Honeywell

Honeywell Cloud Connect

User Guide

Disclaimer

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

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

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 © 2026 Honeywell Group of Companies. All rights reserved.

Web Address: automation.honeywell.com

Trademarks

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

Chrome is a trademark of Google LLC.

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

Patents

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

TABLE OF CONTENTS

Customer Support v
Technical Assistance v

Chapter 1 – Getting Started 1

Introduction 1
HCC Installation Instructions 1
Requirements 1
User Requirements 2
Security Considerations 2
Whitelist URLs 3
Install HCC 3
Sign In and Register a Gateway with Op Intel 7
Upgrade HCC 8
HCC User Interface 8
Create JSON Configuration File 9

Chapter 2 – Printers 11

Mobile Printers 11
Requirements 11
Recommended Settings 12
Manually Onboarding a Mobile Printer 12
Industrial Printers 14
Requirements 14
Recommended Settings 15
Manually Onboarding an Industrial Printer 15

Chapter 3 - Device Discovery and Onboarding 19
Overview 19
Prerequisites 19
File Configuration for Older Printer Firmware 20
Increase Discovery Service Ping Count 20
Define Printer Subnet Range 21
Define Discovery Option Inputs 21
Scheduling Discovery and Onboarding 26
Chapter 4 - Handheld Scanners and Wireless Barcode Scanners 29
Connecting Wireless Barcode Scanners to Wi-Fi Network 29
Onboarding Wireless Barcode Scanners 29
Onboarding Handheld Scanners 30
About Scanner Agent 30
Scanner Agent PC and Network Requirements 30
Using HCC System Created JSON Configuration File 31
Scanner Agent Silent Installation 31
Asset Updates from Op Intel 33
Device Actions 33
Chapter 5 - Troubleshooting 35
HCC Troubleshooting/Service Debug Logs 35
Setting the Service Debug Log Level 35
Set the Debug Log Level for HCC Back-end Services 35
Set the Debug Log Level for HCC Device Discovery and Onboarding Services 36
Set the Debug Log Level for HCC UI 36
Collect Troubleshooting Logs 36
HCC User Interface 37
Connection to HCC Services Failed 37
Username and Password Prompt not Displayed 38
Device not Shown in Op Intel Portal 38
Printers 39

Onboarding Fails 39
Printer Status Incorrectly Shown as Online 39
Message Shows Default Printer Password Needs to be Changed 39
Scanners 40
Device not Detected 40

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 honeywell.com/PSStechnicalsupport.

CHAPTER

1 GETTING STARTED

Introduction

Honeywell Cloud Connect (HCC) is a gateway application that transfers the data received from multiple devices to the cloud. HCC is used for onboarding printers and scanners to Honeywell Operational Intelligence (Op Intel).

HCC Installation Instructions

Follow these steps to perform a fresh installation of HCC.

- If an instance of HCC is already installed, see Upgrade HCC on page 8 for instructions on upgrading to a new version.

Requirements

A host computer with the following:

- A static IP address
- A secure, dedicated port that will be used for communication between HCC and the device agent
- A network connection to devices and access to the cloud
- .NET Framework 4.8.1 installed
- Supported OS: Windows Server 2022 and Windows Server 2025

Note: *We recommend using Windows Server 2022 or Windows Server 2025 16 CPU, 32 GB RAM.*

Note: *HCC and devices should be on the same network. When devices are in a different Subnet, the network group should allow the following device ports:*
From devices to HCC: Default 8883, 21210, 21211, 21212, 21213, 21219, 21221
From HCC to device: Default 8883, 21221
These default ports can be modified during installation.
For Mobile Printer discovery and onboarding, port 9100 should be open.
For Industrial Printer discovery, Printer port 80 should be open.

User Requirements

Users who will log into HCC must first be added in Operational Intelligence with the following roles:

- Administrator - Users with this role can create and manage users, sites, and custom dashboards.
- Device Administrator - Users with this role can access devices remotely or trigger remote commands on a device, as well as create and manage users, sites, and custom dashboards.

If the user does not have these roles assigned, they will receive a Login Failed message when attempting to log into HCC.

Refer to the *Operational Intelligence User Guide* for details on managing users.

Security Considerations

- Principle of Least Privilege: Ensure that users (logging into the HCC system) operate under the least privileges necessary for their role. Limit administrative access and utilize UAC to its fullest extent to mitigate unauthorized changes.
- Use of Endpoint Detection and Response (EDR) Tools: Deploy advanced EDR solutions capable of detecting and responding to suspicious activities, including unusual registry modifications and fileless attack techniques.
- App Security and Installation Folder Permissions:
  - If HCC is installed in the default folder (e.g., C:\Program Files(x86)): Windows automatically protects the application. Standard users cannot modify or tamper with the application files.
  - If installed in a custom folder (e.g., another drive or a custom folder): You must manually configure the folder security permissions to prevent unauthorized changes.
    Configure your folder permissions using NTFS Access Control Lists (ACLs) as follows:
    - Administrators and SYSTEM accounts: Grant “Write” and “Modify” permissions.
    - Standard (non-admin) users: Grant “Read” and “Execute” permissions only.

Warning: Leaving custom folders unprotected allows unauthorized users to modify application files, creating a security risk.

Whitelist URLs

Refer to the *Operational Intelligence Deployment Guide* for a list of URLs that should be whitelisted to allow proper communication for HCC and Operational Intelligence. The Deployment Guide is available at automation.honeywell.com.

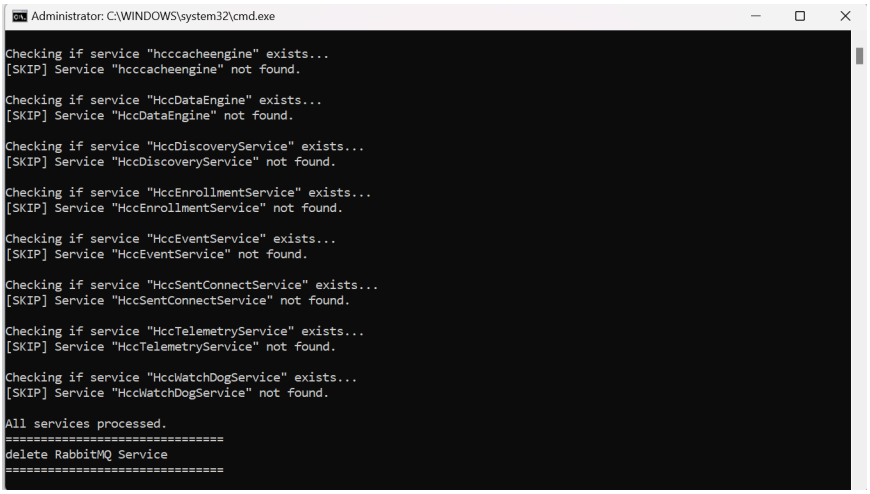
Install HCC

Follow these steps to install HCC.

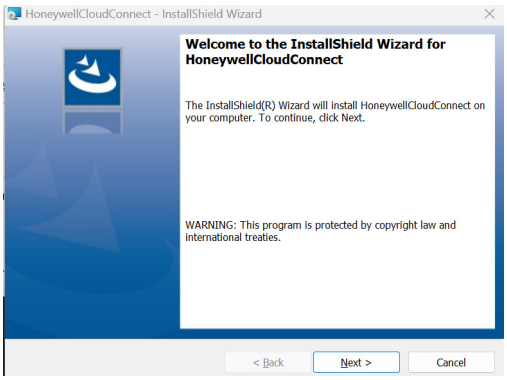
1. Log in to the host PC with admin privileges.
2. Go to the Honeywell software download website at honeywell.com/PSSsoftware-downloads.
3. Create an account if you have not already created one. You must login to download the software.

Note: *If you haven't already, download and install the Download Manager. Click on the link and follow the screen prompts.*

4. Locate the Honeywell Cloud Connect app in the **Software > Software and Tools > Device Management** directory and download HCC_Setup_*.zip, where * represents the latest HCC version.
5. Extract HCC_Setup_*.zip.
6. Right-click on setup.exe and select **Run as administrator**.
   The command window displays while HCC prepares for installation. Do not take any action until the window closes.



7. When the InstallShield Wizard displays, click **Next**.



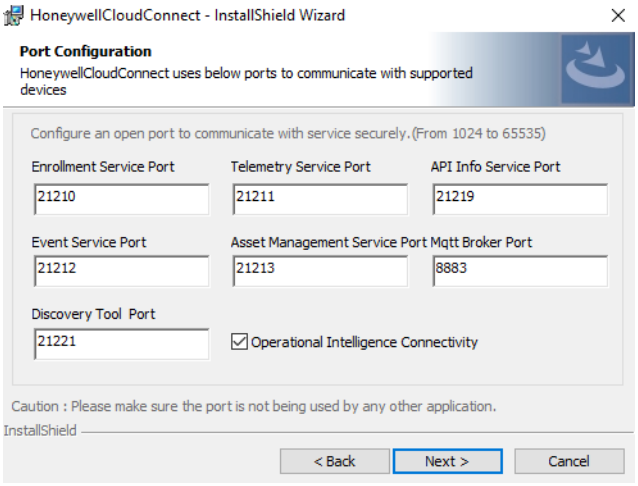
8. Select the radio button for **I accept the terms in the license agreement** then click **Next**.
9. The default location for installation is: C:\Program Files (x86)\Honeywell\HoneywellCloudConnect\.
    a. To select a different location, click **Change** then navigate to the required folder.

Note: *Refer to Security Considerations on page 2 for recommended App Security and Installation Folder Permissions if you select an installation location different from the default.*

    b. Click **Next**.

Note: *You can select to install HCC components in a different location than the default; however, HCC dependency modules (MySQL and RabbitMQ) will be installed at the default path. Subsequent HCC upgrades will continue to use the location selected during the first HCC installation.*

10. The ports to be used to communicate with HCC display the default values. You can accept the defaults or specify a port number between 1024 and 65535.

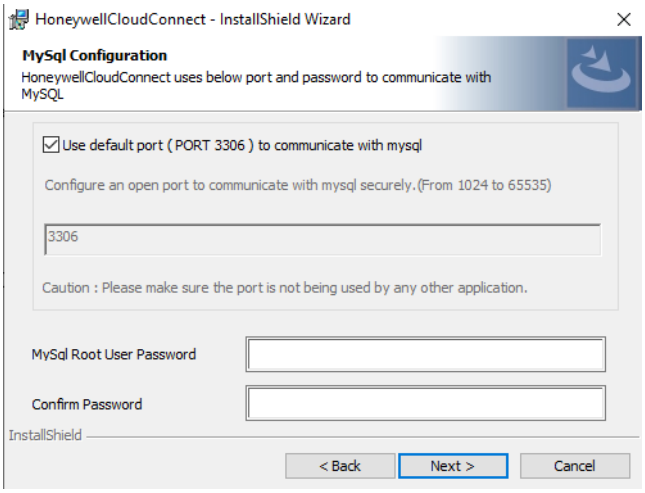


Note: *The HCC Installation Wizard displays the list of default ports used for communication. Firewall exceptions must be in place for these ports: 8883, 21210, 21211, 21212, 21213, 21215, 21219, 21221.*
Make sure that these ports are not occupied by another application. Modify the port number if required.

a. By default, the check box for **Operational Intelligence Connectivity** is selected. Do not uncheck this box.

b. Click **Next**.

11. The default port to communicate with MySQL is 3306.



a. To use a different port, unselect the check box for **Use default port (PORT 3306) to communicate with mysql** and enter a new value.

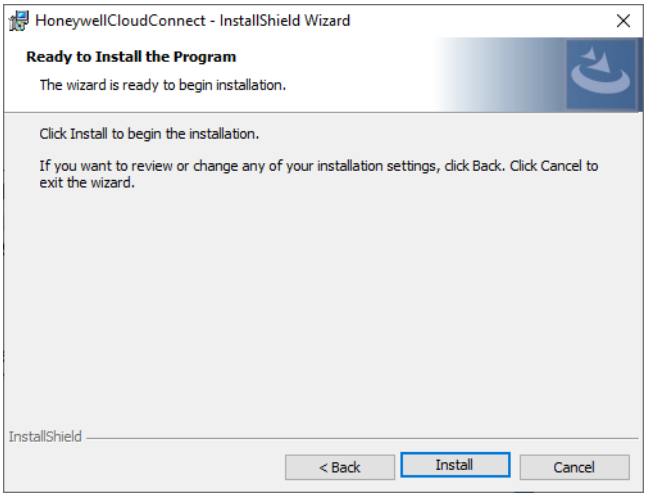
b. Set up a **MySql Root User Password** for access to the database. The password must meet the following criteria:

- Minimum of 8 characters long
- Combination of upper case and lower case letters, numbers, and symbols
- Allowable symbols are: ! @ # $ ^ & * ( )

Note: *You do not have to install MySQL. HCC installer will install an instance for you, and the password you provide here will be set in that instance.*

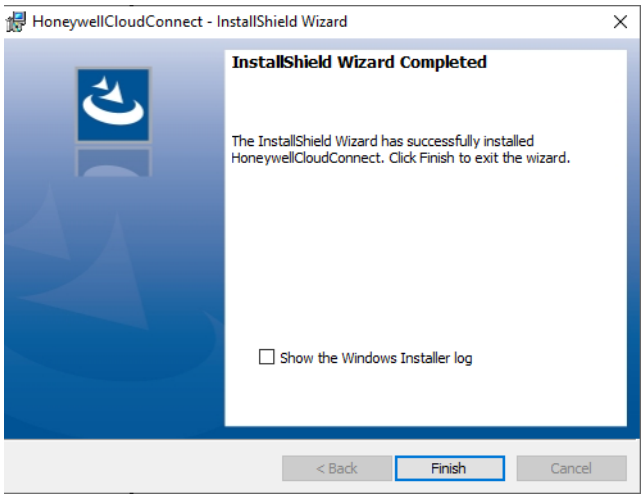
c. Click **Next**.

12. Click **Install**.



HCC installation may take several minutes.

13. Click **Finish**.



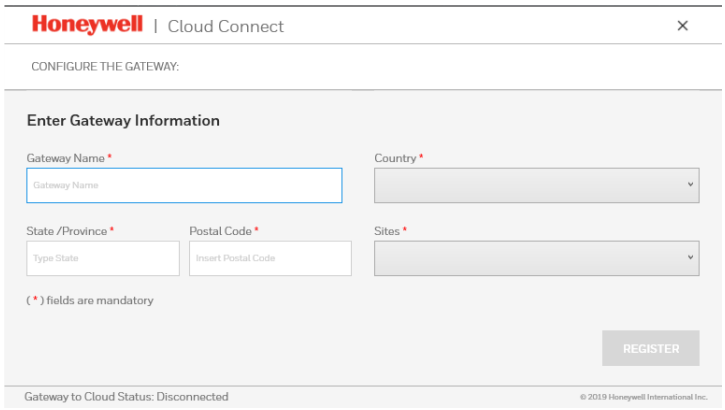
Once HCC has been installed, a shortcut will be added to your desktop.



Note: *After installation, you should delete the HCC setup.exe file from the system because stack protection is not enabled on setup.exe.*

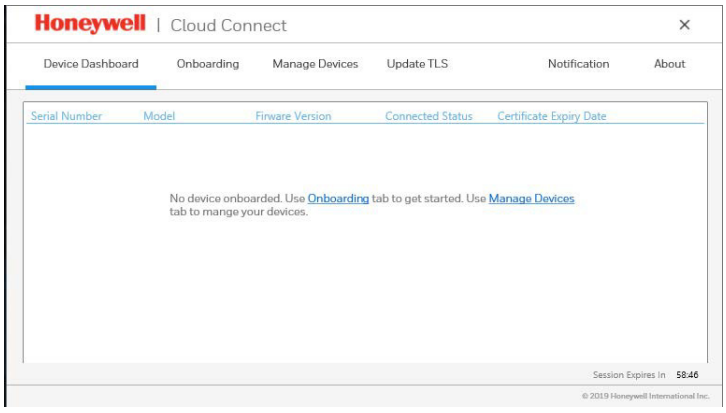
Sign In and Register a Gateway with Op Intel

1. Right-click the Honeywell Cloud Connect desktop shortcut and select **Run as Administrator**.
2. Click **SIGN IN**.
3. Sign in using your Operational Intelligence user credentials (not server administrator account).
4. The first time you log in to HCC you will be required to register a gateway name.



   a. Enter the new **Gateway Name**.
   b. Enter the **State/Province**.
   c. Enter the **Postal Code**.
   d. Select the **Country**.
   e. Select a **Site** from the drop-down list.
   f. Click **REGISTER**.

   A Welcome message will display during the registration and configuration process. Once it is completed, the HCC Device Dashboard will display.



   After HCC has been registered, it will display as a Gateway on the Assets page in the Operational Intelligence user interface. To view an instance of HCC, log into Operational Intelligence and select Assets from the left-hand navigation menu.

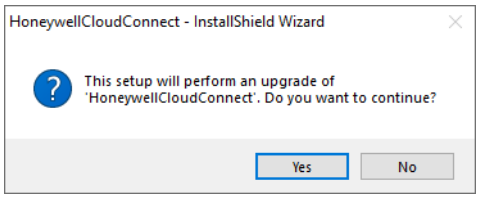
Select the HCC gateway in the list of assets. When you view the HCC gateway information, the Status field indicates if HCC is connected or disconnected. See the Operational Intelligence User Guide for more information.

Upgrade HCC

Follow these steps to upgrade HCC if a previous version is already installed. When you upgrade to a new version, devices that were previously onboarded to HCC will be retained with the upgraded version.

Note: *Only upgrading to a new version of HCC is supported. Attempting to downgrade the HCC version will result in failure.*

1. Log in to the host PC with admin privileges.
2. Go to the Honeywell software download website at hsmftp.honeywell.com.
3. Create an account if you have not already created one. You must login to download the software.
4. Locate the Honeywell Cloud Connect app in the **Software > Software and Tools > Device Management** directory and download HCC_Setup_*.zip, where * represents the latest HCC version.
5. Extract HCC_Setup_*.zip.
6. Right-click on setup.exe and select **Run as administrator**.
7. A pop-up is displayed indicating that an upgrade will be performed.



   Click **Yes**.
8. The InstallShield Wizard launches and prepares HCC for installation. When prompted, click **Next**.
9. When installation completes, click **Finish**.

HCC User Interface

The Device Dashboard tab is the HCC home screen. On all the HCC tabs, a countdown timer in the lower right corner displays how much time remains in the current session. The default session is 60 minutes. Once the session expires, you must sign in again.

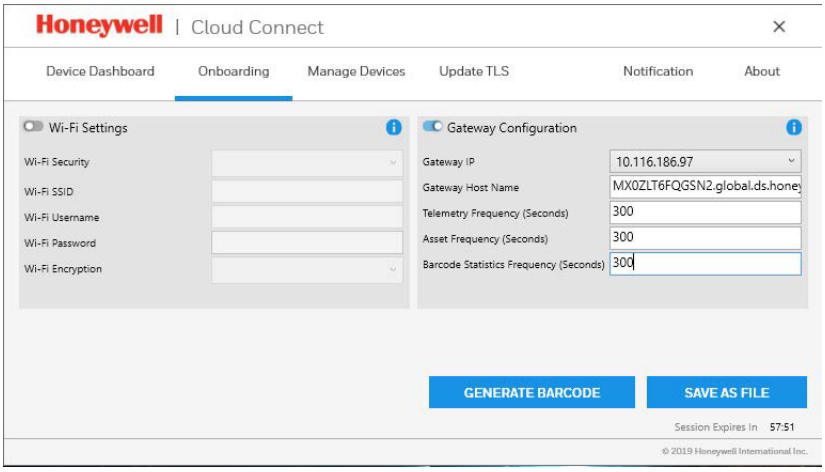
The HCC menu tabs are described in the table below:

Tab	Description
Device Dashboard	Displays devices that have already been onboarded. You can filter the device list using the **Model** drop down list.
Onboarding	Used to enroll scanners and printers in HCC. (See Handheld Scanners and Wireless Barcode Scanners on page 29 and Printers on page 11.)
Notification	Lists updates from devices to HCC.
About	Displays the version of HCC software you are using, the name of your gateway, the ID of the current user, and the Operational Intelligence site to which you are connected.

Create JSON Configuration File

To register devices in HCC, you must point them to the computer where you installed the service by creating a JSON configuration file. Follow these steps to create the file:

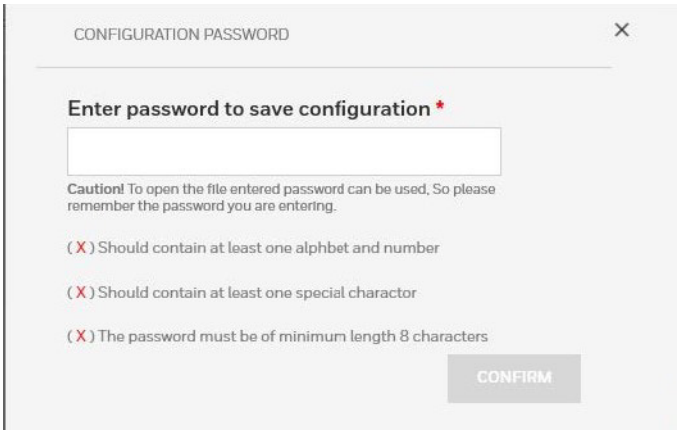
1. Launch HCC using **Run as Administrator**.
2. Select the Onboarding tab on HCC's main screen.



3. Enable the **Gateway Configuration** slider.
4. Enter the required information in the text boxes:
   - **Gateway IP:** IP address of the computer through which printers can be reached
   - **Host Name:** Local computer name is showed by default
   - Frequencies: Enter the period of time which device information will be read in seconds. You may accept the default or enter a different value.
5. Click the **SAVE AS FILE** button.

6. For security reasons, the JSON configuration file will be created as a zip file, which is password protected. You must enter a password that will be required later to unzip the file.

   Enter the password then click **CONFIRM** and choose the target folder to save the file.



CHAPTER

2 PRINTERS

Connected printers will send events, device information and metrics to Honeywell Operational Intelligence through the HCC gateway.

The steps for connecting a printer to HCC will depend on the type of printer:

- Mobile printers (see next section)
- Industrial printers (see page 14)

Mobile Printers

To connect a supported mobile printer to HCC you will either use the NETira CT configuration utility to push information to the printer from a file generated by HCC or use Device Discovery and Onboarding to automatically discover and onboard printers.

Requirements

- Up-to-date firmware installed on the printer
- Active printer network connection via Wi-fi
- HCC installed on your network and accessible from the printer
- HCC and devices should be on the same network. When devices are in a different Subnet, the network group should allow the following ports:
  From devices to HCC: Default 8883, 21210, 21211, 21212, 21213, 21219, 21221
  From HCC to Device : Default 8883, 21221
  These default ports can be modified during installation.
- NETira CT version 1.0.0.111 or higher

  NETira CT is a configuration utility that allows you to make changes to the existing printer set up. It is only required for Mobile Printer manual onboarding. NETira CT is available for download from the Honeywell software download website hsmftp.honeywell.com.

Note: *For information about updating the printer firmware, setting up the Wi-fi connection on your printer, or installing NETira CT, please refer to your printer's user documentation.*

Recommended Settings

Following these recommended settings will ensure that the printer stays connected with HCC, notifies HCC on occurrence of printer events, and responds to commands and device actions issued from HCC.

- For RP2e/RP4e printers:
  - Disable Printer Shutdown (System Settings > Power Down Time) by setting the value to 0.
  - Disable Printer Sleep Mode (System Settings > Sleep Time) by setting the value to 0.
  - Set the printer time to the accurate date and time.
- For RP2f/RP4f printers:
  - Disable Printer Shutdown (System Settings > General > Shutdown Timer) by setting the value to 0.
  - Disable Printer Sleep Mode (System Settings > General > Sleep Timer) by setting the value to 0.
  - Set the printer time to the accurate date and time. Verify that NTP Time Server is enabled and correctly set up to ensure accurate date/time.

Manually Onboarding a Mobile Printer

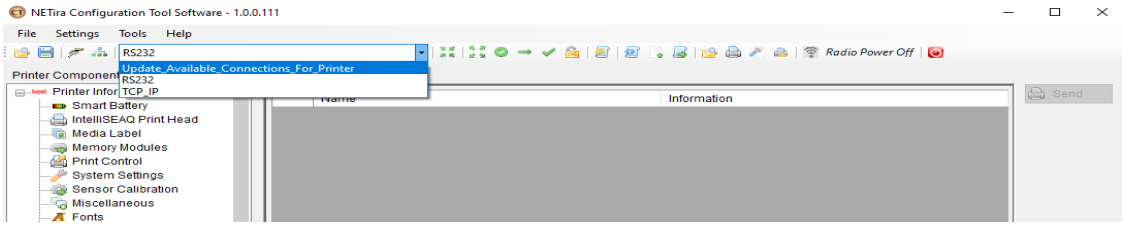
Follow these steps to manually onboard a mobile printer. See Device Discovery and Onboarding for instructions on using HCC to discover and onboard printers on a network.

1. Create the required JSON configuration file for the device. See Create JSON Configuration File on page 9 for instructions.
2. Extract the saved zip file created in step 1. Enter the password when prompted.

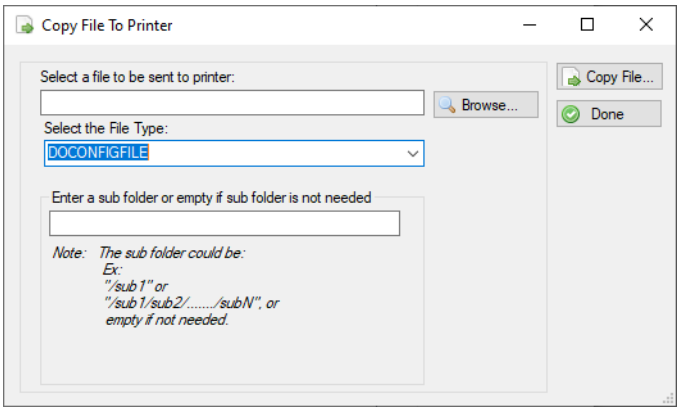
3. Open the extracted file with a text editor, such as Notepad. An example is shown below:

```
{
  "GatewayConfiguration": {
    "IpAddress": "xxx.xx.xx.xxx",
    "HostName": "xxx.xxxxx.xx.xxxxxx.com",
    "Port": 21210,
    "TelemetryFreq": 3000,
    "AssetFreq": 3000,
    "BarCodeStatFreq": 3000
  },
  "AuthenticationConfig": [
    {
      "UniqueId": "xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "SecureFingerPrint": "xxxxxxxxxxxxxxxxxxxxxxxxxxxx"
    }
  ]
}
```

4. Save the file as “CAConfig.json”.
5. Connect the printer to a USB port and turn the printer on.
6. Use the **Run as Administrator** option to open NETira CT.
7. Select **Update_Available_Connections_for_Printer** from the drop-down list in the top toolbar.



8. Once the available connection is found, click **USB_VIRTUAL_COM** in the drop-down list.
9. Click **Tools > Query Printer Configuration** to load the current printer settings.
10. Click **Tools > File Explorer**.
    The Printer File Explorer window opens.
11. Click the **Copy Files** button.
    The Copy File to Printer window opens.



12. Click the **Browse** button and navigate to the file CAConfig.json saved in step 4.
13. In the **Select the File Type** drop-down list, choose “DOCONFIGFILE”.
14. Click the **Copy File** button.
    The file from your PC is copied to the printer.
15. Click the **Done** button.
16. Reboot the printer.
17. Wait for at least 30 seconds then query the printer using NETira. Enrollment should display as “Enrollment Success.”
18. Disconnect the USB cable between your computer and printer.

The printer will now be able to communicate with HCC provided that it is connected to Wi-fi and the host computer is on.

After successfully onboarding the printer, delete the CAConfig.json file because it contains the user name and password.

Note: *Once a printer has been onboarded, it may take a couple of minutes to display in the HCC Device Dashboard.*

Industrial Printers

Use the printer’s web page to connect a supported industrial printer to HCC.

Requirements

- Up-to-date firmware installed on the printer
- Active printer network connection via wi-fi or local area network (LAN)
- HCC installed on your network and accessible from the printer

- Ports 8883, 21210,21211, 21212, 21213 across HCC and the printer must be open

Note: *For information about using the printer web page, updating the printer firmware, or setting up the network connection on your printer, please refer to your printer's user documentation.*

Recommended Settings

For Industrial printers in the PC/PD/PM/PX series, following these recommended settings will ensure that the printer stays connected with HCC, notifies HCC on occurrence of printer events, and responds to commands and device actions issued from HCC.

- Set the printer time to the accurate date and time. Verify that NTP Time Server is enabled and correctly set up to ensure accurate date/time.

Manually Onboarding an Industrial Printer

Follow these steps to manually onboard an industrial printer such as PC42 or PC43 in Operational Intelligence through HCC. The printer must have MR17 firmware version or higher installed. The "Connectivity Agent" option is disabled by default, so to onboard the printer, you must enable the Connectivity Agent and import a configuration file.

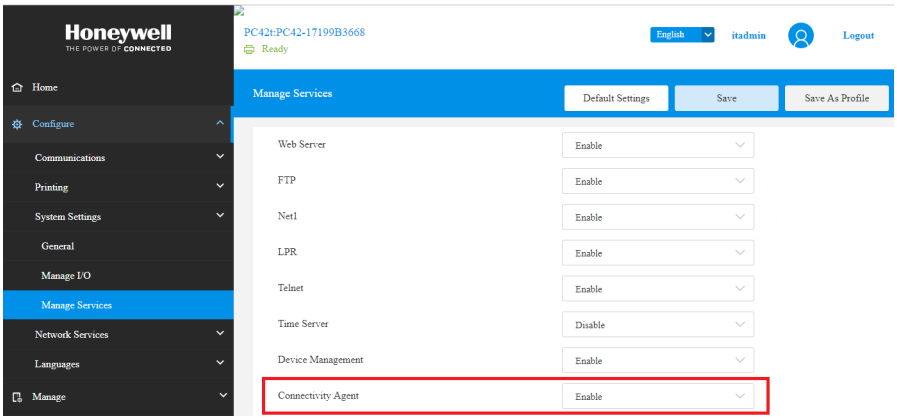
See Device Discovery and Onboarding for instructions on using HCC to discover and onboard printers on a network.

1. Create the required JSON configuration file for the device. See Create JSON Configuration File on page 9 for instructions.
2. Extract the saved zip file created in step 1. Enter the password when prompted.

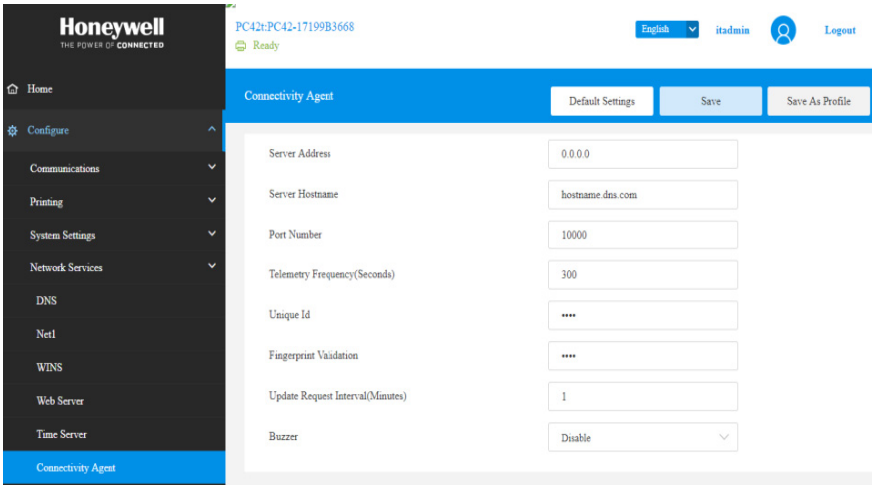
3. Open the extracted file with a text editor, such as Notepad. The file contents should look similar to the example below:

```
{
  "GatewayConfiguration": {
    "IpAddress": "xxx.xx.xx.xxx",
    "HostName": "xxx.xxxxx.xx.xxxxxx.com",
    "Port": 21210,
    "TelemetryFreq": 3000,
    "AssetFreq": 3000,
    "BarCodeStatFreq": 3000
  },
  "AuthenticationConfig": [
    {
      "UniqueId": "xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "SecureFingerPrint": "xxxxxxxxxxxxxxxxxxxxxxxxxxx"
    }
  ]
}
```

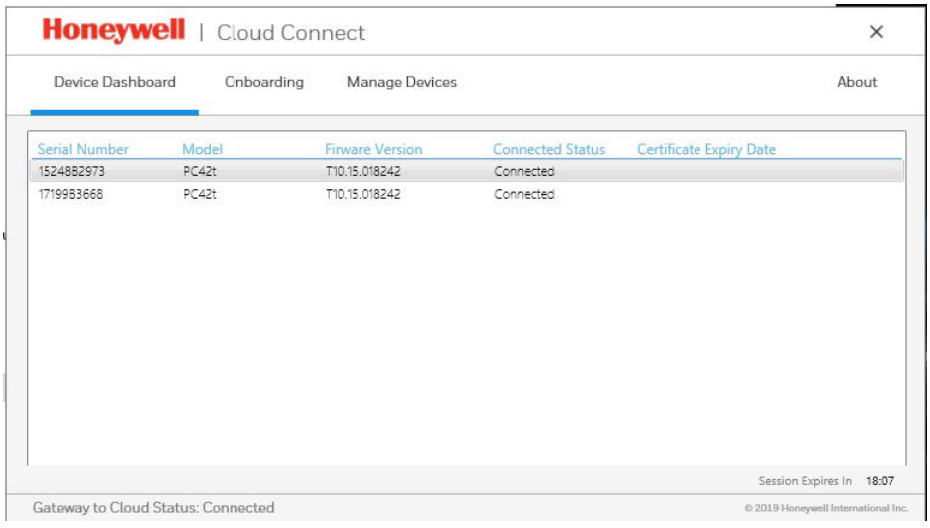
4. Access the printer's web portal using the IP address assigned to the printer.
5. Click **Configure > Network Settings > Connectivity Agent**.
6. Enter the following information into the web page from the HCC file you downloaded:
   - Server address
   - Server Hostname
   - Port number
   - Telemetry Frequency (Seconds)
   - Unique ID
   - Fingerprint Validation
7. Click **Save**.
8. Click **Configure > System Settings > Manage Services**.
9. Select **Enable** from the Connectivity Agent drop-down box. (Enabling the agent after updating the settings will ensure a new registration with the HCC gateway.)



10. Click the **Save** button to save the entered values.



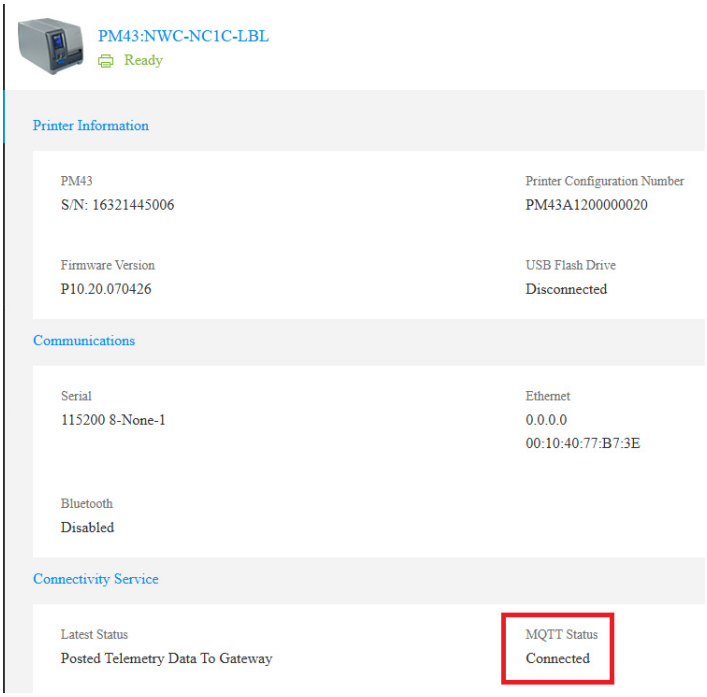
11. After the values are saved, the printer will be shown on the HCC screen in a few minutes with “Connected” status, and it will be automatically registered in the Operational Intelligence console.



The printer will start sending events, device detail information, and metrics to the Honeywell cloud. This information can be managed from Operational Intelligence.

12. Connect to the printer web page. On the Home page, verify that MQTT status is "Connected."

Sample Printer Web Page



CHAPTER

3 DEVICE DISCOVERY AND ONBOARDING

Overview

The HCC Discovery Tool is an application to discover mobile and industrial printers across multiple subnets, upgrade printers, and transfer Honeywell Cloud Connect (HCC) coordinates to onboard printers into the Operational Intelligence Cloud.

Before using the Discovery Tool to onboard printers, we recommend that you first follow the manual onboarding process for at least one device. See Manually Onboarding a Mobile Printer on page 12.

Before using the Discovery Tool to onboard multiple printers on a fresh HCC instance, verify that the printer is connected to HCC through both the HCC UI and the printer web page and that it is reporting in Operational Intelligence. This helps confirm that network connectivity between the various components is configured correctly. In the HCC UI, the printer should be displayed as Connected, and the MQTT connection status on the printer web page should also show as connected. Refer to your printer user guide for instructions on connecting to the printer web page.

Prerequisites

- Honeywell Cloud Connect (HCC) installed and registered
- Network should allow ICMP ping request and response across HCC and Printer IP ranges provided
- Ability to ping printer IP address from HCC system among the IP address ranges provided as input
- HCC and devices should be on the same network. When devices are in a different Subnet, the network group should allow the following ports:
  From devices to HCC: Default 8883, 21210, 21211, 21212, 21213, 21219,21221
  From HCC to Device : Default 8883,21221
  These default ports can be modified during installation.
- For Mobile Printer discovery and onboarding, port 9100 should be open.

- Set the printer time to the accurate date and time. Verify that NTP Time Server is enabled and correctly set up to ensure accurate date/time.
- For Mobile Printer discovery and onboarding, Input Mode should be either “Auto” or “DPL”.
- Approvals from IT team, if necessary. This utility initiates a query for every IP address within the IP address subnet range provided. These operations could be treated as a network intrusion.

File Configuration for Older Printer Firmware

The following steps must be performed if you are using printer firmware older than MR17. This step is required because printer firmware older than MR17 does not support HCC Coordinates in encrypted format. For newer versions, skip this step.

1. Navigate to the folder "C:\Program Files (x86)\Honeywell\HoneywellCloudConnect\HCC_UI.
2. Open the file com.honeywell.opintel.savana.ui.exe.config using Notepad or Notepad++.
3. Search for the parameter “EncryptSFPAndUId” and set the value to false. It should look like this:

   ```
   <add key="EncryptSFPAndUId" value="false"></add>
   ```
4. Save the file
5. Relaunch the HCC UI after making these changes.

Increase Discovery Service Ping Count

For HCC versions 3.0.1.168 or earlier, the default value of ping count is 2. When printers are on a switched network , this value needs to be set to 5.

1. Open C:\Program Files (x86)\Honeywell\HoneywellDiscoveryTool\Service\AutoDiscoveryService.dll.config.
2. Set the value for “PingCount” to 5:

   ```
   <add key="PingCount" value="5"></add>
   ```
3. Save the file.

Define Printer Subnet Range

Use the printer_subnet_range.csv spreadsheet to identify all printers within a specified subnet range. The .csv file is used to import the available subnet range(s). See Define Discovery Option Inputs.

Note: *HCC uses different templates for mobile and industrial printers. The template that is downloaded is based on the value selected in the Choose Printer Family drop-down list.*

1. On the HCC window, select a value in the **Choose Printer Family** drop-down list.
2. Click **Download Template** and save the .csv file to your local system.
3. For every subnet range, specify the Starting IP Address and Ending IP Address in the .csv file.

Note: *Samples are provided in the csv file in rows 3 and 4. Overwrite these rows with the actual subnet ranges.*

For industrial printers, enter the Username and Password. These are the credentials that will be used to login to the printer web page. Make multiple entries if the printer username and password are different for different printers within a given IP Address Range.

Note: *Delete this file after completion of onboarding as these files contain the printer's login credentials.*

4. Save.
5. Close Excel.

Note: *If you enter an incorrect password in the spreadsheet, HCC will return the message, "Printer web login account appears to be locked" during printer discovery. If the printer has firmware version MR10.22.03, HCC will return the message, "Default Password needs to be changed for the Printer."*

Define Discovery Option Inputs

Define the parameters that will be used to discover and onboard printers.

1. Launch HCC using **Run as Administrator**.
2. Click the **Onboarding** tab.
3. Under Gateway Configuration, select the **Gateway IP** address.
   - The **Gateway Host Name**, **Telemetry Frequency**, **S/W Update Query Interval**, and **Barcode Statistics Frequency** display the default values. You may update these if needed. The minimum value for **Telemetry Frequency** is 3600 seconds.
4. Click **ONBOARD PRINTERS**.

5. Select a value from the **Choose Printer Family** drop-down list. Based on the value selected in the Choose Printer Family drop-down list, either the **Browse Firmware** or **Browse Mboot** button will be enabled.

Note: *If printers in the field have already been updated with the recommended printer firmware version and/or Mboot version, you will not need to specify the firmware or boot file path. The operation will discover the printers and update the printer configuration to onboard them to HCC.*

The available options are:

- RP2\RP4: Discover\onboard RP2\RP4 mobile printers at the specified subnet ranges.
- RL3E: Discover\onboard RL3E mobile printers at the specified subnet ranges.
- RL4E: Discover\onboard RL4E mobile printers at the specified subnet ranges.
- PM23\PM43: Discover\onboard PM23\PM43 industrial printers at the specified subnet ranges.
- PM42: Discover\onboard PM42 industrial printers at the specified subnet ranges.
- PX940V\PX940A: Discover\onboard PX940V\PX940A industrial printers at the specified subnet ranges.
- PX6ie\PX4ie: Discover\onboard PX6ie\PX4ie industrial printers at the specified subnet ranges.
- PC23d\PC43d\PC43t\PD43: Discover\onboard PC23d\PC43d\ PC43t\PD43 industrial printers at the specified subnet ranges.
- PD45\PD45s\PX240\PX240S: Discover\onboard PD45\PD45s\PX240\ PX240S industrial printers at the specified subnet ranges.
- PM45\PM45c: Discover\onboard PM45\PM45c industrial printers at the specified subnet ranges.
- PC42t\PC42d: Discover\onboard PC42t\PC42d industrial printers at the specified subnet ranges.
- RP2\4 and RL3e\4e: Discover\onboard all mobile printers. Use this option when you have a combination of mobile printers deployed.
- PC, PD, PM, PX Series and RP2f/4f: Discover\onboard all industrial printers. Use this option when you have a combination of industrial printers deployed. This option does NOT consider onboarding PD45 , PD45s , PX240 , PX240s, PM45, and PM45c printers.

6. Click **Import Subnet Range(s)** then select the printer_subnet_range.csv file. The system displays the Sub Net Ranges for all sites that will be included in the update.
7. Identify the firmware file(s) to use. Click **Browse** then navigate to the firmware file location.

- If you selected a specific Printer Family, such as RP2\RP4 or PM23\PM43, select the firmware file.
- If you selected the Printer Family as “All Honeywell Mobile Printers” or “All Honeywell Industrial Printers,” select the path to a folder that contains all of the required firmware files. A firmware file is required for each of the printer families being onboarded at the site.

Note: *Firmware files must follow the required file naming convention. See the following tables for details.*

RP2\4 and RL3e\4e Printers

Printer Firmware	File Naming Convention	Example
RP2, RP4 Printer Firmware	File name starts with "SAV"	SAV_19.07_002_0409_S14418_2020-03-25.bin
RP2, RP4 Printer Mboot	File name starts with “Mboot_SAV”	MBoot_SAV_21.13.bin
RL3e	File name starts with “RL3e”	RL3e_18.06_0627_S14508_2020-04-16.bin
RL4e	File name starts with “RL4e”	RL4e_18.06_0627_S14508_2020-04-16.bin

Note: *For RP2 and RP4 printers, the mboot version must be 21.13 as printer mboot otherwise this operation will not update the printer firmware.*

PC,PD,PM,PX Series and RP2f/4f Printers

Platform Group	File Naming Convention	Example
PM23\PM23c\PM43 \PM43c	File name starts with "Phoenix_"	Phoenix_firmware-signed.bin
PM42	File name starts with "Phoenixlite_"	Phoenixlite_firmware-signed.bin
PX940V\PX940A	File name starts with "Hydra_"	Hydra_firmware-signed.bin
PX6ie\PX4ie	File name starts with "Atlas_"	Atlas_firmware-signed.bin
PC23d\PC43d\PC43t \PD43\PD43c	File name starts with "Kilimanjaro_"	Kilimanjaro_firmware-unsigned.bin
PM45\PM45c	File name starts with "Solo-t_"	Solo-t_firmware-unsingned.bin
RP2f\4f	File name starts with "Maui_"	Maui_firmware-signed.bin
PX45\PX65	File name starts with "Bora_"	Bora_firmware-signed.bin

Note: *PC42t, PC42d, PD45\PD45S\PX240\PX240s printers do not support printer firmware update over network, so there is no option to update the printer firmware.*

8. If the host name resolution is unavailable and the system is on multiple IP addresses, choose a value from the **Select IP Address** drop-down list to indicate where printer devices and HCC are connected.
9. Select the operation type:
    - **Discover Devices**: Discovers printers on the network, but the printers are not automatically onboarded. On completion of discovery, you can select the desired printer(s) then click the **Onboard Devices** button to onboard only the chosen devices.
    - **Onboard Devices**: Discovers and onboards all printers on the network.
10. Choose when to perform the update.
    - **Start Now**: Performs the update immediately.
    - **Schedule At**: Performs the update at a recurring interval.
      Choose the **Start From** and **End By** dates to define the range of dates on which discovery and onboarding will be initiated.
      Select the **Start Time** to indicate when HCC should begin to perform the update. Choose the **End Time** to indicate when HCC should stop attempting to discover printers. The tool will attempt to discover and onboard printers until either the end time is reached or all printers for the specified IP address have been onboarded.

Note: *Setting the Start and End Times ensures that HCC will not try to update printers during hours they may be in use.*

11. Click **Start**.
    HCC displays a list of printers that have been discovered and indicates the status of the operation.

Note: *To manually end the discovery process before the End Date/Time, click the* ***Stop*** *button.*

12. When the operation completes, the system displays the message, “Discovery Completed : Total Devices <x>.”

Status	Description	Comment
Open	Onboarding not yet started	Printer discovered at given IP Address. Printer will be onboarded if printer state remains at 'Non Enrolled' state
In Progress	Firmware update initiated Firmware file transfer in progress Firmware file transfer completed Firmware update in progress	State while transferring firmware file.
In Progress	Configuration update in progress Configuration updated	Tool is in the process of updating printer with HCC Coordinates (HCC IP Address, UID & FP). Note: If the status remains as Config Update for more than one hour within the scheduled time, refer to the Troubleshooting section Onboarding Fails for possible solutions.
Success	Device onboarded Device already onboarded	Printer successfully onboarded.
Failed	Due to network issue, failed to transfer firmware file. Due to network issue, failed to update configuration. Due to network issue, failed to onboard device. Failed to transfer firmware due to invalid credentials or network issues. Due to network issue, failed to upgrade firmware. Invalid firmware file. Firmware file not found.	Possible causes: Network failures at various stages. User did not provide the firmware file.
Failed	Default Passwords needs to be changed for the printer.	See Message Shows Default Printer Password Needs to be Changed on page 39 for troubleshooting actions.
Failed	Printer web login account appears to be locked.	The password may have been entered incorrectly in the printer_subnet_range.csv spreadsheet. See Define Printer Subnet Range on page 21 for instructions on uploading the spreadsheet.

Scheduling Discovery and Onboarding

This section provides additional information on scheduling discovery and onboarding. You can schedule the dates and times that HCC will attempt to discover and onboard devices. The scheduling function allows you to attempt to discover and onboard devices over multiple dates during only specified hours. By limiting activity to only a specified time period, you can avoid updating firmware while printers are likely to be in use.

You can define the following parameters:

- **Start From** - The first date that HCC will attempt to discover and onboard printers in the selected subnet range(s).
- **End By** - The date that HCC will stop attempting to discover and onboard printers in the selected subnet range(s).

  If the Start From and End By dates are the same, discovery will occur on a single date. If the dates are different, discovery will occur on each defined date during the defined time range (Start Time/End Time).
- **Start Time** - The time (HH:MM) that HCC will begin to discover and onboard printers on each date in the defined date range.
- **End Time** - The time that HCC will stop attempting to discover and onboard printers. The End Time can be on the same day as the Start Time or on the following day so that the process runs overnight. Note that HCC will stop attempting to discover devices at midnight on the End By date regardless of the defined End Time. See the examples below to clarify.

The following table provides examples of discovery and onboarding schedules.

Scheduling Examples

Start From	End By	Start Time	End Time	Behavior
11/15/2020	11/17/2020	05:00PM	09:00PM	Zero Touch Onboarding runs three cycles: 1. 11/15/2020 from 5:00PM to 9:00PM. 2. 11/16/2020 from 5:00PM to 9:00PM. 3. 11/17/2020 from 5:00PM to 9:00PM.
11/15/2020	11/17/2020	05:00PM	06:00AM	Zero Touch Onboarding runs three cycles: 1. 11/15/2020 from 5:00PM to 11/16/2020 at 6:00AM. 2. 11/16/2020 from 5:00PM to 11/17/2020 at 6:00AM. 3. 11/17/2020 from 5:00PM to 11/17/2020 at 11:59PM.
11/15/2020	11/15/2020	05:00PM	06:00AM	Zero Touch Onboarding runs one cycle: 1. 11/15/2020 from 5:00PM to 11/16/2020 at 11:59PM.

CHAPTER

4 HANDHELD SCANNERS AND WIRELESS BARCODE SCANNERS

Connected handheld scanners and wireless barcode scanners (wearable mini computers) will send events, device information and metrics to the Honeywell cloud through the HCC gateway. To communicate with HCC, handheld scanners must be connected to host computers. Wireless barcode scanners must be connected to a wireless network.

Connecting Wireless Barcode Scanners to Wi-Fi Network

Follow these steps to connect wireless barcode scanners to a Wi-Fi network.

1. Open the HCC app.
2. Click the **Onboarding** tab.
3. Make sure **Wi-Fi Settings** is enabled.
4. Specify the settings.
5. Click **SAVE AS FILE** or **GENERATE BARCODE**.

Note: *In this case, the Wi-Fi Username and Wi-Fi Password are presented in plain text. Users should delete the file or scanner output immediately after usage to avoid exposing Wi-Fi credentials.*

Onboarding Wireless Barcode Scanners

Follow these steps to onboard wearable mini computers.

1. Connect the device to the host computer.
2. Open the HCC app.
3. Click the **Onboarding** tab.
4. If **Wi-Fi Settings** is enabled, turn it off using the toggle button.

5. To change the frequency at which HCC sends data to the cloud, tap the **Gateway Configuration** toggle button to enable editing and enter the desired frequencies.
6. Click **GENERATE BARCODE**.
7. To change bar code type or size, use the drop-down lists then click **Apply**.
8. Click **Print** to print the bar code or click **Download** to save the bar code as a .png image file.
9. Scan the bar code with the device that you want to connect to HCC.

Onboarding Handheld Scanners

Follow these steps to onboard handheld scanners using the Scanner Agent application.

About Scanner Agent

Scanner Agent is a Windows-based application that functions as a data collection agent, update facilitator, and communication bridge between handheld scanners and Honeywell's enterprise device management infrastructure, i.e., HCC/ Operational Intelligence. The application must be installed and run on the same host PC to which a Honeywell handheld scanner is physically connected via serial port.

Scanner Agent PC and Network Requirements

You must have a host computer with the following:

- Scanner Agent must be installed on the machine where the scanner is physically connected to the PC via a USB cable.
  Scanner Agent can be downloaded from the Honeywell software download website at honeywell.com/PSSsoftware-downloads in the **Software > Software and Tools > Device Management > OI Agent – Handheld** directory.
- Microsoft Windows 10/Windows 11 Pro operating system. Scanner Agent and HCC are not compatible with Linux machines.
- HCC must be installed on the machine.
- HCC registration must be completed through Op Intel.
- See Requirements on page 1 for all requirements for the host computer.

The machines with HCC and Scanner Agent installed should be on the same network. When Scanner agents are in a different subnet, the network group should allow the following ports:

- From Scanner Agent to HCC: Default 8883, 21210, 21211, 21212, 21213, 21219, 21221

- From HCC to Scanner Agent: Default 8883, 21221

These default ports can be modified during HCC installation.

Using HCC System Created JSON Configuration File

1. Login to the system where HCC is installed.
2. Follow the steps in Create JSON Configuration File on page 9 to create the JSON configuration file.
3. Extract the saved zip file that was created. Enter the password when prompted.
4. Open the extracted file with a text editor, such as Notepad. An example is shown below:

```
{
"GatewayConfiguration": {
"IpAddress": "xxx.xx.xx.xxx",
"HostName": "xxx.xxxxx.xx.xxxxxx.com",
"Port": 21210,
"TelemetryFreq": 3000,
"AssetFreq": 3000,
"BarCodeStatFreq": 3000
},
"AuthenticationConfig": [
{
"UniqueId": "xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
"SecureFingerPrint": "xxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
]
}
```

Note the UniqueId, SecureFingerPrint, HostName, and related ports from this step to be used for Scanner Agent silent installation in the following section.

Scanner Agent Silent Installation

1. Refer to the parameters in the JSON configuration file to construct the command as below. Replace the Hostname, IP address, UID, and SFP with the values from the file.

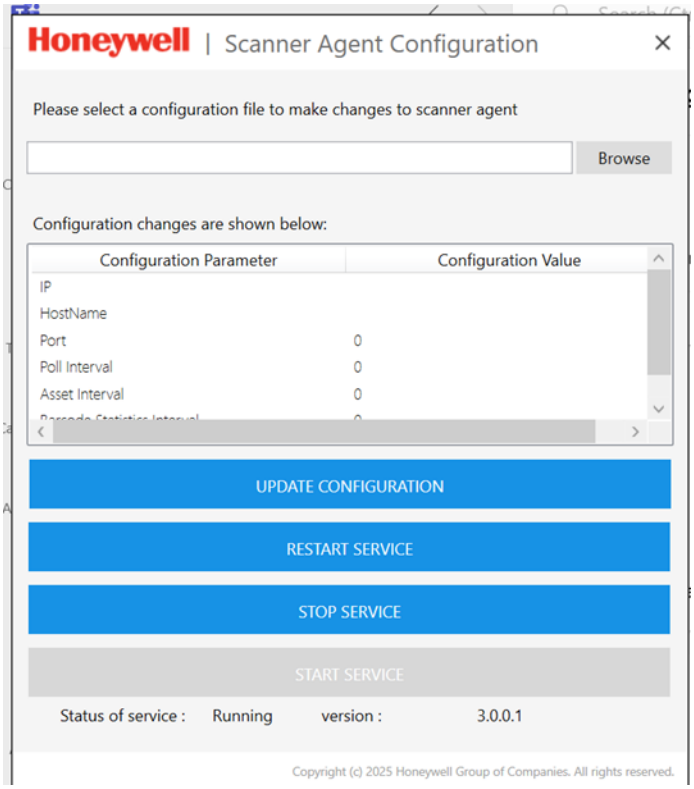
When HCC Host Name can be Resolved at Scanner Agent:

```
Setup.exe /s /v" /qn HOSTNAME=HON-8Z4KDN3.honeywell.com
PORT=21210 UID=3ddb1012-897e-4fcf-af8c-0b51964192f2
SFP=053D9E631C82BCF540E84BB0CFFEFBE2358FBDB6 POLLINTERVAL=21600
BARCODEINTERVAL=3000 ASSETINTERVAL=3000"
```

When HCC Host Name cannot be Resolved at Scanner Agent:

```
Setup.exe /s /v" /qn IPADDRESS=192.168.0.117 PORT=21210
UID=3ddb1012-897e-4fcf-af8c-0b51964192f2
SFP=053D9E631C82BCF540E84BB0CFFEFBE2358FBDB6 POLLINTERVAL=21600
BARCODEINTERVAL=3000 ASSETINTERVAL=3000"
```

2. Extract Setup.exe from the ScannerPlugin_XX.XX.XX.XX.zip package to a local directory.
3. Open a Command Prompt with Administrator privileges and run the command from step 1.
4. After successful installation, you can view Windows services and verify that Scanner Agent service is installed and running. You can also launch Scanner Agent Configuration to verify.



5. In the HCC Device Dashboard, you can view the scanner serial number connected to scanner agent as online. The scanner will also be available to view in Operational Intelligence.

Asset Updates from Op Intel

When an asset update is initiated from Operational Intelligence, if the targeted scanners are not reachable through HCC, HCC retains the update details for up to four hours. The scanner agent will retrieve and apply the updates when it comes back online. If the scanner remains offline for more than four hours, HCC will abort the updates and notify Op Intel that the updates were aborted.

Device Actions

Operational Intelligence supports the following device actions:

- Reboot: Reboots the scanner base.
- Pull Agent Log: Retrieves agent logs from the scanner agent system. After issuing this command, select **Device Administration > Diagnostic Files** from the Op Intel menu to obtain the log file. This process may take up to one minute.
- Pull Device Configuration: Retrieves the scanner configuration. After issuing this command, select **Device Administration > Diagnostic Files** from the Op Intel menu to obtain the log file. This process may take up to one minute.
- Get Device List: Retrieves the serial numbers of connected scanners and scanner bases, along with the Scanner Agent version. The information is displayed in the Device Event view.

CHAPTER

5 TROUBLESHOOTING

This chapter provides information on problems that users may encounter and gives possible solutions to those issues.

If you require assistance from Customer Support, refer to HCC Troubleshooting/ Service Debug Logs on page 35 for instructions on collecting debug logs that can be shared with the support team.

HCC Troubleshooting/Service Debug Logs

This section describes how to enable HCC service debug logs and collect the logs to troubleshoot connectivity issues. For troubleshooting purposes, you will need to change the logging configuration to Debug mode. Once enabled, replicate the issue and gather the resulting log files. The log files can be shared with Customer Support to identify and resolve the issues.

Setting the Service Debug Log Level

Follow these steps to enable HCC Service Debug Logs.

Set the Debug Log Level for HCC Back-end Services

1. Set HCC Service to debug.
    a. Navigate to <InstallationPath>\Honeywell\HoneywellCloudConnect\HCC_Service.
    The default installation path is: C:\Program Files (x86)\Honeywell\HoneywellCloudConnect).
    b. Open HCCService.exe.config in a text editor.
    c. Locate the <root> node and find the level value key.
    d. Change the default value from ERROR to DEBUG.
    e. Save the file.
2. Set HCC Sentience to debug.

a. Navigate to <InstallationPath>\Honeywell\HoneywellCloudConnect\Hcc_Sentience.
b. Open SentienceGrpcServer.exe.config in a text editor.
c. Locate the <root> node and find the level value key.
d. Change the default value from ERROR to DEBUG.
e. Save the file.

Depending on the type of issue you are troubleshooting, perform the following additional actions.

Set the Debug Log Level for HCC Device Discovery and Onboarding Services

If you are troubleshooting Device Discovery and Onboarding failures:

1. Navigate to <InstallationPath>\Honeywell\HoneywellDiscoveryTool\Service.
2. Open the file log4net.config in a text editor.
3. Locate the <root> node and find the level value key.
4. Change the default value from ERROR to DEBUG.
5. Save the file.

Set the Debug Log Level for HCC UI

If you are troubleshooting HCC UI Login or HCC Registration issues:

1. Navigate to <InstallationPath>\Honeywell\HoneywellCloudConnect\HCC_UI.
2. Open the file com.honeywell.opintel.savana.ui.exe.config in a text editor.
3. Locate the <root> node and find the level value key.
4. Change the default value from ERROR to DEBUG.
5. Save the file.

After you update the Debug Log Levels, restart the HCC services to apply the new log levels.

Note: *Revert the configuration values back to ERROR after completing your troubleshooting to prevent excessive disk usage.*

Collect Troubleshooting Logs

Follow these steps to collect the Service Debut Logs.

1. Locate the log folder. The default directory is C:\Program Files (x86)\Honeywell\HoneywellCloudConnectLogs.

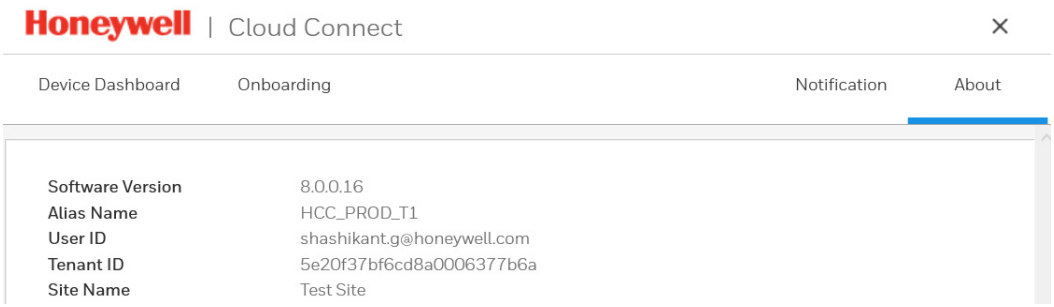
Note: *If a custom installation path was used, navigate to the specified folder.*

2. Compress the files. Select all files within this folder, right-click, and send them to a zipped (compressed) folder.
3. Send the resulting zip archive to the Customer Support team.

   In addition to the zip archive, include this additional information:

   - Windows Server version on which HCC is installed
   - Screen shot of the HCC About screen. This will help Customer Support to determine the HCC ID, HCC version, and tenant details.

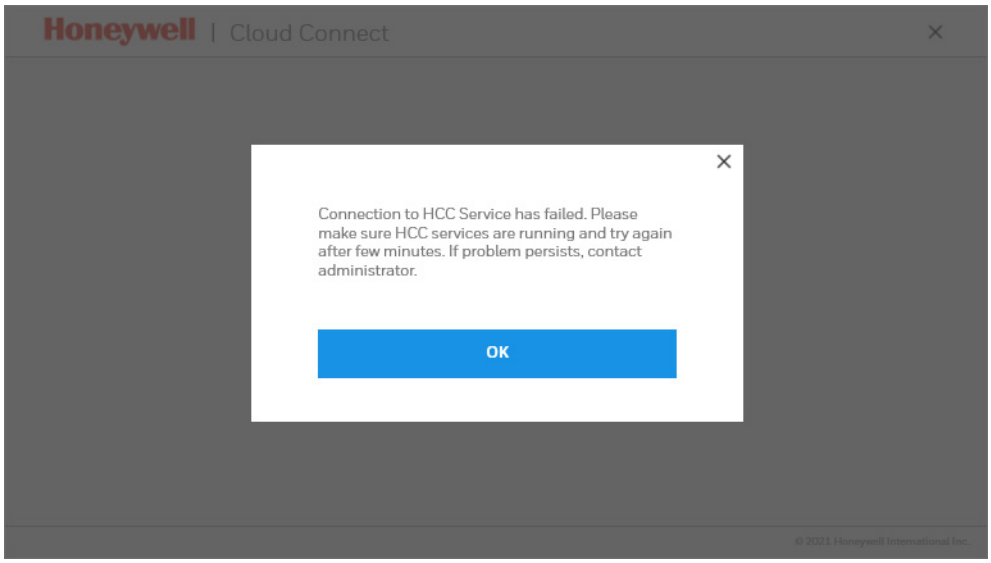
Sample HCC About Screen



HCC User Interface

Connection to HCC Services Failed

Issue: The HCC User Interface displays the message “Connecting to Services” then displays “Connection to HCC services has failed.”



Possible Cause: One or more HCC services are not running.

Solution: Follow these steps:

1. Ensure that all of the services below are available:
   - HccAPIInfoService
   - HccAssetManagmentService
   - HccCacheEngine
   - HccDataEngine
   - HccEnrollmentService
   - HccEventService
   - HccSentConnectService
   - HccTelemetryService
   - HccWatchDogService
2. Restart the service “HccCacheEngine”.
3. Restart the service “HccDataEngine”.
4. On successful restart, launch the HCC UI from the desktop.

Username and Password Prompt not Displayed

Issue: After clicking the Sign In button on the HCC UI, HCC fails to display the dialog prompting Username and Password.

Possible Cause 1: Required URLs are not whitelisted.

Solution: See Whitelist URLs on page 3 for a list of URLs that should be whitelisted to allow proper communication for HCC and Operational Intelligence.

Possible Cause 2: The latest Windows Security Updates have not been installed.

Device not Shown in Op Intel Portal

Issue: After a device has been onboarded through HCC, it is not shown in the Operational Intelligence user interface.

Possible Cause: Required URLs are not whitelisted.

Solution: See Whitelist URLs on page 3 for a list of URLs that should be whitelisted to allow proper communication for HCC and Operational Intelligence.

Printers

Onboarding Fails

Issue: Users are able to login to the industrial printer web page from the HCC system indicating HCC and printer communication, but manual printer onboarding fails or Zero Touch onboarding stays at “In Progress - Configuration updated” for longer than one hour.

Possible Cause: Firewall restrictions on ports used for communication. Firewall exceptions must be in place for these ports: 8883, 21210, 21211, 21212, 21213, 21215, 21219.

Solution: Work with the IT team to open the recommended ports between HCC and the devices.

Printer Status Incorrectly Shown as Online

Issue: HCC UI/Sinaps display shows device status as online even though the printer is powered down or taken out of the network.

Solution: The system is functioning as designed. Device status is marked as offline based on a query to the device at the defined Telemetry interval (default interval is 6 hours). Until that interval, device status will continue to be shown as online. No user action is required.

Message Shows Default Printer Password Needs to be Changed

Issue: HCC displays the message, “Default password needs to be changed for this printer.” This can be caused by a change issued in firmware MR10.22.03 that prevented Op Intel from onboarding printers still using the factory default password.

Solution: One of the actions below is required for HCC to continue onboarding of these devices.

- Update the printer to MR10.22.04 or later. Firmware version MR10.22.04 corrects this issue.
- Update the password for the printer using the printer web page to continue onboarding with HCC seamlessly. Refer to the printer user guide for instructions.

Scanners

Device not Detected

Issue: The device is not detected.

Possible Cause: REM interface is not enabled.

Solution: Ensure that the device has REM interface enabled.

Enable the **REMIFC1** on the device by scanning the following barcode:



After performing this step, the device should show as connected in the HCC UI dashboard.

Honeywell
855 S. Mint St.
Charlotte, NC 28202

automation.honeywell.com

HCC-EN-UG-01 Rev U
9/26