InStock

InStock Installation Guide

V2.3.2.0

1. Table of Contents

Contents

1. Table of Contents 2
2. Copyright / Disclaimer 4
3. Installation 5
   - 3.1 Scanner Device (Android) 5
   - 3.2 Client Host Console (Admin Console) 5
   - 3.2.1 Local PC Installation 5
   - 3.2.2 Run installer on existing installation 8
   - 3.2.3 Uninstall existing installation 9
   - 3.3 Admin Console Interface 13
   - 3.3.1 Backend Services 13
   - 3.3.2 Buttons Panel 14
4. Settings 15
   - 4.1 Settings Tab 15
   - 4.1.1 Configure IP Address 16
   - 4.1.2 Generate Network QR Code 16
   - 4.2 Device App Settings Tab 17
   - 4.3 App Store Tab 18
   - 4.4 Update Centre Tab 19
   - 4.5 Task Scheduler Tab 20
   - 4.6 Reference File Settings Tab 21
5. Register Your Application 22
   - 5.1 Add Licence 22
6. Reference Data 24
   - 6.1 Reload All Reference Files 24
   - 6.2 Reload a Single File 24
7. Setting up your MC33X Device 25
   - 7.1 PBS Launcher App 25
   - 7.1.1 Setting up Apps 25
   - 7.2 InStock App 27
   - 7.2.1 Adding Wi-fi Connection 27
   - 7.2.2 Configure Server Settings 28
   - 7.2.3 Settings Device Name 29
   - 7.2.4 Check Server Connectivity 29

7.2.5 Download Reference Data 30
7.3 Advance Wi-Fi Security 31
7.3.1 WPA3-Personal (SAE) 31
7.3.2 WPA3-Enterprise 31
8. Minimum System Requirements 32
8.1 Admin Console 32
8.2 InStock App (Android) 32

2. Copyright / Disclaimer

Copyright © 1999-2025 Purpose Built Software Pty. Ltd. All rights reserved.

Purpose Built Software Pty. Ltd. Any person is hereby authorized to view, copy, print, and distribute this document subject to the following conditions owns copyright in these documents:

The documents may be used for informational purposes only.
The documents may only be used for non-commercial purposes.
Any copy of these documents or portion thereof must include this copyright notice.

Note that any product, process or technology described in the document may be the subject of other Intellectual Property rights reserved by Purpose Built Software. Pty Ltd. and are not licensed hereunder.

PURPOSE BUILT SOFTWARE MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS PUBLISHED IN THIS DOCUMENT FOR ANY PURPOSE. ALL SUCH DOCUMENTS AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. PURPOSE BUILT SOFTWARE HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, INCLUDING, BUT NOT LIMITED TO, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL PURPOSE BUILT SOFTWARE BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR INFORMATION AVAILABLE FROM THIS PUBLICATION.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. PURPOSE BUILT SOFTWARE PTY LTD MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

3. Installation

3.1 Scanner Device (Android)

The app is pre-installed custom PBS Launcher app and InStock app on the device. If you are unable to locate these Apps on the device, please contact PBS Support Line via email or phone.

3.2 Client Host Console (Admin Console)

3.2.1 Local PC Installation

The download link for the local PC client is available on the Purpose Built Software website, or via email request to support@purposebuilt.com.au.

The link will download the application installer file. Installer file contains:

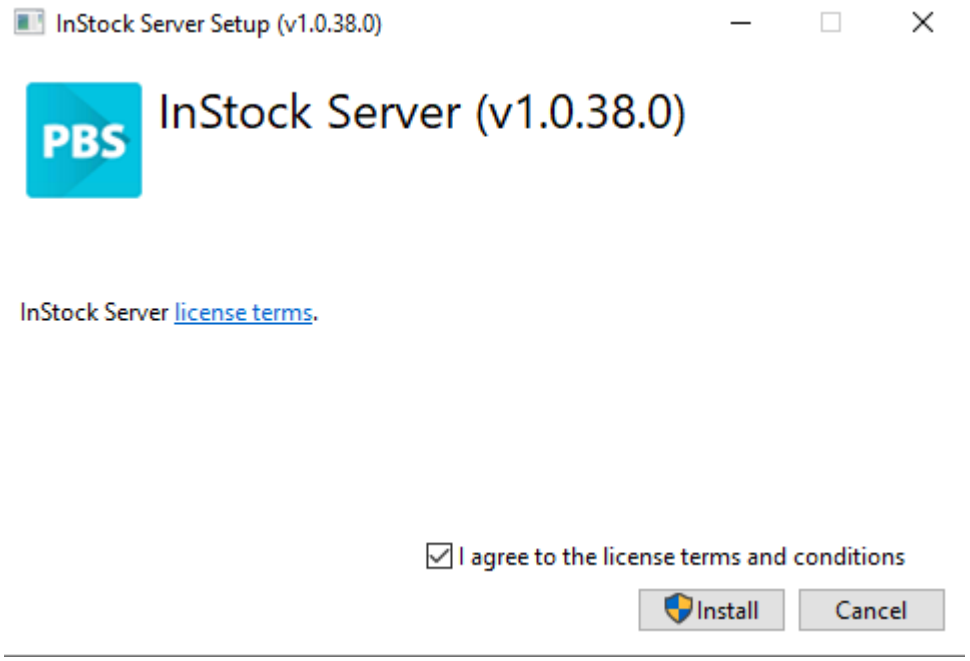
1. .NET Framework 4.8.1
2. InStock Admin Console v1.0.39.0

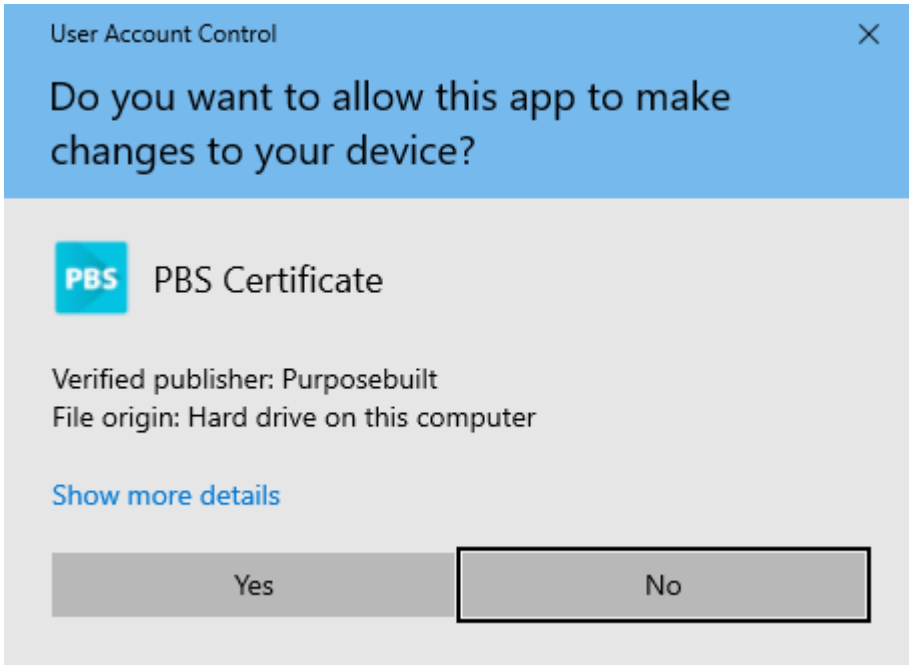
To install the applications right click the chosen installer application and select run as administrator*. Permission make changes to device will be requested.

*Administrator privileges will only be required for install installation. Dependant on user account set up Admin may need to install .NET Framework 4.8.1 prior to proceeding with InStock Installer for v1.0.39.0.

Run the installer application and follow the steps on the screen. For your assistance the steps are detailed below.

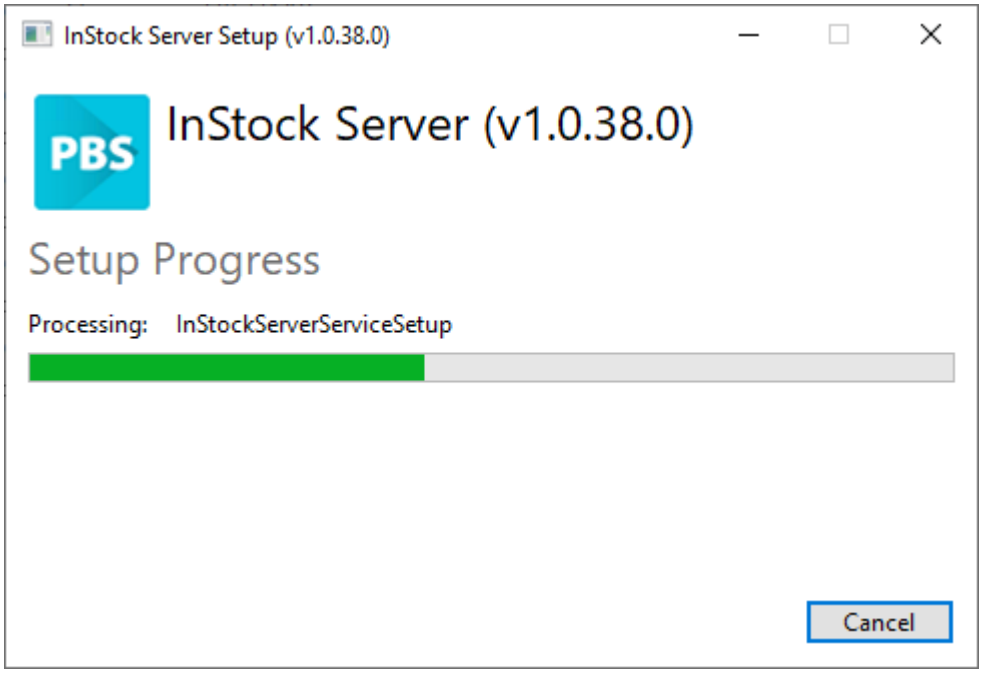
Accept license terms and conditions and click on Install button.



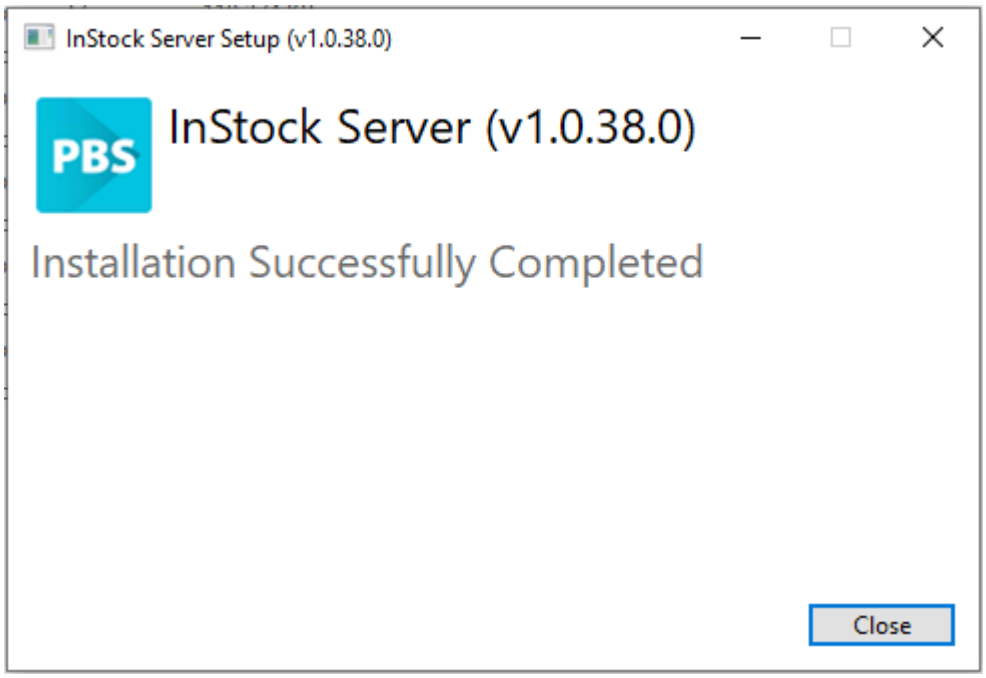


Click on Yes button to install the certificate.

Installation process will begin.



You will see Setup Successful message when installation complete**.**



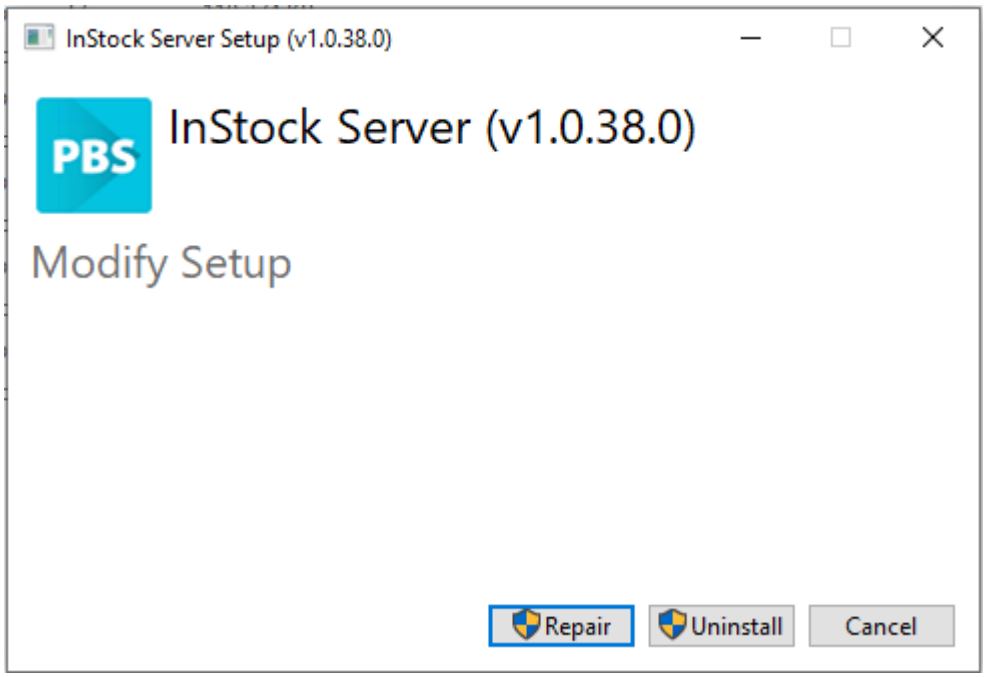
Click CLOSE to exit the installation window.

Upon completion of the installation a shortcut will appear on the desktop.

Double clicking on the shortcut will bring up the InStock Admin Server Panel.

3.2.2 Run installer on existing installation

If the application was already installed on the computer and you are running the same installer, it will show Repair and Uninstall options.

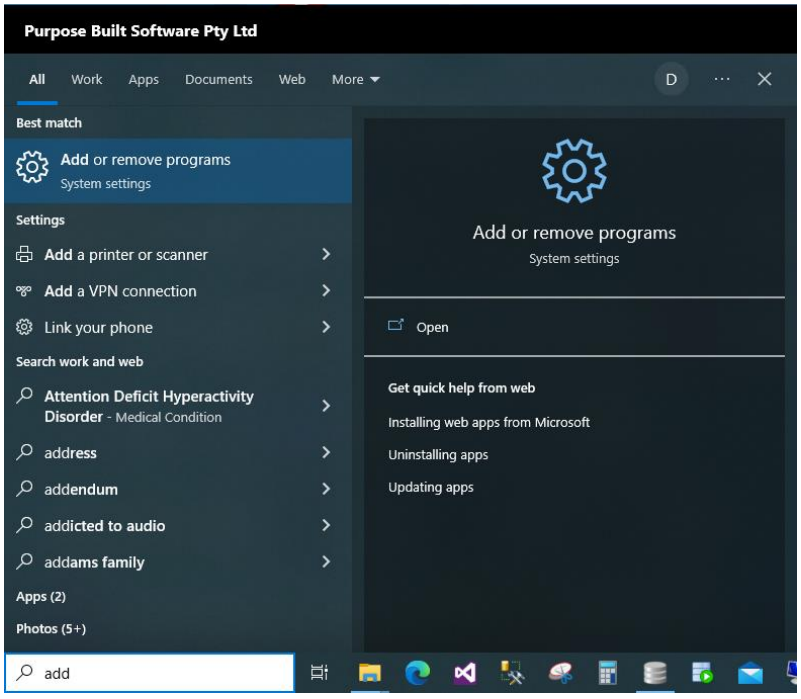


Note: Sometimes, **Repair** is required to fix the installation issues.

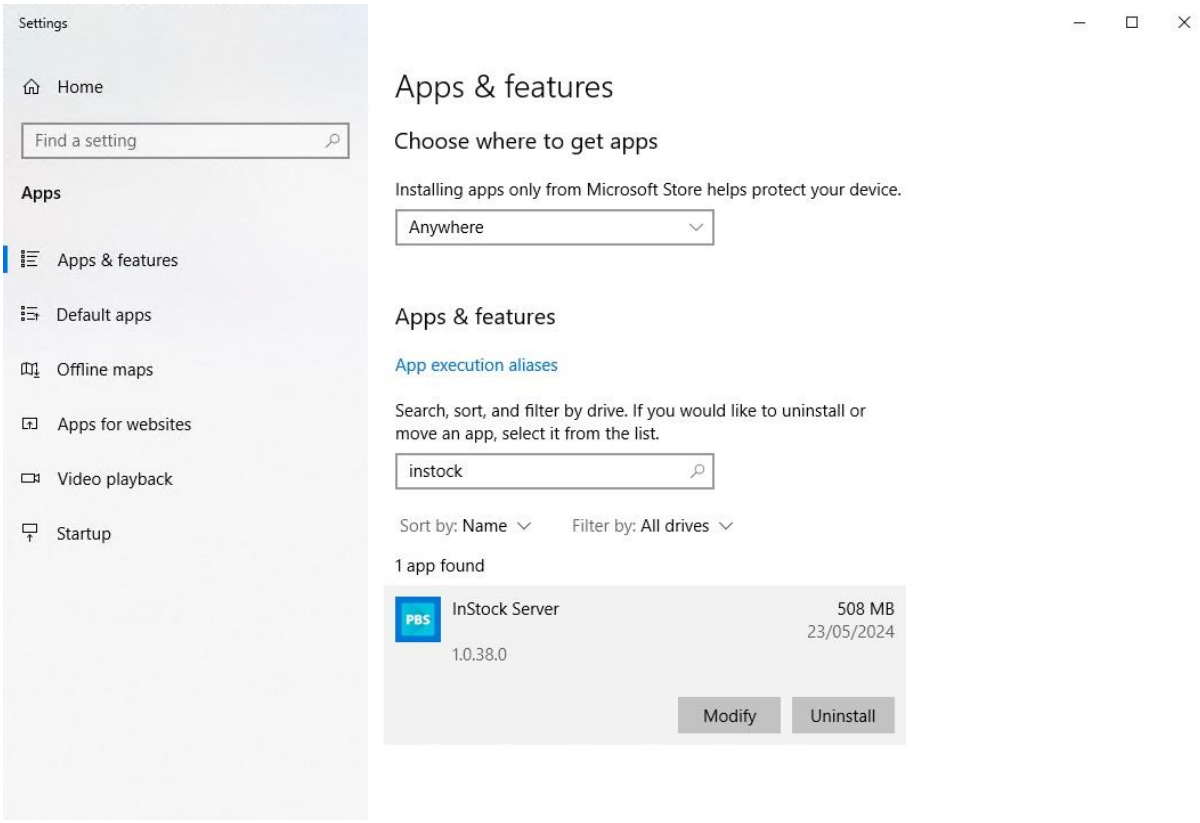
3.2.3 Uninstall existing installation

To uninstall InStock services and Admin console from a computer run the same installer or follow the steps below to uninstall InStock server application from Windows Add Remove Programs:

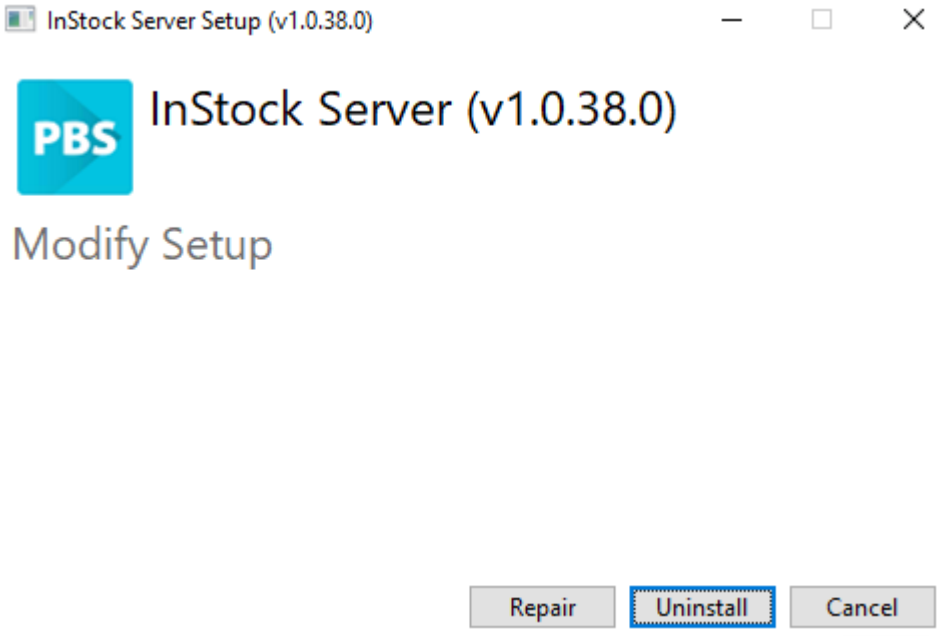
1. On the computer, press windows key and type **Add remove** and select Add or remove programs.



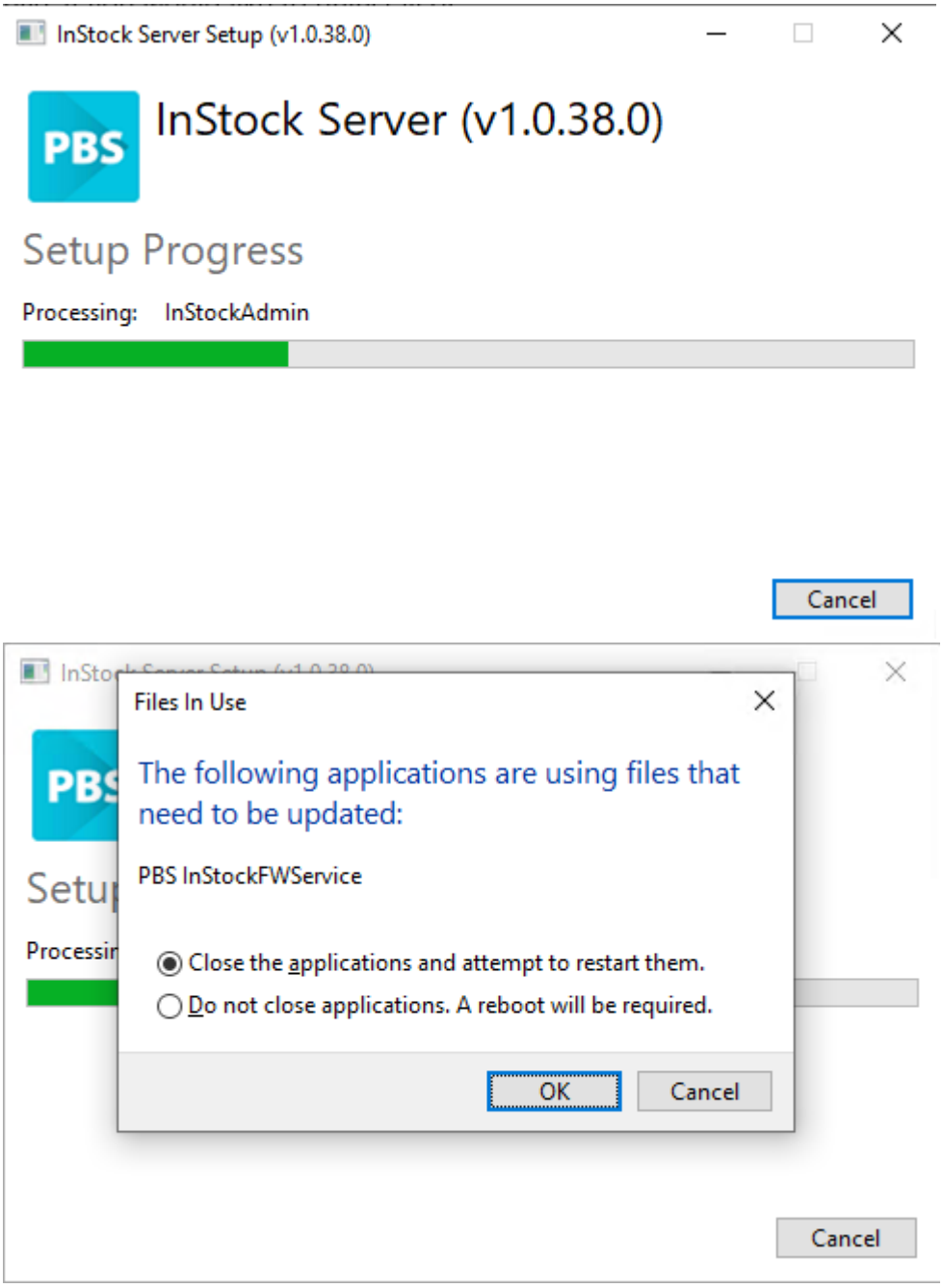
2. In the search field, type InStock. The current InStock installed application will be shown. Click on Uninstall button.



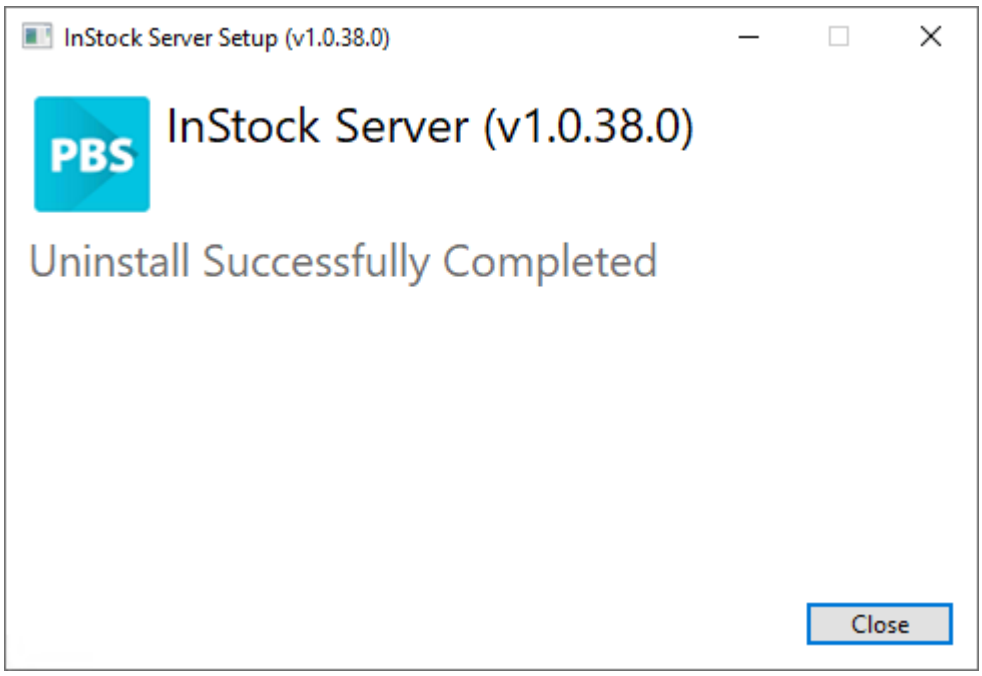
3. InStock setup screen will appear. Select Uninstall from the screen.



Uninstallation will begin.



A Setup Successful message will appear after uninstallation complete.



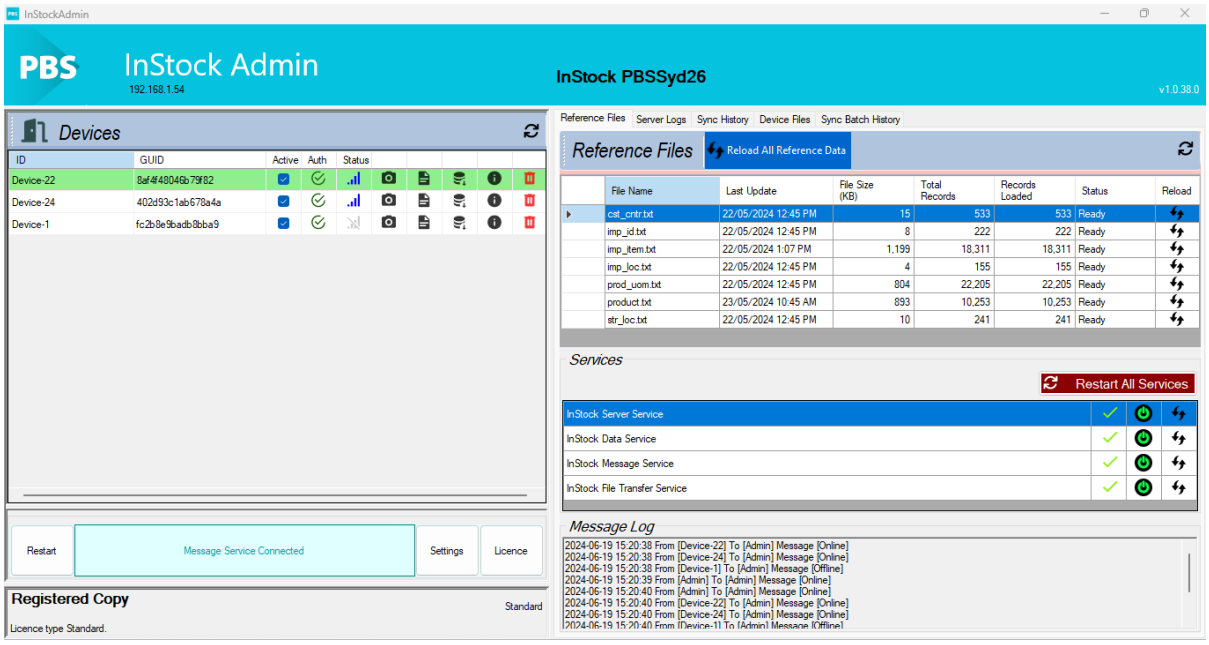
Uninstallation done.

Note: User folder and files will not be removed automatically, you can remove them by remove the **C:\InStock** folder with the files and sub folder. Removing this folder will also remove logs, settings and device uploaded files such as logs, databases and screenshots.

Depending on your system, you may be asked to restart the computer.

3.3 Admin Console Interface

After installation complete, run the InStock Admin console application. The program will appear as below.



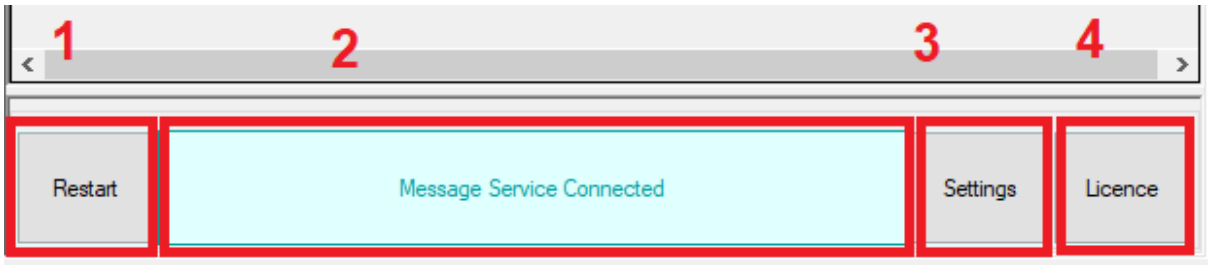
3.3.1 Backend Services

In the Services section ensure all checkmarks and power icons are GREEN. If power button is RED this indicates the service is off. Follow the below to turn service to GREEN.

- Run the admin console as an administrator and click the red power button to start the service. You can also restart all services by clicking the **Restart All Services** Button.
    - **Note**: to restart service from the Admin console, you will need Administrator privileges.
    - OR
    - Restart the computer.

If the services DO NOT start please repair the installer as referred to in section above “Installation 3.2.3”. Please refer to the InStock User guide for further details.

3.3.2 Buttons Panel



1. To restart Admin Console application.
2. This button shows whether the Admin Console application is connected to the message service. If disconnected, then you can click the field to reconnect it.
3. Settings button will pop the settings screen.
4. Licence button will pop the licence and registration screen.

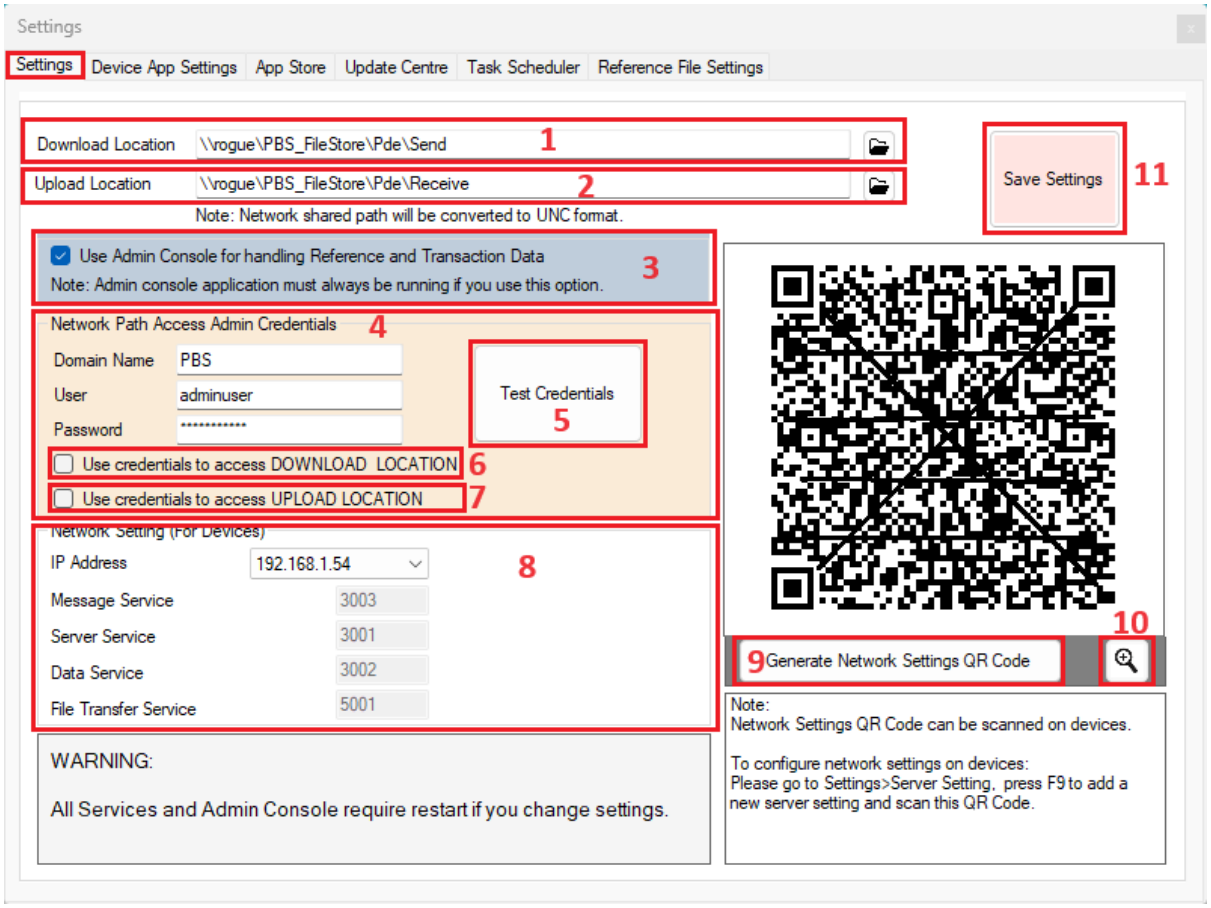
Note: If you install a new version on a previously installed admin console application and the Message Service button is red after running the application, then re-run the setup and chose Repair option.

4. Settings

4.1 Settings Tab

After installation, settings need to be completed.

Select settings from the console's main screen. The following window will appear.



1. Download Location
2. Upload Location
3. Data handling mode
4. Network Credentials for shared locations
5. Test Credentials
6. Setting to use Network Credentials to access Download Location
7. Setting to use Network Credentials to access Upload Location
8. Server IP and Port settings used by backend services
9. Generate Network Settings QR Code
10. Zoom or export QR Code
11. Save settings

Download Location	Download Location is the location of the reference files. Reference files reads automatically or on demand by the services and send to devices on request. This location should be pointed to the folder location where the iPharmacy reference files are stored.

Upload Location	Upload Location is the location where transaction files are uploaded from the devices.
Data handling mode	Data handling mode switched between backend and frontend handling of the reference and transactions data. Admin Console (or frontend) option should only be used if Download or Upload location is a network shared location and backend service is unable to access location with full privileges.
Network Credentials for shared locations	Network Credentials can be used to access network shared location. Only require when Download or Upload location is a network shared location and backend service is unable to access location with full privileges.
Setting to use Network Credentials to access Download Location	Check box to use network credentials for accessing Download Location. Only required if permissions NOT granted already.
Setting to use Network Credentials to access Upload Location	Check box to use network credentials for accessing Upload Location.
Server IP and Port	Server IP and Port settings used by backend services and devices
Generate Network settings QR code	Network settings QR code can be scanned by devices to add, update or switch server settings. This QR Code can also be scanned from the 'Send Transaction Data' screen to upload transactions.
Zoom or export QR Code	Zoom or export QR Code or save QR code to a file

Important: If you want to point to shared folder(s) here then the folder path must be in UNC format (eg: \\AnotherPC\SharedFolder\Send) (path will be automatically changed to UNC format it was a network shared drive), and the folder must have full permissions to the "Computer" where the InStock services are running.

4.1.1 Configure IP Address

You need to select the correct IP address from the dropdown list if the PC has more than one IP.

Save the settings it will prompt to restart the services. If you are running Admin console as an Administrator then the services will restart, alternately you can restart the computer.

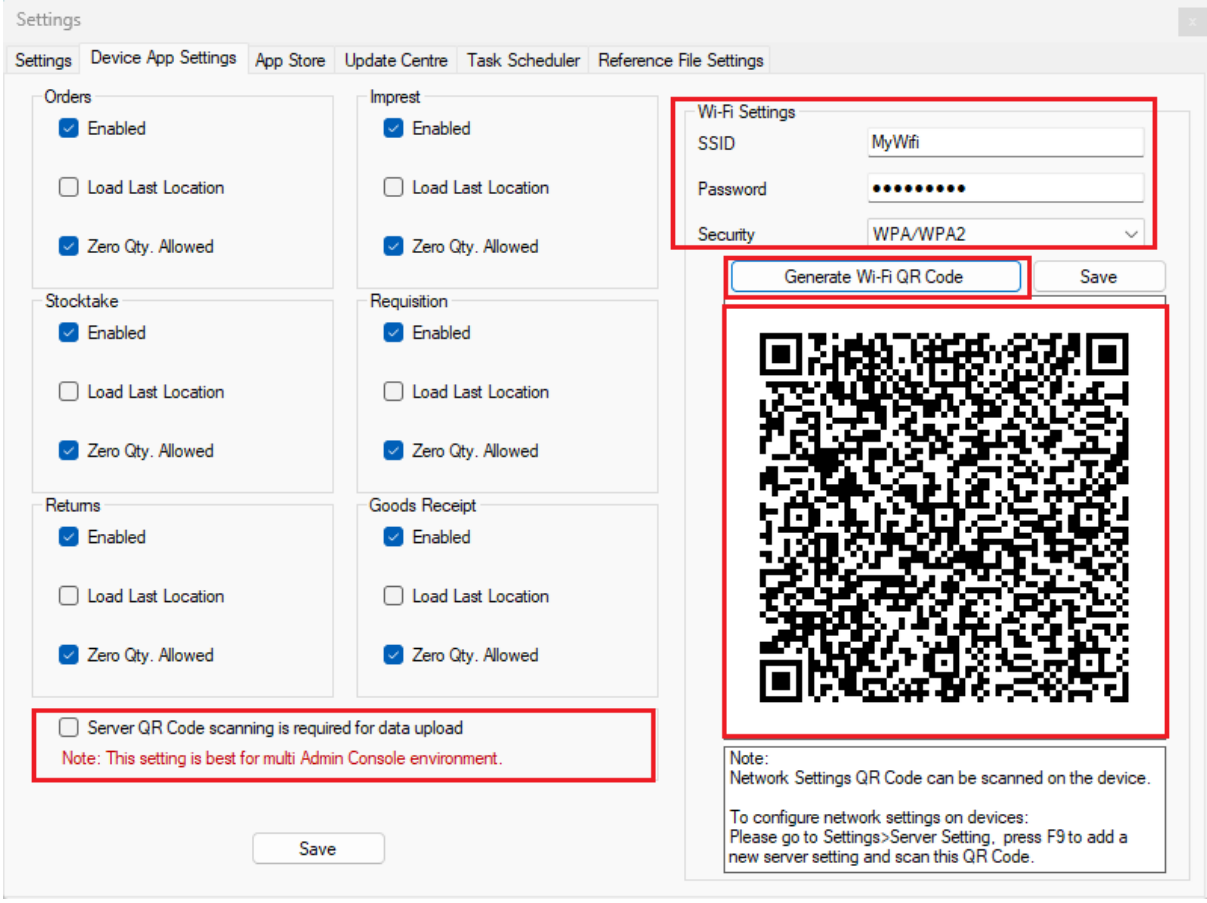
4.1.2 Generate Network QR Code

From the settings tab, you can also generate setting QR code. This QR code can be scanned from the device to configure server settings. Refer to Configure server settings

To save QR Code in a file and print, click on the button and click on **Save to File** button.

4.2 Device App Settings Tab

From the 'Device App Settings' tab, you can customise the device app behaviour. The device will sync the settings automatically.



This screen allows setting behaviour of the InStock App running on MC3300x devices.

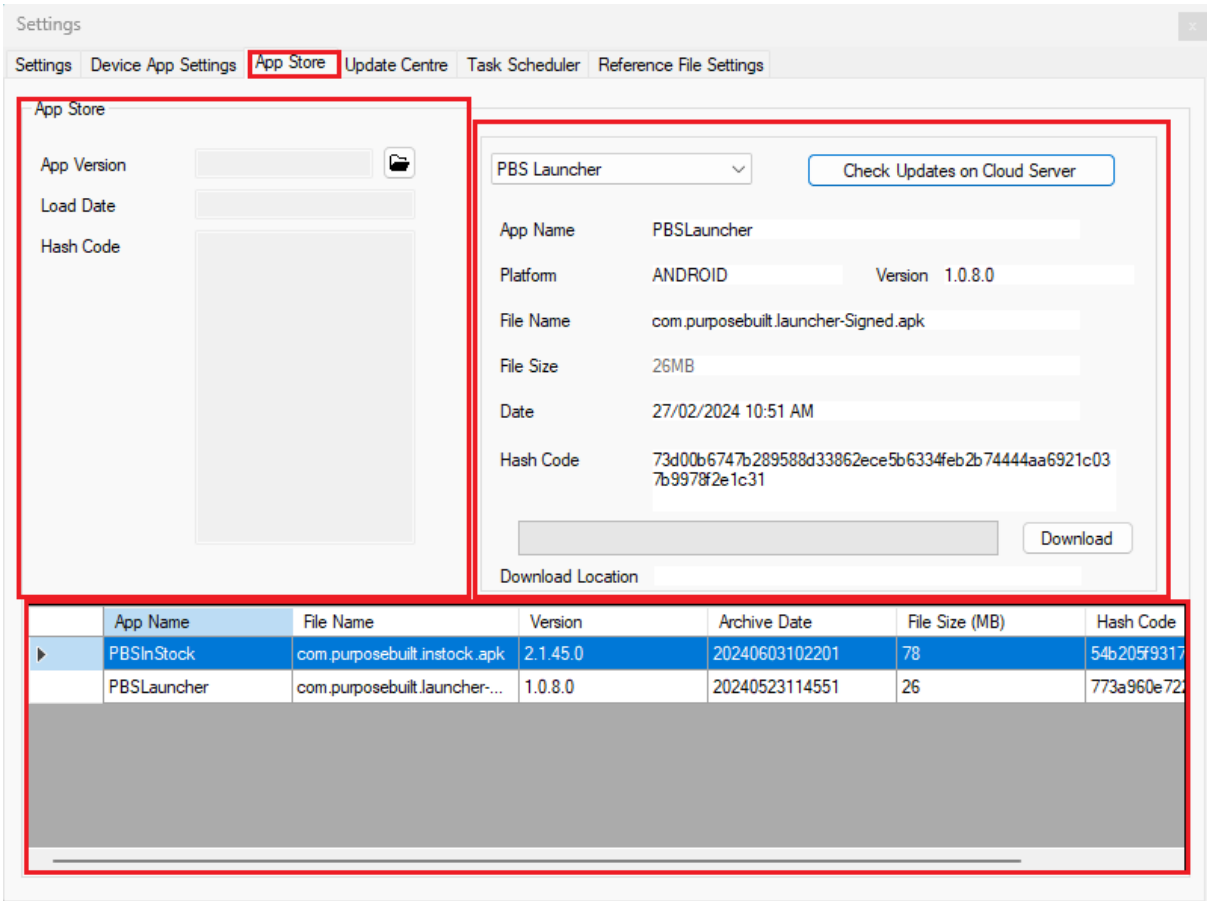
Checking box for "Server QR Code scanning is required for data upload" will prompt user to scan network QR code for each Data Sync Upload to the PC. Best for Kiosk and hot desk environments.

You can also generate QR code for Wi-Fi settings here. Refer to section 7.2.1 of this manual to add Wi-Fi setting to your device.

Note: all the sensitive information, including wi-fi settings are saved as encrypted data.

4.3 App Store Tab

App Store is used to load the latest InStock app. InStock app running on the devices gets updated app from the app store.

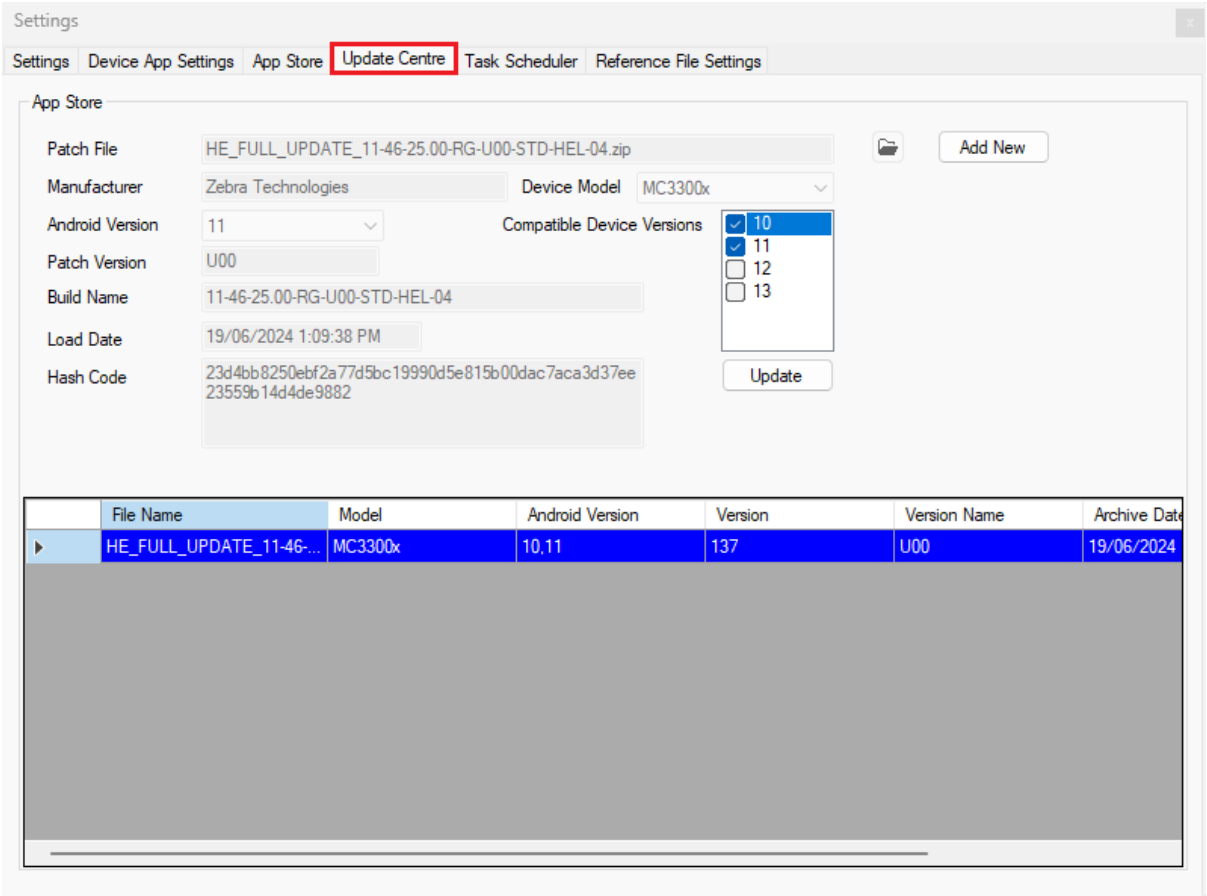


Updates for admin console and device apps can be checked and downloaded from the PBS App Store on the cloud (internet connection required).

4.4 Update Centre Tab

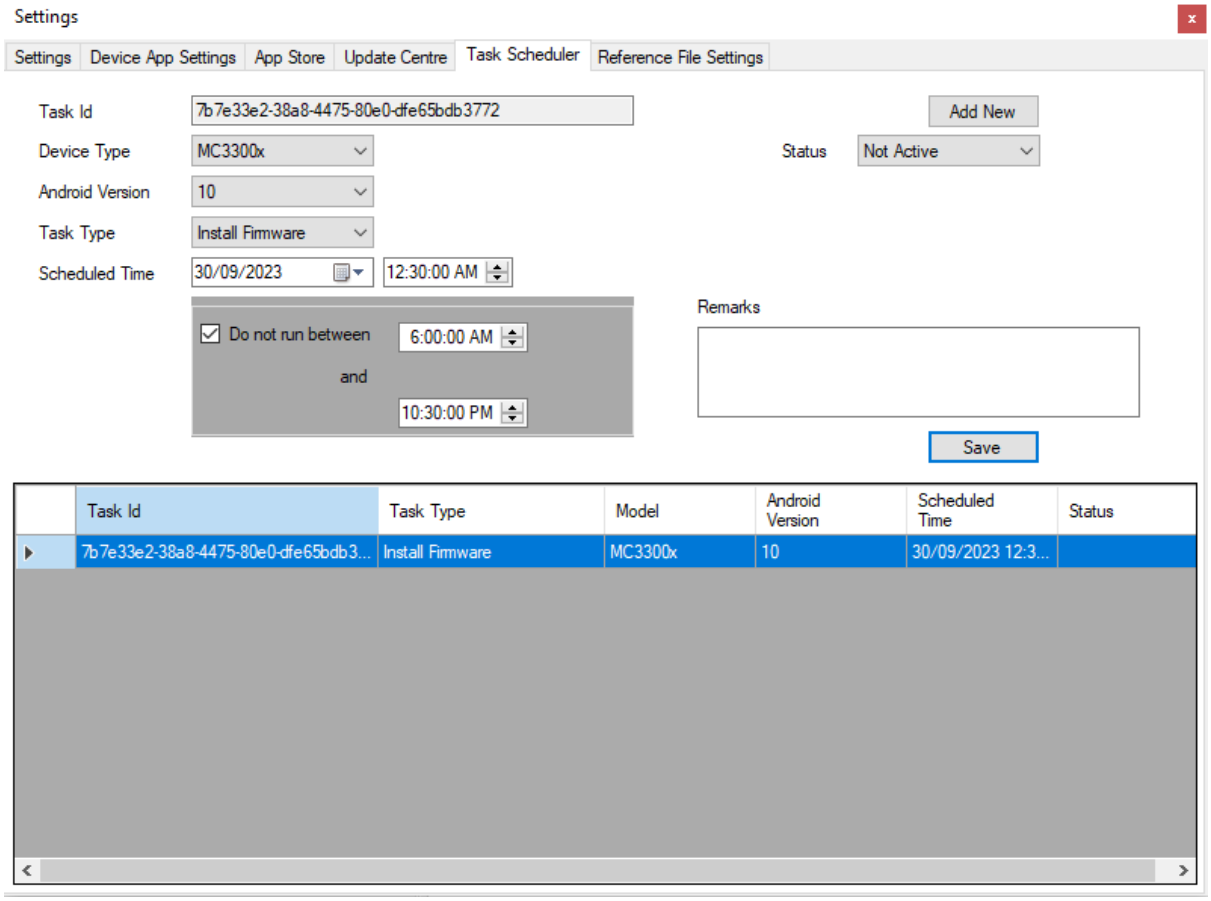
Zebra releases patches and updates for devices and it is crucial to keep update device OS and firmware.

Update Centre is a solution to keep update offline Zebra devices.



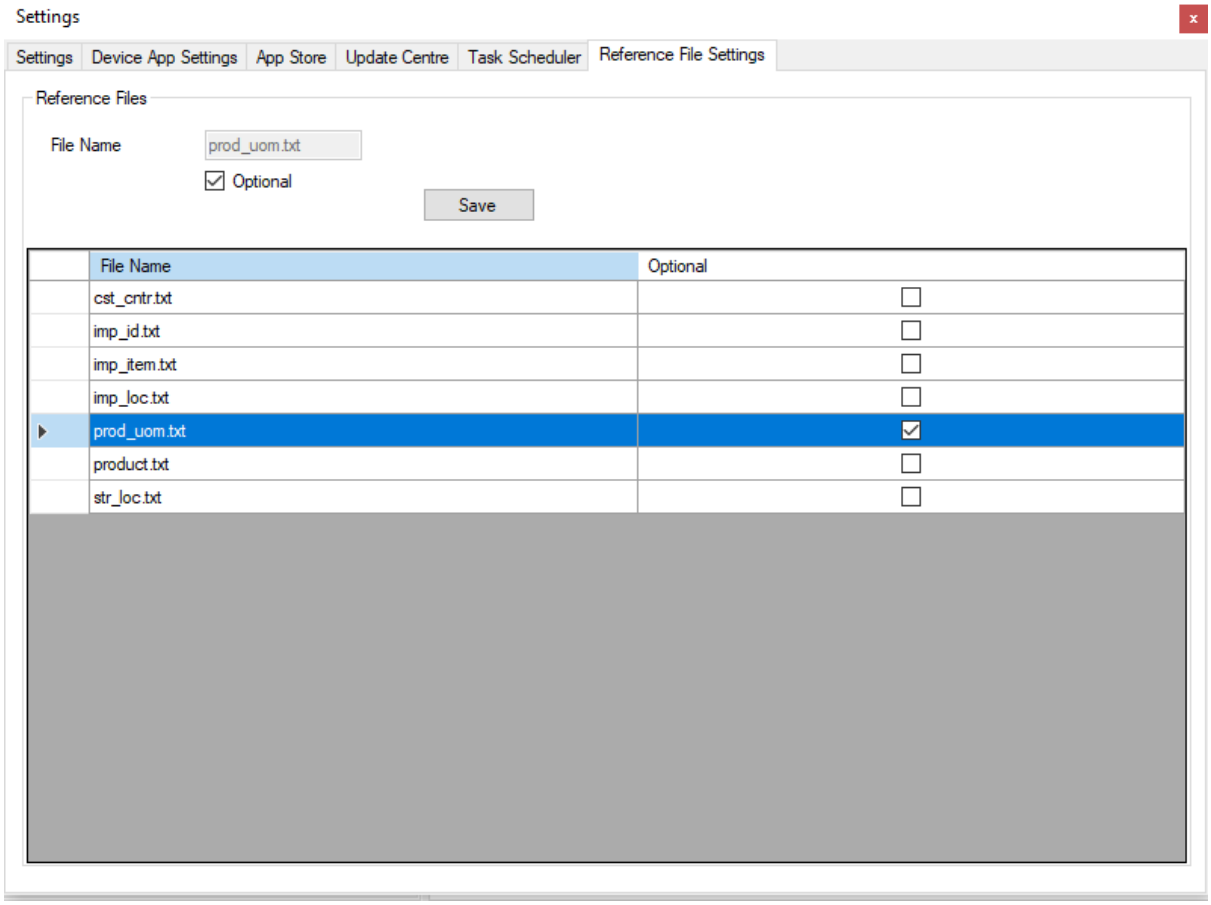
4.5 Task Scheduler Tab

Task schedular allows administrators to schedule tasks to be run on a specific time on the devices. For example a firmware update task can be scheduled to update device firmware at 12:30am.



4.6 Reference File Settings Tab

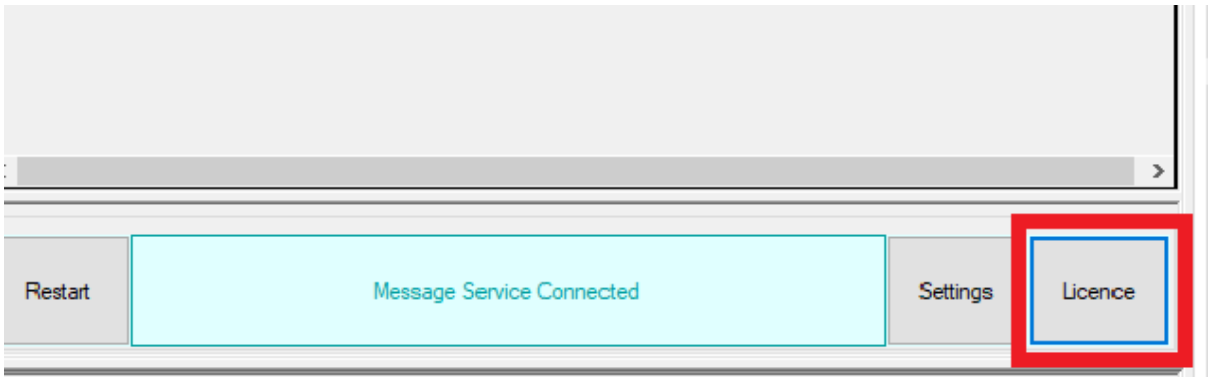
If any iPharmacy reference file is not used then this setting can be used to mark reference file as ‘Optional’. By default, all reference files are required to be loaded into the device.



5. Register Your Application

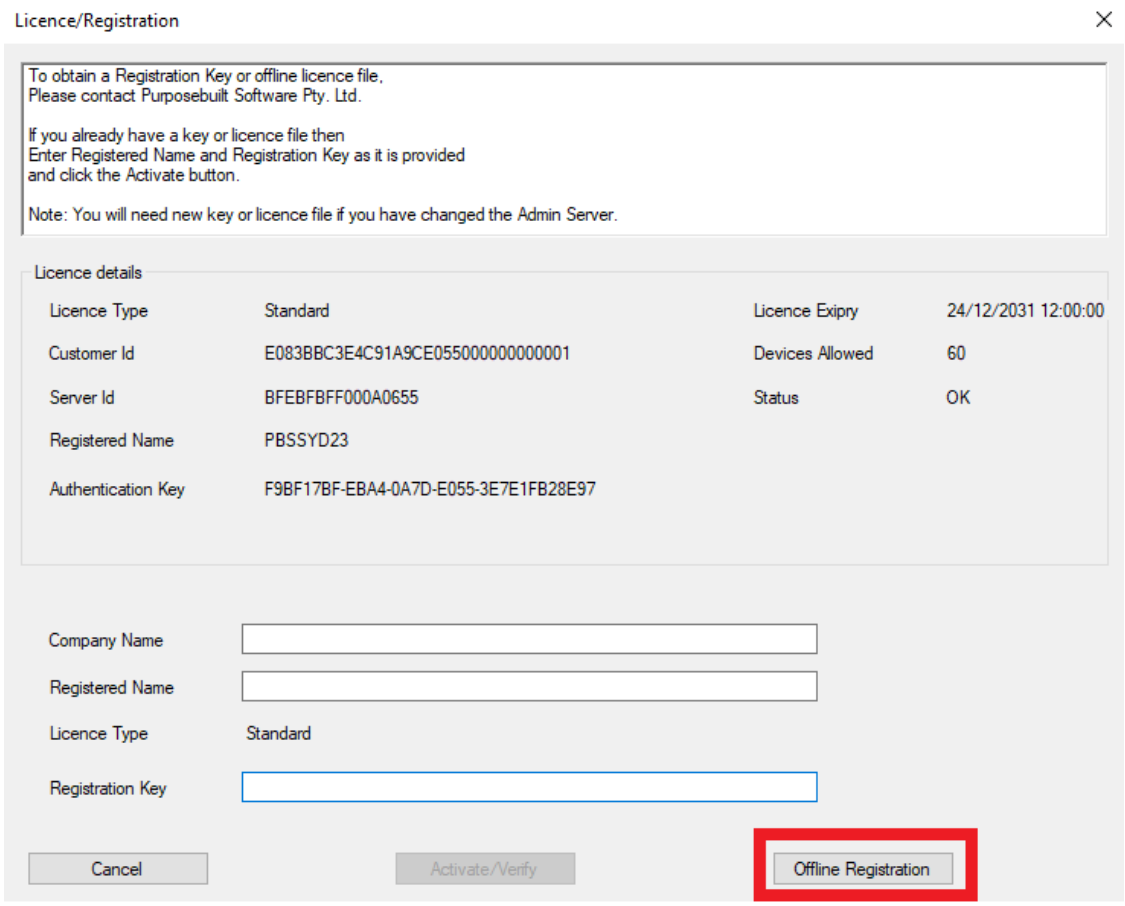
5.1 Add Licence

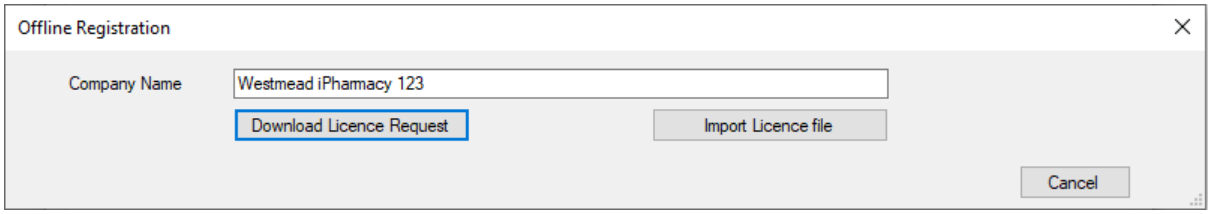
Select 4. Licence from the buttons menu



To add user specific license key, contact Purpose Built Software for details on the registered company name, if not received with your installation file.

Select “Offline Registration” – enter company name into the field and “Download Licence Request”. Send this file to support@purposebuilt.com.au.



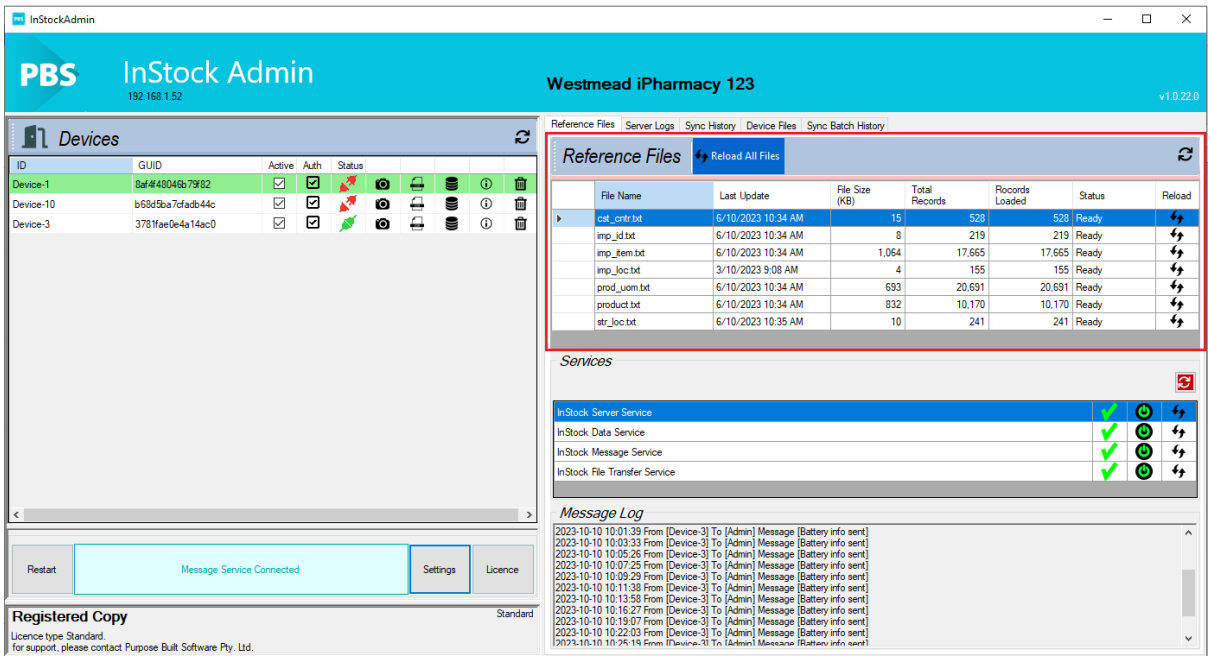


*If you do not have or are unable to locate your licence file, please contact Purpose Built Software Support Team.

*Keep the license file safe as will need to be reloaded upon a reinstall of InStock Server.

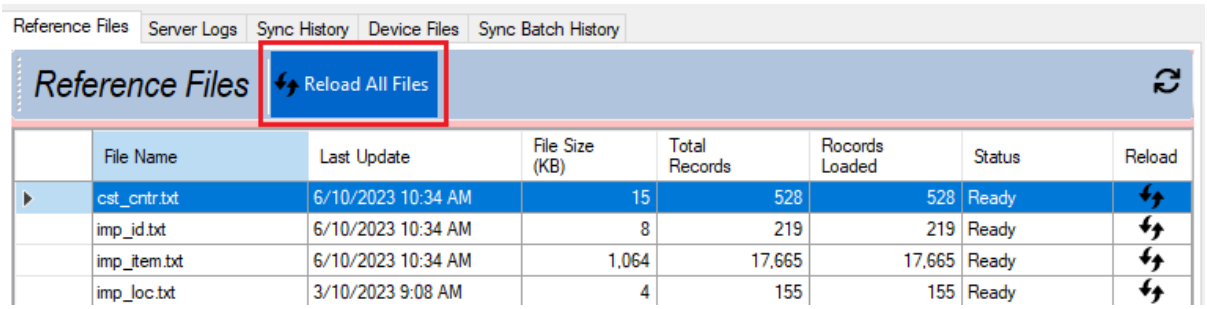
6. Reference Data

When the **Download Folder** setting is configured correctly and there are reference files in the folder, the service will start loading the reference files. You can see loading progress in the Admin console.



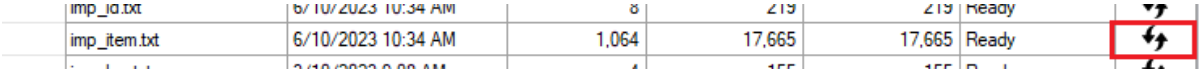
6.1 Reload All Reference Files

Reload all files button will initiate re-loading all reference files.



6.2 Reload a Single File

To reload a single file, use the Reload icon for each row.



7. Setting up your MC33X Device

Your MC33X has pre-installed two apps.

1. PBS Launcher App
2. InStock App

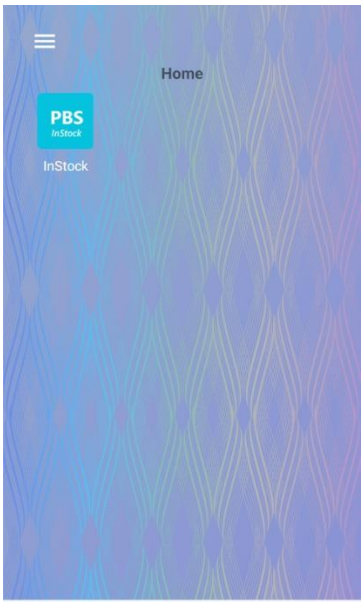
7.1 PBS Launcher App

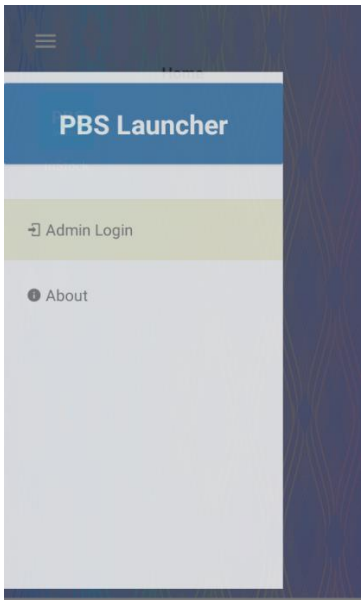
PBS Launcher app is designed to provide administrative control access to apps and settings on the device. Launcher app easily limits access to apps and prevent changes to device settings and locks down the file system. Only Admin users can add/remove apps. Users can only access approved apps.

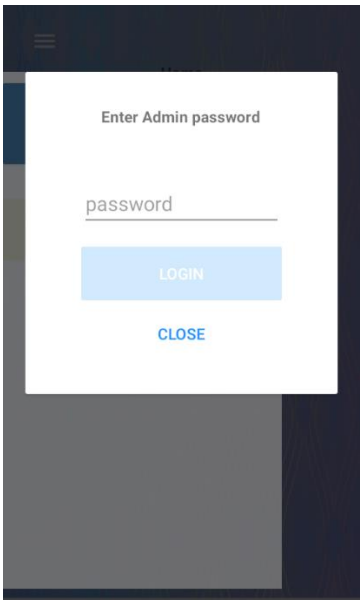
7.1.1 Setting up Apps

To add apps on the launcher home screen,

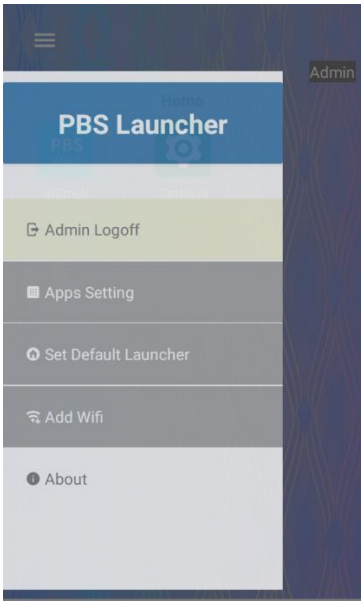
Login as Admin user.

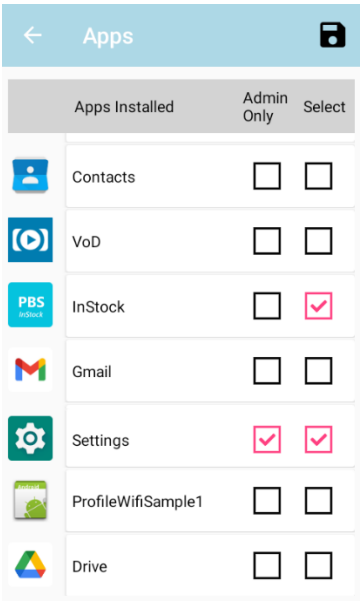






Select Apps Settings option from the fly menu and select the app(s) you want to add on the home screen and save. You can also mark apps for **Admin Only**, those apps will be available only after logged in as admin (Admin mark will be shown top right on the home screen when logged in and disappeared when logged off).


Admin
PBS Launcher
Admin Logoff
Apps Setting
Set Default Launcher
Add Wifi
About


Apps
Apps Installed
Admin Only
Select
Contacts
VoD
InStock
Gmail
Settings
ProfileWifiSample1
Drive

Admin
Home
InStock
Settings

7.2 InStock App

Launch the InStock app on your MC33X by pressing P1 key or tap the InStock app icon on the home screen.

7.2.1 Adding Wi-fi Connection

There are three ways you can add wi-fi connection.

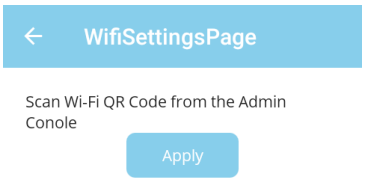
1. Using Android Settings app
2. Using PBS Launcher option
3. Scanning Wi-Fi settings QR code from the InStock app.

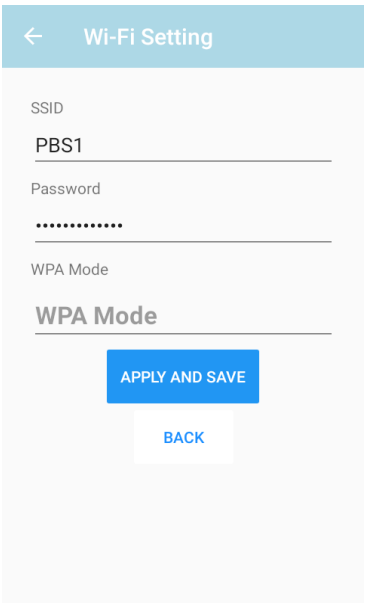
For option 1 and 2, you will need to access the Android's Settings app or select Add Wi-fi option from the fly menu. You can achieve this after login as Admin.

To adding by scanning QR code, in InStock app go to the fly menu and select Utilities->Scan Wi-fi QR code.

On the Admin console application, go to Settings->Device App Settings. Fill the Wi-Fi settings parameters and save, see here for details. After saving the details, you can generate QR code. Now on the device launch the InStock app press and scan it.

After scanning, press the Apply button and you will get to the Wi-Fi PBS Launcher with the pre-filled details. Tap on the Apply and Save button, this will prompt for Admin password if you are not already logged in. Tap Apply and Save button again after login to add the connection. If parameters are correct, the device will be connected to the Wi-Fi. Logoff as admin and press P1 from the device keyboard to get back to the InStock app.

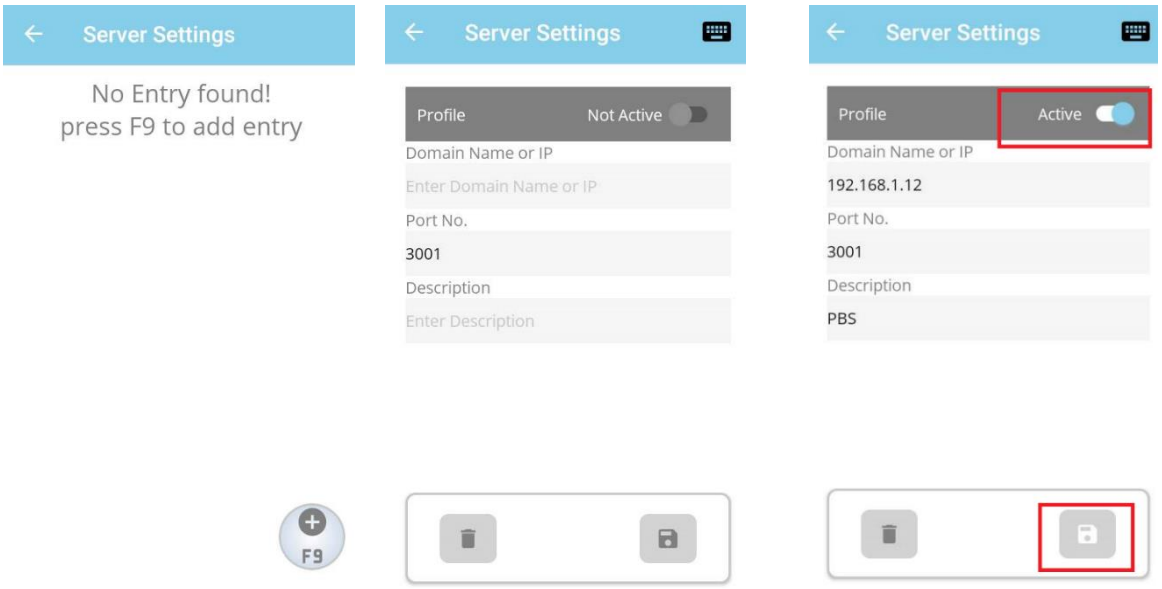




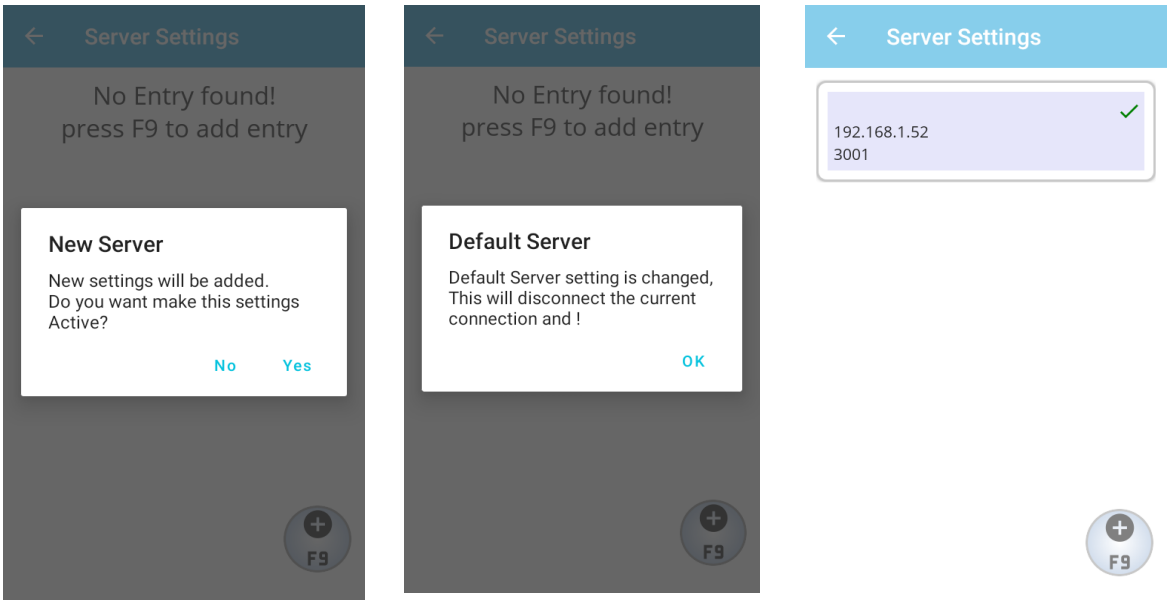
7.2.2 Configure Server Settings

If there is no server setting on the app then the app will request server settings. You can add it manually by pressing F9 here (or tap on the round fly button) or scan a Settings QR code from the Admin console application.

Adding manually. IP Address detail can be found in the InStock Admin console settings tab.

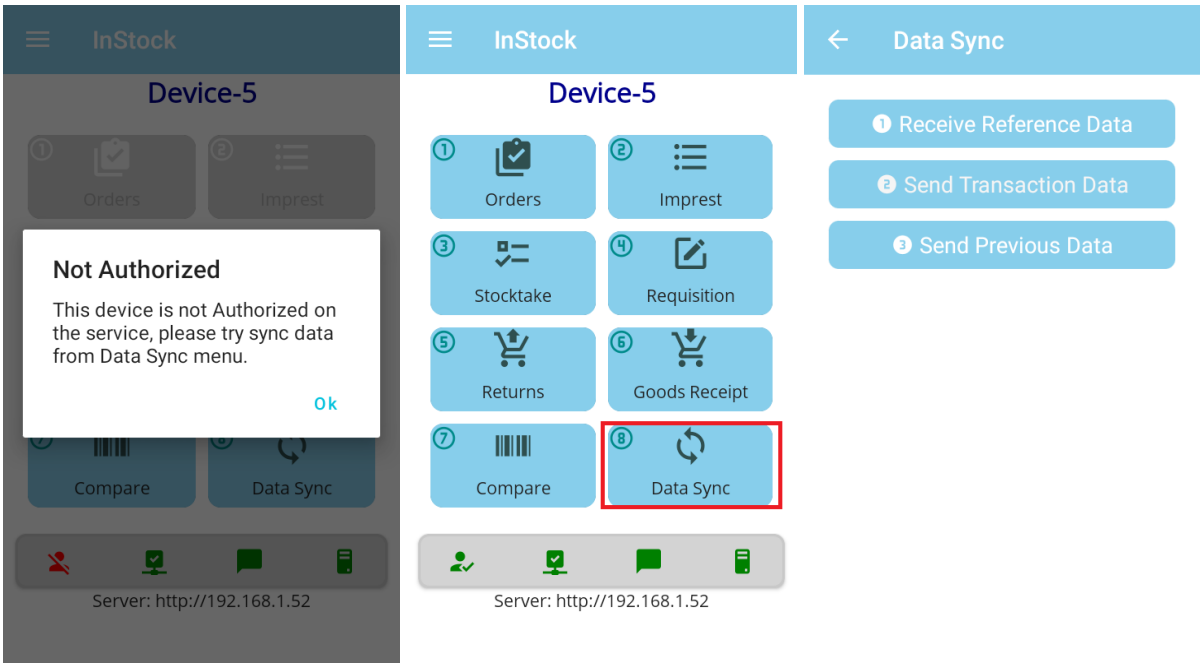


Adding by scanning QR code.



Note: At least one setting must be active or default to connect the backend server.

Go to the home screen and **Not Authorized** message will be shown. Go the Data Sync menu and sync data from the option 1.



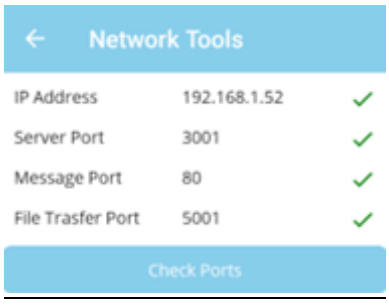
Mark server profile as Active and save changes. Navigate to home screen using the back icon.

7.2.3 Settings Device Name

By default, each device will get a name **Device-1.** It may change when the device is registered with the Admin console/Server and the name was already occupied by another device.

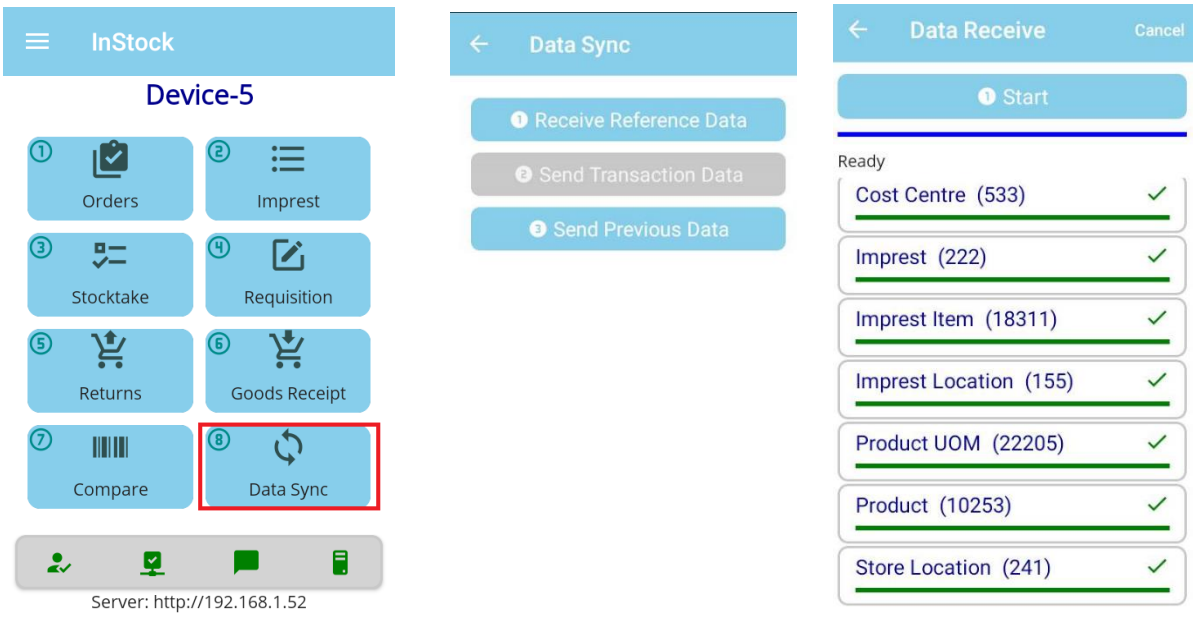
7.2.4 Check Server Connectivity

You can check server ports connectivity on the device from Utilities>Network Tools, if needed.



7.2.5 Download Reference Data

From the main screen, select 8. Data Sync, 1. Receive Reference Data, 1. Start.



Setup is complete.

7.3 Advance Wi-Fi Security

Zebra MC33xx devices support WPA3 Wi-Fi Security.

WPA3 is the next generation of Wi-Fi security, enabling robust authentication and increased cryptographic strength.

WPA3 offers the following features:

- Does not allow outdated protocols.
- Requires use of Protected Management Frames (PMF).
- Backwards compatible with WPA2.
- Supports the following authentication modes:
- WPA3-Personal - Uses simultaneous authentication of equals (SAE)
- WPA3-Enterprise
- Enhanced Open - Based on opportunistic wireless encryption (OWE). Note that this is a separate WiFi Alliance certification program and not WPA3.

7.3.1 WPA3-Personal (SAE)

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) protocol, replacing WPA2-Personal with Pre-shared Key (PSK). SAE is a variant of the Dragonfly protocol which uses a password authenticated key exchange based on zero knowledge proof. In SAE, passwords are used to determine a secret element in the negotiated group, called a password element (PWE). SAE is resistant to offline dictionary attacks.

WPA3-Personal (SAE) has the following modes:

- WPA3-SAE Mode – Devices can only use WPA3-SAE mode and PMF is always required. Information is secured using discrete logarithm cryptography.
- WPA3-SAE Transition Mode – Provides backward compatibility for devices using WPA2. The access point (AP) uses WPA3-SAE Transition Mode to enable both WPA2-PSK and WPA3-SAE at the same time on a single basic service set (BSS).

  WPA (version 1) cannot be used and is not supported on the same BSS as WPA3-SAE. WEP and TKIP cannot be used and are not supported by WPA2-PSK when used on the same BSS as WPA3-SAE.

7.3.2 WPA3-Enterprise

WPA3-Enterprise is based on WPA2-Enterprise but requires Protected Management Frames (PMF) and does not allow outdated WEP and TKIP protocols. WPA3-Enterprise 192-bit Mode requires support for GCMP-256 and SHA384 ciphers.

WPA3-Enterprise has following modes:

- WPA3-Enterprise only Mode - PMF is always required. WPA3-Enterprise devices negotiate PMF when connecting to an AP using WPA3-Enterprise only mode.

- WPA3-Enterprise Transition Mode - Provides backward combability for devices using WPA2-Enterprise. The access point uses WPA3-Enterprise Transition Mode to enable both WPA2-Enterprise and WPA3Enterprise at the same time on a single basic service set (BSS). WPA3-Enterprise devices negotiate PMF when connecting to an AP using WPA3-Enterprise transition mode.
- WPA3-Enterprise 192-bit Mode - PMF is set to required when WPA3-Enterprise 192-bit Mode is used by a client station (STA). The only 802.1X Authentication allowed is EAP-TLS.

To Configure advance Wi-Fi network, exit the InStock App and login as an admin on the launcher app. Launch the Settings app, if you don't see Settings app icon on the home screen, then please check here how to add apps on the launcher screen.

Please refer to the **Zebra WPA3 guide** for the steps how to add WPA3 network on the MC33xx device.

8. Minimum System Requirements

8.1 Admin Console

Operating System

Windows 10 x64 October 2020 Update (version 20H2)

Windows 11 x64

Dot Net Framework

- .NET Framework 4.8.1
- .Net core 3.1.1

Open Ports

Service Name	Default Port
Server Service	3001
Data Service	3002
Message Service	3003
File Service	5001

8.2 InStock App (Android)

Device/Scanner Supported:

Zebra MC33xx

Operating System Supported:

Android 10+

Connectivity Supported:

Ethernet connection (via Ethernet cradle)

Zebra MC330x Wireless LAN capabilities:

Radio	IEEE 802.11 a/b/g/n/ac/d/h/i/r/k/v1/w/mc1; Wi-Fi™ certified; IPv4, IPv6, 2x2 MU-MIMO
Data Rates	5GHz: 802.11a/n/ac — up to 866.7 Mbps 2.4GHz: 802.11b/g/n — up to 300 Mbps
Operating Channels	Channel 1-13 (2412-2472 MHz): 1,2,3,4,5,6,7,8,9,10,11,12,13 Channel 36-165 (5180-5825 MHz): 36,40,44,48,52 56,60,64,100,104,108,112,116,120,124,128,132,136,1 40,144,149,153,157,161,165 Channel Bandwidth: 20, 40, 80 MHz Actual operating channels/ frequencies and bandwidths depend on regulatory rules and certification agency.
Security and Encryption	Channel 1-13 (2412-2472 MHz): 1,2,3,4,5,6,7,8,9,10,11,12,13 Channel 36-165 (5180-5825 MHz): 36,40,44,48,52 56,60,64,100,104,108,112,116,120,124,128,132,136,1 40,144,149,153,157,161,165 Channel Bandwidth: 20, 40, 80 MHz Actual operating channels/ frequencies and bandwidths depend on regulatory rules and certification agency.
Certifications	WFA (802.11n, WMM-PS, 801.11ac, PMF); WiFi Direct WMM-AC, Voice Enterprise
Fast Roam	PMKID caching; Cisco CCKM; 802.11r; OKC