SR3 INSTALLTION GUIDE & USER'S MANUAL

UniKey's Bluetooth Smart Reader

POWERED BY UNIKEY™

SR3 Installation Guide
& User Manual

Table of Contents

SR3 Overview

The UniKey SR3 (Product Number SR3-UK-0001) is a 125kHz Prox and Bluetooth Low Energy all-in-one commercial reader for access control systems. The reader can retrofit legacy PACS systems using proximity, otherwise known as prox and easily implement optional features such as Touch-To-Open® and Inside/Outside Intelligence™ for an enhanced user experience at the door. The reader is both cost-effective and easy to install, without requiring any rewiring or paneling.

The SR3 is intended to be used in conjunction with an access controller as part of the access control system to provide secure access to buildings or areas. The reader is installed and communicates an access request to the controller using the standard Weigand protocol. This request is made by the end user presenting either prox card or fobs using ASK or FSK modulated Wiegand formats; the user can also use a Bluetooth enabled device storing mobile credentials powered by UniKey mobile application.

SR3 Installation Guide

Introduction

This section will walk a professional installer through the steps needed to attach a UniKey Smart Reader 3 (or SR3) (SR3-UK-0001) to an access control panel. The SR3 supports 125 KHz prox cards as well as UniKey mobile credentials. Please review the information below to ensure the reader is installed quickly and properly.

Grounding

- Shield must run continuously from the reader to the panel. At the panel, the reader ground, shield line, and earth ground must be connected together at a single point.
- Do not ground the shield line at the reader end as this will create a potential ground loop.

Power

- A non-switching power supply at the panel is recommended to power the reader for the highest noise immunity and best performance.
- For UL 294 or UL 603 Compliance, the readers shall be connected to a class two power limited power supply or Listed power supply with appropriate ratings.
- The recommended wire gauge is 24 AWG.
- The maximum line length recommended is 500 ft.

Voltage

- The minimum reader voltage required is +6 VDC to a maximum of +16.0 VDC, and 12.0 VDC is recommended.
- The reader will require 100 mA (typical @ 12 VDC) in standard mode, 220 mA (typical @ 12 VDC) in advanced mode.
- The reader is in standard mode by default, advanced mode can be configured via in-app settings using the administrator app.

Connection

- Wiring methods used shall be in accordance with National Electrical Code, ANSI/NFPA 70. Locations where installations are not recommended shall also be included.

Mounting the Reader

- If the unit is used to control a door or pedestrian gate, locate the unit as near as practical to the entry point. If the unit is mounted on or in a wall adjacent to the entry point, be sure the wall is sturdy. The repeated shock and vibration from a slamming access door or spring- loaded pedestrian gate must be isolated from the unit.
- Never mount the reader directly on a moving door or gate.
- Choose a well-lit location near the controlled opening. Wiring access for power, network, and earth ground must be available to the mounting location.

Mullion Mounted

Single-gang Mounted

Mounting

- Both the Mullion and Single-gang readers can be mounted on a wall or any suitable flat surface. The mounting plate can be used to cover various sized holes in the wall or surface.

Mobile Device and Software

- The SR3 utilizes BLE version 5.0 or greater.
- The UniKey SR3 is it to be used in conjunction with the UniKey Mobile App (Version 1.0 or higher).
- In order for the SR3 to function properly, the mobile device’s software must be up to date.
- iOS Devices: iOS 10.0 or higher
- Android Devices: v5.0 (Lollipop) or higher and peripheral mode supported.
- To maintain security users sha~~A means of verification sha~~ll~~ be~~ employ a means of verification ~~ed by the user~~ to enable access to the wireless electronic device such as a PIN or biometric feature.
- The wireless electronic device is not capable of command, control, programming, or any other system manipulation and it is only to be used in the same manner as a physical credential.

Prox Weigand Format

- Modulation technique: ASK or FSK modulated proximity cards or fobs. PSK is not supported.
- Output Weigand format: 26 to 37-bit.
    - Note 26 bit verified by UL
- Frequency: 125 KHz RFID
- The control system can distinguish between the type of credential used. How this is done depends on the access control system being used.

Commented [LJ1]: Note "26 bit verified by UL"

Reader Wiring

Conductor	RED	BLACK	GREEN	WHITE	PURPLE	ORANGE	YELLOW	BLUE	DRAIN
Purpose	DC +6-16 VDC	Ground	Data 0	Data 1	Red LED	Beeper	Card Present	Green LED	Shield Ground

Current Draw: 100mA (typical @ 12VDC)

UL 294 Performance Levels

MODEL #	ACCESS CONTROL LINE SECURITY LEVEL	DESTRUCTIVE ATTACK LEVEL	ENDURANCE LEVEL	STANDBY POWER LEVEL	CONDITION
UniKey SR3	Level I	Level I	Level IV	Level I	N/A

Temperature / Humidity Conditions

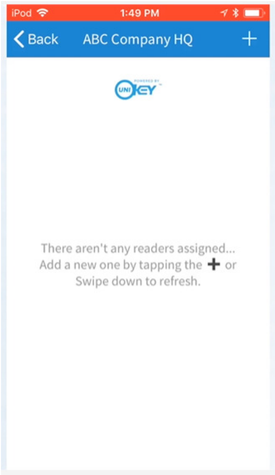
- The recommended ambient temperature conditions for SR3 functionality are between -35 to 66°C
- The recommended humidity conditions for SR3 functionality is less than or equal to 85%.

Commented [LJ2]: "-35"

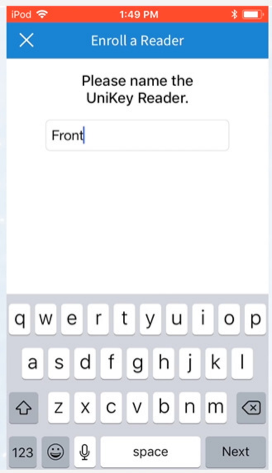
Reader Enrollment

Once the SR3 has been properly installed. It must then be enrolled to an organization using a mobile device using UniKey Mobile App and an installer credential to log in.

- First Select the Organization in the UniKey Mobile App and tap the + button to enroll a reader to the organization
- Then name the reader and tap Next
- Last touch the mobile device to the newly named reader

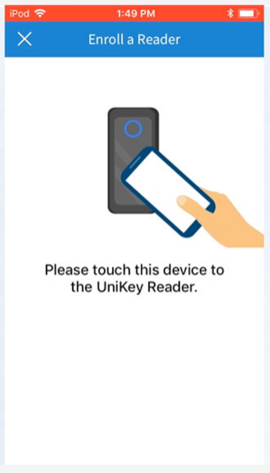


There aren't any readers assigned...
Add a new one by tapping the + or
Swipe down to refresh.



Please name the
UniKey Reader.

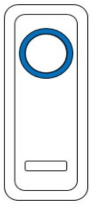
Front



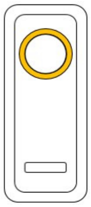
Please touch this device to
the UniKey Reader.

SR3 Animations

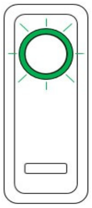
Each animation corresponds with a specific response from the SR3 and can be customized individually for the user's commercial organization. Other animation colors as well as various presentation styles are just some of the alternatives available for the UniKey SR3.



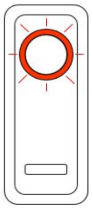
Blue Idle:
The reader is properly enrolled and is idly waiting for an access attempt.



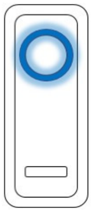
Amber Idle:
The reader is connected to power but not enrolled to an organization.



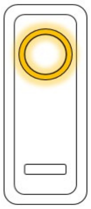
Green Flash:
The reader has granted entry to the access attempt.



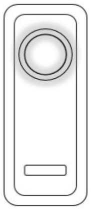
Red Flash:
The reader has denied entry to the access attempt.



Blue Spin:
An access attempt has been made and the reader is processing.



Amber Spin:
The reader is going through the booting process of powering on.



White Spin:
The reader is going through the reboot process of a factory reset.

SR3 Reset

A reset is performed in order to clear the reader of existing organizations and corresponding end user credentials. Access to any specified organization will need to be re-established before continuing reader use.

1. To locate the reset button on the reader, dismount from the installation points. The reset button is located on the back of the reader, as depicted in Figure 1.
2. Confirm that the reader is still connected to power source; The LED ring should display a solid blue animation.
3. Hold down the reset button for a minimum of 5 seconds.
4. After the reader has successfully completed the reset, the LED ring will momentarily flash a series of red, white, and amber blinking. Once the amber is solid, the reset is complete.
5. The reader's enrollment has now been cleared and is ready to be enrolled at a specified organization.

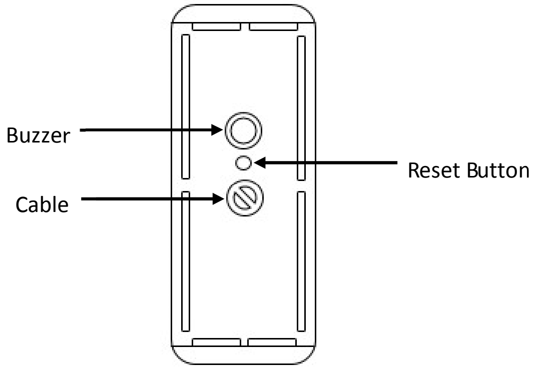


Figure 1: Reset button is located on the back of the reader between the buzzer and cable.

SR3 Factory Reset

A factory reset is performed in order to clear the reader of existing organizations and corresponding end-user credentials, as well as to clear any firmware updates initiated on the reader since manufactured. Access to any specified organization will need to be re-established, and firmware will need to be reinstalled to the latest version before using the reader.

1. To locate the reset button on the reader, dismount from the installation points. the reset button is located on the back of the reader, as depicted in Figure 1.
2. Disconnect the reader from the power source.
3. Begin holding down the reset button; while holding the reset button, reconnect the reader to the power source. [1]
4. Give the reader a minimum of 10 seconds to reset and release the reset button.
5. The LED on the front of the reader will momentarily be off while the reader reconfigures.
6. After the reader has completed the factory reset, the LED ring will momentarily flash white, then change to amber.
7. The reader’s enrollment has now been cleared, along with any firmware updates that have been initiated since manufactured.

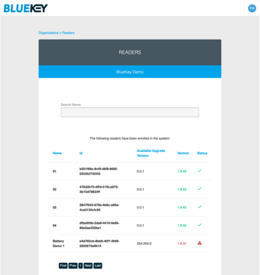
[1] It is important to be sure the reader is re-connected to power while simultaneously holding the reset button; not before or after.

Identifying SR3 Firmware Version

The firmware versions for the SR3 can be identified once the SR3 is enrolled to an organization.

Via the Web Portal

To identify the firmware version for the SR3 in the UniKey web portal. Once logged into the UniKey web portal using an installer credential. Select the Actions menu for the Organization and click on View Readers to see the screen shot. This will display the screen below which allows you to both view and update the reader's firmware.



Organizations > Readers

READERS

BlueKey Demo

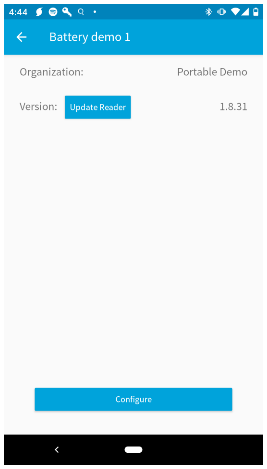
Search Name

The following readers have been enrolled in the system:

Name	Id	Available Upgrade Version	Version	Status
01	b201f68c-8cf9-46f8-9695-0503527353f2	0.0.1	1.8.45	✓
02	476d2b70-dffd-41fb-a975-3b15d79823ff	0.0.1	1.8.45	✓
03	2847f545-679e-4b6c-a95e-4ca3130cfc95	0.0.1	1.8.45	✓
04	dfbe9fdb-2da8-4416-9e66-80e2aa332ba1	0.0.1	1.8.45	✓
Battery Demo 1	e4d782cb-8bb6-40f1-9fd9-2850670a8b14	254.254.0	1.8.31	⚠

Via the Mobile App

To identify the firmware version for the SR3 in the UniKey mobile app. Once logged into the UniKey mobile app using an installer credential. Select the Organization the SR3 is enrolled to. Then select the reader name. This will display the screen below which allows you to both view and update the reader's firmware.



Battery demo 1

Organization: Portable Demo

Version: 1.8.31

UniKey Mobile Credentials

This section provides an overview of commercial mobile credentials within the UniKey platform. The various actors in a typical deployment will be defined as well as a review of the typical lifecycle of the mobile credential.

Definitions

Term	Definition
Credential Credit	A mobile credential that has not yet been assigned to a mobile device
Mobile Credential	A digital key that contains card ID and facility code information that is transmitted from a mobile device to a reader for the purpose of entering a protected area
Redemption Codes	Two numbers that represent a quantity of credential credits. Redemption codes can be redeemed for credential credits within the portal. Partners can specify the number of credits that are assigned to each redemption code.
Partner	Organization that partners with UniKey to leverage our mobile credential solution in their products. Partners purchase redemption codes from UniKey.
Partner Customer	An entity that purchases redemption codes from the partner for resale to End Customers.
End Customers	An entity that manages mobile credentials and access rights to a protected area.
End User	An individual that uses a mobile credential to gain access to a protected area.

Typical Lifecycle

1. Partner orders redemption codes from UniKey by submitting a purchase order.
2. UniKey delivers spreadsheet containing redemption codes.
3. Partner sells redemption codes to partner customer.
4. Partner customer sells codes to end customer.
5. End customer enters redemption codes in UniKey portal and receives credential credits.
6. End customer consumes credential credits by issuing mobile credentials to end users.
7. End users use their mobile credential day to day to enter a door.

When a customer submits a purchase order to UniKey to procure redemption codes, information such as that in the example table below must be included. It is important to note that the number of credentials per code is arbitrary and is defined entirely by the partner.

Qty Redemption Codes	Credentials Per Code	Line Total Credentials
500	100	50,000
260	25	6,500
250	10	2,500
200	5	1,000
	Total Credentials Ordered	**60,000**

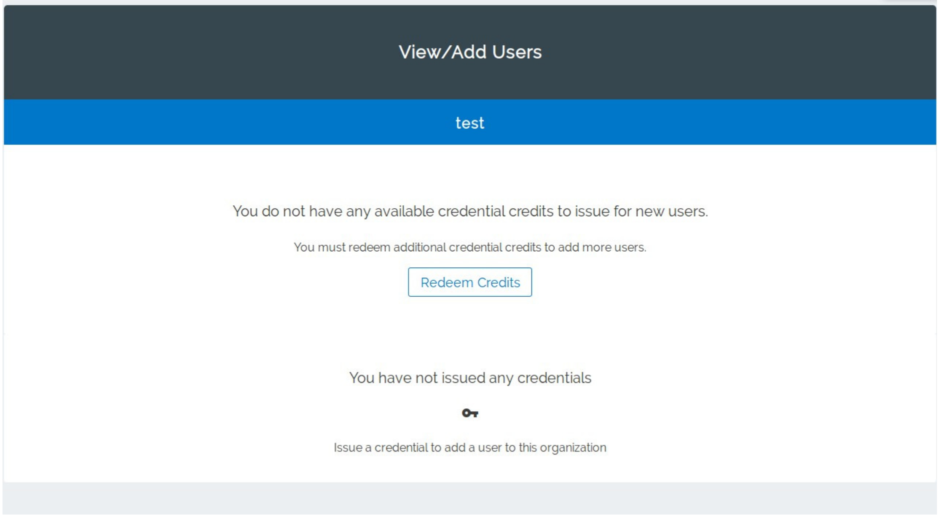
Once UniKey receives and processes the partner purchase order, we will deliver the redemption codes as a spreadsheet formatted similar to the one below.

Example redemption codes delivered to partner:

Serial Number	Authorization Code	Number of Credentials
2000220563	123456	100
2000110088	887474	100
2000118831	898773	5

Once the partner has received these codes that they distribute them by any means of their choosing. Ultimately the codes will be consumed by the end customer. The end customer consumes a credential code in the portal. Once the process is completed, the credential code used will no longer be valid and the end customer will have a balance of credential credits within the portal. This process is outlined in the screenshots below from the perspective of the end customer.

Step 1: End customer navigates to the View / Add Users page in the portal and clicks "Redeem Credits"



View/Add Users

test

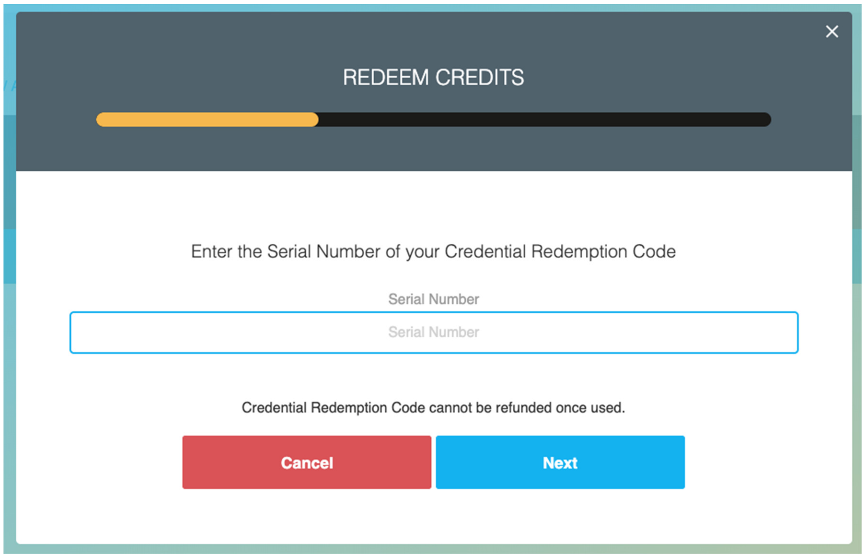
You do not have any available credential credits to issue for new users.

You must redeem additional credential credits to add more users.

You have not issued any credentials

Issue a credential to add a user to this organization

Step 2: End customer enters a valid credential code serial number.



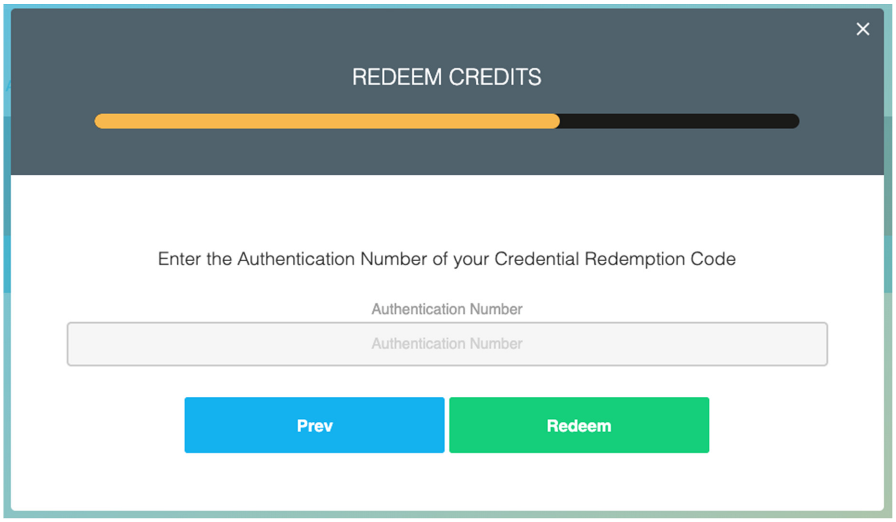
REDEEM CREDITS

Enter the Serial Number of your Credential Redemption Code

Serial Number

Credential Redemption Code cannot be refunded once used.

Step 3: End customer enters valid authentication number for the credential code.

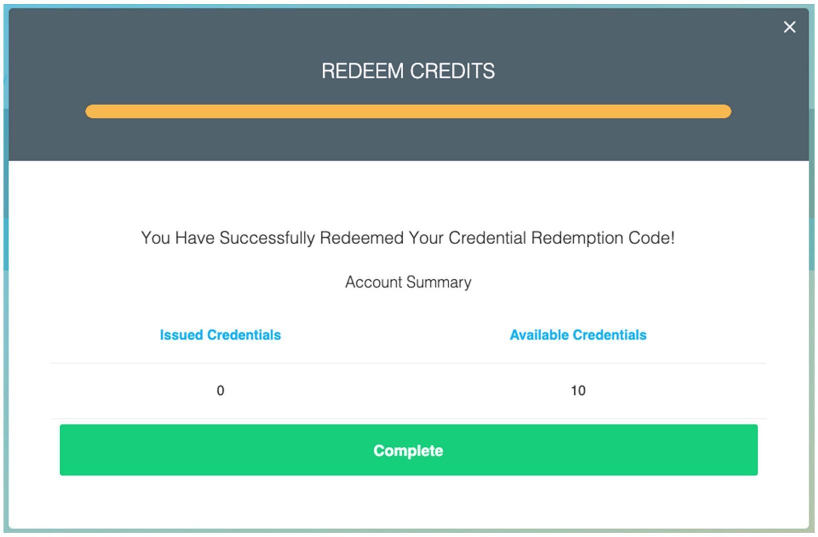


REDEEM CREDITS

Enter the Authentication Number of your Credential Redemption Code

Authentication Number

Step 4: End customer's available credential balance increases. End customer can now send mobile credentials to end users.



REDEEM CREDITS

You Have Successfully Redeemed Your Credential Redemption Code!

Account Summary

Issued Credentials	Available Credentials
0	10

Now that the end customer has mobile credential credits available in their portal account, they can issue mobile credentials to end users. These mobile credentials will allow an end user to enter a door that supports the mobile credential. Every time a mobile credential is issued, a credential credit is consumed. When the credential credit balance of the end customer is depleted, they would be required to purchase an additional credential code from the partner customer before they could issue additional mobile credentials.

One final note - this document is illustrating a typical lifecycle. The number of tiers in the partner distribution scheme of the redemption codes are entirely up to the partner. For example, if the partner has additional levels of resale or distribution in their value chain, the process would still work the same. If the partner chose to sell redemption codes direct to end customers, the system supports that as well. Additionally, if a partner chooses not to issue credits at all and allow unlimited sending of credentials by end customers, that is also possible.

Troubleshooting the SR3

Issue	Corrective Action
The reader will not read the prox card and/or fob.	Check prox card and/or fob to ensure they are ASK or FSK modulated Weigand compatible, 26 to 37-bit and 125 KHz RFID. Also consult the requirements for the controller.
End-user was issued credentials and replaced their mobile device with a newer model. They downloaded the app and used their original e-mail invite link to reinstall credentials on their new device. The installation was unsuccessful.	BlueKey mobile credentials are only good for the life of the original mobile device. Once a new device is purchased, new credentials are required, even if the phone number has not changed.
I installed the system in a multi-tenant residential condominium complex. The property management company wants to re-use mobile credentials from departing tenants, reissuing them to the new tenants moving in. Is there an option in the dashboard to repurpose the same credentials without having to buy them each time this happens?	No. BlueKey Credentials are tied to specific mobile devices. The only way the property management firm could do this is if they owned the mobile devices, repurposing the device from a departing tenant to a new tenant. A more viable and less expensive option would be to use BluePass Bluetooth fobs.
Our customer wants to fully migrate away from 125 KHz cards and fobs, turning off that portion of the reader so it will only read the Bluetooth-based credentials. Can I turn off that portion of the reader?	Currently, you cannot turn off the 125 KHz portion of a reader.

Certifications

FCC

- FCC Compliance Statement: This device complies with Part 15.105 (b) of the FCC rules.
    1. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:
        - Reorient or relocate the receiving antenna
        - Increase the separation between the equipment and receiver
        - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
        - Consult the dealer or an experienced radio/TV technician for help
    2. FCC Part 15 Clause 15.21 [Do not Modify warning]:
        - Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment
        - FCC Part 15.19(a) [interference compliance statement], unless the following statement is already provided on the device label
            - This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
    3. RF Exposure Guidance:
        - In order to comply with FCC RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

ISED

- ISED RSS Gen Notice:
    1. This device complies with Industry Canada’s licence-exempt RSSs. Operation is subject to the following two conditions:
        - This device may not cause interference; and
        - This device must accept any interference, including interference that may cause undesired operation of the device.
    2. Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes:
        - l’appareil ne doit pas produire de brouillage;
        - l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.
- ISED Canada ICES Compliance: CAN ICES-3 (B)/NMB-3(B)
- ISED RF Exposure Guidance:
    1. In order to comply with FCC / ISED RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.
    2. Afin de se conformer aux exigences d'exposition RF FCC / ISED, cet appareil doit être installé pour fournir au moins 20 cm de séparation du corps humain en tout temps.

UL

SECURITY
UL
®
LISTED