Honeywell

Operational Intelligence

Virtual Locker App

User Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. HII makes no representation or warranties regarding the information provided in this publication.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

Web Address: automation.honeywell.com

Trademarks

Android is a trademark of Google LLC.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

For patent information, refer to www.hsmpats.com.

TABLE OF CONTENTS

Customer Support

Technical Assistance

Go to automation.honeywell.com and select Support to search our knowledge base for a solution or to log into the Technical Support portal.

CHAPTER

1 GETTING STARTED

Virtual Locker is a smart device management solution designed to control access and enhance security for shared Honeywell mobile devices. The app provides a way to show the health of a device before a user checks it out, track which users have checked out a device and when they check it back in, and securely lock down a device to prevent unauthorized usage. Users can quickly check the device in and out by scanning a barcode, manually entering their user ID, or using NFC to scan an ID.

The app uses Operational Intelligence's Smart Sync feature to verify that all required software updates have been installed on mobile computers and report errors to the device administrator.

Refer to the *Operational Intelligence User Guide* available at automation.honeywell.com for details on using Op Intel to manage devices.

Prerequisites

- Operating system on the mobile computer must be Android 10 or higher.
- Application settings need to be reviewed and customized as per customer needs. See App Configuration.
- Operational Intelligence Device Connect Agent (also called SSClient) installed on the mobile computer and device onboarded to Operational Intelligence.
  - The Device Connect Agent version must be 5.13.02.0176 or higher.
  - The latest file can be downloaded from Honeywell's software download portal at honeywell.com/PSSsoftware-downloads or from the Google Play store.
- The Operational Intelligence license type must be Professional or Enterprise, and the license must be active.
- Whitelist the following application packages if devices are running with MDM:
  - com.honeywell.oi.virtuallocker
  - com.honeywell.tools.ssclient

Supported Devices

Refer to the *Operational Intelligence Device Support Matrix* for a list of Honeywell mobile computers that have been verified for the Virtual Locker app. The *Device Support Matrix* is available at automation.honeywell.com.

Installation

This section provides instructions on how to install the Virtual Locker app on the mobile computer. See the device user guide for additional information on installing software on the mobile computer.

Download apk Files

The current versions of installation files can be downloaded at honeywell.com/PSSsoftware-downloads. The Virtual Locker apk is located under **Software > Software and Tools > Virtual Locker**.

Be sure that you are using the correct apk files for your device type (Mobility Edge or ScanPal/EDA).

Install Components

Follow these steps for component installation.

Note: *The installation steps must be performed in this order for the application to work correctly.*

1. Install the Operational Intelligence Device Agent (SS_Client) then onboard the mobile computer to Operational Intelligence. Refer to the *Operational Intelligence User Guide* for instructions on onboarding a device.
2. If you need to configure application settings that are different from the defaults, update the **virtuallocker.json** file and copy it to the following path on the mobile computer: **\Internal shared storage\honeywell\persist**.
See App Configuration on page 6 for details.
3. Copy the **com.honeywell.virtuallocker.apk** file to the device and install the app. The installation file can be pushed to your mobile computers from Operational Intelligence using the Software Updates feature or a Smart Sync profile.
4. Launch the application.

Uninstalling the App

The app can be uninstalled using the standard procedure on an Android device.

CHAPTER

2 APP CONFIGURATION

Configuration

The following configuration steps must be performed so that the Virtual Locker app can be used with Operational Intelligence.

1. Add Users to the System.
2. Configure the Standard Check-Out Time.

Note: *The steps must be performed by a user with admin/device admin privileges in Operational Intelligence.*

For additional information on working with Operational Intelligence, refer to the *Operational Intelligence User Guide*, available for download at automation.honeywell.com.

Add Users to the System

The Virtual Locker app allows users who do not have an email address, such as a factory or warehouse worker, truck driver, etc., to check out a device before starting their shift and check the device back in at the end of their shift.

To enable this, the user must be added to Op Intel using a unique identifier, such as an employee ID or email address.

Note: *The user ID is critical information for checking out a device and assigning it to a user. Ensure this ID is unique for each user in the Organization. If an admin tries to add a user and the ID already exists for the site, Op Intel will display an error, and the user will not be added.*

When users are created, they will be assigned to a Site. For a user to check out a device with the Virtual Locker app, both the user and the device must be associated with the same Site. For example, if a user from Site A is trying to check out a device that belongs to Site B, the user will not be recognized as valid because they do not belong to Site B, and they will not be able to check out the device.

Creating Users

To enter an individual user by Email or ID:

1. Log into Operational Intelligence.
2. Click **Admin** then **User Management**.
3. Click **Add Users**.
4. Select a tab based on how the user will be identified in the system: **By Email** or **By ID**.
5. Enter the new user's **First Name**, **Middle Name** (optional), **Last Name**, and **Login Email** address or **EmployeeID**.
6. Using the drop-down lists, select an **Organization** and a **Site**.
7. If the user is being entered By Email, select a user role.
8. Click **SUBMIT**.

To enter users By Email or By ID in bulk:

1. Click **Admin** then **User Management**.
2. Click **Add Users**.
3. Select **By Email (Bulk)** or **By ID (Bulk)**.
4. Click **Download a CSV template** to get a copy of the spreadsheet you can use to upload users.
5. Create a row in the table for each user.
   - To add users by Email, enter the new user's **First Name**, **Middle Name** (optional), **Last Name**, **Login Email**, **Site**, and **Role**.
   - To add users by ID, enter the new user's **First Name**, **Middle Name** (optional), **Last Name**, **EmployeeID**, and **Site**.
   - When all records are entered, save the spreadsheet.
6. Drag the spreadsheet into the Add Users window or click **BROWSE FILES** to search and select the file.
7. The list of users that will be imported is displayed. To delete a user before uploading, click the trash can icon. To remove all users, click **RESET**.
8. To upload the new user records, click **SUBMIT**.

Configure the Standard Check-Out Time

Configure the standard check-out time to define the number of hours a user is expected to have a device before checking it back in. Generally, this is seen as standard shift hours.

1. Log into Operational Intelligence.
2. Click **Admin** then **Site Management.**
3. Select a site.
4. Click the **Check in – Check out** tab.
5. Select the **Standard checkout time** from the drop-down list to indicate how long a user would be expected to have the device checked out.
   The Standard checkout time is used when generating the “Late Returns” report from Op Intel on devices that are due for check-in.

Note: *This change will be effective for new check-ins only and is not applicable for devices that are already checked out.*

Create a Check-In Bar Code

Create a barcode that can be scanned by users to log in and log out from Virtual Locker on a device.

1. Log into Operational Intelligence.
2. Click **Admin** then **Site Management.**
3. Select a site.
4. Click the **Check in – Check out** tab.
5. Click **Create new barcode**.

   A new barcode is generated, and the system displays a message indicating that the barcode was created successfully.
6. After the barcode is created you can either download the .png file or send it by email.
   - Click **Download** to save the file in your default downloads folder.
   - To send a copy of the .png file by email, either leave the **Me** radio button selected to send it to the email address associated with your login or select **Another email** and enter the recipient’s address. Click the **SEND** button.

App Configuration

This section describes options for configuring application settings through the virtuallocker.json configuration file.

Note: *This file must be placed in* ***Internal shared storage\honeywell\persist*** *with the file name "virtuallocker.json". The application runs with the default values shown in the following table unless the file is updated.*

Device Settings

Setting	Property Name	Range	Default Value
OfflineMode			
Offline mode support	OfflineModeSupport	True/False	True
Offline mode reattempt count	OfflineModeReattemptCount	Range in minutes: Min: 1 Max: 15	10
Non-OpIntel user data synchronization frequency	UserSyncFrequency	Range in minutes: Min: 60 Max: 1440	240
Offline transactions synchronization frequency	OfflineTransactionSyncFrequency	Range in minutes: Min: 15 Max: 240	60
Offline transactions limit	OfflineTransactionLimit	Count range: Min: 60 Max: 240	120
Barcode site validation data synchronization frequency	SiteValidationQueryFrequency	Range in minutes: Min: 30 Max: 360	120
ConnectionSettings Supported connection types are Ethernet, Wi-Fi, and WWAN. All connection types are enabled by default.			
Ethernet connection setting	Ethernet	True/False	True
Wifi connection setting	Wifi	True/False	True
WWAN connection setting	WWAN	True/False	True

Setting	Property Name	Range	Default Value
OnlineMode			
Online Mode Reattempt Count	OnlineModeReattemptCount	Count range: Min: 1 Max: 15	10
External Scanner			
External Scanner Support	ExternalScannerSupport	True/False	False
Scanner Priority This parameter indicates the priority and sequence for scanner selection.	ScannerPriority	0 = Internal 1 = External	0
Report Damage			
Report an issue	ReportIssue	True/False	True

Login Settings

Setting	Property Name	Range	Default Value
Login Settings			
NFC enabled in Log In process	LogInNFCSupport	True/False	True
Scanner enabled in Log In process	LogInScannerSupport	True/False	True
Regular expression for reading Employee ID (Badge)	RegexNFCEmployeeId	String	
Regular expression for reading Employee ID (Badge)	RegexBarcodeEmployeeId	String	
Login Timer Settings			
Log in timer enabler	LogInTimerSupport	True/False	True
Log In timer duration	LogInTimerDuration	Range in seconds: Min: 5 Max: 360	60
Log In Alarm enabler	LogInAlarmSupport	True/False	True

Logout Settings

Setting	Property Name	Range	Default Value
Logout Settings			
Location barcode support in Log Out	LocationBarcodeSupport	True/False	True
Log out automatically	LogOutAuto	True/False	True
Log Out timer duration	LogOutTimerDuration	Range in seconds: Min: 1 Max: 15	10

Device Diagnostic Status

Setting	Property Name	Range	Default Value
Device Diagnostic Status			
Device diagnostic status	DeviceDiagnosticSupport	True/False	True
Needs Attention			
Needs attention enabler	NeedsAttentionSupport	True/False	True
Compliance validation	ComplianceValidationSupport	True/False	True
Time between device status rechecks in minutes.	NeedsAttentionDiagFreqMinutes	Integer (time in minutes) Min: 1 Max: 1440	180
Text displayed on the “Needs attention” status screen	NeedsAttentionLabel	String	“Needs attention”
Replace Battery			
Damage battery enabler	HealthBatterySupport	True/False	True
Battery health	BatterySOHLimit	% range: Min: 5 Max: 75	50
Battery age	BatteryAgeLimit	Months range: Min: 5 Max: 120	30
Battery cycle count	BatteryCycleCount	Counts range: Min: 50 Max: 999	500
Using the device when the battery is damaged	UsageWithLowHealthBattery	True/False	True

Setting	Property Name	Range	Default Value
Text displayed on the "Replace battery" status screen	ReplaceBatteryLabel	String	"Replace battery"
Not Ready To Use			
Battery not charged enabler	LowBatterySupport	True/False	True
Using the device when the battery is not charged	UsageWithLowLevelBattery	True/False	True
Text displayed on the "Not Ready to Use" status screen	NotReadyToUseLabel	String	"% charged"
Ready to Use			
Battery charge level	BatteryLevelLimit	% range: Min: 1 Max: 99	75
Minutes between "Ready to Use" status rechecks	ReadyToUseDiagFreqMinutes	Integer (time in minutes) Min: 1 Max: 1440	15
Text displayed on the "Ready to Use" status screen	ReadyToUseLabel	String	"Ready to use"

Note:

- Values outside specified ranges will be replaced by default values.
- For the data to be synced to the cloud in the back-end, ensure that the application is not closed. Once the Check-out/Check-in is completed in offline mode, for the data to sync to cloud in the background, use app switch to move onto the required LOB app. Closing the application would stop the sync, and the next sync would happen only on app launch.

Sample virtuallocker.json

The following example shows a typical configuration for Virtual Locker using default values:

```
{
  "name": "VirtualLocker",
  "Version": "1.0",
  "OfflineMode": {
    "OfflineModeSupport": true,
    "OfflineModeReattemptCount": 1,
    "UserSyncFrequency": 240,
    "OfflineTransactionSyncFrequency": 60,
    "OfflineTransactionLimit": 120,
    "SiteValidationQueryFrequency": 120
  },
  "ConnectionSettings": {
    "Ethernet": true,
    "Wifi": true,
    "WWAN": true
  },
  "OnlineMode": {
    "OnlineModeReattemptCount": 2
  },
  "ExternalScanner": {
    "ExternalScannerSupport": true,
    "ScannerPriority": 1
  },
  "ReportDamage": {
    "ReportIssue": true
  },
  "Login": {
    "LogInNFCSupport": true,
    "LogInScannerSupport": true,
   "RegexNFCEmployeeId": "",
   "RegexBarcodeEmployeeId": "",
    "LoginTimerSupport": true,
    "LoginTimerDuration": 60,
    "LogInAlarmSupport": true
  },
  "Logout": {
    "LocationBarcodeSupport": true,
    "LogOutAuto": true,
    "LogOutTimerDuration": 20
  },
  "DeviceDiagnostic": {
    "DeviceDiagnosticSupport": true,
```

```
    "NeedsAttention": {
      "NeedsAttentionSupport": false,
      "ComplianceValidationSupport": true,
      "NeedsAttentionDiagFreqMinutes": 120,
      "NeedsAttentionLabel": "Needs Attention"
    },
    "ReplaceBattery": {
      "HealthBatterySupport": false,
      "BatterySOHLimit": 50,
      "BatteryAgeLimit": 30,
      "BatteryCycleCount": 500,
      "UsageWithLowHealthBattery": true,
      "ReplaceBatteryLabel": "Replace Battery"
    },
    "NotReadyToUse": {
      "LowBatterySupport": false,
      "UsageWithLowLevelBattery": false,
      "NotReadyToUseLabel": "{x}% charged"
    },
    "ReadyToUse": {
      "BatteryLevelLimit": 10,
      "ReadyToUseDiagFreqMinutes": 15,
      "ReadyToUseLabel": "Ready To Use"
    }
  }
}
```

Note: *This file must be placed in the* ***Internal shared storage\honeywell\persist*** *folder on the mobile device with the name "virtuallocker.json".*

CHAPTER

3 USING THE APP

This section describes how to use the Virtual Locker app after it has been installed on a mobile computer. A valid Operational Intelligence license is required with either Professional or Enterprise tier.

After a user launches the app, two operations can be performed:

- Log In - Allows the user to register who is using the device and check if the battery is charged or if it is working correctly.
- Log Out - Allows the user to return the device, verify that the device is returned to the correct site, and report if it suffered any damage while it was checked out.

Device Status

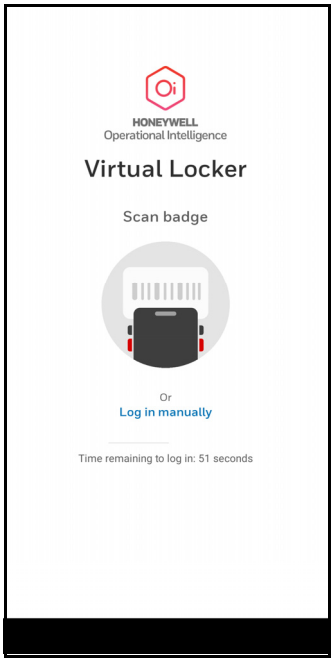
When the device is placed in a charge base, the Virtual Locker app displays a visual indication of its status. The statuses are color-coded for easy identification. Possible device statuses are:

- **Ready to Use** - The device has passed all diagnostic checks.
  When the mobile computer is removed from the charger, the Virtual Locker login screen will be displayed. See Log Into a Device on page 14.
- **Replace Battery** - The battery should be replaced before using the device because the battery health is below a designated threshold.
  See Battery Notification on page 15.
- **% Charged** - Shows the charge percentage for the battery if it is lower than the level required for Ready to Use status. The user can choose to replace the battery, use a different device, or use the device with the current charge.
- **Device Needs Attention** - The device has failed a diagnostic check. A device administrator should perform troubleshooting before the device is used. A device can be put in Needs Attention status if it not compliant based on the Smart Sync profile assigned to the device (for example, a software or firmware update failed). See Device Needs Attention on page 17.

Log Into a Device

When a user removes a mobile computer from the charge base, they will be restricted from using the device until it they log in.

The Virtual Locker login screen is displayed.



Depending on app configuration, users can log in using one of these options:

- Scan a barcode
- Tap their ID badge (NFC required)
- Enter their ID manually

The available login options are configured in Virtual Locker settings.

Login Time Requirement

Virtual Locker can be configured so that users are required to log into the device within a specified amount of time after the device is removed from the charger. The default time is 60 seconds. If the user does not log in within that amount of time, an alarm will sound. The user must either tap **Log In** and log into the device or return the mobile computer to a charger.

Log In Using a Barcode

Follow these steps to check out a mobile computer by scanning a barcode.

Note: *When the application first opens, the scanner can only be used to read the barcode to let the user complete the checkout process. Other functionalities like scanning a barcode to open a web page, etc., are blocked temporarily until checkout is complete. On successful completion of check out, the application can be exited, and the user can continue with their job.*

1. Turn on the device or remove it from the charge base. The Virtual Locker app will launch automatically.
2. Point the scanner at the barcode and press one of the scan buttons on either side of the device.
3. The app indicates that check-out is successful by displaying the user's name. The user can exit the app and use the mobile computer to perform their tasks.

Log In Using an ID Badge

Follow these steps to check out a mobile computer by tapping an ID badge. The mobile computer must have NFC functionality to use this method.

1. Turn on the device or remove it from the charge base. The Virtual Locker app will launch automatically.
2. Tap the ID badge near the NFC antenna on the device.
3. The app indicates that check-out is successful by displaying the user's name. The user can exit the app and use the mobile computer to perform their tasks.

Log In by Signing in Manually

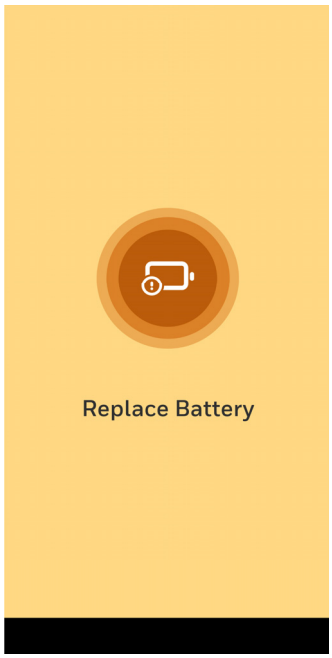
Follow these steps to check out a mobile computer by signing in manually.

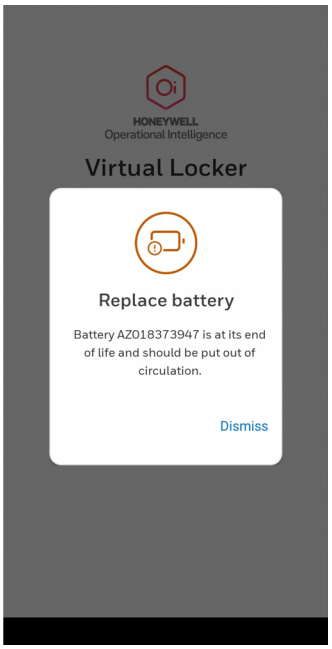
1. Turn on the device. The Virtual Locker app will launch automatically.
2. On the app home screen, tap **Sign in manually**.
3. Tap the **Enter your employee ID** field and enter the assigned ID.
4. Tap **Log In**.
5. The app indicates that check-out is successful by displaying the user's name. The user can exit the app and use the mobile computer to perform their tasks.

Battery Notification

If Virtual Locker detects an issue with the battery health, a warning screen will be displayed when the user removes the device from the charger.

For example, if the device needs a new battery, the following screen will be displayed.





When the user receives an alert screen, they can:

- Return the device to the charger and select a different mobile computer.
- Replace the battery in the mobile computer. The user can turn off the device and replace the battery or perform a hot swap or warm swap without turning off and restarting the device. Refer to the mobile computer user guide for more information on which Battery Swap Mode is supported by your device and for instructions on working with the battery.
- Wait for the alert message to display and tap **Dismiss** to check out the device. The Dismiss option is configurable in Virtual Locker settings. If the Dismiss option is not enabled, the user must replace the battery before using the mobile computer.

Warning: Before you attempt to use, charge or replace the battery in the device, carefully read all labels, markings and product documentation provided in the box or online at automation.honeywell.com. To learn more about Battery Maintenance for Portable Devices, go to honeywell.com/PSS-BatteryMaintenance.

Troubleshooting the Login Operation

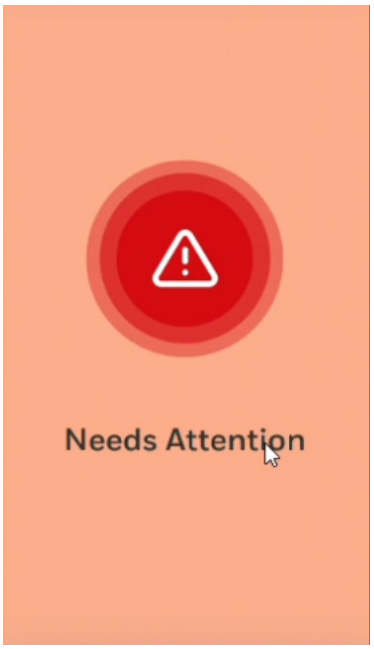
If any of the following issues occur, the user will be prevented from logging into the app until the issue is resolved.

Alert	Cause
User not found	Occurs if the worker is not registered or is not assigned to the correct Org/Site. The alert asks the user to retry the Check Out process.If the employee ID is entered again and the same error is shown, contact the Org/Site admin to verify if the user is assigned to the correct Org/Site or is not registered.
Session Warning	Occurs if the worker currently has another device checked out. The other device must be checked back in before the user can check out another unit. If the user does not have another device checked out, contact the administrator.

Device Needs Attention

When Virtual Locker detects that the device is not compliant with the assigned Smart Sync profile, the status screen will indicate Needs Attention when the mobile computer is in a charge base.

This option is available when the device is included in a Smart Sync profile in Operational Intelligence.



When a user removes the mobile computer from the charger, a message will be displayed indicating that the device is non-compliant and list the reason(s) for this status.

The user can:

- Return the device to the charge base and select a device that is ready to use.
  OR
- Tap **Continue to log in** and follow the standard login procedure.

Log Out of a Device

Users can automatically log out of a device by placing the mobile computer in a charge base or following these steps to log out of the Virtual Locker app.

Log Out Automatically

When the mobile computer is placed in a charge base, the user will be logged out automatically after the number of seconds configured for Logout time duration. The default is 10 seconds.

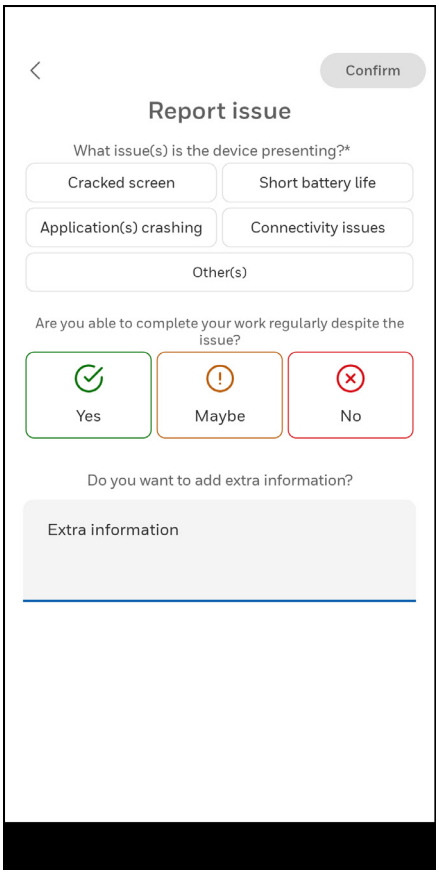
Note: *Users should follow the manual logout procedure on the device if they need to report an issue such as damage to the mobile computer.*

Log Out Manually

Follow these steps to log out of the device manually.

1. Open the Virtual Locker app.
2. Tap **Log Out**.

3. If you notice any issues with the device, such as some damage, you can enter information.
   a. Tap **Report issue**.



   b. Tap one or more of the options to indicate what issue the device is presenting.
   c. Tap **Yes**, **Maybe**, or **No** to indicate if you can complete your work.
   d. To enter additional information, tap the text box and use the virtual keyboard to enter a description of the issue.
   e. Tap **Confirm** to report the issue and continue with the check-in process.

Note: *The device administrator can view user-reported issues in Operational Intelligence. See Viewing Reports on page 22 for details.*

4. Press one of the scan buttons on either side of the device to scan the check-in barcode.
5. The app indicates that check-in was successful.

Troubleshooting Check In

Alert	Cause
Wrong location	Occurs if the check-in code is incorrect for the site. The user will be prompted to perform the process again. If the user performs the operation again and the same alert appears on the screen, contact the Org/Site admin to verify if the barcode belongs to the Org/Site of the device.

Offline Mode

The Virtual Locker application provides offline support to ensure user operations are unaffected in case of temporary network fluctuations so that users can perform the check-in and check-out operations without having an Internet connection on the mobile device.

This is achieved by syncing the user database check-in barcode information from the cloud to the device at regular intervals in the back-end and also syncing the check-in information from the device to the cloud at regular intervals when the network is stable.

Review the application configuration to fine tune the data sync frequencies and network selection as per business needs.

When the device is in Offline mode, a banner will be displayed at the bottom of the screen indicating, “Application is working offline.”

Notes:

- The Virtual Locker app will have to complete at least one "Check-Out" online operation with a network connection to ensure data sync with Web Op Intel.
- All data related to the user's site (like Site Barcode) will be updated onto the device with any online operation. If the device has been used in Offline mode, the user will need to confirm with the local admin if any user's site data was updated since the last time the device was online to return to Online mode device operation.
- Once the user completes a Check-In or Check-Out online operation, all Virtual Locker operations that have been completed in Offline mode will be synced with Web Op Intel within the time frame specified in the virtuallocker.json configuration file.
- Transactions are synchronized when the device successfully re-establishes a Wi-Fi connection. After all offline transactions are successfully synchronized within the configured time, the banner will no longer be visible.

CHAPTER

4 DEVICE MANAGEMENT

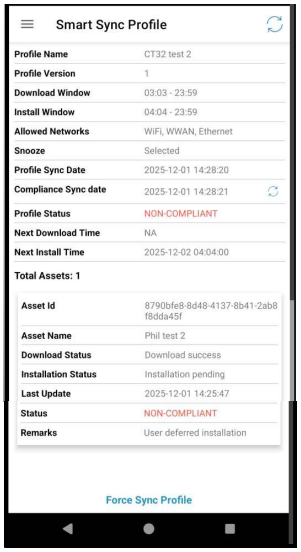
This section describes how to view device information when Virtual Locker identifies that they are not compliant and how to view reports when users have identified issues with a device during check-in.

View Compliance Status

You can verify if the device is in compliance with the Smart Sync profile by checking the Staging Hub app on the mobile computer or viewing the Compliance report in Operational Intelligence.

Check Status on the Mobile Computer

1. Swipe up on the screen to show all apps then tap Staging Hub Agent.
2. Tap the three-bar menu then select **Smart Sync Profile**.



- **Profile Name** displays the name of the Smart Sync profile assigned to the device in Op Intel.

- **Profile Status** indicates if the profile has been applied to the device or not. If the device is non-compliant, you can sync the profile by tapping **Force Sync Profile** or the sync icon .

Check Compliance Status in Op Intel

You can view the compliance status of all devices assigned to a Smart Sync profile in the Smart Sync console in Op Intel.

1. Log into Operational Intelligence.
2. From the navigation menu, select **Device Administration** then select **Smart Sync**.
3. In the list of profiles, click the name of the profile assigned to the device.
4. On the Profile Detail screen, select **Compliance report**.
   The Compliance report lists all of the devices assigned to the profile and the status of each package in the profile (Compliant, Non-compliant, Unverified).

Viewing Reports

Op Intel generates event reports based on activities such as late check-ins or damaged returns. You can view reports in the Op Intel **Reports** menu.

Reported issues will be reflected in Op Intel when the logout transaction is successful. If the device is being used in offline mode, transactions are sent when connectivity is restored.

1. Log into Operational Intelligence.
2. From the navigation menu, select **Reports** then select **Event Reports**.
3. From the **Report** drop-down list, select **Check In - Check Out**.
4. Select a **Timespan** from the drop-down list.
5. Select a **Template** from the drop-down list.
6. Click **SHOW REPORT**.
   The Reports window will display the details of each event in the selected Timespan, including Serial Number, Event Type, Assigned User, Check Out Time, Due Date, Check In Time, and any Notes entered when the device was checked in.

Honeywell
9680 Old Bailes Road
Fort Mill, SC 29707

automation.honeywell.com