screen that has version information –   * IP address * WLAN MAC address * Device MAC address * Bluetooth MAC address * Serial Number * Firmware version * Partner Agent version * Company Portal version * Admin Agent version * Teams Version | M | N/A | No |
| Volume | Volume bar | Setting device volume | O | 50% | N/A |
| Admin Login | Provide password to  login into Admin settings | Ability to login for advance menu options | M | No Password | N/A |

**Notes \***

**Time/Date Format:** Teams app currently supports only one date/time format

**Bluetooth:** Partner needs to enable BLE in firmware

**WiFi**: The WiFi option should be *Disabled* by default if the device supports physical WLAN connection

### Personal Mode/Host User:Admin user interface requirements

Partner must provide an *Admin Only* application. The *Admin Only* application must be password protected and accessed only by administrators with appropriate privileges.

The *Admin Only*application must have the following features:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Settings | Feature Type | Action | M/O | Default | Admin Override (Y/N) |
| Network | Network Configuration | PC Port toggle (On/Off)  WAN Port Options:   * IP Mode * IPv4 Type * IPv4 Static DNS toggle * Ipv6 Type * IPv6 Static DNS toggle   -WiFi Port  -VLAN  -PC Port  -DHCP VLAN toggle  -HTTP Port  -HTTPS Status toggle  -LLDP Status toggle  -CDP Status toggle  Proxy selection | M | N/A | Yes |
| Debug | Reset user settings | Reset all settings that can be controlled by end user to default values | M | Off | Yes |
|  | Reset to factory defaults | Reset firmware version and all options to factory defaults | M | Off | Yes |
| Admin Password | Set and reset password | Ability for admin to set and reset the admin password | M | N/A | Yes |
| Admin  Sign out | Sign out of the admin account | Ability for admin to sign out of admin interface | M | N/A | Yes |

### Shared Mode: Conference Phone /CAP/Hot Desking User: End user interface requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Device Settings | Feature Type | | Action | M/O | Default | Config Y/N |
| Accessibility | | High Contrast Mode | Ability for users to enable/disable high contrast mode | M | Off | No |
| Large text | Ability for users to enable/disable large text | M | Off | No |
| Color correction | Ability for users to select Android standard color correction options | M | Off | No |
| Reboot | | Reboot Phone | Ability to reboot the phone | M | N/A | N/A |
| About\* | | Screen to displaying various device info | About screen that has version information –   * IP address * WLAN MAC address * Device MAC address * Bluetooth MAC address * Serial Number * Firmware version * Partner Agent version * Company Portal version * Admin Agent version * Teams Version | M | N/A | No |
| Volume | | Volume bar | Setting device volume | O | 50% | N/A |
| Admin Login | | Provide password to  login into Admin settings | Ability to login for advance menu options | M | No Password | N/A |

### Shared Mode: Conference Phone /CAP/ Hot Desking User: Admin user interface requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Settings | Feature Type | Action | M/O | Default | Policy Controlled  Y/N |
| Language | List of supported Languages | Ability for users to modify the language of the Microsoft Teams application on the device | M | To be set based on the region SKU | Yes |
| Time/Date Format\* | List of Date/Time Format options | Ability for users to modify the time/date format displayed on the devices | O | To be set based on the region SKU | Yes |
| Time Zone | Ability for users to select from standard Android time zone | M | To be set based on the region SKU | Yes |
| Display | List of Backlight / screen saver options | Ability for users to adjust backlight value | M | 30mins | No |
| Ability for users to adjust backlight DIM timeout | O | TBD | No |
| Ability for users to enable/disable screensaver | M | Enabled | No |
| Ability for users to select screensaver type | O | N/A | No |
| Ability for users to select screensaver waiting time | M | 30 Mins | No |
| Ability for users to select screensaver background | O | Disabled | No |
| Phone Lock | Enable/Disable toggle button | Ability for users to enable/disable phone lock | M | Disabled | Yes |
| Timeout | Ability for users to modify idle time out after which phone is locked | M | 15 Minutes | Yes |
| PIN | When phone lock is enabled, ability for users to set a pin code - 6 digits, digits only, cannot start with Emergency Number of the Number Mask. | M | NA | Yes |
| Bluetooth\* | Bluetooth on/off | Ability for users to Enable and disable the Bluetooth discovery | M | Disabled | No |
| Scan/Discover | When Bluetooth is on, ability for users to scan/discover Bluetooth devices | M | Disabled | No |
| Wi-Fi\* | Wi-Fi Enable/Disable toggle | Ability for users to Enable/Disable Wi-Fi | M | Disable | No |
|  | When Wi-Fi enabled, ability for users to select an available connection from the list and enter connection credentials | M | Disabled | No |
| Network | Network Configuration | PC Port toggle (On/Off)  WAN Port Options:   * IP Mode * IPv4 Type * IPv4 Static DNS toggle * Ipv6 Type * IPv6 Static DNS toggle   -WiFi Port  -VLAN  -PC Port  -DHCP VLAN toggle  -HTTP Port  -HTTPS Status toggle  -LLDP Status toggle  -CDP Status toggle  Proxy selection | M | N/A | N/A |
| Debug | Reset user settings | Ability to reset the device | M | Off | Yes |
|  | Reset to factory defaults | Reset firmware version and all options to factory defaults | M | N/A | N/A |
| Admin Password | Set and reset admin password | Ability for admin to set and reset the admin password | M | N/A | Yes |
| Admin  Sign out |  | Ability for admin to sign out of admin interface | M | N/A | Yes |
| Teams User Sign-out |  | Ability for Admin to sign-out Teams app signed-in user | M | N/A | N/A |

**Notes \***

**Time/Date Format:** Teams app currently supports only one date/time format

**Bluetooth:** Partner needs to enable BLE in firmware

**WiFi**: The WiFi option should be *Disabled* by default if the device supports physical WLAN connection