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.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

Copyright © 2019-2020 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

Android and Chrome are trademarks of Google LLC.

Microsoft, Windows, and Azure are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Mac and OS X are registered trademarks of Apple, Inc.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries.

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

For patent information, refer to www.hsmpats.com.
# TABLE OF CONTENTS

Customer Support .......................................................................................................................... v  
Technical Assistance .................................................................................................................... v  

## Chapter 1 - Getting Started........................................................................................................ 1  

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Requirements</td>
<td>1</td>
</tr>
<tr>
<td>Organizations and Sites</td>
<td>2</td>
</tr>
<tr>
<td>Setting Up Your Locations</td>
<td>2</td>
</tr>
<tr>
<td>Indoor Locationing</td>
<td>2</td>
</tr>
<tr>
<td>Creating an Account</td>
<td>3</td>
</tr>
<tr>
<td>Logging In</td>
<td>3</td>
</tr>
<tr>
<td>Navigation and Tools</td>
<td>3</td>
</tr>
<tr>
<td>Navigation Bar</td>
<td>3</td>
</tr>
<tr>
<td>Toolbar</td>
<td>4</td>
</tr>
<tr>
<td>Zoom</td>
<td>5</td>
</tr>
<tr>
<td>Alerts</td>
<td>5</td>
</tr>
<tr>
<td>Alerts Page</td>
<td>5</td>
</tr>
<tr>
<td>Customizing the Portal</td>
<td>6</td>
</tr>
<tr>
<td>Display Settings</td>
<td>6</td>
</tr>
<tr>
<td>Preferences</td>
<td>6</td>
</tr>
<tr>
<td>Alert Notifications</td>
<td>6</td>
</tr>
<tr>
<td>Notification Report</td>
<td>6</td>
</tr>
<tr>
<td>Logging Out</td>
<td>7</td>
</tr>
</tbody>
</table>
Chapter 2 - Dashboards.......................................................................................9

Introduction ..............................................................................................................9
Selecting a Site .............................................................................................................9
Types of Reports ............................................................................................................9
  Report Options ........................................................................................................10
  Report Detail ............................................................................................................10
  Exporting ................................................................................................................10

Chapter 3 - Assets..................................................................................................13

Navigating the Assets Pages ..................................................................................13
  Sorting .....................................................................................................................13
  Filter Columns .......................................................................................................13
  Filters ......................................................................................................................14
    Filtering by Tag ..................................................................................................14
    Savings Filters ..................................................................................................14
  Exporting ...............................................................................................................14
    Exporting Filtered Data ....................................................................................15

State ..........................................................................................................................15
Tags ............................................................................................................................16
  Adding Tags ..........................................................................................................16
  Editing Tags ..........................................................................................................16
  Removing Tags ......................................................................................................17
  Device Detail .........................................................................................................17
    Tags ......................................................................................................................18
    Renaming a Device ............................................................................................19
    Updating Software on a Device .......................................................................19

Mobile Computers ..................................................................................................19
  Indoor Positioning .................................................................................................19
  Detail .....................................................................................................................20
  Map .......................................................................................................................20
  Adding a Mobile Computer .................................................................................20
  Bulk Edit ...............................................................................................................21

Scanners and Printers ...............................................................................................21
Chapter 6 - Security

Operational Intelligence Security Overview.................................................................35
Disclaimer ......................................................................................................................35
Data Collection, Privacy and Use ...............................................................................35
Secured Edge-Cloud Communication ..........................................................................35
Secured Operational Intelligence Performance Management Portal ................36
Cloud Provider .............................................................................................................36
Security Considerations for Devices Connecting to Honeywell Operational Intelligence..................................................................................................................36
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.
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 28.

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 28)
3. Add users (see page 25)
4. Optional: enable locationing and indoor tracking of mobile computers (see next section Indoor Locationing)
5. Add devices (see Mobile Computers on page 19 and Scanners and Printers on page 21)

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.
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.
Note: Your ability to view and modify data in Operational Intelligence is determined by your assigned user role (see User Management on page 25).

### 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.

<table>
<thead>
<tr>
<th>Toolbar Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Alerts Icon" /></td>
<td>Click the Alerts icon to display notifications (see page 5).</td>
</tr>
<tr>
<td><img src="image" alt="Online Status" /></td>
<td>A green circle will display when you are on line. A red circle will display if you are off line.</td>
</tr>
</tbody>
</table>
| ![Help Icon](image) | 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 |
Alerts

Operational Intelligence Performance Management offers both on-screen 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 Alerts.
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.
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 reports for the site selected at the top of the page.

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.

*Note:* Administrators and Device Administrators can create customized dashboard views and assign them to users (see Creating Views on page 33).

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 reports for the entire organization, while selecting “/ Company ABC / Northwest / District A / Store 1” would display reports for that single site only. For more information about site hierarchy, see page 28.

Types of Reports

The reports displayed on the dashboard will change based on the types of connected devices for the displayed site. For example, scanning reports will not display if no scanners are connected.
Depending on the devices connected, reports may include:

- Alerts (see page 5)
- Device usage and connectivity
- Mobile computer usage, drops, reboots, security patches, and operating systems
- Printer volume, label quantity, faulty dots, ribbon outage, and firmware
- Scanner volume and firmware

**Report Options**

The icon in the upper right corner of a report indicates that the report 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.

**Report Detail**

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

You can narrow the results displayed in the report detail 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 report table by column in ascending or descending order, use the arrows beside a column heading.

**Exporting**

To export a report’s data to .csv:

1. Click on the caption at the bottom of a report. If export is available for that report, the report 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 report’s data will be exported, even if you have used the Search field to limit the displayed results.
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

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 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 19 and Scanners and Printers on page 21.)

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 23.)*

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 Devices.
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 Add**.
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 **Add**. 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 **Scanners** in the Assets submenu to access the Scanners page or **Printers** 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.

**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] 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*. 
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 Provisioneer 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:** The Software Update page is used for uploading and managing software. Use the Assets page to install updates on devices (see page 19).
**Note:** Only users with Device Administrator privileges can access the Software Updates page. For more information, see Roles on page 26.

The Update Software 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 Update page (see Uploading Software on page 24).

For more information, see the **Enterprise Provisioner User Guide**, which is accessible from the Enterprise Provisioner Help tab.
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 .
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 .
6. Click SUBMIT.
Editing Users

To modify 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 .
   Or
   Click then use the Search field to look up the desired user. Click on the user’s name to select it.
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 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.

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. Click Create new dashboard to open the Customize Dashboard window.
4. Enter a name for the new view in the Title field.
5. Click the down arrows to expand dashboard sections.
6. 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).
7. 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.
8. 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 by clicking on a row. A list of all users with the role will display, along with any dashboard views already assigned to that role.
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 by clicking on a row.
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 by clicking on a row.
4. Select the dashboard and click Delete.
5. Click YES to confirm.

Site Management

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 overview tab provides a summary of site information, including address, site hierarchy, and user permissions. Use the arrows to the left of a site name to expand or collapse that site.

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

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.

<table>
<thead>
<tr>
<th>Site Management Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td></td>
</tr>
<tr>
<td>Building</td>
<td></td>
</tr>
<tr>
<td>Floor</td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td></td>
</tr>
</tbody>
</table>
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**.

### Access Points

If you have chosen to use the Access Point Solution for indoor positioning (see page 2), you will use this page to set up and maintain your access points.

Click **Admin** then **Access Points** in the navigation bar and a list of any existing access points will display.

### Creating Access Points

If you have not yet set up any access points you can do so by downloading a blank template, adding your access points, then uploading the new list:

1. Click **Admin** then **Access Points**.
   “You haven’t added any access points” will display.
2. Click **Export Access Points**.
3. Select the location where you want to save a template .csv file.
4. Click **Save**.
5. Open the .csv file. You will see the first row is pre-populated with column headings.
6. Beneath the headings, enter a row for each access point to be added. 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

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.

7. Save the .csv file.
8. Return to the Operational Intelligence Performance Management portal.

10. Drag and drop the .csv file into the window or click BROWSE FILES and select the desired file.
11. 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.

Adding or Editing Access Points

If you have already set up access points and either want to add additional ones or edit existing ones, you can do so by downloading the existing list of access points, making your changes, then uploading it.

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

1. Click Admin then Access Points.
   The current list of access points will display.
2. Click Export Access Points.
3. Select the location where you want to save the .csv file.
4. Click Save.
5. Open the .csv file and make the desired changes. All fields are mandatory.
7. Return to the Operational Intelligence Performance Management portal.
8. Open the Access Points page and click Upload Access Points.
9. Drag and drop the updated .csv file into the window or click BROWSE FILES and select the desired file.
10. 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.

Dashboards

The Dashboard Views page allows you to set up standard dashboard views for users.

Creating Views

1. Click **Admin** then **Dashboards**.
2. Click **Create new view** to open the Customize Dashboard window.
3. Enter a name for the new view in the **Title** field.
4. Click the down arrows to expand dashboard sections.
5. By default, all reports are turned on. To remove a report from a view, click the check box beside a report to de-select it. (The cursor will change to a **hand** when you hover over the check box).
6. To rearrange a report, click and hold anywhere on the report except the check box (the cursor will change to **hand**), then drag it to a new location.
7. Click **SUBMIT** to save your new dashboard view.

Once you have set up the custom dashboards, you can use the User Management page to push the dashboards to users (see **Assigning Dashboards** on page 27).

Editing Views

1. Click **Admin** then **Dashboards**.
2. Select a dashboard view by clicking on . A blue toolbar will display.
3. Click **Edit** on the dashboard to open the Customize Dashboard window. The name of the current view will display in the **Title** field.
4. Click the down arrows to expand dashboard sections.
5. To remove a report from the view, click the check box beside a report to de-select it. (The cursor will change to **hand** when you hover over a check box).
6. To rearrange a report, click and hold anywhere on the report except the check box, then drag it to a new location.
7. Click **SUBMIT** to save the edited dashboard view.

**Deleting Views**

1. Click **Admin** then **Dashboards**.
2. Select one or multiple dashboard views using the check boxes. A blue toolbar will display.
3. Click **Delete**.
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.