BluBØX Partner Services

BluID SDK Requirements and Developer Test Plan

[Partner Name] – [Application Name]

February 1, 2022

Table of Contents

[1 Introduction 4](#_Toc63696096)

[Scope 4](#_Toc63696097)

[2 Requirements 5](#_Toc63696098)

[2.1 Technology Partner Integration 5](#_Toc63696099)

[*2.1.1.* Branding 5](#_Toc63696100)

[*2.1.2. Terminology* 5](#_Toc63696101)

[*2.1.3 Application ID* 5](#_Toc63696102)

[*2.1.4. Application Version/Description* 6](#_Toc63696103)

[*2.2* Configuration 7](#_Toc63696104)

[*2.2.1. Background Scanning* 7](#_Toc63696105)

[*2.2.2. Device Locked/Unlocked* 7](#_Toc63696106)

[*2.2.3. Opening Triggers* 7](#_Toc63696107)

[*2.2.4. Reader Feedback* 7](#_Toc63696108)

[*2.2.5. RSSI* 7](#_Toc63696109)

[*2.2.6. Lock Service Code* 8](#_Toc63696110)

[*2.2.7. Notifications* 8](#_Toc63696111)

[*2.3 Usability* 9](#_Toc63696112)

[*2.3.1. Silent Personalization* 9](#_Toc63696113)

[*2.3.2. Deep Link Personalization* 9](#_Toc63696114)

[*2.3.3. Single Step Issuance* 9](#_Toc63696115)

[*2.3.4. Endpoint Update* 9](#_Toc63696116)

[*2.3.5. Mobile ID revocation* 10](#_Toc63696117)

[*2.3.6. Device Termination* 10](#_Toc63696118)

[*2.3.7. Multiple Mobile IDs* 10](#_Toc63696119)

[*2.3.8. Multiple Invitation Codes* 10](#_Toc63696120)

[*2.3.9. Manual Invitation Code* 11](#_Toc63696121)

[*2.3.10. BLE* 11](#_Toc63696122)

[*2.3.11. NFC* 11](#_Toc63696123)

[*2.3.12. Reader Responsiveness/Feedback* 12](#_Toc63696124)

[*2.3.13. Opening Trigger Tutorial* 12](#_Toc63696125)

[*2.3.14. Photo ID* 12](#_Toc63696126)

[*2.4 Permissions, Notification, and Information* 13](#_Toc63696127)

[*2.4.1. Permission Requests* 13](#_Toc63696128)

[*2.4.2. Location Access Request* 13](#_Toc63696129)

[*2.4.3. Application Terminated Notification* 14](#_Toc63696130)

[*2.4.4. Application Running Information* 14](#_Toc63696131)

[*2.4.5. Apple Wallet Information* 14](#_Toc63696132)

[*2.4.6. BLE Disabled Information* 14](#_Toc63696133)

[*2.4.7. NFC Disabled Information* 15](#_Toc63696134)

[*2.4.8. No Mobile ID Issued Information* 15](#_Toc63696135)

[*2.4.9. BLE Reader Information* 15](#_Toc63696136)

[*2.4.10. Location Disabled Information* 16](#_Toc63696137)

[*2.4.11. Internet Disabled Information* 16](#_Toc63696138)

[*2.5 Support and Diagnostics* 17](#_Toc63696139)

[*2.5.1. Diagnostic Information* 17](#_Toc63696140)

[*2.5.2. Diagnostic Package* 17](#_Toc63696141)

[*2.6 Security and Privacy* 18](#_Toc63696142)

[*2.6.1. Access Logs* 18](#_Toc63696143)

[*.2.6.2. Security and Privacy Information* 18](#_Toc63696144)

[*2.6.3. Portal Device Lock Policy* 18](#_Toc63696145)

[*2.6.4. License Agreement* 18](#_Toc63696146)

[*3.1* *Verify BLUBØX Branding Guidelines* 19](#_Toc63696147)

[*3.2 Verify Configuration View* 20](#_Toc63696148)

[*3.3 Verify Interactions with Reader* 22](#_Toc63696149)

[*3.4 Verify Diagnostic Information* 32](#_Toc63696150)

[*3.5 Verify Security and Privacy information* 34](#_Toc63696151)

[*3.6 Verify Permission Requests/Notification information* 35](#_Toc63696152)

1 Introduction

.

The purpose of this document is to provide an overview of all the requirements of SDK application for developers to build what is expected and partners to validate their solution and share the results with BLUBØX.

The document includes a requirement which should be answered truthfully on their implementation status and a set of test cases that must be verified for each application before submitting for approval.

Scope

The scope of this BluBØX Partner Services document is to:

* Define a list of requirements to collect information about the implementation.
* Outline test steps that should be performed for the application.

2 Requirements

2.1 Technology Partner Integration

 These criteria ensure that your app utilizes the standard design provided by BluBØX.

2.1.1. Branding

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| TP-01Mandatory | Application to display SEOS logo according to the logo branding guides.The application must display the SEOS logo per the BluBØX Global branding guidelines for technology Partners.1. SEOS logo is displayed on the mobile id screen.
2. [Image](https://origo.hidglobal.com/developers/) to be used as provided by BLUBØX
 | [TS-02](#TS_02)Android/iOS |

2.1.2. Terminology

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| TP-02Mandatory | Application utilizes the proper BluID Mobile Identities terminology: * Invitation Code,
* BluID SDK version,
* Mobile ID,
* Seos ID,
* Endpoint App Version.

The application should use BluID Global terminology to display that information to end-users. | [TS-09](#TS_09)Android/iOS |

2.1.3 Application ID

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| TP-03Mandatory | Application to utilize Application ID according to the BluID guidelines.Application ID should be of below format: BLUID-<COMPANY NAME>-<APPLICATION NAME> | [TS-10](#TS_10)Android/iOS |

2.1.4. Application Version/Description

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| TP-04Mandatory | The Application to utilize the proper Application-Version (iOS), Application Description (Android)Application Version should be of below format: BLUID-<COMPANY NAME>-<APPLICATION NAME>-<VERSION> Application Description should be of below format: BLUID-<COMPANY NAME>-<APPLICATION NAME>-<DESCRIPTION> | [TS-10](#TS_10)Android/iOS |

2.2 Configuration

These criteria ensure that your app utilizes the configurations as per the standards.

2.2.1. Background Scanning

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-01Recommended | Application allows you to configure if BLE scanning works in the background.The Application should allow the end-user to configure if BLE scanning works in the background. | [TS-03](#TS_03)Android/iOS |

2.2.2. Device Locked/Unlocked

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-02Recommended | Application allows you to configure if BLE scanning works when device is locked.For enhanced security, the Application should allow the end-user to configure if BLE Openings are allowed when the device is locked. |  [TS-04](#TS_04)Android/iOS |

2.2.3. Opening Triggers

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-03Recommended | Application allows you to select which opening triggers are enabled.The application should allow end-users to select which opening triggers they would like to enable. |  [TS-05](#TS_05)Android/iOS |

2.2.4. Reader Feedback

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-04Recommended | Application allows you to select User feedback (Sound, Vibration) when unlocking reader.The application should allow end-users to select feedback while unlocking the reader |  [TS-06](#TS_06)Android/iOS |

 2.2.5. RSSI

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-05Recommended | App allows you to configure Bluetooth RSSI sensitivity (High, Medium, Low) (Android Only)The application should allow end-users to adjust Bluetooth RSSI sensitivity for accessing the reader  |  [TS-07](#TS_07) Android  |

 2.2.6. Lock Service Code

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-06Recommended | Application allows you to select custom lock service code.As a user I can configure a lock service code to work with a custom lock server set |  [TS-08](#TS_08) Android/iOS |

 2.2.7. Notifications

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| CN-07Recommended | The user of the app should be able to configure the types of Mobile Access notifications they receive.Application should allow to configure the types of Mobile Access notifications they receive |  [TS-01](#TS_01) Android/iOS |

2.3 Usability

These criteria ensure that your app provides the interactions with device and reader appropriately.

2.3.1. Silent Personalization

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-01Best-Practice | Device is personalized without user having to type invitation code.* Provides an option as initialize which works in background to automatically personalize device for respective user logged into the App.
* To create a frictionless experience, it is recommended that the user is not prompted to enter the invitation code.
 |  [TS-11](#TS_11) Android/iOS |

2.3.2. Deep Link Personalization

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-02Optional | Utilize an email link to automatically populate invitation code for personalization.App personalizes the device automatically by clicking on email link which is generated by respective user when logs in. |  [TS-30](#TS_30) Android/iOS |

2.3.3. Single Step Issuance

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-03Recommended | The app handles single step personalization and Mobile ID issuance by polling until a Mobile ID has been delivered.* The application should be able to handle the delay and provide a good process during the provisioning by issuing Invitation Code and Mobile ID at the same time.
* There should not be any delay between the device personalization and Mobile ID issuance.
 |  [TS-34](#TS_34) Android/iOS |

2.3.4. Endpoint Update

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-04Mandatory | The application provides an end-user-initiated way to perform endpoint update such as a button or pull-to-refresh.The application should provide a user-initiated way to perform Endpoint Update. This allows the end-user to troubleshoot Mobile ID issuance issues. |  [TS-35](#TS_35) Android/iOS |
| US-05Recommended | The app utilizes push notifications in background and auto refresh in foreground to perform endpoint update.When App provides an update either in issuing/revoking in Mobile Id (or) credential update, automatic notification should happen at background and refresh in app in foreground to perform endpoint updates |  [TS-36](#TS_36) Android/iOS |

2.3.5. Mobile ID revocation

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-06Mandatory | When a Mobile ID is revoked, the app displays the proper state'No Mobile ID is issued'.When a Mobile ID has been revoked, the application must display the proper state that there is no Mobile ID and Mobile Access will not function. |  [TS-37](#TS_37),  [TS-38](#TS_38),  [TS-39](#TS_39) Android/iOS |

2.3.6. Device Termination

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-07Mandatory | When an endpoint is terminated the application returns to a state where It can consume an invitation code* When a device is terminated, the application must return to a state where a new Mobile ID can be issued.
* The user should be informed clearly that Mobile Access is not setup.
* There should not be any delay in updating the endpoint
 |  [TS-40](#TS_40) Android/iOS |

2.3.7. Multiple Mobile IDs

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-08Optional | The app can support multiple Mobile IDs being issued.* App must be supporting multiple Mobile Ids for users who are experiencing to access the readers in different areas.
* Mobile ids issued must be from different MOB Keys
 |  [TS-41](#TS_41) Android/iOS |

2.3.8. Multiple Invitation Codes

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-09Optional | The app can consume multiple invitation codes.App should be supported to consume multiple invitation codes for secondary devices |  [TS-42](#TS_42)Android/iOS |

2.3.9. Manual Invitation Code

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-10Optional | Manually enter invitation code to personalize device(16 digits, All Caps, hyphen after every four digits)* App should be provided an option to enter only 16 digits and by default all should be in Caps.
* App should also support hyphen after every four digits which provides better experience for user to enter the invitation code
 |  [TS-12](#TS_12)Android/iOS |

2.3.10. BLE

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-11Best-Practice | The Application can perform the Tap operation.App should be configured to use Tap operation while accessing with reader and recommended to perform the operation in Background/Foreground scanning mode. | [TS-13](#TS_13),[TS-14](#TS_14),[TS-15](#TS_15)Android/iOS |
| US-12Optional | The Application can perform Twist and Go operationApp should be configured to use Twist and Go operation while accessing with reader and recommended to perform the operation in Background/Foreground scanning mode. | [TS-16](#TS_16),[TS-17](#TS_17),[TS-18](#TS_18)Android/iOS |
| US-13Optional | The Application can perform seamless opening triggers.The application should be configured and perform seamless opening triggers | [TS-19a](#TS_19a),[TS-19b](#TS_19b)Android/iOS |
| US-14Mandatory | The Application scans for the proper lock service codeApp scans for the proper lock service code and successfully opens against reader | [TS-21](#TS_21)Android/iOS |
| US-15Best-Practice | The Application supports a user initiated opening trigger.It is recommended to always have a user initiated opening trigger. | [TS-20](#TS_20)Android/iOS |
| US-17Best-Practice | The Application supports enhanced Tap.The application should be configured to use Enhanced Tap. | [TS-24](#TS_24), [TS-25](#TS_25)Android/iOS |

2.3.11. NFC

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-18Best-Practice | The Application supports NFC Tap.The application should be configured to use NFC Tap while accessing with reader and recommended to perform the operation in Background/Foreground scanning mode. | [TS-26](#TS_26), [TS-27](#TS_27), [TS-28](#TS_28)Android |

2.3.12. Reader Responsiveness/Feedback

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-16Mandatory | If using background scanning, the application should engage the reader even if not engaged for several hours.App should be worked in background and should successfully engage with reader even after several hours | [TS-22](#TS_22), [TS-23](#TS_23)Android/iOS |
| US-20Mandatory | The application provides feedback when the device communicates with a reader.When the application engages a reader, either in the foreground or background, the end-user should be given any of below feedback:Vibration, Notification(visual), Sound) that the Mobile ID was successfully or unsuccessfully transmitted to the Reader. Note: feedback currently cannot be provided through NFC due to the way NFC callbacks are handled. | [TS-31](#TS_31), [TS-32](#TS_32)Android/iOS |

2.3.13. Opening Trigger Tutorial

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-19Best-Practice | The app displays tutorials for the opening triggers implemented.To have a better experience, App should be provided an explanation for features to end users | [TS-29](#TS_29)Android/iOS |

2.3.14. Photo ID

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| US-21Optional | The app should support Photo ID and display the user’s photo and information.* App should be implemented to use Photo Id feature
* File size should be less than 1 MB.
* “. jfif,.pjpeg,.jpeg,.pjp,.jpg,.png" files are supported by default
* When user tried to upload any other format apart from the above mentioned, should throw an error that it supports only valid image.
 | [TS-33](#TS_33)Android/iOS |

2.4 Permissions, Notification, and Information

These criteria ensure that your app provides the expected functional behavior, with the appropriate level of Permissions and Notifications.

2.4.1. Permission Requests

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-01Recommended | Permissions are requested at an appropriate time and not all at once.The application should request permissions prior to usage, rather than all at once when the application is installed. | [TS-49](#TS_49)Android/iOS |
| PN-02Recommended | The user is informed that they must grant BLE access to utilize Mobile Access prior to allowing Mobile Access usage.* The application should provide an information screen detailing about BLE Access and will allow prior to asking for BLE Permissions.
* The explanation should be clear and explain the value by enabling BLE with mobile access.
 | [TS-56](#TS_56)Android/iOS |
| PN-04Best-Practice | Prior to requesting notification permissions, the application should inform the end-user that notifications will provide a better end-user experience. | [TS-58](#TS_58)Android/iOS |

2.4.2. Location Access Request

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-03Mandatory | The user is clearly informed that location access must be set as Mandatory for Mobile access to work * The application should provide an information screen detailing about location access must be set to always prior to asking for location permissions.
* The explanation should be clear and explain the value by setting location access to always with mobile access.
 | [TS-57](#TS_57)Android/iOS |
| PN-16Best-Practice | Application is provided an option as “Location Permissions” in settings App should enable user to change the location permission easily | [TS-64](#TS_64)Android |
| PN-17Best-Practice | User is provided a support for Android 10 & above location service changes The application should request permissions prior to usage and support for Android version 10 & above  | [TS-65](#TS_65), [TS-66](#TS_66), [TS-67](#TS_67) Android |
| PN-18Best-Practice | User is clearly informed that location access must be set for supporting Android version less than 10 for Mobile access to work | [TS-68](#TS_68), [TS-69](#TS_69)Android |
| PN-19Best-Practice | User is provided a support for iOS location service changes* The application should provide an information screen detailing about location access must be set to always prior to asking for location permissions
* The explanation should be clear and explain the value by setting location access to always with mobile access.
 | [TS-70](#TS_70), [TS-71](#TS_71)iOS |
| PN-20Best-Practice | User is provided a support to change the location permission through Device Enforcement set by organization | [TS-72](#TS_72), [TS-73](#TS_73), [TS-74](#TS_74), [TS-75](#TS_75)Android |

2.4.3. Application Terminated Notification

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-11Best-Practice | If the application is terminated, then the application should inform the user that Mobile Access will no longer work and to relaunch the app to enable Mobile Access. | [TS-51](#TS_51)Android/iOS |

2.4.4. Application Running Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-05Best-Practice | The end-user is clearly informed that the application must be running to use Mobile Access.* If the application is terminated, Mobile Access will no longer work.
* The end-user should be clearly informed that they must keep the application running if want to allow Mobile Access to work in the background.
* If the application is terminated, it is recommended that a notification be displayed informing the end-user to relaunch the application to continue using Mobile Access.
 | [TS-59](#TS_59)iOS |

2.4.5. Apple Wallet Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-06Best-Practice | The end-user should be clearly informed that Apple Pay dialogue will pop-up if they are within NFC range of a reader and that is expected. The end-user is informed any time when an iPhone is near an NFC field and that this is expected behavior and Mobile Access will continue to work. | [TS-60](#TS_60)iOS |
| PN-07Best-Practice | If the app suppresses Apple Pay, then the user should be clearly informed that Wallet will not work while the app is in the foreground | [TS-61](#TS_61)iOS |

2.4.6. BLE Disabled Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-08Mandatory | If BLE Has been disabled, then the application should provide a dialogue clearly informing that BLE is disabled and Mobile Access will not work and provide information on how to re-enable BLE.* If BLE is disabled, the application should clearly inform the end-user that BLE opening triggers will not work.
* To regain use of Mobile Access the end-user should be informed they must enable BLE and give them instructions on how to re-enable BLE.
* The dialogue message should be prominent and clearly displayed when the end-user launches the application.
 | [TS-62](#TS_62)Android/iOS |
| PN-13Best-Practice | If the app is in the background and BLE is disabled, the application will display a notification to the user that BLE has been disabled and to re-enable for Mobile Access to work.* If BLE is disabled, the application should clearly inform the end-user that BLE opening triggers will not work in background.
* Notification should be given to user that BLE has been disabled and request to re-enable for mobile access to work
 | [TS-53](#TS_53)Android/iOS |

2.4.7. NFC Disabled Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-09Best-Practice | If NFC Has been disabled, then the application should provide a dialogue clearly informing that NFC is disabled and Mobile Access will not work and provide information on how to re-enable NFC.* If NFC is disabled, the application should clearly inform the end-user that NFC opening triggers will not work.
* To regain use of Mobile Access the end-user should be informed they must enable NFC and give them instructions on how to re-enable NFC.
* The dialogue message should be prominent and clearly displayed when the end-user launches the application.
 | [TS-63](#TS_63)Android |

2.4.8. No Mobile ID Issued Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-14Best-Practice | When there is no Mobile ID issued, the app indicates that no Mobile ID is issued and ideally who they can contact to obtain a Mobile ID.* The application should provide a screen indicating that no Mobile ID has been delivered to the device.
* The application should also ideally provide information on where to obtain a Mobile ID and a way to manually perform an endpoint update.
 | [TS-54](#TS_54)Android/iOS |

2.4.9. BLE Reader Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-15Best-Practice | When the app is in the foreground, the app provides an indication to the user the reader is in range.* The application should provide indicating that Reader is within range to access it.
 | [TS-55](#TS_55)Android/iOS |

2.4.10. Location Disabled Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-10Best-Practice | If location access is not set, then the application should provide a dialogue clearly informing that location access is not set and Mobile Access will not work and provide information on how to configure location access to be all.* If Location Access is not set, the application should clearly inform the end-user that opening triggers will not work.
* To regain use of Mobile Access the end-user should be informed they must configure permissions appropriately and give them instructions on how to re-enable.
* The dialogue message should be prominent and clearly displayed when the end-user launches the application.
 | [TS-50](#TS_50)Android/iOS |

2.4.11. Internet Disabled Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| PN-12Best-Practice | When internet is disabled on the device and the user attempts to perform an operation that requires internet, a dialogue will be displayed informing the user that they must enable internet for that operation.* If Internet is disabled, the application should clearly inform the end-user to enable internet while user attempts any operation.
 | [TS-52](#TS_52)Android/iOS |

2.5 Support and Diagnostics

These criteria ensure that apps provide the information and support to the end users

2.5.1. Diagnostic Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| SD-01Best-Practice | App displays diagnostic information including Mobile App version, SDK version, opening mode), Endpoint info (Endpoint Status, Seos ID, Last Server Communication, Environment) and Device info (OS Version, Bluetooth, NFC, Location, Permission Granted)The application should display diagnostic information to support end-user troubleshooting. | [TS-43](#TS_43)Android/iOS |

2.5.2. Diagnostic Package

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| SD-02Best-Practice | The application should be able to generate a diagnostics package to provide a support to specialist.App should support with specialist to support end-user for troubleshooting by getting diagnostic package | [TS-44](#TS_44)Android/iOS |

2.6 Security and Privacy

These criteria ensure that apps handle user data and personal information safely.

2.6.1. Access Logs

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| SP-01Best-Practice | App provides an Access Log of recent interactions with reader.App should log the recent interactions with reader that would help the support team for troubleshooting any issues | [TS-45](#TS_45)Android/iOS |

.2.6.2. Security and Privacy Information

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| SP-02Best-Practice | As a user, I should be able to view the Security and Privacy information for Mobile Access. | [TS-46](#TS_46)Android/iOS |

2.6.3. Portal Device Lock Policy

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| SP-03Optional | The application should enforce the portal setting for locked/unlock.Limits the usage of the mobile access app when the mobile device is locked | [TS-48](#TS_48)Android/iOS |

2.6.4. License Agreement

|  |  |  |
| --- | --- | --- |
| **ID/Type** | **Description** | **Linked Test Scenario** |
| SP-04Optional | The License and End User License Agreement is displayed for Mobile Access | [TS-47](#TS_47)Android/iOS |

3 Test Scenarios

3.1 Verify BLUBØX Branding Guidelines

|  |  |  |
| --- | --- | --- |
| TSID  | Description  | Partner Results |
| TS-02  | **Prerequisites**None**Test Steps**• Launch the app• Navigate to credential screen• Validate the SEOS Logo is displayed on Mobile App **Expected Result** The Seos logo is displayed  | ImplementedNotes |
| TS-09  | **Prerequisites**None**Test Steps**• Launch the app• Validate the Terminologies used on Mobile App **Expected Result** Application should utilize the below proper BLUID Mobile Identities terminology: Invitation Code, BLUID SDK version, Mobile ID, Seos ID, Endpoint App Version.                     | ImplementedNotes |  |
| TS-10 | **Prerequisites**None**Test Steps**1.Login to BLUID portal and navigate to user2.Go to the device information section3.Verify the Application Description/Version as per respective IOS/Android Devices Note: Make sure Application Id and Application Description/Version is appropriate for partners, who are not using BLUID portal for their solution**Expected Result** Application ID should be of below format: BLUID-<COMPANY NAME>-<APPLICATION NAME> b. Application Description/Version should be of below format: BLUID-<COMPANY NAME>-<APPLICATION NAME>-<DESCRIPTION/VERSION> Note: Application ID will be verified by BLUID Partner services  | ImplementedNotes |

3.2 Verify Configuration View

|  |  |  |
| --- | --- | --- |
| TSID | Description | Partner Results |
| TS-01 | **Prerequisites**None**Test Steps**1.Launch the App.2.Provide an option to configure the below types of Mobile Access notifications they receive:BLE/NFC/location services,Scanning mode options,Mobile id status updates.**Expected Result** User should be able to configure the types of Mobile Access notifications they receive:BLE/NFC/location services,Scanning mode options,Mobile id status updates. | ImplementedNotes |
| TS-03  | **Prerequisites**None**Test Steps**1.Launch the app2.In Settings, verify that the app provides an option to configure/allow BLE scanning in the background **Expected Result** User should be provided an option to allow the BLE scanning in Background. | ImplementedNotes  |
| TS-04  | **Prerequisites**None**Test Steps**1.Launch the app2.In Settings, verify that the app provides an option to configure/allow BLE scanning when device is locked **Expected Result** User should be provided an option to allow the BLE scanning when device is locked. | ImplementedNotes  |
| TS-05  | **Prerequisites**None**Test Steps**1.Launch the app2.In Settings, provide an option to configure the below opening triggers for accessing the readers: a. Tap, b. Twist &Go,c. Custom, d. Seamless **Expected Result** User should be provided an option to configure any of opening triggers for accessing with the readers. | ImplementedNotes  |
| TS-06  | **Prerequisites**None**Test Steps**1.Launch the app2.In settings, provide an option to configure for unlocking reader:a. Play sound when unlockingb. Vibrate when unlocking **Expected Result** User should be provided an option to configure the feedback while accessing with the reader | ImplementedNotes  |
| TS-07  | **Prerequisites**None**Test Steps**1.Launch the app2.In settings, provide an option to configure RSSI sensitivity for android device  a. High b. Medium c. Low **Expected Result** User should be provided an option to configure BLE RSSI sensitivity for better accessing with reader | ImplementedNotes  |
| TS-08 | **Prerequisites**None**Test Steps**Configure a lock service code to work with a custom lock server set **Expected Result** User should be able to configure a lock service code  | ImplementedNotes  |

3.3 Verify Interactions with Reader

|  |  |  |
| --- | --- | --- |
| TSID | Description | Partner Results |
| TS-11  | **Prerequisites**Partner Organization must have available quantity of Mobile ID and user license.**Test Steps**1.Launch the App2.Automatically redirects to mobile id screen without entering any invitation code/without any registration page3.Validate the Mobile id is issued automatically.**Expected Result** User should be able to view Mobile Id issued successfully without entering any invitation code | ImplementedNotes  |
| TS-12  | **Prerequisites**Partner Organization must have available quantity of Mobile ID and user license.**Test Steps**1.Launch the app 2. Enter Invitation code issued by operator to register device.**Expected Result** Invitation code should be provided by 16 digits capital letters by default and after every 4 digits Hyphen is automatically displayed | ImplementedNotes  |
| TS-13 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed.**Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Foreground scanning for TAP opening type.**Expected Result** User should be able to access with reader by performing TAP operation in Foreground | ImplementedNotes  |
| TS-14 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Background scanning (device is Unlocked) for TAP opening type.**Expected Result** User should be able to access with reader by performing TAP operation in Background (when device is Unlocked) | ImplementedNotes  |
| TS-15 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Background scanning (device is locked) for TAP opening type.**Expected Result** User should be able to access with reader by performing TAP operation in Background (when device is locked) | ImplementedNotes  |
| TS-16 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Foreground scanning for TWIST AND GO opening type.**Expected Result** User should be able to access with reader by performing TWIST AND GO operation in Foreground. | ImplementedNotes |
| TS-17 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Background scanning (device is Unlocked) for TWIST AND GO opening type.**Expected Result** User should be able to access with reader by performing TWIST AND GO operation in Background (when device is Unlocked) | ImplementedNotes |
| TS-18 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Background scanning (device is locked) for TWIST AND GO opening type.**Expected Result** User should be able to access with reader by performing TWIST AND GO operation in Background (when device is locked) | ImplementedNotes |
| TS-19a | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Foreground scanning when Bluetooth & location services is ON using Seamless operation.**Expected Result** User should be able to perform Seamless operation with reader in Foreground | ImplementedNotes |
| TS-19b | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3. Check the access against the reader for issued mobile id in Background scanning when Bluetooth & location services is ON using Seamless operation.**Expected Result** User should be able to perform Seamless operation with reader in Background | ImplementedNotes |
| TS-20 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Foreground scanning for CUSTOM option.**Expected Result** User should be able to access with reader using CUSTOM option in Foreground | ImplementedNotes |
| TS-21 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id.**Expected Result** App scans for the proper lock service code and successfully opens against reader | ImplementedNotes |
| TS-22 | **Prerequisites**1.Bluetooth/NFC is turned on2. Location services permission is allowed3. At least 1 BLUID Mobile ID available**Test Steps**1.Launch the App2. Engage the reader with mobile for frequency check i.e., after every 1hr,4hrs,12hrs,24hrs of the first scan in Foreground.**Expected Result** Should successfully engage with reader after every 1hr,4hrs,12hrs,24hrs | ImplementedNotes |
| TS-23 | **Prerequisites**1.Bluetooth/NFC is turned on2. Location services permission is allowed3. At least 1 BLUID Mobile ID available**Test Steps**1.Launch the App2. Engage the reader with mobile for frequency check i.e., after every 1hr,4hrs,12hrs,24hrs of the first scan in background (Device is locked and unlocked)Note: The app should not be brought to foreground during this testing.**Expected Result** Should successfully engage with reader after every 1hr,4hrs,12hrs,24hrs when app is running in background | ImplementedNotes |
| TS-24 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id for Enhanced TAP opening type in foreground scanning.**Expected Result** User should be able to access with reader by performing Enhanced TAP operation in foreground | ImplementedNotes |
| TS-25 | **Prerequisites**1.Bluetooth is turned on.2.Location services permission is allowed**.****Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id for Enhanced TAP opening type in Background scanning (When device is locked/Unlocked)**Expected Result** User should be able to access with reader by performing Enhanced TAP operation in Background (When device is locked/Unlocked) | ImplementedNotes |
| TS-26 | **Prerequisites**NFC is turned on.**Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Foreground scanning for TAP opening type.**Expected Result** User should be able to access with reader by performing TAP operation in Foreground | ImplementedNotes |
| TS-27 | **Prerequisites**NFC is turned on.**Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Background scanning (device is Unlocked) for TAP opening type.**Expected Result** User should be able to access with reader by performing TAP operation in Background (device is Unlocked) | ImplementedNotes |
| TS-28 | **Prerequisites**NFC is turned on.**Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id in Background scanning (device is locked) for TAP opening type.**Expected Result** User should be able to access with reader by performing TAP operation in Background (device is locked) | ImplementedNotes |
| TS-29 | **Prerequisites**None**Test Steps**1.Launch the App.2.App is provided with video tutorials for the opening below triggers implemented: Tap,Twist and Go,Smartwatch.**Expected Result** Should be able to provide video tutorials for end users | ImplementedNotes |
| TS-30 | **Prerequisites**Issue invitation code via email through API / Portal**Test Steps**1.Click on the link provided in email2.Automatically redirects to app through that invitation code link**Expected Result** Should utilize an email link to automatically populate invitation code for personalization | ImplementedNotes |
| TS-31 | **Prerequisites**1. Bluetooth/NFC is turned on2. Location services permission is allowed3. At least 1 BLUID Mobile ID available**Test Steps**1.Launch the App2.Issue Mobile id for device3.Check the access against the reader for issued mobile id4.Verify at least one below feedback from the device while accessing:a. Audible, b. Visual, c. Vibration.**Expected Result** Feedback should be provided from the device while accessing with reader | ImplementedNotes |
| TS-32 | **Prerequisites**1. Bluetooth/NFC is turned on2. Location services permission is allowed3. At least 1 BLUID Mobile ID available**Test Steps**1.Launch the App2.Check the access against the reader3.Error feedback from device when unable to communicate with a reader.**Expected Result** Feedback should be provided while unable to communicate with reader | ImplementedNotes |
| TS-33 | **Prerequisites**Create user in API / portal along with Photo Id uploaded**Test Steps**1.Launch the App and navigate to mobile id screen2.Click on Mobile id and Photo Id should be displayed which is uploaded3.File size should be less than 1 MB4.Check ".jfif,.pjpeg,.jpeg,.pjp,.jpg,.png" files are supported by default5. Ensure when user tries to upload file which is different from supported files, throws error as ”Please upload a valid image”.**Expected Result** Photo Id should be displayed when clicked on Mobile id  | ImplementedNotes |
| TS-34 | **Prerequisites**1.Login to BLUID portal and create user2. Select below option in invitation & Mobile Issuance section: "Select and reserve Mobile ID(s) that will be issued when this user accepts the invitation code to register his or her device."**Test Steps**1.Launch the App2. Enter the Invitation code which is issued3. Validate the Mobile id is issued automatically after issuing invitation code.**Expected Result** Mobile Id should be issued in App | ImplementedNotes |
| TS-35 | **Prerequisites**Issue invitation code and Mobile ID through API / Portal**Test Steps**1.Launch the App2.Check the issued mobile id in APP3.Provide refresh option on the mobile id screen in case mobile id is not reflected automatically Check that whenever user tries to perform any of below operations, app will allow user-initiated way to perform endpoint update: a. Mobile Id update (Issuing/revoking) b. Device update (Add/Delete device)**Expected Result** App should be provided an option to refresh the endpoint updates | ImplementedNotes |
| TS-36 | **Prerequisites**Issue invitation code and Mobile ID through API / Portal**Test Steps**1.Launch the App after issuing mobile id in portal2.App should allow push notifications in background and auto refresh in foreground to perform endpoint update: a. Mobile Id update (Issuing/revoking) b. Device update (Add/Delete device)**Expected Result** Automatically endpoint updates should be performed  | ImplementedNotes |
| TS-37 | **Prerequisites**At least 1 BluID Mobile ID available**Test Steps**1.Launch the App2.Revoke the issued mobile id in portal3.Launch the App and verify that mobile id is revoked4.Verify below message is displayed"no Mobile id is issued".**Expected Result** “No Mobile Id is issued” message should be displayed | ImplementedNotes |
| TS-38 | **Prerequisites**At least 2 BLUID Mobile ID available**Test Steps**1.Launch the App2.Check the access against the reader for issued mobile id’s3.Revoke one mobile id among multiple mobile id’s issued in portal4.Launch the App and verify the mobile id is revoked5.Verify that still able to view remaining mobile id’s which is not revoked.**Expected Result** Mobile ids should be displayed according to actions performed.If mobile id is revoked, then mobile id should not be displayed in app  | ImplementedNotes |
| TS-39 | **Prerequisites**At least 2 BLUID Mobile ID available**Test Steps**1.Launch the App2.Verify the multiple mobile id’s issued in credential screen3.Check the access against the reader for issued mobile id’s4.Revoke all the mobile id’s issued in portal5.Launch the App and verify below message is displayed"no Mobile id is issued".**Expected Result** Mobile ids should be displayed according to actions performed.If mobile id is revoked, then mobile id should not be displayed and below message should be displayed:"no Mobile id is issued" | ImplementedNotes |
| TS-40 | **Prerequisites**At least 1 active device is available.**Test Steps**1.Login to the portal2.Delete the device for respective user in portal3.Launch the App and automatically should navigate to user identification page where user should provide invitation code to access.**Expected Result** Once device is terminated, automatically should redirect to user identification page. | ImplementedNotes |
| TS-41 | **Prerequisites**Issue invitation code and multiple Mobile ID through API / Portal**Test Steps**1.Launch the App2.Verify the multiple mobile id’s issued in credential screen3.Check the access against the reader for issued mobile ids.**Expected Result** User should be allowed to issue multiple mobile id’s and he/she could access as per restrictions provided at various locations | ImplementedNotes |
| TS-42 | **Prerequisites**None**Test Steps**1.Issue invitation code and Mobile ID through API / Portal2.Launch the App3.Check the issued mobile id in APP.4.Issue one more(multiple) invitation code for secondary devices5.Check the issued mobile id in APP6.Check the access against the reader for issued mobile id in secondary device.**Expected Result** User should be able to allow the invitation code for multiple devices | ImplementedNotes |

3.4 Verify Diagnostic Information

|  |  |  |
| --- | --- | --- |
| TSID | Description | Partner Results |
| TS-43 | **Prerequisites**At least 1 active device and mobile id is available.**Test Steps**1.Launch the App2. App is provided with below Diagnostic information: Application Info:a. BLUID Mobile Access Versionb. BLUID SDK versionc. Opening Moded. ReadersEndpoint Info:a. Endpoint Statusb. Seos IDc. Last Server Communication d. Endpoint App Version e. EnvironmentDevice Info: a. OS version b. Bluetoothc. Bluetooth Permissiond. Location Servicese. Location Services Permissionf. NFCg. NFC Permissionh. SIM Alliance API version **Expected Result** App should be provided an option to view diagnostic information | ImplementedNotes  |
| TS-44 | **Prerequisites**At least 1 active device and mobile id is available**.****Test Steps**1.Launch the App2. App is provided with Diagnostic information.**Expected Result** App should be able to generate a diagnostics package to provide a support to end users by partners.Below information should be provided to partners:Application Info:a. BLUID Mobile Access Versionb. BLUID SDK versionc. Opening Moded. ReadersEndpoint Info:a. Endpoint Statusb. Seos IDc. Last Server Communication d. Endpoint App Version e. EnvironmentDevice Info: a. OS version b. Bluetoothc. Bluetooth Permissiond. Location Servicese. Location Services Permissionf. NFCg. NFC Permissionh. SIM Alliance API versionError LogsScreenshots for reference | ImplementedNotes  |

3.5 Verify Security and Privacy information

|  |  |  |
| --- | --- | --- |
| TSID | Description | Partner Results |
| TS-45 | **Prerequisites**At least 1 active device and mobile id is available.**Test Steps**1.Launch the App.2.Navigate to Access Log section to view logs for recent interactions.3. Able to email the access log.**Expected Result**App should be provided an option to view logs for recent interactions with reader under Access Log section and provides a capability to email access log. | ImplementedNotes  |
| TS-46 | **Prerequisites**None**Test Steps**1.Launch the App.2.Navigate to Security and Privacy information for Mobile Access.**Expected Result**Should be able to view the Security and Privacy information for Mobile Access | ImplementedNotes  |
| TS-47 | **Prerequisites**None**Test Steps**1.Launch the App.2.Navigate to License and End User License Agreement for Mobile Access**Expected Result**App should be displayed with the License and End User License Agreement for Mobile Access | ImplementedNotes  |
| TS-48 | **Prerequisites**None**Test Steps**1. Login to the BLUID portal2.In Settings, Select the checkbox for limiting the usage of mobile access app when device is locked.**Expected Result**App should enforce the usage on unlocked mobile devicesNote: Limits the usage of the mobile access app when the mobile device is locked. | ImplementedNotes  |

3.6 Verify Permission Requests/Notification information

|  |  |  |
| --- | --- | --- |
| TSID | Description | Partner Results |
| TS-49 | **Prerequisites**None**Test Steps**1.Launch the App.2. Request the permissions at an appropriate time.**Expected Result**While engaging the reader, should get permission requests for BLE/NFC/location permission access. | ImplementedNotes  |
| TS-50 | **Prerequisites**Location Service are not enabled.**Test Steps**1.Launch the App.2.App displays persistent warning when Location Services are not set, and information on how to re-enable them to support.**Expected Result**Below warning message should be displayed:“Location Services needs to be enabled for Bluetooth to work; Mobile Access might not work properly.” Also, should provide information to re-enable to support in background.  | ImplementedNotes  |
| TS-51 | **Prerequisites**None**Test Steps**1.Launch the App.2.Issue Mobile Id to device 3.Verify the Mobile Id in App4.Delete the device. 5.Verify the Application Terminated Notification is displayed**Expected Result**App should be provided an information to relaunch the app to enable Mobile access when the application is terminated else Mobile Access will no longer work | ImplementedNotes  |
| TS-52 | **Prerequisites**None**Test Steps**1.Turnoff the internet connection in device2.Issue mobile id in portal3.Launch the App4.Will not view any mobile id in app and should be prompted as "Turn-on the Internet connection for updates"5.Turnon the connection and view the updates6.Check the mobile id issuance7.Turnoff the connection in device and revoke mobile id in portal8.Launch the App9.Still can view the mobile id in app as refresh is not happened and should be prompted that "Turn-on the Internet connection for updates"10. Turn-on the connection and view the updates.11.Mobile id will be revoked.**Expected Result**App should be displayed with a below dialogue informing that the user must enable internet for attempts to perform any operation that requires internet:"Turn-on the Internet connection for updates" | ImplementedNotes  |
| TS-53 | **Prerequisites**BLE is disabled.**Test Steps**1.Launch the App.2.Now make the App to run in background and check the notification when BLE is disabled.**Expected Result**App should display notification to the user that BLE has been disabled and to re-enable for Mobile Access to work, if the app is running in the background and BLE is disabled | ImplementedNotes |
| TS-54 | **Prerequisites**None**Test Steps**1.Launch the App.2. Verify that message is displayed when there is no Mobile ID issued for device.**Expected Result**"no Mobile id is issued" message should be displayed  | ImplementedNotes  |
| TS-55 | **Prerequisites**None**Test Steps**1.Launch the App.2.Access the device near to reader3. Check the app.**Expected Result**App should be provided an indication as "Reader is in range" to the user when reader is in range in foreground | ImplementedNotes  |
| TS-56 | **Prerequisites**None**Test Steps**1.Launch the App.2. Permissions request for BLE to utilize Mobile Access prior to allowing Mobile Access usage will be displayed.**Expected Result**Grant the permissions to BLE to utilize Mobile Access prior to allowing Mobile Access usage. | ImplementedNotes  |
| TS-57 | **Prerequisites**None**Test Steps**1.Launch the App.2.Location permissions request is displayed to utilize Mobile Access.**Expected Result**Should grant access to location services to utilize Mobile Access | ImplementedNotes  |
| TS-58 | **Prerequisites**None**Test Steps**1.Launch the App.2. App will be informed to the end-users that notifications will provide a better end-user experience. **Expected Result**Prior to requesting notification permissions, app should inform the end-user that notifications will provide a better end-user experience. | ImplementedNotes  |
| TS-59 | **Prerequisites**None**Test Steps**1.Launch the App.2.Verify that App can view the information that App is running and provides clear view to use Mobile Access.**Expected Result**Should be able to view the information that App is running and provides clear view to use Mobile Access | ImplementedNotes |
| TS-60 | **Prerequisites**None**Test Steps**1.Launch the App.2.Verify that end-user is clearly informed that Apple Pay dialogue will pop-up if they are within NFC range of a reader and that is expected.**Expected Result**Should be informed by displaying a pop-up if they are within NFC range of a reader  | ImplementedNotes  |
| TS-61 | **Prerequisites**None**Test Steps**1.Launch the App.2.Verify the pop-up is not displayed by Apple pay while app is in in foreground.**Expected Result**Apple Pay should be disabled to not show the user and the user should be informed that Apple Pay is being suppressed with a message while the app is in the foreground | ImplementedNotes  |
| TS-62 | **Prerequisites**BLE is disabled.**Test Steps**1.Launch the App.2. App displays persistent warning when BLE is disabled and informs the user to re-enable to utilize BLE opening triggers.**Expected Result**Below warning message should be displayed:“Bluetooth is OFF and Mobile Access might not work properly.” | ImplementedNotes  |
| TS-63 | **Prerequisites**NFC is disabled.**Test Steps**1.Launch the App.2. App displays persistent warning when NFC is disabled and informs the user to re-enable to utilize NFC opening triggers.**Expected Result**Below warning message should be displayed: “NFC is OFF and Mobile Access might not work properly.” and, should provide instructions on how to re-enable it to utilize NFC Tap | ImplementedNotes  |
| TS-64 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.Navigate to settings screen4.Validate the location permissions option5.Validate that when user clicks on location permissions option, it navigates to App permissions and from there location permissions can be updated.**Expected Result**Should be able to change the location permissions from Settings screen | ImplementedNotes  |
| TS-65 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow all the time
* Allow only while using the app
* Deny

4.Verify that by default the “Allow Mobile Access when” option in app settings will be set to “Always” when the user selects “Allow all the time” from the location permission when launching the app for the first time5.Verify that Location Permissions in App settings also displays as “Granted Always”**Expected Result**If Location permissions is selected as “Allow all the time” then by default “Allow Mobile access when” option is set as “Always” and other options “App is in foreground” and “Device is unlocked” should be enabled for user to select according to his action | ImplementedNotes  |
| TS-66 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow all the time
* Allow only while using the app
* Deny

4.Verify that the “Allow Mobile Access when” option in app settings will be set to “App is in Foreground” when the user selects “Allow only while using the app” from the location permission when launching the app for the first time5.Verify that Location Permissions in App settings also displays as “Granted while using app”**Expected Result**If Location permissions is selected as “Allow only while using the app”then “Allow Mobile access when” option is set as “App is in Foreground” and other options “Device is unlocked” and “Always” should be in disabled mode.Also below note is displayed:Android occasionally terminates apps running in the background. Consequently, “Device is unlocked” and “Always” modes sometimes require opening the app to restore | ImplementedNotes  |
| TS-67 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow all the time
* Allow only while using the app
* Deny

4.Verify that when the user selects “Deny” from the location permission, then Warning message is displayed in app as below “Location permissions is required for Bluetooth to work; Mobile Access might not work properly”5.Verify that Location Permissions in App settings also displays as “Denied”**Expected Result**If Location permissions is selected as “Deny”then Mobile access will not work and continuous below warning message should be displayed:“Location permissions is required for Bluetooth to work; Mobile Access might not work properly” | ImplementedNotes  |
| TS-68 | **Prerequisites**NeedAndroid device which has version less than 10**Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.Verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow
* Deny

4.Verify the access with reader when the user selects “Allow” from the location permission**Expected Result**If Location permissions is selected as “Allow” then Mobile access should work and able to access with reader with BLE | ImplementedNotes  |
| TS-69 | **Prerequisites**NeedAndroid device which has version less than 10**Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow
* Deny

4.Verify that when the user selects “Deny” from the location permission, then Warning message is displayed in app as below “Location permissions is required for Bluetooth to work; Mobile Access might not work properly”**Expected Result**If Location permissions is selected as “Deny”then Mobile access will not work and continuous below warning message should be displayed:“Location permissions is required for Bluetooth to work; Mobile Access might not work properly” | ImplementedNotes  |
| TS-70 | **Prerequisites**NeediOS device **Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.Verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow Once
* Allow While Using app
* Don’t Allow

4.Verify the access with reader when the user selects either “Allow Once” or “Allow While Using app” from the location permission**Expected Result**If Location permissions is selected as either “Allow Once” or “Allow While Using app”, then Mobile access should work and able to access with reader with BLE | ImplementedNotes  |
| TS-71 | **Prerequisites**NeediOS device **Test Steps**1.Launch the App.2.Enter Invitation code and Issue Mobile id to Device.3.verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow Once
* Allow While Using app
* Don’t Allow

4.Verify that when the user selects “Don’t Allow” from the location permission, then Warning message is displayed in app as below “Location permissions is required for Bluetooth to work; Mobile Access might not work properly”**Expected Result**If Location permissions is selected as “Don’t Allow”then Mobile access will not work and continuous below warning message should be displayed:“Location permissions is required for Bluetooth to work; Mobile Access might not work properly” | ImplementedNotes  |
| TS-72 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Login to BLUID portal2.Navigate to Settings under respective organization3.Limit the usage of Mobile access app when device is locked by selecting the checkbox under “Mobile Access App usage on unlocked mobile devices” section.4.Create user and issue invitation code.5.Launch the App.6.Enter Invitation code and Issue Mobile id to Device.7.Verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow all the time
* Allow only while using the app
* Deny

8.Verify that user selects “Allow all the time” from the location permissions dialog9.Validate the Location permissions & Allow Mobile access section in Settings**Expected Result**WhenDevice enforcement is set for organization, User’s choice should be overridden as “Device is unlocked” though location permissions are set as “Allow all the time” while launching the app. Also, the user should be able to still choose either App in foreground or Device is unlocked while the Always option is disabled or greyed out.Note: User should be notified with below message as well: “Enterprise Policy enforced on this setting”“Android occasionally terminates apps running in the background. Consequently, “Device is unlocked” and “Always” modes sometimes require opening the app to restore” | ImplementedNotes |
| TS-73 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Login to BLUID portal2.Navigate to Settings under respective organization3.Limit the usage of Mobile access app when device is locked by selecting the checkbox under “Mobile Access App usage on unlocked mobile devices” section.4.Create user and issue invitation code.5.Launch the App.6.Enter Invitation code and Issue Mobile id to Device.7.Verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow all the time
* Allow only while using the app
* Deny

8.Verify that user selects “Allow only while using the app” from the location permissions dialog9.Validate the Location permissions & Allow Mobile access section in Settings**Expected Result**WhenDevice enforcement is set for organization, User’s should be able to view option for “Allow Mobile Access when” as “App is in Foreground” when location permissions are set as “Allow only while using the app” while launching the app. Also, the user should be able to view “Device is unlocked” & “Always” options are disabled or greyed out.Note: User should be notified with below message as well: “Enterprise Policy enforced on this setting”“Location Permission enforced on this setting”“Android occasionally terminates apps running in the background. Consequently, “Device is unlocked” and “Always” modes sometimes require opening the app to restore” | ImplementedNotes |
| TS-74 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Login to BLUID portal2.Navigate to Settings under respective organization3.Verify that “Mobile Access App usage on unlocked mobile devices” is not checked4.Create user and issue invitation code.5.Launch the App.6.Enter Invitation code and Issue Mobile id to Device.7.Verify that below is displayed when location permission dialog is shown while launching the app for the first timeAllow BLUID Mobile Access to access this device's location* Allow all the time
* Allow only while using the app
* Deny

8.Validate that Mobile Access with reader works according to location permissions set by user.**Expected Result**Mobile Access app should work with reader according to location permissions set by user* If Location permissions set as “Allow all the time” then Mobile access app should work in both Foreground and Background
* If Location permissions set as “Allow only while using the app” then Mobile access app should work in Foreground mode
* If Location permissions set as “Deny” then Mobile access app should not work with reader and continuous warning message should be displayed.
 | ImplementedNotes |
| TS-75 | **Prerequisites**NeedAndroid device which has version 10 or more**Test Steps**1.Login to BLUID portal2.Navigate to Settings under respective organization3.Limit the usage of Mobile access app when device is locked by selecting the checkbox under “Mobile Access App usage on unlocked mobile devices” section.4.verify that settings can be updated only once/week**Expected Result**If changes are made, then user should be modified only after week and below message is displayed:Note: For security reasons, the setting can only be updated once / week. You can update it on Mon 00, 0000 00:00:00 | ImplementedNotes |