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.hsmcontactsupport.com.

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.

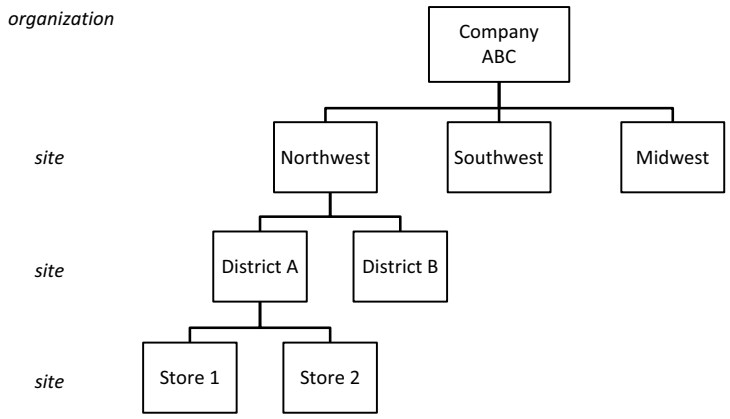
For information about Operational Intelligence licensing, please contact Honeywell Sales.

Requirements

Operational Intelligence Performance Management requires Google Chrome™ as 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 42.

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 42*)
3. Add users (see page 39)
4. Optional: enable locationing and indoor tracking of mobile computers (see next section Indoor Locationing)
5. Add devices (see Mobile Computers on page 20 and Scanners and Printers on page 22)

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 46.

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 13). Click the Assets icon a second time to display the Assets submenu:  Mobile Computers (see page 20)  Scanners (see page 22)  Printers (see page 22)
	Displays the Software Updates page (see page 35).
	Displays or hides the Admin submenu (see page 39):  User Management (see page 39)  Site Management (see page 42)  Access Points (see page 46)  Dashboard Views (see page 50)

Note: *Your ability to view and modify data in Operational Intelligence is determined by your assigned user role (see User Management on page 39).*

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.
	Click the Help icon to access the following: **Help** - Operational Intelligence user documentation **Legal** - patents, terms and conditions, privacy, OSS (software) agreement, and cookies **About** - link to more information about Operational Intelligence

Toolbar Element	Description
(your initial)	Click your initial to access the User Profile menu, including: **Settings** - change the appearance of the portal, including the language **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 6 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 17).

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 or language.
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

To receive an email whenever an alert is generated:

1. Click **Preferences** in the User Profile menu.
2. Click **Email Notifications**.
3. Toggle email notifications on.
4. Select the alerts you wish to be notified about via email.

Notification Report

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 name for the new report.
5. Select a site from the drop-down list or type a site name.
6. Select a report frequency.
7. If you chose weekly or monthly, select a day on which the report should be generated.
8. Specify a start date and time.
9. Click **SUBMIT**.

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 cards for the site selected at the top of the page. Each card provides data related to system and asset usage. The Dashboard also displays alerts that have been received.

Use the arrows to expand or collapse a section.

From other pages, you can navigate to this page by selecting **Dashboards** on the navigation bar on the left side of the portal.

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 same 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 cards for the entire organization, while selecting "/ Company ABC / Northwest / District A / Store 1" would display cards for that single site only. For more information about site hierarchy, see page 43.

Types of Cards

The cards 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, cards 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

Display Options

The ⋮ icon in the upper right corner of a card indicates that the card can be customized. Click the icon to display the options.

To clear any previous change and return to the default value, click ⋮ then click **Reset**.

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.

Additional Details

If additional detail is available beyond what is displayed on the card, the mouse pointer will change from  to  when you hover above the caption at the bottom of the card. Click on the caption and a data table will display in a new window.

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, use the arrows beside a column heading.

Exporting

To export data to a .csv file:

1. Click on the caption at the bottom of a card. If export is available for that card, a table will display.
2. Click  **Export**.
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.*

Customize Dashboard View

Users can customize the dashboard to display only the sections and cards that they are interested in. These settings apply to the logged in user only and do not change the default view for other users.

To customize your view:

1. Select **Dashboards** in the navigation bar.
2. Click **Customize My View**.
3. On the Customize Dashboard Display window, check or uncheck the sections and cards that you want displayed. Use the arrows to expand or collapse a section.
4. Click **Submit** to update the dashboard display.
5. To reset your display to the default settings, open the Customize Dashboard Display window and click **Reset to Default**.

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.

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:

- Mobile Computers
- Scanners
- Printers
- Other

Navigating the Assets Pages

The Assets, Mobile Computers, Scanners, and Printers 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.

Filter Columns

Click  to 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.

Filters

To narrow the displayed information by connection status, model, site, and/or tag on the Assets page click  . Use the arrows to expand the filter options.

The number of devices that match the selected filter(s) will be shown in blue on the filter icon. 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 next time you log in.

To filter by model, site or tag, you can select from the drop-down list or type in the filter field.

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.

Note: *Resetting all filters will not affect column filters.*

Filtering by Tag

Tags are user-defined identifiers you can use to filter devices. (For information about setting up tags, see page 16.)

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.

Savings Filters

Operational Intelligence Performance Management will remember the applied filters the next time you log in to the portal. However, if you have filter sequences you use often, you can save them for future use by bookmarking the page.

Exporting

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**.

State

The State column 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. To change a device's status:

1. Select an assets page 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 State**.
4. Select a new state.
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 18).

Adding Tags

To create and assign tags to devices:

1. Select an assets page from the navigation bar (i.e., Assets, Mobile Computers, Scanners, or Printers).
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 20 and Scanners and Printers on page 22.)

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. Mobile computers will have an additional Trends report. To zoom into an area of a line graph, 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. You can also see the tags assigned to the device.

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 16.

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 updates by clicking the blue text beneath the **Software** heading.

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 35.)

Mobile Computers

Access the Mobile Computers page by clicking in the Assets submenu. 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.

To exit the device detail page, click **Mobile Computers** 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.

Map

If location services are enabled on the mobile computer, its most recent location will display on the detail page.

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

Adding a Mobile Computer

1. Click to access the Assets page or to access the Mobile Computers page.
2. Click **Add Assets**.
3. Select a site from the drop-down list.
4. Specify how many devices will be onboarded with the QR code. The default is 10 devices, the maximum is 100.
5. Specify how many days the QR code should remain active. The default is 7 days, the maximum is 30.
6. Accept the terms and conditions by clicking the check box.
7. Click **NEW QR CODE**. The QR code will display.
8. 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.*

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.

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 an Other Asset

1. Click  to access the Assets page or  to access the Other page.
2. Click  **Add Assets**.
3. Select **Connected** or **Non-Connected**.
4. To add a Connected device:
   a. Select a site from the drop-down list.

b. Enter the number of devices that the QR code can be used for.
c. Enter the number of days after which the QR code will expire.
d. Check **Include tenant information** if applicable.
e. Check the box to indicate that you have read the terms and conditions and privacy policy.
f. Click **NEW QR CODE** to generate an image.
g. Click  to download the QR code as a .png file that you can scan with the device or  to download XML code that can be uploaded to a device.

5. To add a Non-Connected device:
   a. Select a site from the drop-down list.
   b. Click **Download an import template** to get an Excel file that you can use to upload assets.
   c. 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 assets have been added before downloading the template. See Assets Configuration for more information.*

   d. 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.
   e. Click **Submit**.

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. Enter the **Check In Time**. **Check Out Time** defaults to the current date and time and cannot be modified.
   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 Filter Columns 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.

Device Wipe

Use Device Wipe to perform a factory reset of a device.

Note: *Only users with the role of Device Administrator have the ability to use Device Wipe.*

1. From the Assets menu, select **Mobile Computers**.
2. Click an asset in the list.
3. Click **Device Wipe**.

4. A system prompt asks if you are sure you want to reset the device. Click Yes.

Remote Control

Remote Control 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 Control:

- 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 Control

To connect to a device using Remote Control:

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 Control**.

   When a remote connection is successfully established, a new window opens for the device. Once the window 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.

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

Button	Function
Home	Go to the device Home screen
Page Up	Scroll up on a page or menu
Page Down	Scroll down on a page or menu
Power	Turn the device power on or off
Search	Open the Search window
Unlock	Unlock the device. To unlock click Power then Unlock.

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.

CHAPTER

4 SITE ANALYTICS

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

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

The Site Analytics 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 Site Analytics icon a second time to display the Site Analytics submenu:

- Site Rankings

Customize the Site Analytics Display

The Site Rankings page provides several predefined reports. You can customize the display based on what information you want to see in each report.

Select Sites for Site 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.

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.

Change Sites for Site Rankings

You can change the site you are viewing results for in the Site Rankings analysis.

To change sites:

1. Click **Change** 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**.

Select Asset Type

You can view reports for any of the available asset types (Mobile Computers, Printers, Scanners). Select the tab for the device you want to view.

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.

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
- Proximity Report

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. Select the **Time Range** from the drop-down list.
   a. If you select “Custom,” enter the **Start Time** and **End Time** on the Custom time range window then click **Apply**.
4. Select the **Operation Type** to filter by a specific activity.

5. Select a **User** to view activity for only one user.
6. Select a **Site** to display only actions associated with one site.
7. 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.*

Proximity Report

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 User Proximity Log to review instances where proximity alerts were reported. The report can be filtered based on user names, a range of time, and/or the duration of contact events.

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

Viewing Proximity Reports

1. Expand the **Reports** menu on the navigation bar on the left side of the portal.
2. Click **Proximity Report**.

3. Select one or more users from the **Name** drop-down list.
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 **Proximity 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.
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
- Printers:
  - Fonts
  - Configuration files
  - 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 19).*

Note: *Only users with Device Administrator privileges can access the Software Updates page. For more information, see Roles on page 40.*

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

The **Updates** tab displays all available software updates.

The **Schedule** tab displays all scheduled updates.

The **History** tab displays the status of current, completed or expired updates.

Uploading Software

To upload software updates so that they are available to devices:

1. Click **Software Updates**.
2. Click **Upload Software.**
3. Enter the update name.
4. Select a 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. Optional: enter a version number and specify a device model.
7. Drag and drop the update file into the window or click **BROWSE FILES** and select the desired file.
8. Click **UPLOAD**.
9. Refresh your browser window and the uploaded file will display in the list of available updates.

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 Uploading Software on page 36).

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

Updating Software

Operational Intelligence allows you to push updates to one or more devices. Updates can be performed immediately or scheduled for a future time.

To update software on your devices:

1. Click **Software Updates**.
2. Select an available update from the table on the Updates tab.
3. Click **Launch Update**.
4. On the Configuration tab, enter any required information. The information will vary depending on the specific update.
5. Click **Next**.
6. Choose an option for how you want to select the devices to be updated.
    a. If you selected **By Site**, choose a site from the drop-down list.
    b. If you selected **By Tags**, choose a group from the drop-down list.
    c. If you selected **From List**, the system displays a list of the available compatible devices. Check the box for each device to update or select the box in the header row to select all devices. The maximum number of devices that can be updated in a single request is displayed on the screen. You cannot select more than the allowed number of devices.
7. Click **Next**.
8. Select the time to perform the updates.
    a. Select **Immediate** to perform the updates as soon as you submit them.
    b. Click **Schedule** then enter the **Time Zone**, **Schedule Date**, and **Time** to perform the updates at a later time.
9. Click **Next**.
10. Review the information on the Confirmation screen and click **Submit**.

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. The User Management page has two tabs: **Users** and **Roles**.

Users

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

Creating Users

1. Click **Admin** then **User Management**.
2. Click **New User**.
3. Enter the new user's first name, middle name (optional), last name and login email address.
4. Using the drop-down lists, select an organization and a site.
5. Select a user role. For more information about available roles, click (i).
6. 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.
- 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.

The **Roles** tab of the User Management page displays the number of users by role. To see the specific users assigned to each user category, click on the Role name.

You can also use the Roles tab to create customized dashboard views tailored to each role's function and assign them to users.

Creating a View

1. Click **Admin** then **User Management**.
2. Click the **Roles** tab.
3. Select a role and click **View Details**.
4. Click **Add dashboard**.
5. Click **Create new dashboard** to open the Customize Dashboard window.
6. Enter a name for the new view in the **Dashboard Title** field.
7. Click the down arrows to expand dashboard sections.
8. By default, all reports are turned on. To remove a report from a view, click the check box beside a report to deselect it.

   (The cursor will change to a when you hover over the check box).
9. To rearrange a report, click and hold anywhere on the report except the check box (the cursor will change to), then drag it to a new location.
10. Click **SUBMIT** to save your new dashboard view.

Assigning Dashboards

Once you have set up customized dashboards, you can assign them to users on the Roles tab.

1. Click **Admin** then **User Management**.
2. Click the **Roles** tab.
3. Select a role and click **View Details**.
4. Click **Add dashboard**.
5. Select a dashboard from the drop-down list.
6. Click **ADD**.

Editing Assigned Dashboards

1. Click **Admin** then **User Management**.
2. Click the **Roles** tab.

3. Select a role and click **View Details**.
4. Select the dashboard and click **Edit**.
5. Make the desired changes.
6. Click **SUBMIT**.

Deleting Assigned Dashboards

1. Click **Admin** then **User Management**.
2. Click the **Roles** tab.
3. Select a role and click **View Details**.
4. Select the dashboard and click **Delete**.
5. Click **YES** to confirm.

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.
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**.

Uploading a Building's Floor Map

To upload a map of a building's layout:

1. Click **Admin** then **Site Management**.
2. Select a site and building.
3. Click **Upload Map**.
4. Drag and drop a .png file into the window or click **BROWSE FILES** and select the desired file.
5. Click **SUBMIT**.

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**.

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 an Other Asset 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**.

All selected devices are reassigned to the Recommended Site.

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.

Honeywell
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com