Honeywell

Operational Intelligence

Performance Management

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. The information in this publication does not represent a commitment on the part of HII.

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: www.honeywellaidc.com

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

TABLE OF CONTENTS

Customer Support

Technical Assistance

To search our knowledge base for a solution or to log in to the Technical Support portal and report a problem, go to www.honeywellaidc.com/working-with-us/contact-technical-support.

For our latest contact information, see www.honeywellaidc.com/locations.

CHAPTER

1 GETTING STARTED

Introduction

Operational Intelligence Performance Management is a cloud-based software solution that communicates with Honeywell mobile computers, scanners and printers to gather metric and telemetry data. Operational Intelligence tracks device usage and identifies current issues and pending maintenance needs as well as monitoring consumable replacements such as batteries, labels, print heads and more.

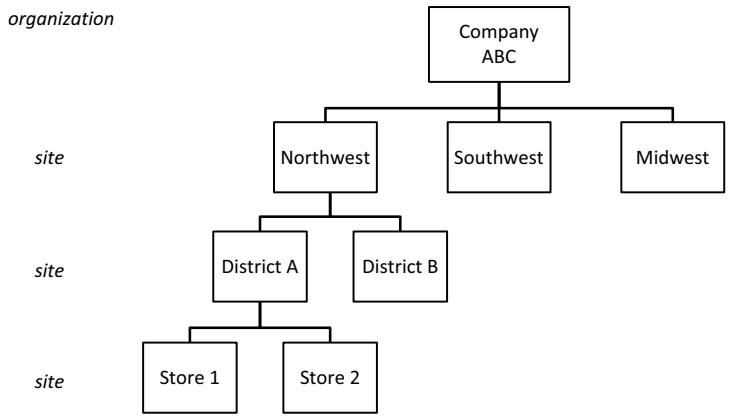
For information about Operational Intelligence licensing, please contact Honeywell Sales.

Requirements

Operational Intelligence Performance Management requires Google Chrome™ as the default browser.

Organizations and Sites

In Operational Intelligence Performance Management, you will set up your locations by establishing a hierarchy, with child sites below a parent organization. Organizations are set up by Honeywell, but you can create multiple levels of sites. For example:



For more information about location structure, see Site Management on page 65.

Note: *If you need additional organizations, please contact Honeywell Support.*

Setting Up Your Locations

When your company first starts to use Operational Intelligence Performance Management, you will need to complete the following steps:

1. Create a login account (see page 3)
2. Add sites to your organization (*see page 65*)
3. Add users (see page 63)
4. Optional: enable locationing and indoor tracking of mobile computers (see next section Indoor Locationing)
5. Add devices (see Mobile Computers on page 31 and Adding Non-Connected Assets on page 37)

Indoor Locationing

Honeywell Operational Intelligence Performance Management offers two solutions for locating mobile computers based on existing wi-fi infrastructure:

- An indoor positioning service (IPS) that employs the Site Survey application on mobile computers to “fingerprint” zones so that devices can be tracked to a 10mx10m area. The IPS captures a device’s location by building, floor and zone.

For more information, see the *Operational Intelligence Indoor Positioning Service for Mobile Computers Implementation Guide.*

- An Access Point solution that requires less time to set up than the IPS but is less precise. The Access Point solution captures only building and floor data for a device, and accuracy depends on the number of access points. For more information, see Access Points on page 69.

Creating an Account

1. Contact your local admin to request access.
2. Go to the login page, then click **Create an Account**.
3. Fill out the required fields, then click **CREATE AN ACCOUNT.**

Logging In

1. Go to the login page.
2. Enter your email address and password.
3. Click **SIGN IN.**

Navigation and Tools

Navigation Bar

On the left side of the portal there is an expandable navigation bar. To expand or collapse the navigation bar, click ☰. If the navigation bar is expanded, you can also use the up and down arrows to expand or collapse the Assets and Admin submenus.

Navigation Bar Icon	Description
	Displays the Dashboard (see page 9).
	Displays the Assets page (see page 21). Click the Assets icon a second time to display the Assets submenu:  Mobile Computers (see page 31)  Scanners (see page 37)  Printers (see page 37)
	Displays the Software Updates page (see page 53).
    	Displays or hides the Admin submenu (see page 63): User Management (see page 63) Site Management (see page 65) Access Points (see page 69) Dashboard Views (see page 74)

Note: *Your ability to view and modify data in Operational Intelligence is determined by your assigned user role (see User Management on page 63).*

Toolbar

The toolbar is located in the top right corner of the Performance Management portal. Various secondary toolbars may display beneath it, depending on the page you are viewing.

Toolbar Element	Description
	Click the Alerts icon to display notifications (see page 5).
(online status)	A green circle will display when you are on line. A red circle will display if you are off line.

Toolbar Element	Description
	Click the Help icon to access the following: **Help** - Operational Intelligence user documentation **Legal** - patents, terms and conditions, privacy, OSS (software) agreement, and cookies **Release Notes** - provides links to descriptions of product updates for the most recent releases; Pre-Release Notes describe new features and fixes targeted for future releases. **About** - link to more information about Operational Intelligence
	Click your initial to access the User Profile menu, including: **Settings** - change the appearance of the portal, including the language and unit type displayed. **Preferences** - set your notification preferences (see Alerts on page 5) **Log out** - sign out of Operational Intelligence For more information, see Customizing the Portal on page 6.
Organization	If you manage more than one organization in Operational Intelligence, you can choose to have the system filter all records so that only data for one of the organizations is displayed. If you do not select an organization, information for all of the organizations you manage will be displayed. To filter by organization, select a value from the **Organization** drop-down list. If you do not manage more than one organization, this field will not be displayed in the toolbar.

Zoom

On any page, you can zoom in by holding down the CTRL key on your keyboard then hitting the **+** (plus sign) key. To zoom out, hold down CTRL and hit the **–** (minus) key.

Alerts

Operational Intelligence Performance Management offers both onscreen alerts and email notifications. Examples of alerts include devices being dropped, power being disconnected with less than 90% charge, and printers running low or running out of ribbon or media.

Note: *See Preferences on page 7 to learn how to set up email notifications and alert reports.*

The Alerts icon  in the toolbar will display a red circle and a number if there are new notifications, for example  . Alerts are updated hourly. You can also view alerts on the Dashboard (see page 9).

To display any new notifications, click .

Note: *Alerts will remain tagged as new until you mark them as read on the Alerts page.*

To list all alerts, click then click **View all.**

Alerts Page

The Alerts page can be accessed by clicking in the tool bar. To filter alerts by status, severity or site click . To remove filters applied to the Alerts page, click then click **Reset all filters**.

The Alerts page displays summary notifications. Device-level alerts are displayed on the Device Detail page (see page 29).

System Updates

Operational Intelligence is updated to provide new features and introduce fixes to improve performance. You will be alerted of available updates in two ways:

- When you log into Operational Intelligence and updates are available, a blue message ribbon will display at the top of the window. Click the ribbon to load the latest updates. The software version number is displayed at the bottom of the browser window.

Note: *If software updates do not load when you click the banner, you might need to clear the browser cache to update to the latest version.*

- To view information on software updates, click the Help icon then select **Release Notes** from the drop-down list. A pop-up window provides links to release notes for the most recent releases. Pre-release notes may also be available to provide information on new features or fixes that will be delivered in future releases. A red dot will be displayed on the help icon to indicate that new release notes are available. You can subscribe to receive an email when new release notes are published in Email Notifications.

Customizing the Portal

The User Profile menu allows you to personalize the Operational Intelligence interface. All your settings will be saved when you exit the portal.

To access the menu, click the User Profile icon (your initial) in the toolbar.

Display Settings

Click **User Profile > Settings** to choose a display theme, language, or unit of measurement (Metric or Imperial). To exit the settings page, click the **X** in the upper right corner.

Preferences

Operational Intelligence Performance Management can notify you via email whenever an alert is generated. You can also choose to receive scheduled alert reports.

Alert Notifications

You can select to view information only for certain alerts rather than all alerts available in the system. When you configure alert notifications, only the selected alerts will be displayed in the Alerts section of the Dashboard. These alerts will also be displayed on the Assets page when you view asset details.

To receive an email whenever an alert is generated:

1. Click **Preferences** in the User Profile menu.
2. Click **Alerts**.
3. Toggle **Instant Alert Configuration** to on.
4. Select the alerts you wish to be notified about.
    - Alerts are categorized by asset or function type (i.e., Mobile Computers, Mobile Printer, Maintenance, etc.). To view the alerts within a category, click the category name to expand the menu.
    - Select the issues you want to receive alerts about. To select or unselect all alerts in a category, check the box next to the category heading.

Email Notifications

You can choose to receive an email when certain events occur or information is available. For example, you can subscribe to receive an email when release notes are published.

1. Click **Preferences** in the User Profile menu.
2. Click **Email Notifications**.
3. Select the **Sites** you want to receive email notifications about.
4. Select the issues you wish to receive email notifications for.
    - Choose **Same as Alerts** to apply the same choices you set in the Alerts section.

- Issues are categorized by asset or function type (i.e., Mobile Computers, Mobile Printer, Maintenance, etc.). To view the issues within a category, click the category name to expand the menu.
- Select the issues you want to receive emails about. To select or unselect all alerts in a category, check the box next to the category heading

Email Report

You can select alerts that you want to receive in an email report rather than viewing on the Operational Intelligence dashboard. Reports can be sent to your email on a daily, weekly, or monthly schedule.

To set up an alerts report to be emailed to you:

1. Click **Preferences** in the User Profile menu.
2. Click **Email Report**.
3. Click ⊕ **New Report.**
4. Enter a **Report name** for the new report.
5. Select one or more Sites.
6. Click **NEXT**.
7. Select the issues to include in the report.
   - Choose **Same as Alerts** to apply the same choices you set in the Alerts section.
8. Click **NEXT**.
9. Select a report frequency.
10. If you chose Weekly or Monthly, select a day on which the report should be generated.
11. Specify a Start Date and Time.
12. Click **CONFIRM**.

You can also edit or delete existing notification reports.

Logging Out

To exit the portal, click the User Profile icon (your initial in the toolbar). Then click **Log Out**.

CHAPTER

2 DASHBOARDS

Introduction

The Dashboard is comprised of a series of tiles for the site selected at the top of the page. Each tile provides data related to system and asset usage. The Dashboard also displays alerts that have been received.

Navigate to this page by selecting **Dashboards** on the navigation bar on the left side of the portal.

Use the arrows to expand or collapse a section.

Selecting a Site

Use the drop-down list at the top of the dashboard to select a site or type a site name in the field to quickly search for and select a particular site.

The reports displayed on the dashboards will be specific to that site.

Site names reflect their hierarchy. The first portion of the site name indicates the organization.

For example, selecting a top-level "/ Company ABC /" would display tiles for the entire organization, while selecting "/ Company ABC / Northwest / District A / Store 1" would display tiles for that single site only. For more information about site hierarchy, see page 66.

Types of Tiles

The tiles displayed on the dashboard will change based on the types of connected devices for the selected site. For example, scanning information will not display if no scanners are connected.

Depending on the devices connected, tiles may include:

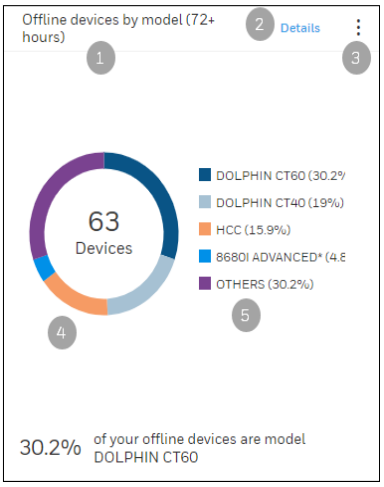
- Alerts (see page 6)

- Device usage and connectivity
- Battery health
- Mobile computer usage, drops, reboots, security patches, and operating systems
- Printer volume, label quantity, faulty dots, ribbon outage, and firmware
- Scanner volume and firmware

See Dashboard Tiles on page 15 for descriptions of all available tiles.

Example

This example shows the key features of dashboard tiles. Not all tiles will include a Details link or Display Options icon.

<table>
<tr>
<td> 
</td>
<td>1 - Title: Description of the data contained in the tile.</td>
</tr>
<tr>
<td></td>
<td>2 - Additional Details link - Click the link to display more information.</td>
</tr>
<tr>
<td></td>
<td>3 - Display Options - Click to view options for customizing the tile. In this example, you can select to change the minimum number of offline hours.</td>
</tr>
<tr>
<td></td>
<td>4 - Graph - The graph provides a visual representation of the data. This example shows a circle graph. Other tiles use different types of graphs. You can move your mouse pointer over a section of the graph to display detailed information.</td>
</tr>
<tr>
<td></td>
<td>5 - Key - Indicates what each color in the graph represents.</td>
</tr>
</table>

Display Options

The ⋮ icon in the upper right corner of a tile indicates that the tile can be customized. Click the display options icon then enter or select a new value. The display will be updated with the selected parameter.

To clear any previous change and return to the default value, click ⋮ then click **Reset**. When you change a display option, the selected value only applies for your current dashboard session. The next time you log in, the default value will be displayed.

To zoom into an area of a line graph, click and drag over the section of the report you want to expand. While the graph is expanded, a gray box will display in the right corner of the report. To reset the report, click the gray box.

To display specific details of a chart, mouse over an area of a bar or circle graph to show the exact value for that area of the graph.

Additional Details

If additional information is available beyond what is displayed on the tile, a **Details** link will be displayed. Click the link to display a table with the additional information. The specific data that is displayed depends on the information in the table.

- You can narrow the results displayed in the table by using the **Search** field. If you have narrowed the results, delete the text in the **Search** field to display the complete report data.
- To sort the table by column in ascending or descending order, click a column heading.
- If an arrow is displayed in a row in the Details table, you can click the arrow to expand the row to view additional information. The expanded rows will show the specific devices (mobile computers, printers, scanners) that are included in the data. When you click the Alias name for the device, Op Intel will navigate to the assets page for that device.
  For example, the Details table for the "Device by usage levels" tile displays a row for each site. You can expand the row to show the devices assigned to that site and the usage level for each.

To return to the main display, click **Back to Dashboard**.

Export Details

The data on the Details page for a tile can be exported to a .csv file.

1. Click the Details link on a tile.
2. Click **Export**.

   If the rows in a table can be expanded at the site level to provide more information, you can choose to export the data either for all sites or for a specific site. To export information for all sites, click the **Export** link at the top of the table. To export information for an individual site, expand the row then click **Export** on that row.
3. Select a location to save the file to.
4. If desired, change the file name.
5. Click **Save**.

Note: *All of the data will be exported, even if you have used the Search field to limit the displayed results.*

Tag Assets from the Dashboard

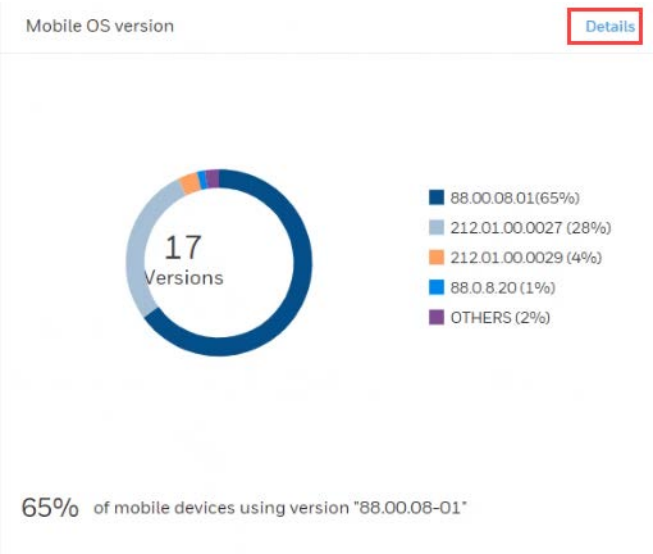
Some tables allow you to assign tags that can then be searched in the Assets page to identify the specific assets that the data applies to. For example, the Details table for the Mobile OS Version tile shows the number of mobile devices that have

each OS version, but it does not identify the specific devices. To identify the assets, you can select an OS version in the table, assign a tag to all devices with that OS, then search for that tag in Assets.

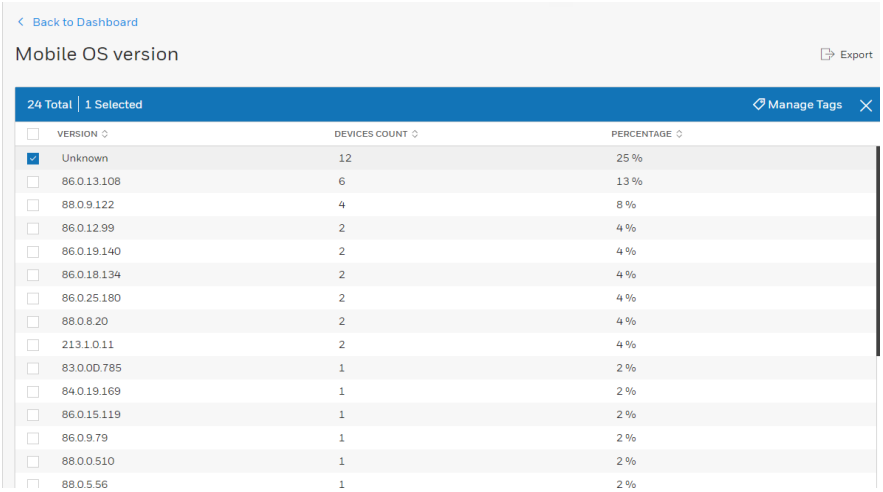
See Tags for more information on adding and editing tags.

To add a tag from the Dashboard:

1. On the Dashboard page, scroll to the tile you want to view then click the **Details** link.



2. Select one or more rows in the Details table.



   A blue toolbar displays indicating the total number of rows in the table and the number of rows that are selected. This toolbar only displays when a row has been selected.

3. Click **Manage Tags**.

4. On the Manage Tags window, click **New tag**.

5. Enter a **Name** for the tag or select an existing name.
6. Enter a **Value** or select an existing value.
7. Click **SUBMIT**.
8. Click **APPLY**.
9. Click **Back to OS Dashboard**.
10. To search for devices with the tag assigned, navigate to the Assets window then filter the table by Tags using the Name and Value you applied. See Filtering by Tag for more information.

Customize Dashboard View

Users can create custom dashboard views so that only sections of the dashboard that they want to view will be displayed instead of all available tiles.

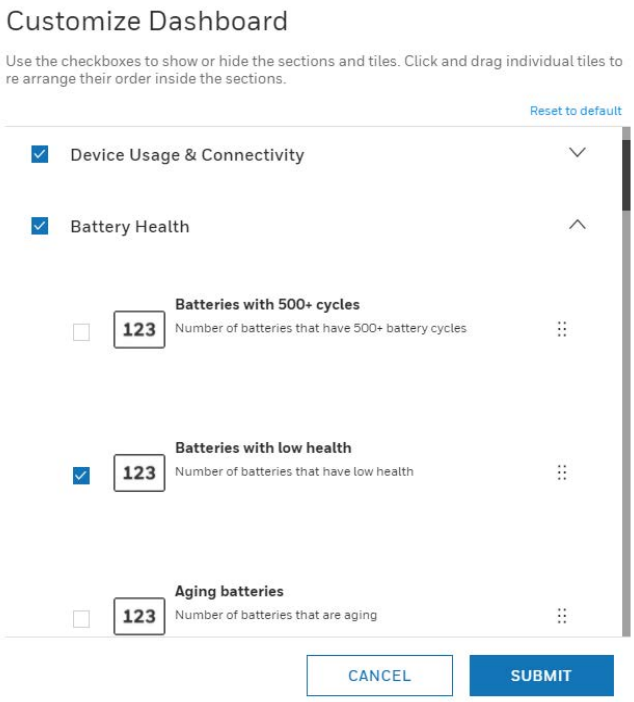
The default dashboard view is called “My Dashboard.” This view is associated with the user’s login, so it will be the default display for the user on any device they use to log into Operational Intelligence.

Customize Default View

You can update the view to display only the sections and tiles you want to view when you first login. These settings apply to the logged in user only and do not change the default view for other users.

To customize your default view:

1. Select **Dashboards** in the navigation bar.
2. Click **Customize My View**.



3. On the Customize Dashboard window, check or uncheck the sections and tiles that you want displayed.
   - The top level of each section represents a dashboard category (Alerts, Battery Health, etc.). When a category is unchecked, none of the tiles in that group will be displayed.
   - Use the arrows on the right to expand or collapse a section to select individual tiles to add or remove from the dashboard.
   - In the example above, all tiles in the Device Usage & Connectivity section will be displayed, and only the “Batteries with low health” tile will be displayed in the Battery Health section.
4. Click **SUBMIT** to update the dashboard display.

Create New Views

Users can create custom dashboard views, which can quickly be selected to display only relevant dashboard sections and tiles. The drop-down list displays the available views.

To create a new view:

1. Select **Dashboards** in the navigation bar.
2. Click **Create New View**.
3. Enter a **Dashboard Title**.

4. On the Customize Dashboard window, check or uncheck the sections and tiles that you want displayed.
    - The top level of each section represents a dashboard category (Alerts, Battery Health, etc.). When a category is unchecked, none of the tiles in that group will be displayed.
    - Use the arrows on the right to expand or collapse a section to select individual tiles to add or remove from the dashboard.
5. Click **SUBMIT** to create the view.
6. To apply a view, select it from the drop-down list.

Edit a Custom View

After you have created a view, you can edit it to change the tiles that are displayed when that view is selected.

To edit a custom view:

1. Select **Dashboards** in the navigation bar.
2. Select a view from the drop-down list.
3. Click **Customize this View**.
4. You can edit the **Dashboard Title** if required.
5. On the Customize Dashboard window, check or uncheck the sections and tiles that you want displayed.
6. Click **SUBMIT** to save the updated view.

Dashboard Tiles

This section describes the information displayed on each tile in the dashboard.

Device Usage & Connectivity

Tile	Description
Onboarded devices	The total number of devices that have been onboarded and have initiated communication with Operational Intelligence.
Never used	The number of devices that have been onboarded using the Bulk Provision tool but have not been put on the network. To identify devices that have not been used, select Assets in the navigation menu. In the Assets table, “Provisioned” is displayed in the Connection Status column for “Never Used” devices.
Registered devices	Number of devices that have been onboarded but have not communicated with the cloud.

Tile	Description
Onboarded batteries	Total number of batteries that have been onboarded for the site. Click Details to view a list of onboarded batteries, including the last device they were associated with. When you are viewing details, you can click the serial number in the Last Device column to open the Assets window for that device. If a battery is no longer in use, you can select it in the table and click Delete to remove it from the list of onboarded batteries. The battery will be added to the list on the Deleted Batteries tile under Battery Health.
Sites with devices	Number of sites in the selected Organization where devices have been onboarded.
Devices supporting smart batteries	The number of devices that support smart batteries. Smart batteries maintain information about the battery, such as serial number and health.
Devices by type	Graph showing the number of each type of device (mobile computer, printer, etc.)
Devices by site	Graph showing the number of devices associated with each site within the organization.
Devices by model	Graph showing the number of devices by model.. Click Details to view a table indicating the number of devices for each model and the percentage of the total devices it represents.
Offline devices by type	Number of devices that are offline sorted by type. The default display is devices that have been offline for 72+ hours. Click the more options menu to set the offline time to 1+ or 2+ days.
Offline devices by site	Number of devices that are offline sorted by site. Click Details to view a table with the number of devices that are offline for each site. The default display is devices that have been offline for 72+ hours. Click the more options menu to set the offline time to 1+ or 2+ days.
Offline devices by model	Number of devices that are offline sorted by model. Click Details to view a table with the number of devices that are offline by each model. The default display is devices that have been offline for 72+ hours. Click the Display options menu to set the offline time to 1+ or 2+ days.

Battery Health

The tiles in the Battery Health section report the health of the batteries for all device types (mobile computers, printers, scanners) associated with a site.

Tile	Description
Batteries with 500+ cycles	The number of batteries with more than the selected number of charging cycles. Click Details to view a list of all batteries, including the last device they were associated with. Click the Last Device to view the Assets page for the device. The default is 500+ cycles. Click the Display options menu to edit the minimum cycle count.
Batteries with low health	Number of batteries with health below a defined charge percentage. The default is 75%. Click the Display options menu to enter a different percentage. Click Details to view a list of all batteries, including the last device they were associated with. Click the Last Device column to view the Assets page for the device.
Aging batteries	Number of batteries with an age over a certain number of months. **Note:** Battery age is calculated from the manufacturing date of the battery not the date the battery was put into use.
Batteries to replace soon	Indicates the number of batteries that need to be replaced soon. Mouse over the tile title to display the parameters used to determine when a battery needs to be replaced.
Batteries to replace now	Number of batteries that should be replaced now. Mouse over the tile title to display the parameters used to determine this.
Number of low battery events	Number of low battery events generated by the devices. A low battery event usually represents a battery charge lower than 15%; however, this parameter is defined by the battery manufacturer and may vary by battery model.
New batteries in the current month	The number of new batteries that were added in the last 30 days.
Batteries not reporting 30+ days	The number of batteries that have not sent data to Operational Intelligence in the last 30 days. Click Details to view a list of batteries that have not reported. The default is 30+ days. Click the Display options menu to edit the number of days.
Deleted batteries	The number of batteries that have been deleted from Operational Intelligence. Click Details to view a list of deleted batteries. If a battery should not have been deleted, it can be added back to the list of onboarded batteries. Select the battery in the table then click the **Add** button.

Mobile Computers

Tile	Description
Device by usage levels	Usage based on active screen time. (Does not include sleep time.) Click Details to view a table of usage by organization. Expand the row for an organization to view the devices at that site and specific usage information for each device.
Devices with 8+ hours of use per day	Number of devices with over 8 hours screen on time per day. Eight hours is the default. The number of hours per day can be configured by clicking the Display options menu. Click Details to view a table of devices by organization. Expand the row for an organization to view the devices at that site and specific usage information for each device.
Mobile OS version	Displays a chart with all operating system versions installed on devices. Click Details to view the number and percentage of devices with each OS. You can tag devices based on operating system to make it easier to search by OS on the Assets page. See Tag Assets from the Dashboard for more information.
Dropped devices	Number of times devices were dropped in the last 30 days. Click Details to view a list of dropped devices and the type of impact event that occurred. Impact types are determined based on the free fall distance and gravitational force (G) inputs from the SDM600's free fall sensor and the Mobility Edge device's internal accelerometer. A free fall event occurs when the device drops more than approximately 60cm. A "Big G" event occurs when the device is subjected to approximately 5G of force. Impact types are defined as: **Hard Impact** - Free fall occurred with a Big G event or a single Big G event occurred without free fall. **Soft Impact** - A throw and catch event occurred without a Big G event or two or more Big G events occurred with a small interval between. **Free Fall** - Free fall occurred without a Big G event.
Reboots	Number of times devices were rebooted in the last week. Click Details to view a list of rebooted devices.
Security patch	Displays the percentage of devices with security patches installed at various time intervals. Click Details to view a more detailed list of dates on which security patches were applied. You can tag devices based on when security patches were updated to make it easier to search for them on the Assets page. See Tag Assets from the Dashboard for more information.

Tile	Description
Application usage time	Shows time used by apps on mobile devices, including third party applications. Click Details to view usage information on each app. Expand the app row in the Details table to view usage by each mobile device.
Network I/O	Displays data usage by apps on mobile devices. Click Details to view usage information on each app. Expand the row for an app in the Details table to view usage by each mobile device.

Printers

Tile	Description
Printers firmware version	Displays the firmware versions on all printers in the organization. Click Details to view a list of devices and firmware by version. You can tag devices based on the firmware version to make it easier to search by version on the Assets page. See Tag Assets from the Dashboard for more information.
Fixed printer usage by label quantity	Displays the number of labels printed for fixed printers. Click Details to view the usage level (light, moderate, heavy) for each device. Expand a row in the table to view the usage levels for each printer associated with the site.
Fixed printer usage by linear meters	Displays the linear meters of labels used for fixed printers. Click Details to view usage statistics for each site. Expand a row in the table to view the usage levels for each printer associated with the site.
Print volume	Print volume by day for the last 30 days.
Mobile printer usage by label quantity	Number of labels printed by mobile printers by month. Click Details to view the usage level (light, moderate, heavy) for each device. Expand a row in the table to view the usage levels for each printer associated with the site.
Mobile printer usage by linear meters	Amount of linear meters of labels used by mobile printers by month. Click Details to view the usage level (light, moderate, heavy) for each device. Expand a row in the table to view the usage levels for each printer associated with the site.
Printers with faulty dots	The number of printers where the print head has reported faulty dots. Click Details to view a list of the printers with faulty dots.
Out of media today	The number of incidents in which printers were out of media on the current date. Click Details to view a list of the printers that were out of media.

Tile	Description
Out of ribbon today	The number of incidents in which printers were out of ribbon on the current date. Click Details to view a list of the printers that were out of ribbon.

Scanners

Tile	Description
Scan volume	Total scan volume for all devices.
Scanner firmware version	Displays the firmware versions on all scanners in the organization. Click Details to view a list of devices and firmware by version. You can tag devices based on the firmware version to make it easier to search by version on the Assets page. See Tag Assets from the Dashboard for more information.
Trigger pulls resulting in barcode scans	Displays the total number of trigger pulls and the number of trigger pulls that did and did not result in a barcode being scanned.

CHAPTER

3 ASSETS

The Assets page displays summary information about all connected devices.

Access this page by clicking **Assets** on the navigation bar on the left side of the portal to expand the Assets submenu.

The Assets submenu narrows the information displayed by device type. If the navigation bar is expanded, you can use the arrows to display or hide the submenu. If the navigation bar is collapsed, click the Assets icon a second time to display the Assets submenu:

- All
- Mobile Computers
- Scanners
- Printers
- Other

Navigating the Assets Pages

The All assets, Mobile Computers, Scanners, Printers, and Other pages can be navigated in the same way.

Sorting

To sort the displayed asset table by column in ascending or descending order, use the arrows beside a column heading.

Selecting Assets

You can select one or more assets in a table by clicking the check box in the row for each asset. To select all assets in a table, select the check box in the heading row.

Note: *There is a limitation in the system that tables can only load a specified number of rows at a time regardless of how many total records there are. Because of this, when you check the box in the heading row to select all assets, only the assets that have been loaded to be displayed in the table will be selected, even if the system indicates that you have more total assets. You will need to scroll down in the table to load the remaining table rows then select all again. For example, if you have 150 assets, when you check the box in the heading row, the system will indicate that you have 150 assets total and 100 assets are selected. Scroll down in the table until unselected assets are displayed then click the select all box in the heading row again. The system will now indicate that there are 150 total assets and 150 are selected. Repeat this until all assets are selected.*

Selecting Columns to View

Click  to display a drop-down list where you can choose which columns you want displayed on the Assets page. Operational Intelligence Performance Management will remember your column filter choices if you navigate to another page in the portal. The column filter will also be applied the next time you log in. Not all columns apply to each type of asset. If a column is not relevant to the selected asset type, it will not be available to view. For example, if you select Mobile Computers, the “Labels printed” column will not be shown in the drop-down list.

Column Descriptions

This table provides a description of the columns that are available in the asset table views. When you view All assets, the File column displays an icon indicating the type of asset.

Mobile Computers

Column	Description
Alias	The alias name assigned to the asset.
Model	The model name/number of the asset.
Serial Number	Serial number assigned to the asset.
Connection status	Indicates whether an asset is connected to Operational Intelligence or not. See Connection Status for more information.
Last Communication	Shows when the device was most recently online.
State	Indicates whether a device is active, lost, out for repair, or out for service. If a device’s status is “Not Specified”, its state was not established when it was added to Performance Management.
Site	The name of the site the device is assigned to.

Column	Description
IMEI	International Mobile Equipment Identity number.
Phone Number	Phone number assigned to the mobile computer. (Mobile computers only)
Agent Version	Version of the the Op Intel device agent package installed on the device. This package is also called Staging Hub Agent.
Building	Name of the building the device is located in if you are using Indoor Positioning Service.
Floor	Name of the floor the device is located on if you are using Indoor Positioning Service.
Zone	Name of the zone the device is located in if you are using Indoor Positioning Service.
Battery level	The charge percentage of the battery.
IP Address	The IP address assigned to the device.
Status	The connection status of the device (Connected, Disconnected, Not Available)
Assigned User	The user a device has been checked out to.
Check Out Time	Date and time the asset was checked out.
Check In Time	Date and time the asset was checked in.
Notes	Displays any notes entered related to the asset.

Scanners

Column	Description
Alias	The alias name assigned to the asset.
Model	The model name/number of the asset.
Serial Number	Serial number assigned to the asset.
Connection status	Indicates whether an asset is connected to Operational Intelligence or not. See Connection Status for more information.
Last Communication	Shows when the device was most recently online.
State	Indicates whether a device is active, lost, out for repair, or out for service. If a device's status is "Not Specified", its state was not established when it was added to Performance Management.
Site	The name of the site the device is assigned to.
Firmware	The current firmware version on the device.
Battery level	The charge percentage of the battery.
Scan Volume	The number of scans the device has performed. (Scanners only)
IP Address	The IP address assigned to the device.
Status	The connection status of the device (Connected, Disconnected, Not Available)
Assigned User	The user a device has been checked out to.
Check Out Time	Date and time the asset was checked out.
Check In Time	Date and time the asset was checked in.

Column	Description
Notes	Displays any notes entered related to the asset.

Printers

Column	Description
Alias	The alias name assigned to the asset.
Model	The model name/number of the asset.
Serial Number	Serial number assigned to the asset.
Connection status	Indicates whether an asset is connected to Operational Intelligence or not. See Connection Status for more information.
Last Communication	Shows when the device was most recently online.
State	Indicates whether a device is active, lost, out for repair, or out for service. If a device's status is "Not Specified", its state was not established when it was added to Performance Management.
Site	The name of the site the device is assigned to.
Firmware	The current firmware version on the device.
Labels printed	The number of labels the device has printed.
Odometer	Current odometer reading.
IP Address	The IP address assigned to the device.
Status	The connection status of the device (Connected, Disconnected, Not Available)
Assigned User	The user a device has been checked out to.
Check Out Time	Date and time the asset was checked out.
Check In Time	Date and time the asset was checked in.
Notes	Displays any notes entered related to the asset.

Connection Status

The Connection Status column indicates whether an asset is connected to Operational Intelligence or not. A colored dot also indicates whether the device is online or offline.

Indicator	Status	Definition
	Connected	The device is online and Op Intel is receiving a signal at regular intervals.
	Disconnected	The device has previously sent data to the cloud but is currently offline for Op Intel data collection (in Sleep mode).
	Provisioned	The device has been provisioned but has not sent data to the cloud.
	Not available	No connection status is available. This usually applies to non-IOT assets.

Search

Use the Search text box to look for data in the table that contain the search text. The Search box displays a list of the columns that will be searched when you enter a value in the text box. For all assets, the search is applied to Alias, Serial Number, and Assigned User. For Mobile Computers only, the search also includes IMEI and Phone Number.

To perform a search, type in the Search field. The filter is automatically applied when you type in the Search box, and only assets with values in the specified columns and displays rows that match all or part of the search text are displayed.

Filters

Use the filters drop-down list to limit the display based on the values in one or more columns. Records that do not match the selected value will not be displayed. For example, you can select to apply a filter to the Status column so that only assets with a status of “Checked Out” are displayed.

To apply a column filter, click . Use the arrows to expand the filter options then select the filter you want to apply.

The number of filters that are applied will be shown in a blue circle on the filter icon. A blue dot is also displayed next to each category in the drop-down list where a filter is applied.

The system will remember your column filter choices if you navigate to another page in the portal. The column filter will also be applied the next time you log in.

To remove filters, click the Filters icon, then click **Reset all filters**. The filter reset option will display only if there is at least one filter applied.

Filtering by Tag

Tags are user-defined identifiers you can use to filter devices. (For information about setting up tags, see page 27.)

To filter by tag:

1. Select an assets page from the navigation bar (i.e., Assets, Mobile Computers, Scanners, or Printers).
2. Click .
3. Select from the tag **Name** drop-down list or type in the desired tag.
4. Select from the tag **Value** drop-down list or type in the desired tag. (For example, if you have set up tags for device operating system, you could select “OS” from the **Name** field and “Android” from the **Value** field.)
5. Click and the filtered results will display.

6. Repeat step 3-5 to add additional tags to your filter.

To remove a tag from your filter, click the **X** next to the tag name.

Operational Intelligence Performance Management will remember the applied filters the next time you log in to the portal.

Edit Asset Information

You can edit the Alias, State, or Site for one or more devices from the assets table.

1. Select an assets page (All, Mobile Computers, etc.) from the navigation bar.
2. Use the check boxes to the left of each row to select the desired devices.

   A blue toolbar will display.

3. Click **Edit**.
4. Update the **Alias**, **State**, and/or **Site**.
   For **State** and **Site**, you can select a status in the first row then check the **Apply to all Devices** box to set the same value for all devices.
5. Click **APPLY**.

Export Asset Information

You can export the entire asset table to .csv or limit the export to only selected devices.

To export data for specific units, use the check boxes to the left of each row to select the desired devices. To deselect a device, click the corresponding check box. To clear all check boxes, click the check box in the column heading.

If no specific devices are selected, all the data will be exported.

1. Select an assets page from the navigation bar (i.e., Assets, Mobile Computers, Scanners, or Printers).
2. Select specific devices or leave the check boxes clear to export all data.
3. Click **Export**.
4. Select the location where you want to save the .csv file.
5. If desired, change the file name. (The default file name will be the type of asset, the date, and the time.)
6. Click **Save**.

Exporting Filtered Data

To export filtered asset data:

1. Apply a filter to the Asset page by clicking .
2. Click the top of the check box column to select all rows in the filtered results.
3. Click **Export**.
4. Select a location and a file name.
5. Click **Save**.

Tags

Operational Intelligence Performance Management allows you to set up your own tags for filtering devices. For example, if you wanted to filter devices by operating system, you could set up a tag for each OS you use. Devices can have multiple tags.

Use the tags function on the Assets pages to manage tags for one or more devices. You can also use the Device Detail page to manage tags for a single device (see page 29).

Adding Tags

To create and assign tags to devices:

1. Select an assets page from the navigation bar (i.e., Assets, Mobile Computers, Scanners, Printers, or Other).
2. Use the check boxes to the left of each row to select the devices you want to assign a tag to.

   A blue toolbar will display.
3. Click **Manage Tags**.
4. Click **New tag**.
5. Select an existing **Name** from the drop-down list or enter a new one.
6. Select an existing **Value** from the drop-down list or enter a new one.
7. Click **SUBMIT**.
8. Click **APPLY**.

For example, to set up a tag for operating system, you could enter “OS” in the **Name** field and “Android” in the **Value** field.

Editing Tags

To edit a tag, for example if you want to change the name:

1. Select an assets page from the navigation bar.
2. Use the check box to the left of a row to select a device that has already been assigned the tag you want to change.

   A blue toolbar will display.
3. Click **Manage Tags**.
4. Select the tag you want to edit.
5. Click **Edit**.
6. Change the **Name** and/or **Value** field as needed.
7. Click **APPLY**.

Removing Tags

To remove a tag from a single or multiple devices:

1. Select an assets page from the navigation bar.
2. Use the check boxes to the left of each row to select the devices that have been assigned the tag you want to remove.

   A blue toolbar will display.
3. Click **Manage Tags**.
4. Select a tag.
5. Click **Remove from devices**.
6. Click **SUBMIT**.

Device Detail

Click on a device row on the Assets page to access more detail about that unit. The detail will differ based on the type of device. (See Mobile Computers on page 31 and Adding Non-Connected Assets on page 37.)

To return to the full asset list, click on the page name above the device alias at the top of the detail page.

For example, if you are viewing the detail for a mobile computer, **Assets > Mobile Computers** > will display at the top of the page. You can return to either the Assets page or the Mobile Computers page by clicking on the corresponding text.

All of the device details pages will contain some of the same types of information about the units, whether they are mobile computers, scanners, printers or gateways, and whether there are any alerts for the device. In addition, the detail page will list the location of the device in the organization's hierarchy.

There are also reports for the device at the bottom of the page. All devices will have Performance, Properties, and Events reports as well as information on the Tags assigned to the device.

Mobile computers have an additional Trends tab, which provides information on battery functions over the last week. Hover your mouse pointer over an area of the card to see details for a specific point on the trend line.

Tags

To display the tags assigned to a device, click **Tags** at the bottom of the Device Detail page. You can also add, edit, and remove tags. To manage tags for multiple devices, see page 27.

Assigning Tags to a Device

1. Select an assets page from the navigation bar.
2. Click on a row to display that device's details.
3. Click **Tags**.
4. Click **Manage Tags**.
5. Click **New tag**.
6. Select an existing **Name** from the drop-down list or enter a new one.
7. Select an existing **Value** from the drop-down list or enter a new one.
8. Click **SUBMIT**.
9. Click **APPLY**.

Editing the Tags Assigned to a Device

To edit a tag, for example if you want to change the name:

1. Select an assets page from the navigation bar.
2. Click on a row to display that device's details.
3. Click **Tags**.
4. Click **Manage Tags**.
5. Click the tag you want to edit.
6. Click **Edit**.
7. Change the **Name** and/or **Value** field as needed.
8. Click **APPLY**.

Removing Tags from a Device

1. Select an assets page from the navigation bar.
2. Click on a row to display that device's details.
3. Click **Tags**.
4. Click **Manage Tags**.
5. Select a tag.
6. Click **Remove from devices**.
7. Click **SUBMIT**.

Renaming a Device

The steps for renaming a device are the same regardless of device type:

1. Select an assets page from the navigation bar.
2. Click on a device to access its details page.
3. Click  to the right of the device's current name.
4. Enter the new name.
5. Click ✓.

Note: *Gateway names cannot be edited.*

Updating Software on a Device

On any detail page, you can check for available software by clicking the blue text beneath the **Software** heading. The available software options are pulled from the list of software that has previously uploaded into Software Updates and identified as compatible with the device model of the selected device.

1. Select an assets page from the navigation bar.
2. Click on a device to display its details page.
3. Click **Check for Available Updates** or **Updates Needed** (in blue).
4. Select the desired software package(s) using the check boxes.
5. To download and install the software immediately, click **Update**.

   Or

   To schedule the software update, enter a date and time, then click **Update**.

(For information on how to upload software so that it is available for devices, see Software Updates on page 53.)

Mobile Computers

Access the Mobile Computers page by clicking  in the Assets sub-menu. A list of all enrolled mobile computers will display.

Indoor Positioning

If indoor positioning has been set up for a device, its building, floor and zone (IPS only) will display on the Mobile Computers page.

For more information, see Indoor Locationing on page 2.

Detail

Click on a device on the Mobile Computers page to access the detail page for that unit.

For a mobile computer, the details information displays:

- Device info - Serial number and model of the device. Click the **Check available updates** link to see if software updates can be applied.
- Connectivity - Current connectivity status for the device and IP address.
- Battery info - Battery health, Serial number, and Charge level
- Alerts - Displays any alerts related to the device
- Site hierarchy - Displays the site the device is assigned to and any sites above it in the hierarchy.
- Map and Location History - A map view of the device's current location and timeline of the device's location history
- Performance - Displays metrics related to device performance.
- Trends - Provides information on battery usage.
- Properties - Displays additional information on the device and the battery that is currently installed in it. See Performance for more information the data that is displayed.
- Events - Provides a record of events that have been sent from the device.
- Tags - Displays a list of Tags associated with the asset.

To exit the device detail page, click **Mobile Computers** at the top of the screen or use the navigation bar. To return to the Assets page, click **Assets** at the top of the screen or use the navigation bar.

Map

If location services are enabled on the mobile computer, its most recent location will display on the detail page. The Location History panel provides a record of recent locations.

Use the plus and minus icons to zoom in and out of the map.

Performance

The Performance tab displays the following tiles. Information is provided for the last 30 days.

- Scan volume - Number of scans per day
- Reboots - Number of times the device was rebooted
- Daily hours of use - Number of hours the device was used each day
- Drops - Total number of times the device was dropped in the last 30 days

- Application usage time - Time used by applications on the device, including third party apps
- Network I/O - Data consumption by app

Trends

The Trends tab displays information

Properties

The Properties tab provides detailed information on the mobile device and the battery currently installed in the device.

Device IDs

Field	Description
Serial Number	Serial number of the device
IMEI	International Mobile Equipment Identity number
MEID	Mobile Equipment Identifier
Configuration Number	Configuration for the selected mobile device

Storage

Field	Description
Available Internal Shared Storage	Storage space available in the device's internal memory.
Available IPSM Card Storage	Storage space available in the device's IPSM card.
Available SD Card	Storage space available on SD cards, if installed.
Total Available Storage	Total storage available on internal storage, IPSM card, and SD cards.

Software

Field	Description
OS Version	Version of the operating system on the device
Firmware Version	Version of the firmware on the device
Security Patch Level	Last date a security patch was installed
Agent Version	Device agent version

Connectivity

Field	Description
IP Address	IP address of the device
Bluetooth MAC Address	Bluetooth identifier of the device
Wi-Fi MAC Address	MAC address of the device

Field	Description
Phone Number	Phone number for the device, if the device is equipped with a phone. **Note:** Phone Number is not enabled in the default settings for mobile computers. To display the phone number for a device, the DeviceOpIntel.xml file must be updated to enable this setting.
Network Name (SSID)	Name of the Wi-Fi network
Frequency	Frequency band the device uses

Location

Field	Description
GPS location	GPS coordinates of the device's last reported location
Last location update	Date and time the location was last updated

Usage

Field	Description
System runtime	Total number of hours the device has been in use
Hits, drops, falls and hard impact events	Total number of impact events

Scanning

Field	Description
Total barcodes scanned	Total number of barcodes successfully scanned
Total attempted scans	Total attempted barcode scans, including failed scans

Manufacturer Information

Field	Description
Serial Number	Serial number of the battery installed in the device
Manufacturer	Name of the battery manufacturer
Date of manufacture	Date the battery was made
Type	Type of battery
Voltage	Voltage of the battery

Condition

Field	Description
Age	Age of the battery. Battery age is calculated from the manufacturing date of the battery not the date the battery was put into use.
Health	Current charging health of the battery
Cycle count	Number of charging cycles the battery has gone through

Field	Description
Current capacity	Current battery capacity
Full charge capacity	Capacity when the battery is fully charged
Designed capacity	Capacity the battery is designed for

Charging

Field	Description
Time till fully charged	If the battery is charging, the amount of time until it reaches a full charge
Time of charge remaining	Time remaining for the current charge in minutes
Charging status	Indicates if the battery is charging or not
Charger type	Type of charger being used if the battery is charging
Charge level	Current percentage of charge

Temperature

Field	Description
Minimum temperature	Minimum recommended temperature for the battery
Maximum temperature	Maximum recommended temperature for the battery
Current temperature	Current temperature of the battery

Scanners and Printers

Click in the Assets submenu to access the Scanners page or to access the Printers page.

Note: *For information about enrolling scanners and printers in Operational Intelligence, see the Honeywell Cloud Connect User Guide.*

Detail

Click on a device on the Scanner or Printer page to access the detail page for that device.

To exit the device detail page, click **Printers** or **Scanners** at top of screen, or use the navigation bar. To return to the Assets page, click **Assets** at the top of the screen or use the navigation bar.

Other

Other assets are items that do not fall into the Mobile Computers, Scanners, or Printers categories but are things that a user might need to check out to use with a device, for example, a spare battery, protective equipment, carrying case, etc. Other assets can be either connected or non-connected items.

Access the Other page by clicking in the Assets submenu. A list of existing assets will display.

Detail

Click on a device on the Other page to access the detail page for that unit.

To exit the device detail page, click **Other** at top of the screen or use the navigation bar. To return to the Assets page, click **Assets** at the top of the screen or use the navigation bar.

Adding Assets

Use **Add Assets** to onboard new devices. You can create a QR code or xml file, which can be used to onboard connected assets, such as mobile devices, or you can onboard non-connected assets, such as batteries or other accessories, by uploading a file with a list of the assets.

Note: *Printers and scanners can also be onboarded using Honeywell Cloud Connect. See the Honeywell Cloud Connect user guide for more information.*

Adding Connected Assets

Use the Add Assets function to create a QR code or xml file that can be used to onboard new devices. When you create a QR code or xml file, it can be used for six months. There is no limit to the number of devices that can be added using the code.

1. Click to expand the Assets menu then select All or a specific type of asset.
2. Click **Add Assets**.
3. Select the **Connected** tab.
4. Select a site from the drop-down list.
5. Accept the terms and conditions by clicking the check box.
6. Click **NEW QR CODE**.
   The system generates a QR code.

7. You have two options for using the code to onboard a device:

   - Click  to download the bar code as a .png file. Then print the bar code or open the file. With Provisioning mode turned on, scan the bar code with each device to be onboarded.

   Or

   - Click  to download the bar code as an .xml file. Then use a mobile device management (MDM) tool to push the file to multiple devices. When pushing an .xml file:
     - Turn Provisioning mode on.
     - Push the file to the Storage>IPSM>Honeywell>Persist folder on the device.
     - Reboot the device to complete the onboarding process.

Note: *When distributing the onboarding bar code via MDM, do not change the default name of the .xml file from "DeviceOnboarding.xml".*

Note: *Only factory-registered mobile computers can be enrolled in Operational Intelligence Performance Management. If you try to add a device and you receive a message that it is not yet registered, contact Honeywell Support.*

Adding Non-Connected Assets

1. Click  to expand the Assets menu then select All or a specific type of asset.
2. Click  **Add Assets**.
3. Select **Non-Connected**.
4. Select a site from the drop-down list.
5. Click **Download an import template** to get an Excel file that you can use to upload assets.
6. Enter the required information for the assets in the template.

Note: *The first column of the template contains a drop-down list that is populated with Asset Models that have been added to the system using the Assets Configuration function. The drop-down list contains Asset Models in the format <Manufacturer>\|\|<Asset Type>\|\|<Asset Model>. Use the template to add specific units based on serial number. Verify that any required asset models have been added to the system before downloading the template. See Assets Configuration for more information.*

7. Drag the Excel or .csv file that contains the assets you want to upload onto the Add Assets window or click the **Browse Files** button to locate the file.
8. Click **Submit**.

Bulk Edit

You can use the Bulk Edit function to push a configuration file to multiple mobile computers rather than adding them one by one using a bar code.

1. Click **Mobile Computers**.
2. Click **Bulk Edit**.
3. Select a site using the search field.
4. Select a device type.
5. Select a model.
6. Enter a device's serial number, then click ⊕. Repeat for additional serial numbers.

   Or

   Drag and drop a file containing device data into the box on the lower left or click **BROWSE FILES** and select the desired file. (You can download a sample file to use as a template by clicking where indicated on the page.)
7. Click **Submit**.

Once the provisioning process has completed, the outcome will display at the bottom of the page. Click where indicated to download a .csv file of the results.

Gateways

On the main Assets page, you will see an additional type of device listed along with mobile computers, scanners and printers: gateways.

The icon indicates a Honeywell Cloud Connect (HCC) gateway. A gateway is a host computer through which HCC connects a printer or scanner to Operational Intelligence Performance Management. To display a list of gateways, use the **Device type** filter on the Assets page.

For more information about gateways, see the *Honeywell Cloud Connect User Guide*.

Check Out and Check In Assets

You can check out an asset to indicate that it has been assigned to a specific user. When the user returns the asset, it can be checked back in.

Note: *This feature can also be used from a mobile device.*

Check Out an Asset

To check out an asset:

1. Select an assets page from the navigation bar (i.e., Assets, Mobile, Computers, Scanners, or Printers).
2. Select the check box for each asset you want to check out. If you are checking out multiple assets, they all must be assigned to the same user.

Note: *You cannot check out an asset that is already assigned to a user. If one of the assets you select is checked out, the Check Out option will not be displayed.*

3. Click **Check Out**.
4. The Check Out window displays the assets to be checked out.
   a. To add a note to an asset, click ⊕ in the Notes column.
   b. Enter the note in the text box.
5. Click **Next**.
6. Click a user **Name** in the table to select the user the device will be checked out to. To narrow the list of users displayed, enter all or part of the name in the Search User field.
7. Click **Next**.
8. **Check Out Time** defaults to the current date and time and cannot be modified. Enter the **Check In Time**. This represents the suggested time to return the asset.
   a. To allow the assigned user to return the asset to one or more locations other than the check out location, click **Add Additional Location**.
   b. Select a location from the drop-down list.
   c. Repeat for each additional location.
9. Click **Next**.
10. Review the check out information then click **Submit**.

When the asset is checked out, the name of the Assigned User will be displayed on the Assets screen.

Note: *The Assigned User column is displayed by default on assets pages. You can display additional columns, such as Check In Time, Notes, etc., by selecting them from the Filter Columns menu. See Selecting Columns to View for more information.*

Check In an Asset

To check in an asset:

1. Select an assets page from the navigation bar (i.e., Assets, Mobile, Computers, Scanners, or Printers).
2. Select one or more assets that are checked out.
3. Click ✓ **Check In**.
4. To add a note to a returned asset, click ⊕ in the Notes column then enter the note in the text box.
5. Select the **Damaged** check box if an asset was damaged while checked out.
6. Click **Confirm**.

Device Maintenance

Use the Maintenance tab to acknowledge that regularly scheduled cleaning has been performed. Users will receive an alert that the device must be sanitized based on a rule created in Admin. (See Maintenance.) Alerts are sent based on the device that is checked out to the user.

For a mobile device with a screen, the user will acknowledge that maintenance has been performed by tapping a button on the screen. For a device without a screen, such as a printer, the user must acknowledge that the maintenance activity has been performed by entering confirmation in the Assets area.

Confirm Maintenance

1. Select an assets page from the navigation bar (i.e., Assets, Mobile, Computers, Scanners, or Printers).
2. Click an asset in the list.
3. Click **Maintenance**.
4. Select the **Operation** from the drop-down list
5. Select the **Action** that was performed.
6. Select the **Timestamp**.
7. Click **Confirm**.

The action will be recorded in the Event log for the device.

Remote Access

Remote Access allows an authorized user to connect to a device and perform the same actions as a user who is physically in possession of the unit. For example, an administrator can remotely unlock a device, switch between apps, search using the virtual keypad on the device, open the camera and capture photos and videos, and

run videos remotely for training and guiding a worker's daily needs. If you use the Mobility Edge "Soft Scan" button feature, you can open the scanner. This allows you, for example, to troubleshoot or test the scanning functionality.

Prerequisites for using Remote Access:

- Only users with the role of Device Administrator have access to this feature.
- You must be using the correct version of Operational Intelligence. You will be prompted to upgrade if necessary.
- The device you want to connect to must be online.

Using Remote Access

To connect to a device using Remote Access:

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.

Note: *Depending on how devices are configured in Operational Intelligence, it can take up to 5 minutes to accurately reflect the status of the device as online or offline. This effect is more pronounced when the device goes into sleep mode, is changing a network, or is rebooting. In this case, you will see an error message indicating that the system is unable to reach the device.*

3. Click **Remote Access**.

   The remote viewer opens in a new browser tab. Once the tab is opened, you can return to the main window and establish a connection with another device. You can have multiple devices open at the same time.

Note: *If user consent is required to give the administrator access to the device, the device user must select to allow access. See Require User Consent for Remote Access for more information.*

4. Use your mouse and keyboard to interact with the virtual display of the device. You can perform all functions that you would be able to do using the physical device. You can also use the device command buttons that are displayed at the bottom of the remote access window. To unlock the device, click the **Power** button then click the **Unlock** button.

Button	Function
App Switch	Switch between open applications on the device
Back	Return to the previous page on the device
Home	Go to the device Home screen
Menu	Open the menu for the app that is currently displayed on the device.
Search	Open the Search window
Camera	Turn on the device camera.

Button	Function
Contacts	View the Contacts added on the device
Page Up	Scroll up on a page or menu
Page Down	Scroll down on a page or menu
Call	Make a call from the device.
Email	Access the default email app on the device.
Unlock	Unlock the device. To unlock click Power then Unlock.
Power	Turn the device power on or off
Reboot	Restart the device

5. To exit the session, close the browser window displaying the device.

After a device has been accessed remotely, information captured during the remote session will be available in the device Events log.

Require User Consent for Remote Access

The Remote Access feature offers an option to allow the mobile device user to accept or deny a remote access request. If this function is enabled, the user will receive a pop-up message on the mobile device asking, “Allow Operational Intelligence to take control of the device?” The user must tap “Allow” to let the administrator connect to the device using Remote Access. If the user taps “Deny,” a pop-up message will be displayed in Operational Intelligence to let the administrator know that the request has been denied. If the user does not respond to the request for remote access within 30 seconds, the system treats it as a response of “Deny,” and the administrator will not be allowed access.

By default, user consent is turned off and the administrator will always be allowed to access a device. To turn this feature on, the RemoveViewerConsent setting in DeviceOpIntel.xml must be enabled. (To enable this setting in Enterprise Provisioner, select “Wait for user acknowledgment for remote control” in the Diagnostics Data Capture settings.)

View Device Files

Use the remote management File Explorer view to access the files on a mobile device. Within this view, you can upload, download, and delete files on the mobile device that is being accessed remotely.

1. With the device accessed remotely, turn the **File explorer** toggle to on.

   The File explorer view is displayed. The left side of the screen displays a tree view of the folders on the device. Select a folder to view the files in it.

2. Some folders can only be accessed when Provisioning mode is turned on. This includes folders in the Honeywell directory. Select the toggle for Provisioning mode if you need to view these folders.

3. To upload a file from your computer to the mobile device, click the  Software Upload button, select the file and file location on the device, and click the Upload button.

   A progress bar will indicate when the upload completes.

4. To download a file from the mobile device to your computer, select one or more files then click the  Download button.

Note: *The maximize file size that can be uploaded or downloaded is 2MB.*

5. To delete files from the mobile device, select the files in the File Explorer and click the  Delete button.

Actions

The Actions menu provides tools to remotely update a mobile computer or to troubleshoot a device.

Device Actions

Use the Device Actions menu to remotely reboot or reset a mobile computer. The Sync Data function can be used to update telemetry information on-demand.

Refer to the user guide for the specific device for more information on performing an Enterprise Data reset or Factory Data reset.

Reboot a Mobile Computer

The reboot option will restart a remote device.

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.
3. Click the Actions menu then expand Device Actions.
4. Select **Reboot**.
5. A system prompt verifies that you want to reboot the device. Click **OK**.

   The system indicates if the reboot was successful or not.

Enterprise Data Reset

You can perform an Enterprise data reset if a reboot did not improve the condition and all other troubleshooting methods have not resolved the issue. This method provides a clean configuration for troubleshooting by erasing all data from the **`Internal shared storage`** location on the computer. Data is not erased from the **`IPSM Card`** location.

Caution: An Enterprise data reset results in data loss. Only perform this procedure if all other recovery methods have failed. All personal content is erased including, but not limited to emails, pictures, contacts, Google account information, system settings and app settings.

Perform an Enterprise Data Reset

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.
3. Click the Actions menu then expand Device Actions.
4. Select **Enterprise Data Reset**.
5. A prompt indicates that an enterprise data reset will erase all data from the phone's internal storage. Click **OK** to continue.

   The system indicates if the enterprise data reset was successful or not.

Factory Data Reset

A Factory Data Reset should only be performed if you have exhausted all other troubleshooting options. This method reverts the computer back to the factory state by erasing all data in **`Internal shared storage`** and the **`IPSM Card`** storage locations on the computer.

Caution: A Factory data reset results in data loss. Perform this procedure only if all other recovery methods have failed and have no other option. All personal content is erased including, but not limited to emails, pictures, contacts, Google account information, system settings and app settings.

Perform a Factory Data Reset

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.
3. Click the Actions menu then expand Device Actions.
4. Select **Factory Data Reset**.
5. Click **OK** to continue.

   The system indicates if the factory data reset was successful or not.

Sync Data

Telemetry information for mobile devices is updated in Operational Intelligence at four hour intervals. Use the Sync Data function to pull telemetry information on-demand.

Devices must be online for telemetry to be updated.

Sync Device Data

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.
3. Click the Actions menu then expand Device Actions.
4. Select **Sync Data**.
5. Click **OK**.

   The system indicates if the device command was successful or not. When telemetry information is updated successfully, the current information received from the device is displayed.

Troubleshoot

Use the Troubleshoot menu to update Heartbeat and Telemetry information from a mobile computer. This is useful, for example, if a device shows that it is in Connected status but the Last Communication shows as several weeks or months ago.

The device heartbeat is sent from the device at a defined interval. The default time period for sending the heartbeat data is 120 seconds. Device heartbeat impacts the connection status in Operational Intelligence. A device not sending heartbeat for 5 minutes is marked as "Disconnected" in Operational Intelligence.

Note: *Devices stop sending the heartbeat when there is no network, when there are network connectivity issues, or when the device is in sleep mode or powered down.*

Refresh Heartbeat Timestamp

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.
3. Click the Actions menu then expand Troubleshoot.
4. Select **Heartbeat Timestamp**.

   The system displays the last date and time that a heartbeat was received from the device.
5. Click **REFRESH** to see the latest data.

Refresh Telemetry Timestamp

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list to view its information.
3. Click the Actions menu then expand Troubleshoot.

4. Select **Telemetry Timestamp**.

   The system displays the latest telemetry timestamp from the device.
5. Click **REFRESH** to see the latest data.

CHAPTER

4 SITE ANALYTICS

Site Analytics provide charts that can be used to compare the asset performance between different sites.

Access this page by clicking **Site Analytics** on the navigation bar on the left side of the portal

- Site Comparison shows how selected sites compare to each other.
- Site Rankings shows the top sites in selected categories.

View Site Comparisons

The Site Comparison pages provides several predefined reports, which show how different sites compare to each other.

Select Sites for Comparison

When you view the Site Comparison report, you will select the sites you want to include in the comparisons. Each site added will be displayed in a different color, which will be identified in the key for each tile. You can include up to six sites in the comparison.

To select sites:

1. Click **Add Site** in the Site box.
2. Select a site on the Filter Site window. Use the arrows to expand the nodes in the tree view.
3. Click **SELECT**.
4. Repeat for each site to be included.

Select Asset Type

You can view reports for any of the available asset types (Mobile Computers, Printers, Scanners).

Note: *In the Site Analytics reports, a scanner is considered to be any device that can scan a barcode, including both handheld scanners and mobile computers.*

Select Days to Display

You can view reports that include data for a specified number of days. To change the number of days, select the days drop-down list and choose, from the available values. The selected value will be applied to all reports.

View Site Rankings

The Site Rankings pages provides several predefined reports that show how sites are ranked. The top or bottom five sites in the selected organization are included in the rankings.

Select Number of Sites

By default, the Site Rankings page includes five sites. You can also display ten sites. Select the value from the drop-down list.

Select Site Ranking to Display

You can view reports based on the top ranked sites or bottom ranked sites. This value can be defined within each tile. To change the ranking display, select Top Sites or Bottom Sites from the drop-down list.

CHAPTER

5 REPORTS

The Reports menu provide standard reports that can be used to analyze performance.

Access this page by clicking **Reports** on the navigation bar on the left side of the portal.

The Reports submenu narrows the information displayed by report type. If the navigation bar is expanded, you can use the arrows to display or hide the submenu. If the navigation bar is collapsed, click the Reports icon a second time to display the Reports submenu:

- User Activity Log
- Contact Tracing
- Event Reports

User Activity Log

The User Activity Log displays the actions performed by users in the system. You can filter the display to limit the time range, operation type, user, and site.

Display Log Data

To view the User Activity Log:

1. Expand the **Reports** menu on the navigation bar on the left side of the portal.
2. Click **User Activity Log**.
3. To display all user events without applying any filters, click **SEE ALL DATA IN THE LAST 12 HOURS**.

4. To create a report with other parameters:
    a. Select the **Time Range** from the drop-down list. If you select "Custom," enter the **Start Time** and **End Time** on the Custom time range window then click **APPLY**.
    b. Select the **Operation Type** to filter by a specific activity.
    c. Select a **User** to view activity for only one user.
    d. Select a **Site** to display only actions associated with one site.
    e. Click **SHOW LOG**.

Searching User Activity Log

When log data is returned, a Search field is displayed. You can use this field to further filter the data.

When you start typing in the Search field, the system immediately applies the filter. The more characters you enter, the more the results will be filtered.

To remove the filter, clear the Search field.

Exporting User Activity Log Data

To export user log data to .csv:

1. With user activity displayed in the table, click **Export**.
2. The file is created in your Downloads folder.

Note: *All of the report's data will be exported, even if you have used the Search field to limit the displayed results.*

Contact Tracing

To maintain social distancing and worker safety, mobile devices can be set to trigger a proximity alert when enabled devices come closer together than a defined range. When devices are too close together, a warning will be displayed on each device so that users know to move apart.

Administrators can view the Contact Tracing report to review instances where proximity alerts were reported. The report can be filtered based on user names or devices, a range of time, and/or the duration of contact events.

The Contact Tracing Report is designed to work with Honeywell apps that can be installed on your devices.

Viewing Contact Tracing Reports

1. Expand the **Reports** menu on the navigation bar on the left side of the portal.
2. Click **Contact Tracing**.
3. Select one or more user names or devices from the **Name** drop-down list. Each user or device you select is displayed in the table.
4. Click **Timespan** to filter the report to a specified range of days to view.
   a. Select the date and time for the **Start Time**.
   b. Select the date and time for the **End Time**. The maximum is 90 days.
   c. Click **APPLY**.
5. Select the **Contact Duration** to limit the results to only incidents that lasted over a specified amount of time.
6. The report automatically updates based on the selected criteria.
7. Click the arrow next to a user's name to expand the display to show contacts for that user.

Event Reports

Event Reports provide information based on templates that have been created to return specific information gathered from event logs. For example, the "Check In - Check Out" report provides a record of when users checked a device out and when it was returned.

Viewing Event Reports

1. Expand the **Reports** menu on the navigation bar on the left side of the portal.
2. Click **Event Reports**.
3. Select a **Report** from the drop-down list.
4. You can select a **Timespan** from the drop-down list to display events within a specific range of time.
   - To view a time range other than a default in the list, select "Custom" then enter a **Start Time** and **End Time** and click **APPLY**.
5. You can select a **Template** from the drop-down list to filter the results based on predefined criteria for the selected Report. For example, if you are viewing the "Check In-Check Out" Report, you can select the "Damaged Returns" Template to only display assets that were marked as "Damaged" on check-in.

6. Click **SHOW REPORT**.

The system displays all events that meet the criteria selected for the report. The information is display only.

CHAPTER

6 SOFTWARE UPDATES

The Software Updates page lists available firmware, provisioning files and operating system updates.

Access the page by clicking **Software Updates** in the navigation bar on the left side of the portal.

Using this page, Device Administrators can view existing updates, upload new updates, view scheduled updates, and display update history. You can also access a web-based version of Enterprise Provisioner to generate configuration files.

The types of supported updates differ based on the type of device:

- Mobile Computers:
  - Application (.apk) files
  - Device configuration files
  - Provisioning files
  - Full and incremental operating system updates
  - SSClient updates
  - Honeywell software updates (e.g., Common ES)
- Scanners
  - Configuration files
  - Certificates
- Mobile Printers:
  - Device configuration (non-XML)
  - Fonts
  - Images
  - Certificates
- Industrial Printers:
  - Device Configuration (XML)

- Application files
- Fonts
- Images
- Certificates

Note: *Use the Software Updates page to select an update then choose the device(s) to schedule the update for. Use the Assets page to select device(s) then install updates on the devices (see page 31).*

Note: *Only users with Device Administrator privileges can access the Software Updates page. For more information, see Roles on page 65.*

The Software Updates page has three tabs: Honeywell Updates, My Software and History. Each tab can be filtered by clicking .

- The **Honeywell Updates** tab displays maintenance releases that are available from Honeywell. To view information on what is included in the release, click an update name. The row expands to show release notes for the selected item.
- The **My Software** tab displays all available software updates, including pending updates that are scheduled for a future date.
- The **Updates Status** tab displays the status of current, completed or expired updates.

Upload Software

Before software updates can be pushed to devices, an administrator must upload any files and create an update package. To upload software updates to Operational Intelligence so that they are available to be pushed to devices:

1. Click **Software Updates**.
2. Select the My Software tab.
3. Click **Upload Software.**
4. Select the **Device Type**.
5. Select a **File Type**. The File Type field will not be active until you select a device type. Available file types will differ based on the selected device type.
6. Select one or more **Device models**, if applicable. The list of available Device models depends on the selected Device Type.
7. Enter an **Update name**.

   If the File Type is an incremental update, the Update name must follow the naming convention of the incremental file update.
8. You may specify an optional **Version** number.

   If the File Type is an incremental update, the Version is required. Enter the Version in the format <current version>_<new version>. For example, if you are

applying an update from version 1.0 to version 2.0, enter the Version as "1.0_2.0".

9. You may enter the **Compatible version** number.

   If the File Type is an incremental update, the Compatible version is required. This value indicates the currently installed version that will be replaced if it is found on the device. If a version other than the Compatible version is found, the incremental update will not be performed on that device, and the status will be set to "Failed" with a comment that the file was not compatible.

10. Drag and drop the update file(s) into the window or click **BROWSE FILES** and select the desired file(s).
11. Click **UPLOAD**.
12. Refresh your browser window and the uploaded file will display in the list of available updates on the My Software tab.

Edit Files

After a software update file has been created, the file owner may edit the Device models, Update name, Version, and Compatible version fields. The Device Type and File Type cannot be modified.

Users can only edit files that they created. The Upload By column shows the name of the user who created the file.

To edit a file:

1. Click **Software Updates**.
2. Select the My Software tab.
3. Select a file in the table.
4. Click **Edit Configuration**.
5. Make any required changes.
6. Click **SAVE**.

Delete Files

After an update has been performed successfully, you can delete the file from the software list. This is useful, for example, if you have test files that you no longer need, which can be removed from the list.

Users can only delete files that they created. You cannot delete another user's files. If you try to delete a file that is not available for you to remove, the Delete button will not become active. The Upload By column shows the name of the user who created the file.

To delete a file:

1. Click **Software Updates**.
2. Select the My Software tab.
3. Select a file in the table.
4. Click **Delete File**.
5. A prompt asks if you want to delete the file. Click **YES**.

   A prompt indicates that the request was accepted, and the file is removed from the software list.

Update Software

Operational Intelligence allows you to push software updates to registered devices. Updates can be performed immediately or scheduled for a future time. You can also define a specific time range during which updates will be sent so that the system is not attempting to push software updates while devices are in use.

Software updates can be either packages that were created in Operational Intelligence or general maintenance releases that were pushed from Honeywell.

- The **My Software** tab displays a list of available updates that were added to Operational Intelligence using the Upload Software function.
- The **Honeywell Updates** tab lists maintenance releases that are available from Honeywell. Users cannot add updates on this tab. Updates will be added to this list as they are released by Honeywell.

Note: *If you are installing an Operational Intelligence software license, see License Manager on page 59.*

Update Software

To update software on your devices:

1. Click **Software Updates**.
2. Select the My Software tab or the Honeywell Updates tab.
3. Select an available update.
4. Click **Launch Update**.
5. The Configuration tab displays information about the update such as Version and File Size. The information will vary depending on the specific update. Click **NEXT**.
6. Select the devices that will be updated.

a. Select **By Site** to push the update to all devices assigned to a certain location. Choose the site name from the drop-down list. If the site has a hierarchy that includes child sites, you can include assets from the child sites by selecting the **Include children sites** check box. If this box is not selected, software updates will be applied to devices associated with the selected site but will not be applied to the assets at any child sites beneath it in the hierarchy.

b. Select **By Tags** to push the update to all devices with a specified tag assigned. Choose a group from the drop-down list. (See Tags on page 27 for more information.)

c. Select **From List** to choose individual assets from a list of available compatible devices. Check the box for each device to update or select the box in the header row to select all devices. You can use the Search field to limit results by Alias or Serial Number. Use the filter menu in the toolbar to filter the results by Type, Model, or Firmware version.

Note: *Depending on how many assets you have in the system, you might need to scroll to load additional assets before they can be selected in the* ***From List*** *table. See Selecting Assets on page 22 for information. Only 1000 assets can be updated at one time when using the From List option.*

7. Click **NEXT**.
8. Select when to perform the updates.
   a. Choose **Immediate** to push the update as soon as you submit it.
   b. To start the update at a later time, choose **Schedule**.
   Enter the **Date Range** during which the update will be pushed. **Starts** is the date that Operational Intelligence will begin pushing the update. **Ends** is the last date the system will try to push the update.
   You can also enter a **Time Range** so that the system will only attempt to push updates during a certain window of time, such as after work hours when devices are charging but not in use. Select the **From** and **To** times to define this window of time.
9. Click **Next**.
10. Review the information on the Confirmation screen and click **UPDATE**.

View Update Status

After an update has been performed, you can use the Update Status tab to view the status of the job. If multiple devices were updated in one job, the Update Status tab will indicate how many of the devices were updated successfully.

1. Click **Software Updates**.
2. Select the Updates Status tab.

   For each update, the tab displays the Status to indicate if the job has completed successfully or not. The Devices Updated column shows how many devices were updated successfully. For example, if the update was being applied to four devices and only one was updated successfully, the Devices Updated column will show “1/4.”

To view the status for each device that the update was pushed to, click the arrow to expand the Summary display in the table then click **View devices**.

Retry Updates

If not all of the devices were updated successfully, you can attempt to perform an update again.

1. Click **Software Updates**.
2. Select the Updates Status tab.
3. Expand the row for the update.
4. Click **Retry updates on failed devices**.
5. The Schedule Update window displays the list of failed devices. Click **NEXT**.
6. Select when to perform the update. You an choose **Immediately** or schedule a date and time for the update.
7. Click **NEXT**.
8. Review the information on the Confirmation screen and click **UPDATE**.

Cancel Update

After a software update has been initiated, you have the option to cancel the update. If a job is scheduled for a future time, the update will be canceled for all devices. If the job has started, it will only be canceled for devices on which the update has not been initiated, such as devices that are offline. Once the process has been initiated on a device, it cannot be canceled.

To cancel an update:

1. Click **Software Updates**.
2. Select the Updates Status tab.
3. Select the job to cancel.
4. Click **Cancel update**.
5. A prompt asks if you want to cancel the update. Click **YES**.

   The status of the job is updated to “Canceled.”

License Manager

Use the License Manager to install licenses on selected assets. The licenses must be purchased prior to installation.

Installing a license involves three steps:

1. Import license information.
2. Create a license bundle.
3. Install bundle on selected devices.

Prerequisites

The following prerequisites must be met to work with License Manager and install licenses:

- The user acting as License Administrator must have Device Administrator privileges. See Roles for more information.
- You must have a License Activation ID. The Activation ID is issued when a new purchase order is created. The Activation ID is sent by email along with all necessary details.

Import Licenses

Follow these steps to import software licenses.

1. Select **Software Updates** in the navigation menu.
2. On the Software Updates screen, click **License Manager**.

   License Manager opens in a new tab.
3. Click **Import Licenses**.

   The Import Licenses window opens.
4. Enter the **Activation ID** you received by email.
5. Enter the **Number of Licenses**. This must be less than or equal to the number of licenses available. The system validates against the total number of purchased licenses associated with the Activation ID.
6. Select the **Site** where the licenses will be installed.
7. Click **IMPORT**.

   A message indicates if the license was imported successfully or not. The import status will also be displayed on the Alerts menu. Click the +1 icon in License Manager to view alerts. If the license was imported successfully, the license information will be displayed on the Licenses tab in License Manager.

Install Licenses

After a license is imported, it can be pushed to a device for installation. The license can be installed immediately, scheduled to be installed at a specified date and time, or saved for future installation.

1. With License Manager open, select the Licenses tab.
2. Select one or more licenses from the available list.

   If you select more than one license, they must all belong to the same site.
3. Click **Install**.

   The License Installer window opens.
4. Verify that the correct software is listed then click **NEXT**.
5. On the Devices tab, enter a **Bundle Name** and select the devices where the license will be installed. Click **NEXT**.
6. Select an option on the Schedule tab to indicate when License Manager will attempt to push the bundle to the selected devices.
   - **Immediate** - License Manager will immediately attempt to push the bundle to the selected devices.
   - **Schedule** - License Manager will push the bundle at a specified date and time. For example, installation can be scheduled to occur during hours when the device will not be in use. Select the **Time Zone**. Select the **Starts** and **Ends** dates to define a range of dates when License Manager will try to push the bundle to the devices. Use the **From** and **To** drop-down lists to define the time range when the bundle can be pushed on the selected dates.
   - **Save bundle for later use** - This option will create a bundle that can be pushed to mobile devices, but License Manager will not automatically push it. The bundle will be available for selection on the License Bundles tab.
7. Click **NEXT**.
8. Review the information on the Confirmation screen and click **SAVE**.

   A confirmation message indicates that the bundle was created. The bundle will be displayed on the License Bundles tab.

Install Saved License Bundle

After a software bundle has been created with the “Save bundle for later use” option, it becomes available to be pushed to selected devices. You can also update the devices and schedule information that were selected when you created the bundle.

1. With License Manager open, select the License Bundles tab.
2. Select a bundle in the list.
3. Select an option:

- **Edit** - Modify the contents of a bundle that has been created. The Edit option allows you to add devices or modify the schedule information. Devices that were previously selected cannot be removed.
- **Schedule** - Modify the scheduled date and time for when the bundle will be pushed.
- **Install Now** - Push the selected bundle to the assigned devices without making any changes.

4. Review your changes on the Confirmation screen then click **SAVE**.

View Status

To view the status of licenses that have been pushed to mobile devices, select Software Updates from the main Operational Intelligence menu then select the Update Status tab. (Note that the left-hand navigation menu is not available on the License Manager tab.) You can use this information to determine if updates have been pushed successfully or need to be retried. See View Update Status on page 57 for more information.

Enterprise Provisioner

Enterprise Provisioner is an application used to configure Honeywell Android devices. Navigate to **Software Updates** then click **Enterprise Provisioner** to access a web-based version. A desktop version of Enterprise Provisioner can also be downloaded from the Honeywell software download website at https://hsmftp.honeywell.com.

Enterprise Provisioner allows you to create configuration and provisioning files that you can then upload to Operational Intelligence Performance Management using the Software Updates page (see Upload Software on page 54). When you access Enterprise Provisioner from within Operational Intelligence, files you save are automatically added to the list of available software in Operational Intelligence.

For more information, see the *Enterprise Provisioner User Guide*, which is accessible from the Enterprise Provisioner **Help** tab.

Note: *If you are not a licensed Operational Intelligence user, you can still have access to the cloud-based version of Enterprise Provisioner to configure your Honeywell devices. Users who attempt to log into Operational Intelligence but do not have the required permissions will be redirected to a site that provides access to Enterprise Provisioner - Lite Version. Click the **Visit** link to access Enterprise Provisioner.*

CHAPTER

7 ADMIN

The Admin menu allows you to manage users and set up sites. Access the Admin menu by clicking **Admin** on the navigation bar on the left side of the portal. Functions on the Admin menu are limited by the assigned user role.

User Management

Access the User Management page by clicking **Admin** then **User Management** in the navigation bar. A list of all current users will display. On the Users tab, you can add, edit, or delete users in the system. When you add a user, you will assign one or more roles, which define what each user can do within Operational Intelligence. See Rolesfor more information.

Users

Use the Search field to look up a user by name.

Creating Users

When you add a new user, the user can be associated with either an email address or an employee ID number. Users who are associated with an employee ID can be entered individually or added in bulk by using a spreadsheet.

To enter an individual user:

1. Click **Admin** then **User Management**.
2. Click **Add Users**.
3. Select a tab based on how the user will be identified in the system: **By Email** or **By ID**.
4. Enter the new user's **First Name**, **Middle Name** (optional), **Last Name**, and **Login Email** address or **EmployeeID**.

5. Using the drop-down lists, select an **Organization** and a **Site**.
6. If the user is being entered By Email, select a user role. For more information about available roles, click the (i) icon.
7. Click **SUBMIT**.

To enter users By ID in bulk:

1. Click **Admin** then **User Management**.
2. Click **Add Users**.
3. Select **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. 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**.

Editing Users

To modifying an existing user's settings:

1. Click **Admin** then **User Management**.
2. Scroll down the list of users and click on the desired name, then click **Edit User**.

   You can use the Search field to look up a desired user or filter the list.
3. Change the information as needed, then click **Submit**.

Deleting Users

To remove a user:

1. Click **Admin** then **User Management**.
2. Scroll down the list of users and click on the desired name, then click .

   Or

Click then use the Search field to look up the desired user. Click on the user's name to select it.

3. Click **Delete**.

Roles

All Operational Intelligence users are assigned a role based on the permissions each person requires:

- An **Administrator** can create and manage users, sites, and custom dashboards.
- A **Device Administrator** can access devices remotely or trigger remote commands on a device, as well as create and manage users, sites, and custom dashboards. This role can only be added by a Honeywell Professional Services user.
- An **Organization Administrator** can create and manage roles.
- An **Installer** is responsible for installing and configuring devices and can enroll new devices.
- A **User** has limited privileges and has view-only access to the dashboard and devices pages.
- A **Device User** is assigned one or more devices to use in performing their job.
- Additional custom roles can be created by the Organization Admin as needed.

Site Management

Note: *Parent-level organizations are set up by Honeywell. If you need additional organizations, please contact Honeywell Support.*

The Site Management page allows you to view, create and edit sites, buildings, floors and zones as part of the OI Indoor Positioning System (IPS). Using the IPS, Operational Intelligence Performance Management can track devices to a 10mx10m zone. However, those zones must first be set up, or "fingerprinted", as per the *Operational Intelligence Indoor Positioning Service for Mobile Computers Implementation Guide*.

To access this page, click **Admin** then **Site Management** in the navigation bar.

The Site Information tab displays the site hierarchy and address. address, site hierarchy, and user permissions. Use the arrows to the left of a site name to expand or collapse that site.

Site Management Tab	Description
Site Information	Displays the site's hierarchy and address.
Permissions	Displays the users assigned to certain roles.

Site Management Tab	Description
Access Points	Set up and maintain access points for use with indoor positioning.
Maintenance	Allows users to set alerts for device cleaning
Network Ranges	Defines a range of IP addresses for a site.
People Counter	Sets a limit for the number of people allowed in a site and allows users to track entry and exit

Site Hierarchy

The general hierarchy for a location will be Organization > Site. You can also have sub-sites (e.g., Organization > Site > Site > Site). If you are enabling indoor positioning, the hierarchy will include buildings, floor and zones.

Site Management Icon	Description
	Site
	Building
	Floor
	Zone

Adding Locations

When you select an organization, site, building or floor in the hierarchy on the Site Management page, icons will display to the right of the location name to allow you to create the next level down. For example, if you click on the organization, icons for adding a new site or a new building will display. If you click on a building, an icon to add a new floor will display. If you click on a floor, an icon to add a new zone will display.

Buildings, floors and zones are only required if you are enabling indoor positioning. They must be set up in the following order:

1. Site
2. Building
3. Floor
4. Zone

For more information about indoor locationing, see the *Operational Intelligence Indoor Positioning Service for Mobile Computers Implementation Guide*.

Adding a Site

1. Click **Admin** then **Site Management**.
2. Click on the organization name to select it.
3. Click to the right of the organization name.
4. Enter the new site's name.
5. Enter the site address.
6. Click **CREATE**.

Note: *Refresh your browser before adding devices to the new site.*

Adding a Building

1. Click **Admin** then **Site Management**.
2. If the site hierarchy is collapsed, expand the levels using the arrows on the left.
3. Select the site you want to add a building to.
4. Click the building icon to the right of the site name.
5. Enter the new building's name.
6. Enter the building's full address.
7. Click **CREATE**.

Adding a Floor

1. Click **Admin** then **Site Management**.
2. If the site hierarchy is collapsed, expand the levels using the arrows on the left.
3. Select the building you want to add a floor to.
4. Click the floor icon to the right of the building name.
5. Enter the new floor's name.
6. Click **CREATE**.

Zones

Setting up zones is only required if you have chosen to use the Operational Intelligence Indoor Positioning Service.

Site Preparation

Before setting up zones in the Operational Intelligence Performance Management portal, you should first visit the site to determine how best to arrange the zones on each floor.

Divide each floor into 10m x 10m zones and create a zone map. Zones can be equidistant or functional (e.g., by department).

Adding a Zone

Once the site, building and floors have been set up in the portal, you can begin to enter the zones you identified in your site preparation:

1. Click **Admin** then **Site Management**.
2. If the site hierarchy is collapsed, expand the levels using the arrows on the left.
3. Select the floor you want to add a zone to.
4. Click the zone icon to the right of the floor name.
5. Enter the new zone's name.
6. Click **CREATE**.

Editing Sites, Buildings, Floors and Zones

1. Click **Admin** then **Site Management**.
2. Select a site, building, floor or zone in the hierarchy panel on the left.
3. Click .
4. Make the necessary changes.
5. Click **SAVE**.

Site Information

Use the Site Information tab to enter and maintain address information for the site.

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Site Information** tab.
4. Click **Edit**.
5. Update address field as required.
6. Click **Save**.

Permissions

The Permissions tab displays all users assigned to specified roles for a selected site.

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Permissions** tab.

All information is display only. See Roles for information on assigning roles to users.

Access Points

If you have chosen to use the Access Point Solution for indoor positioning, you will use this tab to set up and maintain your access points.

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Access Points** Tab.

Adding Access Points

You can add access points using two methods: enter each point individually or upload a file.

Creating Individual Access Points

To enter access points one at a time:

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Access Points** tab.
4. Click **Create Access Point**.
5. Enter the following information. All fields are mandatory.

   Name - the location of the access point (e.g., department or room)

   SSID - the name of the network to which the access point is connected

   BSSID - the BSSID of the access point

   Building - the building where the access point is located

   Floor - the floor on which the access point is located
6. Click **CREATE**.

Uploading Access Points

You can also bulk add access points by uploading a .csv file. You can first download the existing file, even if no access points are set up yet, and use that as a template for your upload file. Use this same procedure to bulk edit existing access points by downloading the current list, modifying it, then uploading it.

Warning: Uploading a new file will overwrite existing access point data.

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Access Points** tab.
4. Click **Create Access Point**.
5. Click **Export Access Points**.
6. Select the location where you want to save the .csv file.
7. Click **Save**.
8. Open the .csv file. You will see the first row is pre-populated with column headings.
9. Beneath the headings, enter a row for each access point to be added. All fields are mandatory.

Note: *For the Access Point solution, Building and Floor do not need to be set up through the Site Management page as required by the IPS solution.*

10. Save the .csv file.
11. Return to the Operational Intelligence Performance Management portal.
12. Go to the **Access Points** tab of the Site Management page.
13. Click **Upload Access Points**.
14. Drag and drop the .csv file into the window or click BROWSE FILES and select the desired file.
15. Click **SUBMIT**.

Operational Intelligence Performance Management will validate the data in the file. If the upload is completed successfully, a confirmation message will display. If any fields are missing, an error message will display.

Maintenance

Use the Maintenance tab to configure and establish cleaning procedures to support safe work environments.

Administrators can create alerts, which will be triggered to remind users to clean their devices. Users will receive an alert that the device is scheduled to be cleaned and will have to acknowledge that the required cleaning has been performed. On a mobile device, the user will tap a button on the screen to acknowledge the alert. For a device that does not have a screen, such as a printer, the user will receive an alert indicating that the device must be sanitized. The user will then need to select the device under Assets and verify that maintenance has been performed. (See Device Maintenance.)

The system will keep a record in the Events log of which users have had a device and whether the required cleaning has been performed.

Creating a Rule

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Maintenance** tab.
4. Click **Create Rule**.
5. The Create Rule window opens.
   a. Enter a **Name** for the rule.
   b. Select to **Apply to Checked out devices only**. Checking this box will apply the rule only to devices that are checked out to a user. When this is not selected, alerts will be sent to all devices.
   c. Enter the **Date** and time to begin sending the alert.
   d. To make the alert occur on multiple days, check **Repeat**.
      - Select the **Time Zone** of the site.
      - In the **Repeat** drop-down list, select the frequency to send the alert.
      - Select the **Days** to send the alert on.
      - Select the **From Hour** and **To Hour** to define the hours during which the alert will be sent.
6. Click **Save**.

The rule is created and will apply to all devices in the selected site.

Viewing Rule Details

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Maintenance** tab.
4. Click **View**.

   The View Rule windows shows the details for the rule. All fields are display-only.

Deleting a Rule

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Maintenance** tab.
4. Click **Delete**.

Network Ranges

Use Network Ranges to define IP addresses that set the boundaries for a location. Network ranges are used with the Devices Out of Range feature. Network ranges can be added manually or uploaded in a .csv file.

Creating a Network Range

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Network Ranges** tab.
4. Click **Add Network Range**.
5. Enter the **Start IP Address**.
6. Enter the **End IP Address**.
7. Enter a **Description**.
8. Click **Create.**

Uploading a Network Range

You can also bulk add one or more network ranges by uploading a csv file. You can first download the existing file, even if no network ranges are set up yet, and use that as a template for your upload file. Use this same procedure to bulk edit existing network ranges by downloading the current list, modifying it, then uploading it.

Warning: Uploading a new file will overwrite existing access point data.

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **Network ranges** tab.
4. Click **Export Network Ranges**.

5. Select the location where you want to save the .csv file.
6. Click **Save**.
7. Open the .csv file. You will see the first row is pre-populated with column headings.
8. Beneath the headings, enter a row for each access point to be added. All fields are mandatory.
9. Save the .csv file.
10. Return to the Operational Intelligence Performance Management portal.
11. Go to the **Network ranges** tab of the Site Management page.
12. Click **Upload Network Ranges**.
13. Drag and drop the .csv file into the window or click BROWSE FILES and select the desired file.
14. Click **SUBMIT**.

Operational Intelligence Performance Management will validate the data in the file. If the upload is completed successfully, a confirmation message will display. If any fields are missing, an error message will display.

People Counter

People Counter provides a way to track the number of people at a site, for example, customers in a store. The Admin user sets a maximum number of people who are allowed in the site at one time, then one or more individuals using the Operational Intelligence People Counter function on mobile devices can maintain a count as people enter or exit the site. As the users indicate that people are entering or exiting the site, the count is maintained in real time, even with multiple entry or exit points being monitored by users on separate devices. This lets users know whether more people can be allowed to enter or if the defined capacity has been reached.

Setting Capacity

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **People Counter** tab.
4. Enter a value for **Limit number of people in site**.
5. Click **Save**.

Reset Count to Zero

1. Click **Admin** then **Site Management.**
2. Select a site.
3. Click the **People Counter** tab.
4. Click **RESET NOW**.
5. The number of **Current people in site** is set to zero, and the count is updated on the People Counter tool.

Assets Configuration

Use the Assets Configuration function to set up Asset Models that will be used when adding Non-Connected assets. Each Asset Model consists of a Manufacturer, an Asset Type, and information for the specific model. Manufacturers and Asset Types can be used in any combination to create as many Asset Models as you require.

After Asset Models are created, they are added to the drop-down list in the first column of the “Operational Intelligence Import Non-IoT Template.xlsx” file, which can be downloaded and used to import Non-Connected assets. See Adding Non-Connected Assets for more information.

Add Manufacturer

1. Click **Admin** then **Assets Configuration.**
2. Click **Add Manufacturer**.
3. Enter the **Manufacturer** name.
4. You may enter a **Company Name**.
5. You may enter a **Contact Email**.
6. You may enter an **Address**.
7. You may select the **Country**.
8. Click **SAVE**.

Add Asset Type

1. Click **Admin** then **Assets Configuration.**
2. Click **Add Asset Type**.
3. Enter the **Type**.

4. Click **SAVE**.

Add Asset Model

1. Click **Admin** then **Assets Configuration.**
2. Click **Add Asset Model**.
3. Enter the **Model Name**.
4. Select a **Manufacturer** from the drop-down list.
5. Select an **Asset Type** from the drop-down list.
6. You may enter a **Description** of the asset model.
7. Click **SAVE**.

Devices Out of Range

Use the Devices Out of Range function to identify assets that have been moved from their assigned Network Ranges and relocate them to a new site if required. This feature allows you to quickly reassign devices that have been physically moved from one site to another. For example, if one site has been closed and all of its assets were sent to another site, the system will detect that these devices are out of their assigned network range and suggest that they be reassigned to the network range for the site where they are currently located. You can then reassign all of the devices at once rather than dealing with each device individually.

Note: *A network range must be assigned for the site to use this function.*

Access the Devices Out of Range page by clicking **Admin** then **Devices Out of Range** in the navigation bar.

Reassign Devices

To reassign devices that are out of range:

1. Click **Admin** then **Devices Out of Range**.

   For each device found to be out of range, the table displays the Recommended Site. This represents the Network Range that the device is currently located in.
2. You can filter the devices that are displayed by selecting the Filter menu and entering one or more values or by entering characters in the Search field. The system automatically updates the list to only display devices containing the search string.
3. Select each device to reassign or check the box in the heading row to select all devices.

4. Click **Update Site**.
5. The Update Site window displays a list of devices. Click **UPDATE**.

All selected devices are reassigned to the Recommended Site.

Device Administration

The Device Administration menu provides access to tools that can be used to automate device maintenance functions.

Rules Engine

Use the Rules Engine to automatically push software updates to devices when specific events occur. Rules are configured at the site level to ensure that when a device becomes associated with that site, it will be updated with the required software.

Only users with a role of Device Administrator have access to the Rules Engine screen.

After you create a rule, you can determine if it has been triggered and whether it completed successfully by looking on the Software Updates screen. See View Update Status for more information.

Create a Rule

1. In the navigation bar, expand the **Device Administration** menu then select **Rules Engine**.
2. on the Rules Engine screen, click then select **New Rule**.
3. Define Rule Settings.
   a. Enter a **Rule Name**.
   b. Select one or more sites that the rule applies to from the drop-down list. You can select multiple sites from the drop-down list. To include child sites for the selected site, select the check box.
   c. Click **NEXT**.
4. Define the Rule Conditions.
   a. Choose a value from the **Select the Event** drop-down box.

When you select the event that will trigger the rule, the value in the drop-down list is called “Device moved.” This option includes five triggering events that can be sent to Operational Intelligence from a device. If any of these events occur, the rule will be triggered:

- Device onboarded by reading a barcode

- Device onboarded using XML
- Device onboarded using bulk provisioning
- The device is manually assigned to a new site on the Assets page
- A new site is recommended for the device because it has moved to a new network range (see Devices Out of Range for more information)

b. Select the **Device Type**.

c. You can also select one or more options from the **Device Model** drop-down list. The options in this list are filtered based on the selected Device Type. For example, if the Device Type is "Printer," only printer models will be available to select.

Note: *If you do not choose any Device Models, Operational Intelligence will try to push the update to all models of the selected device type. Selecting values for Device Model ensures that the update is only pushed to devices that it applies to. For example, if you have two models of mobile devices, they might each require a different SSClient. You should create a separate rule for each model.*

d. Click **NEXT**.

5. Define the rule Actions.

a. Select the action that will be executed from the drop-down list. Currently, the only option is "Update software."

b. Under **Choose software for the update**, click **Add Software**.
The Software Selection window opens.

c. Choose the software or bundles to apply in the update. You can choose from Honeywell Updates or select the My Software tab to choose items that you have uploaded.
Only software and bundles that apply to the Device Type and Model(s) selected on the previous screen will be available to choose.

d. To select when the update will be applied, click **Change Schedule**. You can choose to trigger the rule when a device event occurs or to only trigger the rule if the device event occurs during a scheduled time period.

- If you select **On device event**, the rule will be triggered when one of the five events listed above occurs. Enter the **Retry Duration** and select the unit (Hours, Days, or Weeks) from the drop-down list. The Retry Duration tells the system how long to keep trying to push the update. If the triggering events do not occur during that amount of time, the system will stop trying to push the update.
- Select **Schedule** to only apply the rule during a specified time period. For example, if you do not want to push an update while a device will be in use, you an schedule the update to occur outside of normal working hours. Select the **Timezone**, **Start Time**, **End Time**, and and enter **Retry for (days)**. If the triggering events do not occur within that number of days, the system will stop trying to push the update.

Note: *The retry duration applies to each instance of a rule being triggered and restarts when the rule is triggered for another device. For example, you can create Rule A with a retry duration of two days. When a triggering event is received from Device 1, Rule A will try to push the update to Device 1 for two days. If a new triggering event is received from Device 2, Rule A will try to push the update to Device 2 for two days starting at the time the event was received.*

- Click **NEXT**.

e. Click **REVIEW**.

6. Confirm the update.
   a. The Confirmation screen displays the Rule Name, Affected Sites, Conditions required for the update to be pushed, and Actions that will occur when a triggering event is received.
   b. Verify that the information is correct, then click **SUBMIT**.
7. The new rule will be displayed in the Rules table.

Activate or Deactivate a Rule

When a rule is created, it is set to Activated by default. The user who created the rule can choose to activate or deactivate a rule. Users can only change the activation status of rules that they have created.

As long as the rule is Activated, it will attempt to push the update to the selected device types whenever a triggering event is received.

1. In the navigation bar, expand the **Device Administration** menu then select **Rules Engine**.
2. On the Rules Engine screen, select the slider in the ACTIVATE column to turn the rule on or off. If you do not have permissions for a rule, the system will indicate that you cannot change the status.

View Rule Details

Users with access to the Rules Engine screen can view the details of a rule even if they did not create it. The Details screen displays the Affected Sites, Conditions, and Actions defined for the rule.

1. In the navigation bar, expand the **Device Administration** menu then select **Rules Engine**.
2. Mouse over a rule in the table and click the icon.

   The details of the rule are displayed. All information is display-only.
3. Click **BACK** to return to the Rules Engine screen.

Delete a Rule

If a rule is no longer required it can be deleted. Only the user who created the rule can delete it.

1. In the navigation bar, expand the **Device Administration** menu then select **Rules Engine**.
2. Mouse over a rule in the table and click the icon.

Tools

The Tools menu provides access to features that an administrator can use to maintain capacity limits and analyze access point information.

Access this page by clicking **Tools** on the navigation bar on the left side of the portal

- People Counter tracks the number of individuals going in and out of a site to track capacity.
- Access Point Insights provides statistics on usage for access points at a site.

People Counter

Use People Counter to track the number of individuals going in and out of a site, such as a retail location. The capacity limit for the site is set in the Site Management menu on the People Counter tab.

Count People at a Site

1. Click **Tools** then **People Counter**.
2. Click **In** to add a person to the site. Click **Out** to indicate that a person has left.

   Each time a button is clicked, the Remaining Capacity is automatically updated.

Use the People Counter tab in Site Management to reset the counter to zero.

Access Point Insights

Use the Access Point Insights screen to view information on how many devices have been associated with an access point, the average time the devices were associated with the access point, and the average signal strength of the access point.

Signal strength is always displayed as a color indicating the signal strength for the access point. The key for the colors is displayed at the bottom of the table. To view the signal strength in average dB, move your mouse over a column

Note: *Access point information is reported every 15 minutes, so the information displayed in this table represents a snapshot captured at regular intervals.*

View Access Point Data

You can select whether to view devices, time, or both.

1. Click **Tools** then **Access Point Insights**.
2. Select a **Site** from the drop-down list.
3. Select the information to view. You can view:
   - **Devices reporting on each access point** - the average number of devices associated with the access point.
   - **Average time spent on access point** - the average amount of time devices were associated with the access point.
   - **Both** - Displays both reports in the form <devices>/<time>.
4. Select the **Date Range**. You can a range of up to five days at a time.

   The access point insights for the selected date range are displayed.
5. To filter the display based on the access point ID, type the access point in the Search box. The results are automatically filtered as you type.

Configure Signal Strength

Signal strength is defined as Excellent, Good, or Poor based on a range of -120 to 1 dBm. You can configure the range that defines each rating.

1. With the Access Point Insights screen displayed, click ⋮ then select **Set signal strength ranges**.
2. Use the slider to define the range for Good Signal Strength. The Poor and Excellent signal strength ranges are automatically updated.
3. Click **APPLY** to update the settings.

Export Access Point Insights

You can export the information in the Access Point Insights table to a .csv file.

1. Click **Export**.
2. Cick **CSV**.

   The CSV file is saved to your default downloads location.

CHAPTER

8 SECURITY

Operational Intelligence Security Overview

Disclaimer

This is an overview of cybersecurity and data privacy measures that have been put in place as part of the Honeywell Operational Intelligence offering and is not a legally binding cybersecurity or data privacy agreement. Honeywell may update this overview from time to time, with or without notice. Customers are encouraged to frequently check honeywellaid.com for the latest version of this user guide.

Data Collection, Privacy and Use

The data collected by Honeywell Operational Intelligence does not contain any personally identifiable information about the users of connected devices. Telemetry and diagnostic data are used to construct meaningful reports and analytics for our customers without using any data that could be categorized as Personally Identifiable Information under such regulatory guidelines as CCPA or GDPR. The collected data and the data processing results are always under our customers' control and ownership.

Secured Edge-Cloud Communication

Operational Intelligence-enabled devices communicate with the back-end platform using only encrypted protocols with industry-leading ciphers for encryption. The secured channel ensures that data is protected and cannot be accessed by unauthorized entities as it travels from the devices to the Operational Intelligence platform.

Secured Operational Intelligence Performance Management Portal

Operational Intelligence insights, including dashboards and reports, are delivered via the Operational Intelligence web portal, which is secured using a defense-in-depth methodology. This means we are using multiple layers of defense from active monitoring, encryption using the highest levels of ciphers for data-in-motion, in processing, as well as data-at-rest. This ensures a secure channel for data exchange between the Honeywell cloud and the user's browser. As Honeywell Operational Intelligence segregates tenant data logically, each customer can view and interact with only their own telemetry and diagnostic data and reports. In other words, dashboards and reports are private to every customer.

Honeywell has a documented security incident response plan, a summary of which can be provided upon request (subject to confidentiality requirements).

Cloud Provider

Honeywell Operational Intelligence leverages the world's leading cloud infrastructures, such as Microsoft® Azure®, that provide best-in-class physical and cyber security services. Honeywell continuously endeavors to not only comply with the best cybersecurity practices recommended by our providers but to meet or exceed those industry-leading practices by incorporating cybersecurity measures in the very design of the solution and keeping those measures current with changes in the cybersecurity landscape throughout the offering life cycle. The entire Operational Intelligence platform including customer-owned data is hosted within the United States, and we will comply with any additional local regulatory requirements during the term of our contractual commitments.

All stored data is encrypted at the tenant level using keys that are unique to each organization. All encryption keys are securely stored in a vault solution separate from encrypted data. All customer data is segmented from the Honeywell network and kept in its own production instance. There is no interaction with development systems or infrastructure, which are also kept separate.

Security Considerations for Devices Connecting to Honeywell Operational Intelligence

One of the common weaknesses of system management as reported by Open Web Application Security Project (OWASP) is "not keeping software up to date." It is critical to install the latest patches and software versions on all operating systems that support or connect to components of Honeywell Operational Intelligence.

Note that Honeywell Operational Intelligence may require specific versions and/or updates of third-party software. Refer to documentation and release notes.

Honeywell recommends that you establish a level of privilege for all external accounts and enforce a strong password policy.

Honeywell Operational Intelligence only requires outbound encrypted connections to our cloud management portal via a TLS connection on port 443. It is not necessary to make any changes to your firewalls or other network security infrastructure to allow for inbound connections.

Honeywell encourages its customers to keep their Operational Intelligence-enabled devices up to date. For the Operational Intelligence Performance Management portal, Honeywell requires an OEM-supported operating system with a major web browser.

APPENDIX

A APP CONFIGURATION

Overview

Honeywell provides applications that can be used on mobile devices to improve user safety and efficiency. This section provides information on how to use Operational Intelligence to configure and install apps. The devices must be registered with Operational Intelligence.

Installing an app generally has three steps:

1. Configure files using Enterprise Provisioner, which can be opened from within Operational Intelligence, or another editor such as EZConfig.
2. Upload provisioned files to cloud services using Operational Intelligence. See Upload Software for additional information.
3. Use Operational Intelligence to push the software to the mobile devices. See Update Software for more information.

This guide provides an overview of how to set up applications, including configuration that can be done from within Operational Intelligence Performance Management. Refer to the user guide for the app for additional information on usage and configuration. For configuration of a specific device, refer to the user guide for that device.

Social Distancing App

The Social Distancing app is a solution based on Bluetooth technology augmented with Operational Intelligence for contact tracing of employees. The app can alert the employees when they are near to each other in their working environment and provides alerts and reports that can be viewed in the Contact Tracing report or on the Events tab for the device.

Components

The Social Distancing app requires the installation of three components.

- Beacon Transmitter Service - Beacon Transmitter service allows the device to broadcast beacons at a one second interval. The beacon broadcasts the model number and serial number of the device. This is a background service which runs on all the devices. By default this service is turned off. To enable Beacon Transmitter Service, the Start option must be enabled in FMD.xml.
- Social Distancing Service - Social distancing service enables Honeywell Mobility Edge devices to scan for beacons around the device. This service does the tracking and distance measurement of the beacons in the area. If users are closer than the proximity distance limit, an alert is provided.
- Operational Intelligence Rules Engine - This service connects the device to Operational Intelligence and provides a way to configure the alerts by user.

Additional configuration must be performed in the following XML files:

- FMD.xml
- DeviceConfig.xml
- RulesEngine.xml

After the files are configured, use Enterprise Provisioner to create a bundle that can be pushed to mobile devices.

Upload Steps

This section provides an overview of the steps required to set up and deliver the application files to your mobile devices. The Social Distancing app requires the following files:

- OperationalIntelligenceRulesEngine.apk
- BeaconTransmitter.apk
- FMD.xml
- DeviceConfig.xml
- RulesEngine.xml

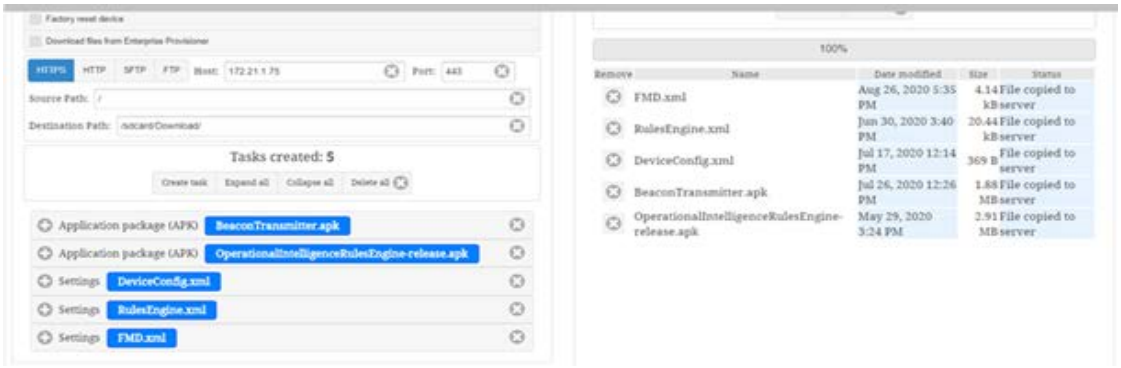
To prepare and upload the files:

1. Use Software Update to upload BeaconTransmitter.apk, and OperationalIntelligenceRulesEngine.apk to cloud services. On the Upload Asset screen, select the **File Type** as “Application (apk file).”
2. Configure the following option then upload FMD.xml.
    - FMDTransmitter – Turn on the option for **Start or Stop Service**.
3. Configure and upload RulesEngine.xml.
    - Configuration of RulesEngine.xml depends on the functionality you want for the Social Distancing app. See the *Social Distancing App User Guide* for information on configurable settings in RulesEngine.xml.
4. Configure the following option then upload DeviceConfig.xml.

- Bluetooth - Set to **Enable**.

5. Use Enterprise Provisioner to create a provisioner bundle. Arrange the tasks in this order:
   - BeaconTransmitter.apk
   - OperationalIntelligenceRulesEngine-release.apk
   - DeviceConfig.xml
   - RulesEngine.xml
   - FMD.xml

Your Enterprise Provisioner screen will look similar to this:



Note: *When you save the provisioning bundle in Enterprise Provisioner, it will automatically be added to the available software list to upload in Operational Intelligence.*

6. Use Software Updates to push the provisioner bundle to mobile devices as required.
7. See the *Social Distancing App User Guide* for instructions on how to start the service.

Honeywell
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com

HOI-PM-EN-UG-01 Rev G
06/21