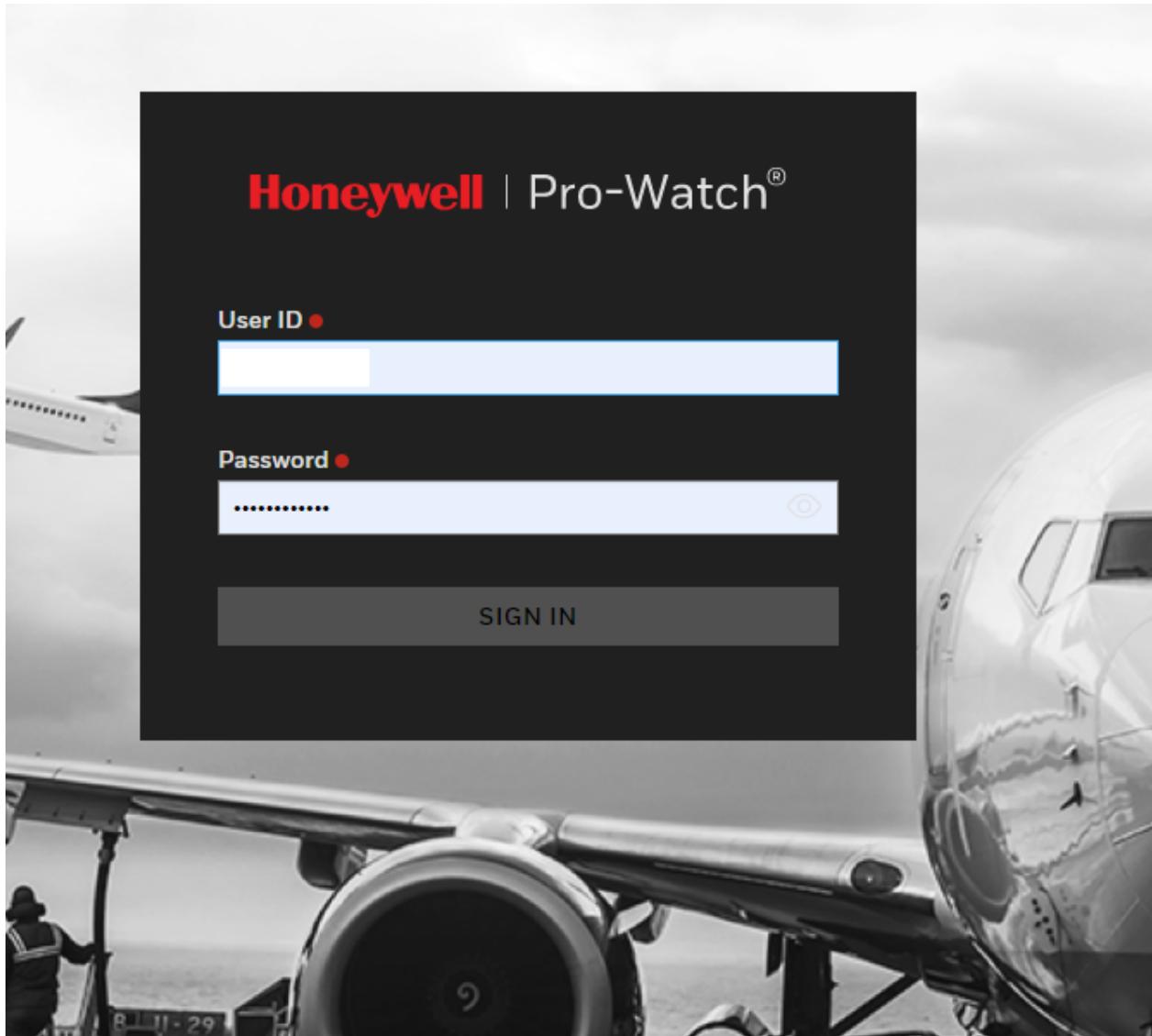


Honeywell

Pro-Watch Intelligent Command

5.0

800-12235V17 | May 2020



User Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

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

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 © 2020 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidec.com

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.

Copyright © 2020 Honeywell. All rights reserved.

Pro-Watch® Web Client is a registered trademark of Honeywell, Inc. All other product and brand names are the service marks, trademarks, registered trademarks or registered service marks of their respective owners. Printed in the United States of America. Honeywell reserves the right to change any information in this document at any time without prior notice.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation. Windows Server is a trademark of Microsoft Corporation.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met.

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Binaries, source code and any other parts of this distribution may not be incorporated into any software licensed under the terms of the GNU General Public License (GPL) or the GNU Lesser Public License (LGPL). Binaries, source code and any other parts of this distribution may not be incorporated into any software licensed under any license requiring source code disclosure of derivative works.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

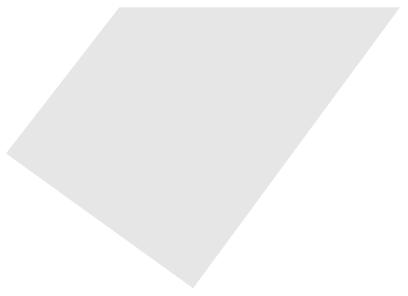
Ordering Information

Please contact your local Honeywell Access Systems representative or visit us on the web at <http://www.honeywellintegrated.com/> for information about ordering.

Feedback

Honeywell Access Systems appreciates your comments about this manual. Please visit us on the web at <http://www.honeywellintegrated.com/> to post your comments.

TABLE OF CONTENTS



Chapter 1 Overview

1.1 Pro-Watch Intelligent Command	2
1.2 Purpose of This Document.....	2
1.3 Audience	2
1.4 Pro-Watch.....	2
1.5 Pro-Watch Intelligent Command Web Client	3
1.6 System Specifications	4
1.7 Reference Documents	5
1.8 System Specifications.....	6
1.8.1 Recommended Deployment Model	6
1.8.2 Environment Recommendations - Browser	6
1.9 Pro-Watch Intelligent Command Installation Prerequisites.....	7
1.9.1 Frameworks & Software:	9

Chapter 2 Pro-Watch Web Client

2.1 What's New in Pro-Watch Intelligent Command 5.0	12
2.2 IMPORTANT - Critical Notes	12
2.3 Supported Web Browsers.....	12
2.3.1 SigPlusWeb Plug-In for Google Chrome.....	12
2.4 Prerequisites for the Client Machine	13
2.5 Supported Hardware	13
2.6 Security Certificate Requirement	13
2.7 Web Client User Account Prerequisites	13
2.7.1 Create a Valid Pro-Watch User Account.....	13
2.7.2 Assign Web Client Workstation to the User Account.....	13
2.7.3 Enable Your Web Password	14
2.7.3.1 Setting the Web Password.....	15
2.7.4 Grant Web Badge Maintenance Functions	15
2.8 Pro-Watch Web Client Login	17
2.9 Home Page.....	19
2.9.1 Home Navigation Links	20
2.9.2 Time out for Session	25
2.10 Modules	25
2.11 Badging.....	26
2.11.1 Adding a Badge Record.....	26
2.11.1.1 Adding an Individual	26
2.11.1.2 Cards Tab.....	28
2.11.1.3 Assets Tab	31

2.11.1.4 Activity Log Tab	31
2.11.2 Adding People in Bulk.....	32
2.11.3 Adding a Group.....	33
2.11.3.1 Notes Tab.....	34
2.11.4 Editing a Badge Record	35
2.11.5 Editing a Badge Image	35
2.11.6 Deleting a Badge Record.....	39
2.11.7 Searching for a Badge	39
2.11.8 Advanced Search Filters	40
2.11.9 Adding a New Custom Filter	40
2.11.10 Adding Badges in Bulk.....	42
2.11.11 Adding a New Card	44
2.11.12 Dependencies Between PW Windows and Web Applications....	50
2.12 Alarms.....	51
2.12.1 Alarm Management	51
2.12.1.1 New features	51
2.12.2 Acknowledging and Clearing Alarms	51
2.12.3 Managing the Columns of the Alarms Table	52
2.12.4 Freezing and Unfreezing Alarms.....	53
2.12.5 Acknowledging an Unacknowledged Alarm.....	53
2.12.6 Alarm Camera View.....	54
2.12.7 Actions	56
2.12.7.1 Masking and Unmasking	57
2.12.7.2 Alarm Landing Screen	59
2.12.8 Acknowledging Workflow-Associated Alarm(s)	62
2.12.8.1 Acknowledging a Workflow-Associated Alarm	62
2.12.8.2 Acknowledging a Workflow-Associated Rolled-Up Alarm ...	63
2.12.8.3 Acknowledging Multiple Alarms	65
2.12.9 Clearing Incident Associated Alarm(s)	67
2.12.9.1 Clearing an Alarm Which Has an Open Incident Ticket.....	67
2.12.9.2 Clearing a Rolled-Up Alarm with Associated Incidents.....	67
2.12.9.3 Clearing Multiple Acknowledged Alarms or All Alarms.....	68
2.12.10 View Rollup Details	68
2.13 Events	70
2.13.1 Pausing Events.....	71
2.13.2 Filtering Events	72
2.13.2.1 Filtering by Message Type	72
2.13.2.2 Filtering by Text Search.....	73
2.13.3 Clearing Events	73
2.13.4 FAQs - Troubleshooting and Functional Workarounds.....	74
2.14 Reports	75
2.14.1 Report Terminology.....	76
2.14.2 Report Limitations	76
2.14.3 Add, Edit or Delete a Report	76
2.14.4 View or Run a Report.....	77
2.14.5 Printing a Report.....	78
2.14.6 Exporting a Report.....	78
2.15 Settings	80
2.15.1 People & Group (Badging) Settings	81
2.15.2 Workflow Settings	82
2.15.2.1 Creating a New Workflow.....	82
2.15.2.2 Editing a Workflow.....	84

2.15.2.3 Deleting a Workflow.....	84
2.15.2.4 Importing a Workflow	84
2.15.2.5 Associating Workflows at the Event Level	85
2.15.2.6 Associating Workflows at the Point Level.....	88
2.15.3 Reports Settings	91
2.15.3.1 Reports General Settings.....	91
2.15.3.2 Reports Email Settings	92
2.16 Simplified Device Maintenance	93
2.16.1 Recommendations for Firmware and Password Updates.....	93
2.16.2 Firmware Update.....	93
2.16.2.1 Camera Hardware Configuration	93
2.16.2.2 Not Supported.....	97
2.16.2.3 NVR and Pro-Watch Upgrade Notes	98
2.16.2.4 Displaying Current Versions	98
2.16.2.5 Cameras	98
2.16.2.6 Display All Cameras.....	100
2.16.3 Uploading a Camera's Firmware	101
2.16.3.1 Search Function.....	109
2.16.3.2 Dynamic Filtering	110
2.16.4 To Delete Firmware.....	111
2.16.5 Multi-User Known Issue.....	112
2.16.6 Passwords.....	113
2.16.6.1 Updating a Password	115
2.16.6.2 Filtering Cameras for Password Updates	118
2.16.7 Events Under Simplified Maintenance	119
2.17 Enterprise Manager	120
2.17.1 Creating an Enterprise Server.....	121
2.17.2 Selecting Table Groups	122
2.17.3 Creating a Region Server.....	122
2.17.4 Selecting Table Groups	124
2.17.5 Deleting the Enterprise	124
2.17.6 Updated Enterprise Screen.....	125
2.18 Incidents.....	126
2.18.1 Incident Permissions.....	126
2.18.2 Incidents Landing Page.....	127
2.18.3 Incident Management Screen.....	128
2.18.4 Creating an Incident.....	129
2.18.5 Responding to an Incident.....	131
2.18.6 Activity Log	133
2.18.7 Dismissing an Incident.....	134
2.19 Maps	135
2.19.1 Map Permissions.....	135
2.19.2 Adding (Level) Maps to Pro-Watch Intelligent Command.....	135
2.19.3 Generating Maps.....	137
2.19.4 Configuring Devices on the Map	140
2.19.5 Viewing Video and Alarms on Maps Device Popup.....	141
2.19.6 Controlling Zoom Level.....	141
2.19.7 Controlling the Video Playback	143
2.19.8 Removing a Device from the Map	143
2.19.9 Displaying Maps in Web Client	144
2.19.10 Live Camera View	145
2.19.11 Zoom Level	145

2.19.12 Playback.....	146
2.19.13 Acknowledging the Alarms in Map	147
2.19.14 Clearing the Alarms in Maps	147
2.19.15 Browsing by Location.....	148
2.19.16 Browsing by Map Objects	149
2.20 Known Issues and Recommendations, System Settings	150
2.20.1 Installation.....	150
2.20.2 Firmware Inventory file store	150
2.20.3 If you face any Login issues:.....	150
2.20.3.1 Possible resolutions:.....	151
2.20.4 If you get a "Certificate Error" at Login:	151
2.20.5 If VMS and Pro-Watch data are out of sync:.....	151
2.20.6 Unable to add firmware inventory file	151
2.20.7 Other Issues and Recommendations:.....	151
2.21 Honeywell Camera Models Supported for Simplified Device Maintenance....	153

Overview

In this guide...

[Pro-Watch Intelligent Command](#)

[Audience](#)

[Use of Symbols](#)

[Pro-Watch](#)

[Pro-Watch Intelligent Command Web Client](#)

1.1 Pro-Watch Intelligent Command

An integral part of the new Pro-Watch suite is Pro-Watch Intelligent Command (PWIC), a web-based, thin client option that provides significant reductions in operational costs.

Pro-Watch Intelligent Command is a common user interface that provides valuable enhancements to security systems. These ensure compliance with stringent industry regulations. For instance, Intelligent Command enables operators to respond rapidly and effectively to alarms or incidents by providing a Standard Operating Procedure (SOP) that shows the process that should be followed. This reduces both compliance exceptions and security risks.

The Pro-Watch interface gives users a stronger situational awareness of the whole security system through a single map view of all the access, video and intrusions solutions. It provides actionable intelligence that enhances the protection of people and property. It's an intuitive approach to combining video and access control that enables alarms to be associated with the corresponding video.

1.2 Purpose of This Document

This document guides you in setting up a beta test environment with the Pro-Watch Intelligent Command and introduces you to the new features in it.

1.3 Audience

This guide is written for the Pro-Watch system administrators, Pro-Watch Badging Operators, and Pro-Watch Reporting Users.

Pro-Watch 5.0 web interface offers new components such as:

- Alarm Monitoring Admin Module
- Events Module
- Enterprise Module
- Maps Module
- Incidents Module
- Maintenance Module
- Firmware Upgrade
- Password Change

1.4 Pro-Watch

The Pro-Watch platform is a complete access control system of hardware and software for small, mid-size, and global-enterprise sites. The user can configure sites that range from five users and 64 doors to an unlimited number of users and doors.

The Pro-Watch system supports Honeywell and third-party access control hardware and software, including panels, readers, intercom units, and CCTV equipment.

The supported Intercom units are:

- Command system servers GE200, GE300, GE700 and GE800
- Stentofon Alphacom via TouchLine (MPC) Protocol - AMC 07.60
- Stentofon Alpha Seven

There are two interfaces available for this product:

- An application-based interface
- A browser-based interface

These interfaces support both a server component and a client component.

This guide describes how to use the browser-based interface.

For information on the application-based product, see the Pro-Watch® Software Suite Release 5.0 User Guide.

1.5 Pro-Watch Intelligent Command Web Client

NOTE: If you are upgrading from Pro-Watch versions earlier than 4.3.5 to PW 5.0, all users with web passwords must reset their passwords.

The Pro-Watch Intelligent Command is a web based application that allows access to certain Pro-Watch functionalities remotely from any location within domain.

The functional hierarchy of the Pro-Watch Intelligent Command, Pro-watch Web API and Pro-watch Server are as follows:

1. The Pro-Watch Intelligent Command sends a request to the Pro-Watch Web API.
2. The Pro-Watch Web API interacts with Pro-Watch Server and processes the request.
3. Finally the result of request is sent back to the Pro-Watch Intelligent Command.

1.6 System Specifications

FEATURE	SMALL SYSTEM REQUIREMENT (FOR EACH WEB TIER & APP TIER SERVER)	LARGE SYSTEM REQUIREMENT (FOR EACH WEB TIER & APP TIER SERVER)
Recommended Processor	Intel® Xeon® processor E5 or E7 family 3.6 GHz or higher (24 cores or greater)	Intel® Xeon® processor E5 or E7 family 3.6 GHz or higher (32 cores or greater)
Recommended Operating System	Windows Server 2012/2016/2019 Standard	Windows Server 2012/2016/2019 Standard
Recommended Database System	SQL Server 2012/2014/2016/2017/2019	SQL Server 2012/2014/2016/2017/2019
Recommended PC Type (Server or Workstation)	Server hardware recommended	Server hardware recommended
Recommended System Memory (RAM)	24 GB minimum, 32 GB recommended	32 GB minimum, 64 GB recommended
DVD Drive	Yes	Yes
Hard Drives	Capacity, Speed, Interface:	Capacity, Speed, Interface:
	160 GB SSD or 7,200RPM or higher SATA or SAS	RAID Array 1: (OS or hardware based RAID 1) 160 GB SSD or 7,200RPM or higher SATA or SAS (SSD preferable) RAID Array 2: (Application Databases) (Hardware based RAID 5 or RAID 10) 300 GB 7,200RPM or higher SATA or SAS
Network connection	100Mbits/sec or greater, GB recommended	100Mbits/sec or greater, GB recommended
Video resolution	1920x1080 pixels; 24 bit color or higher	1920x1080 pixels; 24 bit color or higher
	Standard VGA Graphics Adapter (Display adapter)	Standard VGA Graphics Adapter (Display adapter)

¹ For a system to be considered small, the Pro-Watch system shall have less than 5 clients, no more than 128 online readers, less than 5000 historical events per day, and proper database maintenance conducted by the end user or servicing dealer. For a system to be large, it must have between 5000 and 50,000 historical events per day, between 128 and 512 online readers, between 5 and 15 client workstations, and proper database maintenance conducted by the end user or servicing dealer. If the system will have more than 50,000 events per day, exceed 512 online readers,

exceed 15 client workstations, or use Pro-Watch server side functions like anti-passback, event triggers and procedures, Real Time Data Transfer Utility, HSDK, etc. please consult Honeywell for custom server sizing.

² RAID technology is used for the larger system server – Disk sets 1 and 2. When several physical disks are set up to use RAID technology, the operating system will be installed on a single disk (OS installed on RAID1 mirrored set) and the Database and Storage on a separate disk (RAID 5 or 10 disk set).

³ To estimate database storage space, use the following approximations and add to the base DB size of 500MB:

- Badgeholder storage = (# of badgeholders) x (75KB)* estimate based on typical captured picture size
- Event history storage = (# of events per day) x (2.5 KB) x (# of days to retain in server)
- Audit history storage = (# of cardholder changes per day) + (# of system configuration changes per day)(# of events per day)(# of operator system changes per day)* (1.2KB) x (# of days to retain in server)

⁴ Honeywell highly recommends some type of removable media for daily database backups. Database backups should be removed from the server and stored in a safe, secure location so in the event of system failure this valuable data can be recovered. We recommend two or more removable media per server based upon end user processes. Alternatively, Honeywell system installers can engage the end-user's IT group to participate in some type of network backup program.

• **Important Notice** – These server and workstation hardware guidelines are intended for use as a reference only. The specifications are subject to changes due to market conditions, software updates, manufacturing changes, and other variables outside of our control. Honeywell recommends for planning based on system growth and expansion, operating system updates and upgrades, database engine updates and upgrades, end user system expansion, historical data retention requirements, and archive data storage requirements. Please consult with Honeywell as applicable for assistance

1.7 Reference Documents

- Pro-Watch 5.0 Software Suite User Guide, Doc # 7-901071V19
- Pro-Watch VMS User Guide

1.8 System Specifications

A recommended system specification and deployment model is given below.

1.8.1 Recommended Deployment Model

Server (boxes)	Services or Components	Build Recommendation
1	PW DB + VMS DB	
2	PW Core + PW Intelligent Command- Core Services	PW 5.0 Core: 12042, PW IC 5.0.0.174
3	PW Intelligent command-App Tier Services	PWIC 5.0.0.174
4	PW Intelligent Command-Web Services	PWIC 5.0.0.174
5	VMS Server	PW-VMS R650 Build 664
6	NVR Server	PW-NVR R6.5 Build 664

1.8.2 Environment Recommendations - Browser

Use Chrome (browser) latest version for Pro-Watch Intelligent Command web client.

1.9 Pro-Watch Intelligent Command Installation Prerequisites

The following prerequisites should be available in any target machine for the installer to continue and install successfully.

Installer will exit if any of the prerequisites are not available.

1. Turn ON the following Windows IIS features:

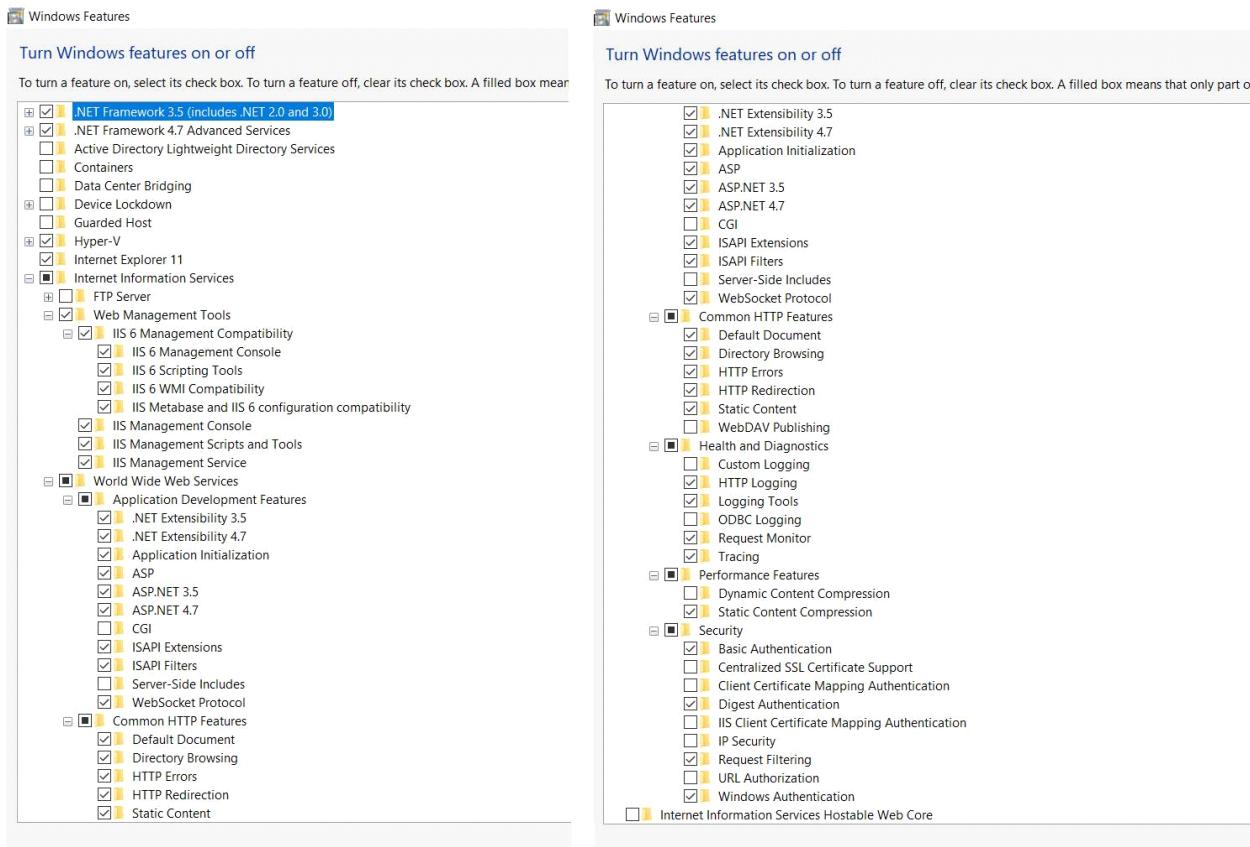
- IIS Metabase
- IIS Web Socket
- IIS Application Initialization
- IIS 6 WMI Compatibility
- IIS Windows Authentication
- IIS Basic Authentication
- IIS 6 Scripting Tools
- IIS 6 Management Console
- IIS Management Console
- IIS Management Scripts and Tools
- IIS Management Service
- IIS ASP.Net
- IIS Http Errors
- IIS Static Content
- IIS .NET Framework
- IIS Digest Authentication
- IIS Tracing
- IIS Request Monitor
- IIS Logging Tools
- IIS HTTP Logging
- IIS Directory Browsing
- IIS HTTP Redirection
- IIS Static compression

Note: Disable WebDAV settings in IIS.

Overview

Pro-Watch Intelligent Command Installation Prerequisites

2. Refer to the below image for the list of Windows IIS features to be turned ON:



3. Install the following software and frameworks:

- a. Dot Net Framework 4.7.1
- b. Dot Net Framework 4.8
- c. Dot Net Core Hosting Bundle 2.2.5
- d. Dot Net Core Hosting Bundle 3.1.1
- e. VC++ 2010 (x86) redistributable
- f. VC++ 2010 (x64) redistributable
- g. VC++ 2013 (x86) redistributable
- h. VC++ 2013 (x64) redistributable
- i. VC++ 2015-2019 (x86) redistributable
- j. VC++ 2015-2019 (x64) redistributable
- k. SQL Native Client 11
- l. Re-Write Software (rewrite_amd64_en-US.msi)

4. Ensure that Pro-Watch 5.0 core is installed first.

5. Net.Tcp Port Sharing Service.

1.9.1 Frameworks & Software:

- a. Dot Net Framework 4.8
- b. Dot Net Framework 4.7.1
- c. Dot Net Core Hosting Bundle 3.1.1
- d. Dot Net Core Hosting Bundle 2.2.5
- e. VC++ 2013 (x86) redistributable
- f. VC++ 2013 (x64) redistributable
- g. VC++ 2015-2019 (x86) redistributable
- h. VC++ 2015-2019 (x64) redistributable
- i. VC++ 2013 redistributable
- j. VC++ 2015-2019 redistributable
- k. SQL Native Client 11
- l. Re-Write Software (rewrite_amd64_en-US.msi)

Overview

Pro-Watch Intelligent Command Installation Prerequisites

Pro-Watch Web Client

In this guide...

[What's New in Pro-Watch Intelligent Command 5.0](#)

[IMPORTANT - Critical Notes](#)

[Supported Web Browsers](#)

[Prerequisites for the Client Machine](#)

[Supported Hardware](#)

[Security Certificate Requirement](#)

[Web Client User Account Prerequisites](#)

[Configuring the Browser Mode](#)

[Web Client User Account Prerequisites](#)

[Pro-Watch Web Client Login](#)

[Home Page](#)

[Modules](#)

[Badging](#)

[Alarms](#)

[Events](#)

[Reports](#)

[Settings](#)

[Simplified Device Maintenance](#)

[Firmware Update](#)

[Passwords](#)

[Enterprise Manager](#)

[Incidents](#)

[Maps](#)

[Known Issues and Recommendations, System Settings](#)

[Honeywell Camera Models Supported for Simplified Device Maintenance](#)

2.1 What's New in Pro-Watch Intelligent Command 5.0

Entire Pro-Watch Web UI components (Screens: Login, Alarm monitor, Event viewer, People & Badge, Reporting, Incident Workflow, Maps, Enterprise sync, Settings) are now updated with the latest **Honeywell dark theme**.

Here are some quick links to these new modules:

- [Alarm Management](#)
- [Video Integration](#)
- [Workflow Settings](#)
- [Incidents](#)
- [Maps](#)
- [Firmware Update and Password Update](#)
- [Known Issues and Recommendations, System Settings](#)

2.2 IMPORTANT - Critical Notes

Note: Web server workstation name must be registered in Pro-Watch Server.

Note: **Web Badging Field “Display Photo” is mandatory to display the Image Gallery in web.**

Note: **Badge holder photo/signature in Pro-Watch will only work in Print, if BLOB is kept a part of DB. It will not work if it’s in File Storage.**

Note: **Photo Capture not supported in IE. We recommend Google Chrome.**

Note: Other than Card, Assets and Activity Log tabs, **all other tabs are dynamically created**. By default Pro-Watch badge UI provides an “**Employee**” tab to collect Badge holder detail, but the Badge Administrators are free to change it the way they like.

2.3 Supported Web Browsers

The Pro-Watch Web Client supports

- **Recommended:** (Windows) **Google Chrome Version 53 or above.**

2.3.1 SigPlusWeb Plug-In for Google Chrome

1. In **Google Chrome** browser’s URL field, type **chrome://settings/content** and press the **Return** key to display Chrome’s **Plugins** page.
2. Find the **SigPlusWeb** plugin and select the “**Always allowed to run**” check-box right next to it. This will allow you to capture signature without being prompted for permission to run.

2.4 Prerequisites for the Client Machine

1. The end-user must install the following software on the client machine for the Pro-Watch web interface to work properly:
 - **Topaz Signature Pad** Web component (<http://www.topazsystems.com/Software/download/sigplusweb.htm>) for capturing signatures in the Badge Module. Download the sigplusweb_npapi.exe file for correct web operation. This is available from the Topaz website.
 - **Adobe Flash Player** (<http://get.adobe.com/flashplayer/>)
2. “Display internet sites in Compatibility View” option must be disabled.

2.5 Supported Hardware

- Any Honeywell-recommended webcam or Logitech Webcam c110.
- Topaz Signature Pad Model: T-L460-HSB-R.

2.6 Security Certificate Requirement

You need to have a security certificate to use the Pro-Watch Web Client properly. Please consult your system administrator for obtaining an appropriate security certificate.

2.7 Web Client User Account Prerequisites

Make sure you do the following before attempting to log in.

Note: Web User permissions are granted and revoked at the Class or User level in the thick client. Certain permissions are required for various administrative tasks.

2.7.1 Create a Valid Pro-Watch User Account

Refer to the *Pro-Watch Software Suite 5.0 User Guide*, Chapter 58 “DBC - Users.”

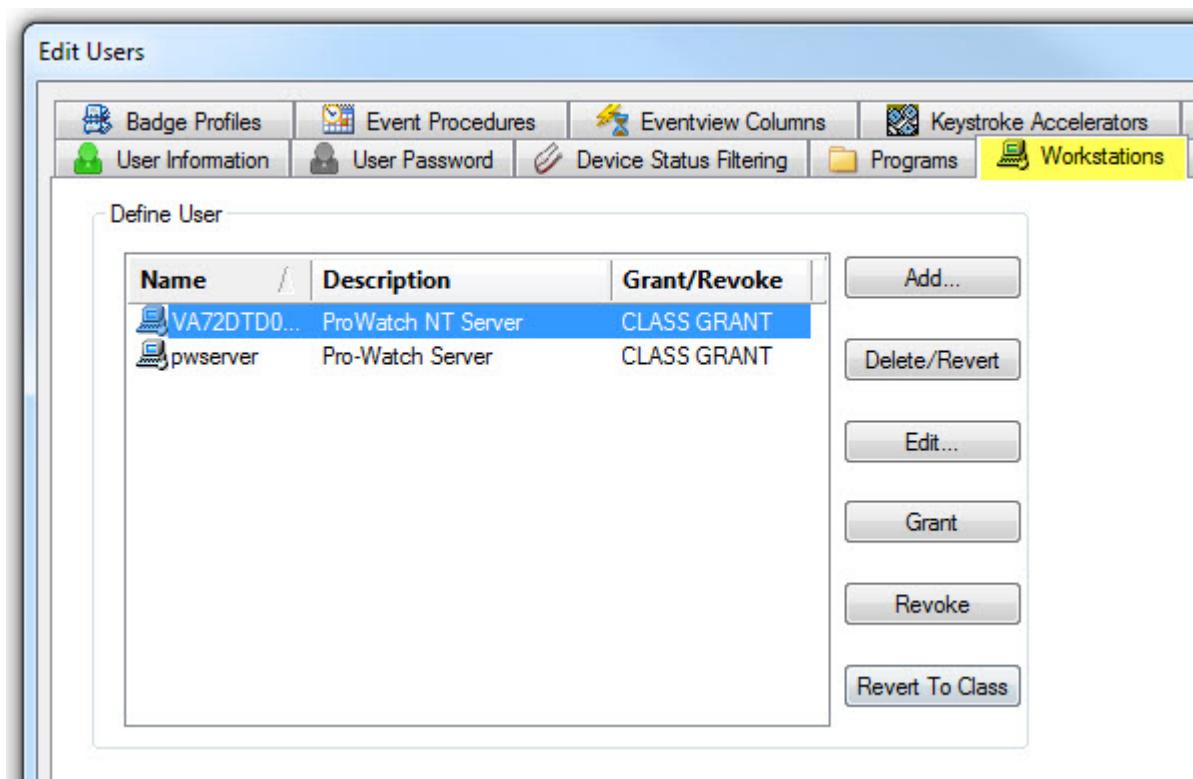
2.7.2 Assign Web Client Workstation to the User Account

1. In Pro-Watch, select **Database Configuration > Users** from the navigation panes to display the user icons on the right pane.

Pro-Watch Web Client

Web Client User Account Prerequisites

2. Double click your user account to display the **Edit Users** screen:



3. If your workstation is not displayed in the **Define User** list, click the **Add** button, browse and find your workstation and add it to the list.
4. If the workstation is not in grant status, select the workstation and click the **Grant** button.
5. When done, click the **OK** button at the bottom of the **Edit Users** screen to close it.

Note: Web server workstation name should be registered in PW Server. **Example:** Registering PW client workstations in Pro-Watch server.

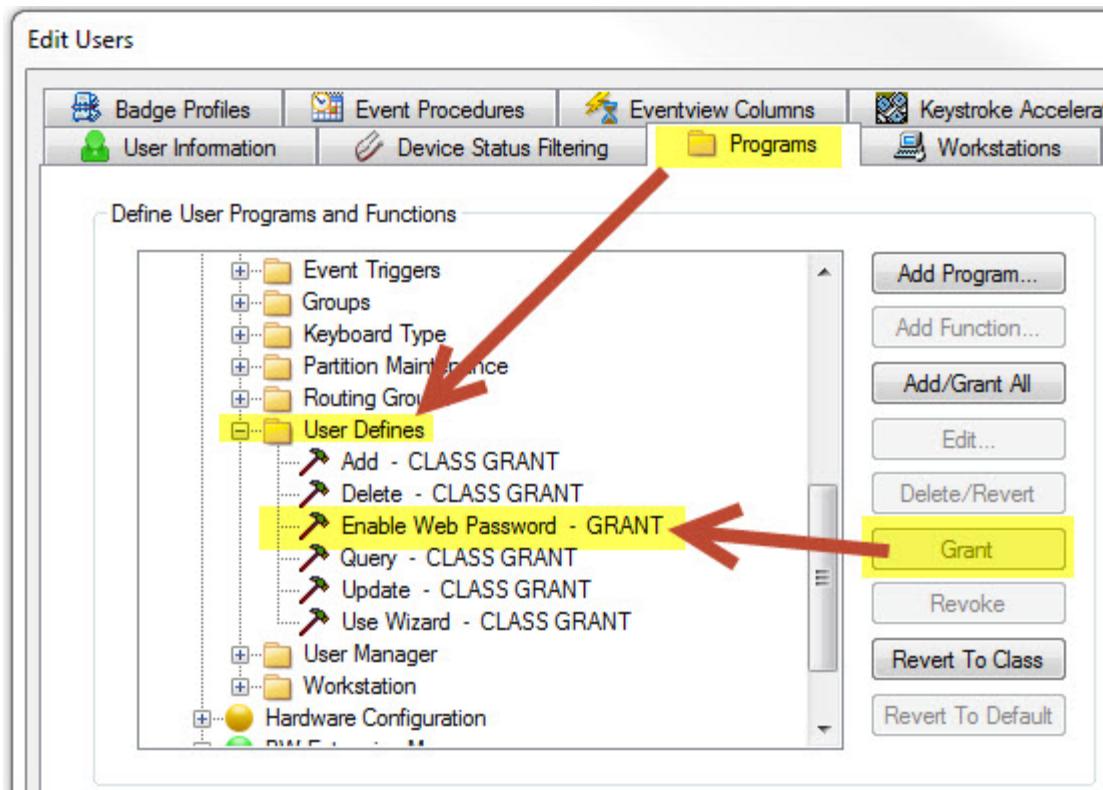
For more information refer to the *Pro-Watch Software Suite 5.0 User Guide*, 7-901071V17, Chapter 59 “DBC - Users” and Chapter 60 “DBC - Workstation.”

2.7.3 Enable Your Web Password

Note: Web Password is ONLY required for Basic authentication, not where installing as Windows Authentication.

1. Select **Database Configuration > Users** from Pro-Watch navigation pane.
2. Double-click your user name/icon to display the **Edit Users** screen.
3. Select the **Programs** tab.
4. In the tree-view, select **Database Configuration > User Defines**.

5. In the **User Defines** list of functions, find the “**Enable Web Password**” function and grant it by clicking the **Grant** button on the right.



6. If “Enable Web Password” is not listed, Click the **Add Function** button, find and select the “**Enable Web Password**” from the list and click **OK**. If the function displays as “Revoked,” repeat Step 5 above and continue with Step 7 below.
7. Click **OK** to close the **Edit Users** screen.

2.7.3.1 Setting the Web Password

1. In the Pro-Watch, click and select **Database Configuration** from the **Viewers** list on the leftmost pane.
2. From the middle pane, click and select the **Users** option.
3. In the right pane, double click the selected user profile to display the **Edit Users** screen.
4. In the **User Information** tab, enter a web password into the **Web Password** field and click **OK**.

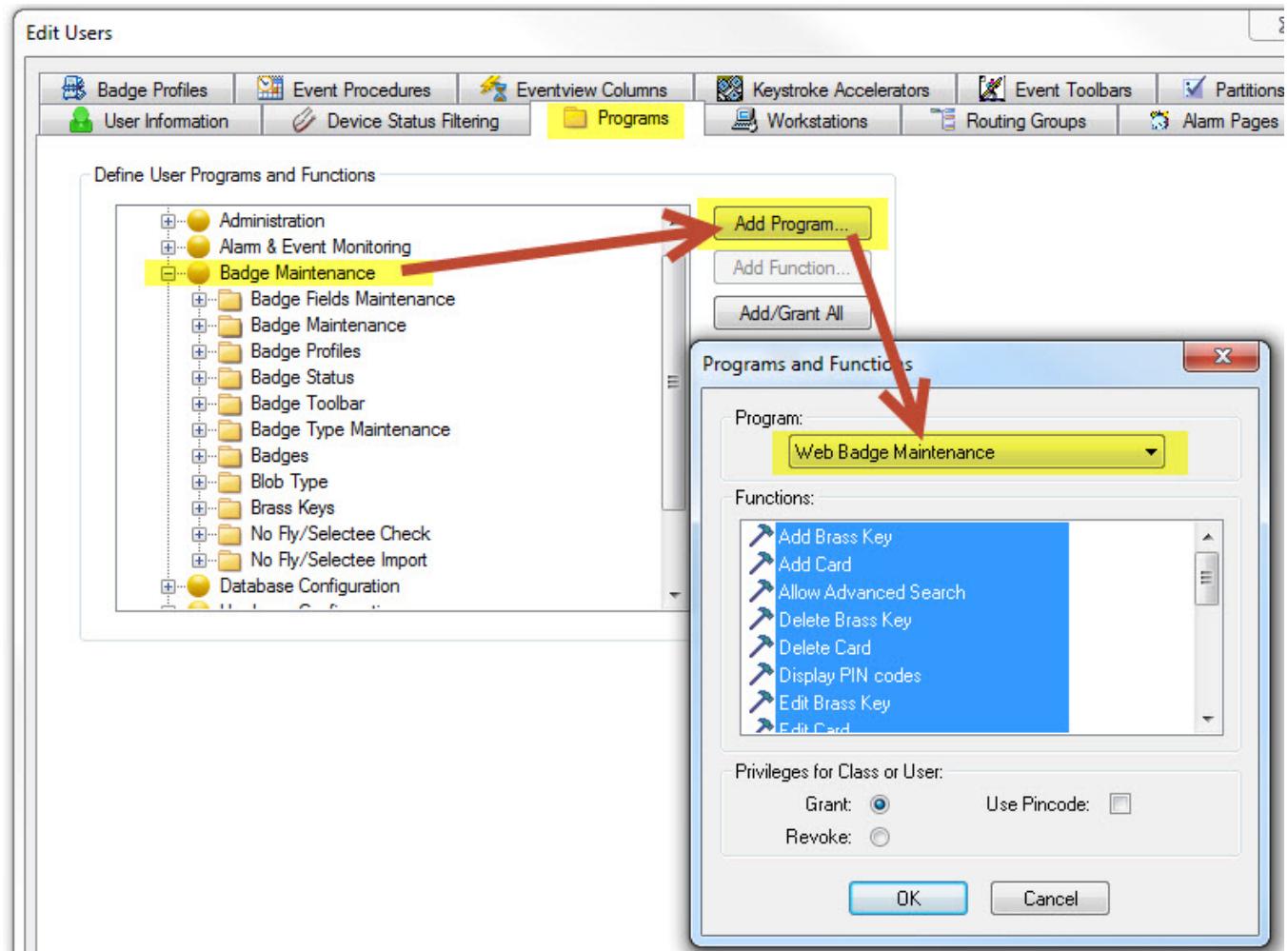
2.7.4 Grant Web Badge Maintenance Functions

1. Select **Database Configuration > Users** from Pro-Watch navigation pane.
2. Double-click your user name/icon to display the **Edit Users** screen.
3. Select the **Programs** tab.
4. In the tree-view, select **Badge Maintenance**.

Pro-Watch Web Client

Web Client User Account Prerequisites

5. Click the **Add Program** button to display the **Programs and Functions** dialog box.
6. In the **Program** drop-down list, find and select the “**Web Badge Maintenance**” program.
7. Press **Shift** and click to select all desired functions for the user in the **Functions** list box:



8. Click **OK** to display the “**Web Badge Maintenance**” sub-directory under the **Badge Maintenance** directory. Make sure those functions you want inside the directory are “granted.” If not select them one by one and click the **Grant** button.
9. Click **OK** to close the **Edit Users** screen.

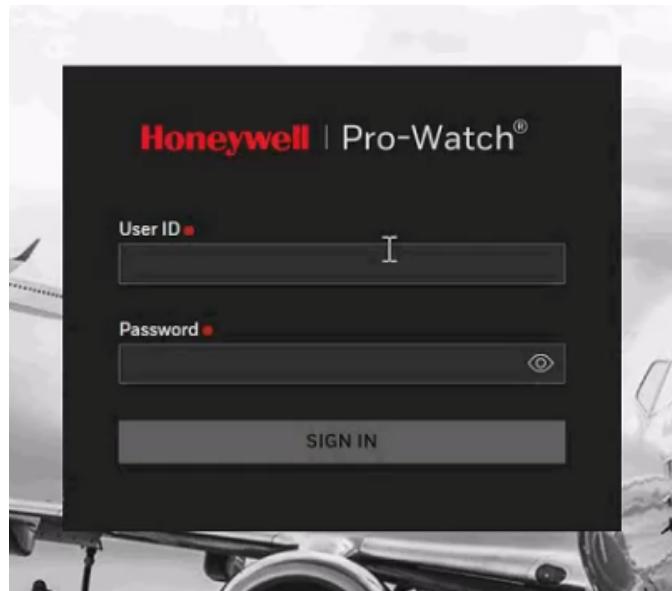
2.8 Pro-Watch Web Client Login

To access the Pro-Watch Web Client:

1. Either double-click the Pro-Watch icon on your desktop or open your browser and navigate to <https://WebServerName/ProWatch> to display the login page.

Note: Make sure that you always use the hostname to access the web pages.

Figure 1 Pro-Watch Web Login Page



2. Type in your **User ID** and **Password**.

Note: This is not the Windows login UserID/Password, it is the Pro-Watch Login Name and Web Password set in Pro-Watch. Refer to [Editing Users in Pro-Watch® Software Suite Release 5.0 User Guide](#), 7-901071V17 about setting Web Client passwords for Pro-Watch users. Also see [Enable Your Web Password](#) in this section.

3. Click the **Login** button to display the Pro-Watch Web Client interface page.
 - **If the login is successful, the Pro-Watch Web Client Home page** [Figure 2](#) is displayed. By default, only the badge-holder list will be displayed after the login. The details as shown in [Figure 2](#) will be displayed only after the user selects a badge-holder.
 - **If the login is not successful in 3 consecutive attempts**, then the system locks the account.

Figure 2 Pro-Watch Web Client Home Page

Honeywell Pro-Watch | People & Group

People Group ⊕ ⋮

🔍 *Search* FILTER

6 People

	ARIS, JHON Contractor
<input type="checkbox"/>	CARTER, JENNY Standard Employee
<input type="checkbox"/>	DHARMA, VINOOTH Standard Employee
<input type="checkbox"/>	EARL, CARTER Standard Employee

Employee Cards Assets Activity L...

First Name
JHON

Expire Date
01/22/2120

2.9 Home Page

The Pro-Watch Web Client **Home page** is shown in [Figure 2](#) on page 17. The following sections describe the features of the Pro-Watch Web Client Home page.

2.9.1 Home Navigation Links

Table 1 Home Navigation Links

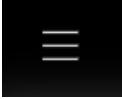
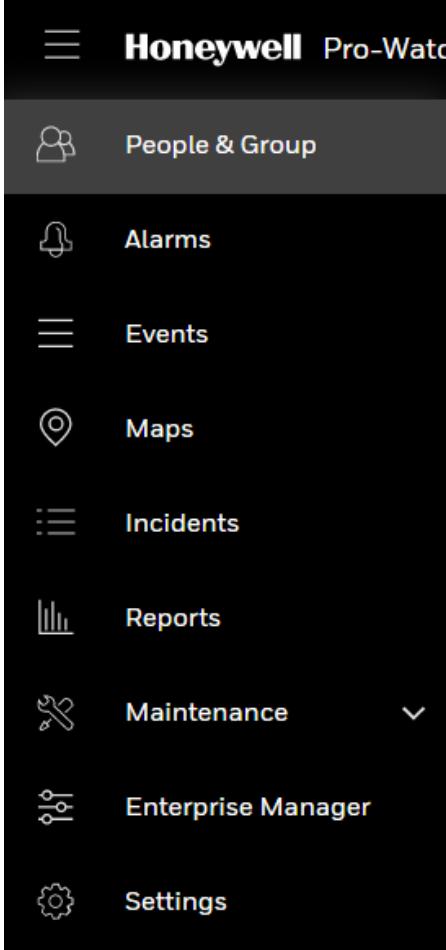
Link	Description
	<p>Click the 3 horizontal bars to display the Honeywell Hamburger Menu to display the following options:</p>  <p>The menu includes the following items:</p> <ul style="list-style-type: none"> People & Group Alarms Events Maps Incidents Reports Maintenance (with a dropdown arrow) Enterprise Manager Settings <p>Click People & Group to display the Badging module. Click Alarms to display the Alarms module. Click Events to display the Events module. Click Maps to display the Maps module. Click Incidents to display the Incidents module. Click Report to display the Report module. Click Maintenance to display the Firmware and Passwords sub-menus. Click Enterprise Manager to display the Enterprise Module Click Settings to display the Settings module. NOTE: You can display this menu by clicking the “People & Group” title as well.</p>

Table 1 Home Navigation Links

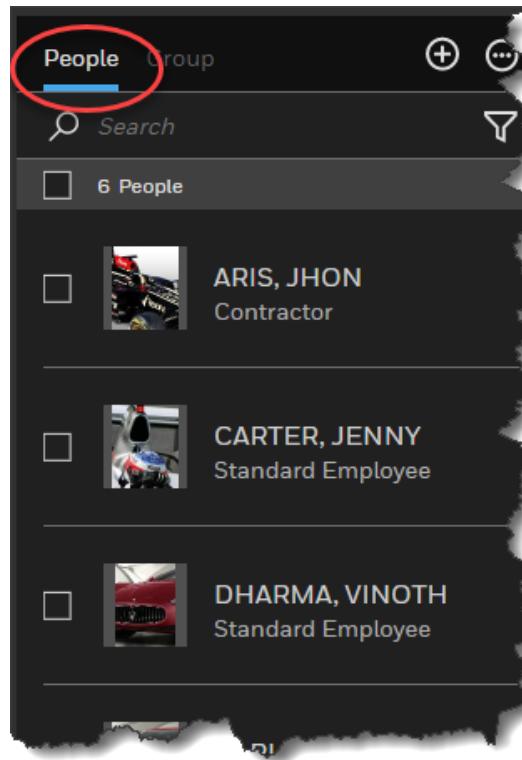
Link	Description
People	<p>Click People to display the list of badge-holders:</p>  <p>Click a badge-holder name to display the respective badging record information on the right pane.</p>

Table 1 Home Navigation Links

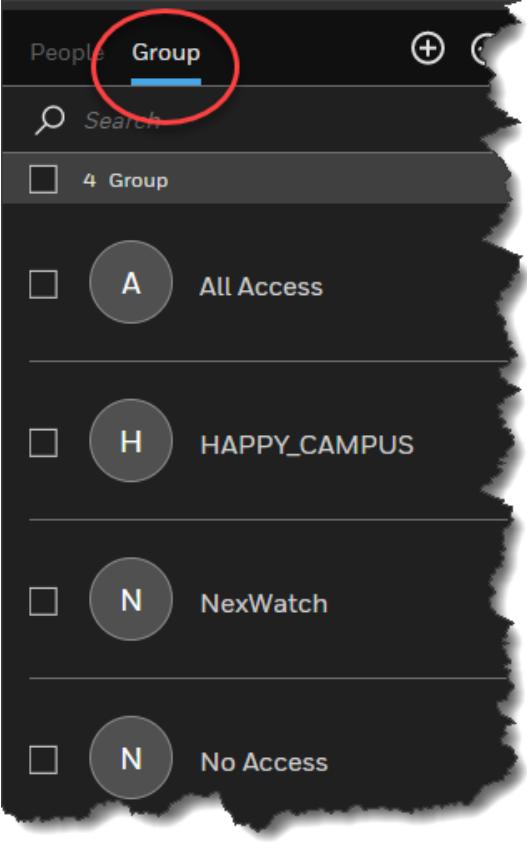
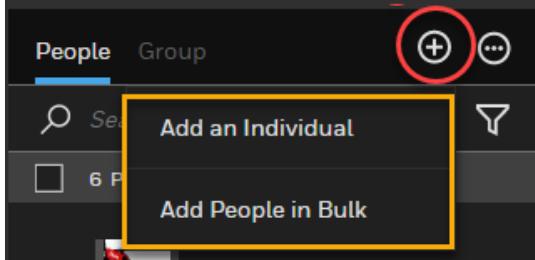
Link	Description
Group	<p>Click Group to display the list of groups available to assign to individual badge-holders:</p>  <p>Click a group name to display the respective group information on the right pane.</p>
	<p>Click the ADD link to add a new badge record (displayed in the right pane):</p> 

Table 1 Home Navigation Links

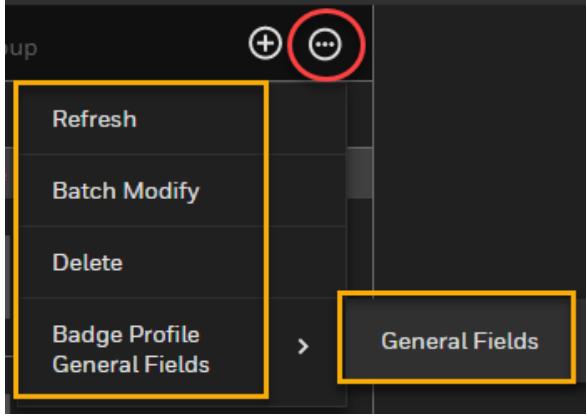
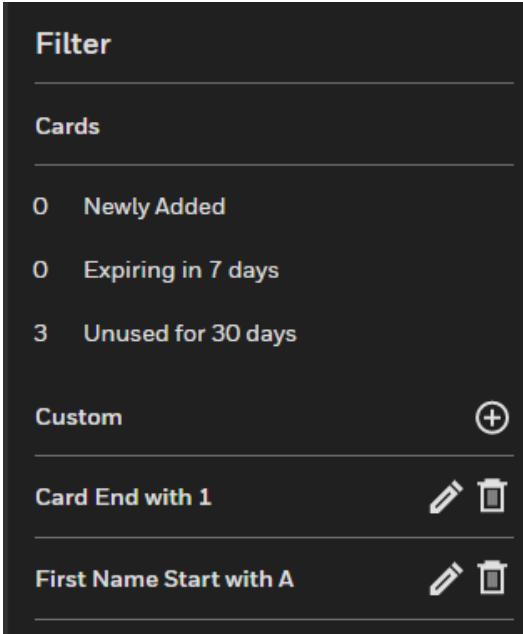
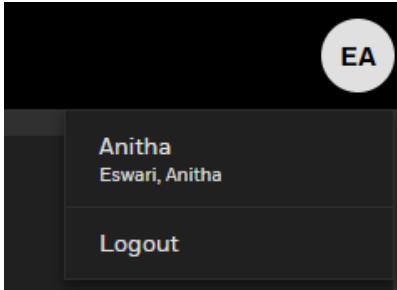
Link	Description
	Click the Actions link to display badge-related links Refresh , Batch Modify , Delete , and Badge Profile > General Fields : 
	Click the Filter link to display the list of predefined and user-defined custom filters. More about this in the Filtering section: 

Table 1 Home Navigation Links

Link	Description
 Search	Search the badge records by typing in a case-insensitive search term. The search term can be partial as well, provided no letters are omitted from the beginning of the word.
Logout	 <p>Click the Name index at the Top-Right corner of the window, Click Logout at the bottom of the menu to log out of the web client.</p>

2.9.2 Time out for Session

The Pro-Watch Web Client session will time out after a stipulated amount of time when:

- the user leaves the web session for a stipulated time without any actions.
- there is no activity performed by the user within the session.
- the browser is closed without logging off the session.

You can set the session time out in the **web.config** file located on the Pro-Watch Web Server Host, as shown below:

```
-->
```

```
<sessionState mode="InProc" customProvider="DefaultSessionProvider" timeout="20" cookieless="false">
  <providers>
    <add name="DefaultSessionProvider" type="System.Web.Providers.DefaultSessionStateProvider, System.Web.Providers, Version=1.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
  </providers>
</sessionState>
<customErrors mode="Off" />
</system.web>
<custom webServer>
```

Note: The default value for timeout session is 480 minutes.

2.10 Modules

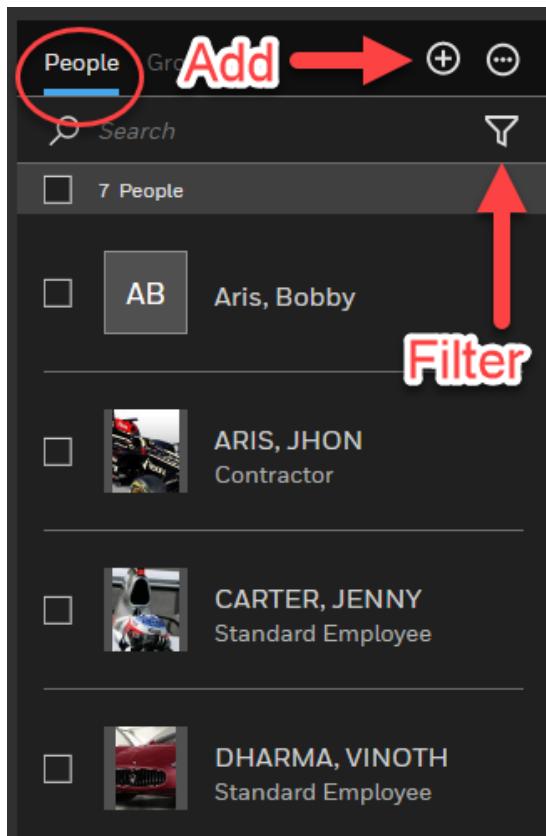
The Pro-Watch Web Client allows the user to access the following modules:

- **People & Group.** Refer to the [Badging](#) section.
- **Alarms.** Refer to the [Alarms](#) section.
- **Events.** Refer to the [Events](#) section.
- **Reports:** Refer to the [Reports](#) section.
- **Settings.** Refer to the [Settings](#) section.
- **Maintenance.** Refer to the [Simplified Device Maintenance](#) section.
- **Incidents.** Refer to the [Incidents](#) section.
- **Maps.** Refer to the [Maps](#) section.

Note: Other than **Card**, **Assets** and **Activity Log** tabs, **all other tabs are dynamically created**. By default Pro-Watch badge UI provides an “**Employee**” tab to collect **Badge** holder detail, but the Badge Administrators are free to change it the way they like.

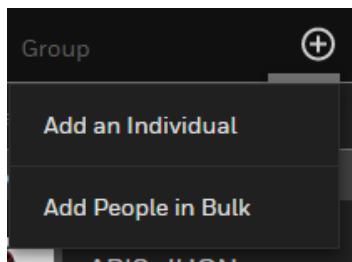
2.11 Badging

Click the **Honeywell Hamburger Menu** (3 horizontal bars) on the Home page and select **People & Group** link to display the **Badge-Records Badging screen**:



2.11.1 Adding a Badge Record

Click the “+” sign to display the drop-down add list:



2.11.1.1 Adding an Individual

Click **Add an Individual** to display the **Employee** pane on the right:

Click the **ADD** link to display the **EMPLOYEE** tab of a new badge record.

The screenshot shows the Pro-Watch Web Client Badging interface. At the top left, there's a navigation bar with a search icon, a filter icon, and a plus sign icon (circled in red). To the right of the navigation bar is a large red arrow pointing towards the top right corner of the main content area. The main content area has a dark background with white text. It features a navigation bar at the top with tabs: Employee (circled in red), Cards, Assets, Activity L..., and a 'Card' tab on the far right. Below the tabs are several input fields and dropdown menus. The 'Employee' tab is active, indicated by a blue underline. The fields include:

- First Name: [Input Field]
- Last Name *: [Input Field]
- Issue Date: 02/12/2020 [Calendar Icon]
- Expire Date: 02/12/2120 [Calendar Icon]
- Badge Type: [Dropdown Menu]
 - Contractor
 - Standard Employee
- Partition: [Dropdown Menu] (with a grid icon)

At the bottom right of the main content area, there are two buttons: 'CANCEL' and 'SAVE' (in a blue box). On the far left, there's a sidebar with a list of employee names: NY Employee, OTH Employee, and RU Employee.

For Editing

2.11.1.2 Cards Tab

Select the **Employee(s)** to whom you'd like to add a card.

The screenshot shows the Honeywell Pro-Watch web client interface for managing people and groups. The title bar reads "Honeywell Pro-Watch | People & Group". The left sidebar has "People" selected under "People" and "Group". It includes a search bar, a filter icon, and a button with an upward arrow. Below the sidebar, there are six employee entries:

- ARIS, JHON (Contractor) - checked
- CARTER, JENNY (Standard Employee)
- DHARMA, VINOOTH (Standard Employee)
- EARL, CARTER (Standard Employee)
- GANDHI, RAJIV

The main content area has tabs for "Employee", "Cards" (which is selected), "Assets", and "Activity L...". To the right of the employee list, there is a large circular icon containing a smartphone and a badge. A red arrow points from the top-left employee list towards this icon. Another red arrow points from the circular icon to the text "You have not added any Cards yet". At the bottom right, there is a blue "ADD CARD" button.

1. Click ADD CARD button to display the **Add New Card** dialog box:

The screenshot shows the 'Add New Card' dialog box. The top bar says 'People & Group'. The main title is 'Add New Card'. The 'Badge Detail' section contains fields for 'Card Number' (mandatory), 'Card Status' (Active dropdown), 'Card Type' (dropdown), 'PIN' (Type field with a double arrow icon), and 'PIN Verify' (input field). The 'Permissions' section contains 'Access Group' and 'Additional Rights' dropdowns. At the bottom are 'CANCEL' and 'ADD' buttons.

2. Enter values for the mandatory fields **Card Number**, **Card Status**, and **Card Type**.
3. Enter values for the other fields **PIN** and **PIN Verify**, if appropriate.

Pro-Watch Web Client

Badging

4. Scroll down to display the other card fields:

The screenshot shows the 'Add New Card' interface. In the 'Permissions' section, there are two main sections: 'Access Group*' and 'Additional Rights'. Each section has a dropdown menu icon. Below these sections is a link: 'Or, Copy access from an existing card'.

Validity

Activate

02/12/2020 12:00:01



Deactivate

02/12/2021 11:59:59



Set to profile expiry date

5. Select or enter the appropriate values for the remaining fields.

The screenshot shows the 'Cards' tab selected in the navigation bar. On the left, a card summary box displays the card number '123456' and the expiration date 'Expires on 02/13/2021'. To the right, the 'Card Details' section is active, showing fields for 'Card Number' (123456), 'Card Status' (Active), 'Card Type' (Standard Employee), and 'PIN' (1234). There is also a 'View More' link. At the bottom right are 'CANCEL' and 'SAVE' buttons.

6. Click **Save**.

2.11.1.3 Assets Tab

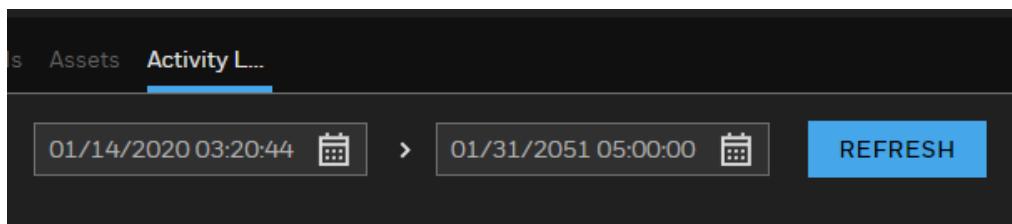
1. Click **Add Device** to display the **Add Device** dialog box:

The screenshot shows the 'Add Device' dialog box. It contains several input fields and buttons. At the top left is the title 'Add Device'. Below it are two rows of fields: 'Device' (dropdown menu with 'Select') and 'Assets No' (text input field with placeholder 'Add Assets No'). The second row contains 'Status' (dropdown menu with 'Select') and 'Issue Date' (text input field with placeholder '02/13/2020' and a calendar icon). The third row contains 'Due Date' (text input field with placeholder 'Select' and a calendar icon) and 'Date Returned' (text input field with placeholder 'Select' and a calendar icon). Below these is a 'Note' section with a text area containing 'Add Note'. At the bottom right are two buttons: 'CANCEL' and 'ADD'.

2. Enter or select all the appropriate values and click **Add**.

2.11.1.4 Activity Log Tab

Click and select the **Activity Log** tab for the badge holder:

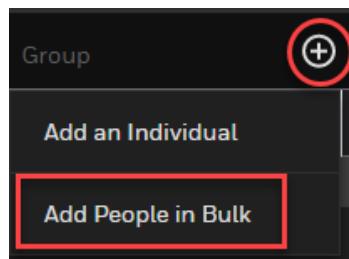


Perform an activity search by selecting appropriate **Start Date & Time** and **End Date & Time** from the respective pop-up calendars.

2.11.2 Adding People in Bulk

You can enter up to 1000 people starting from a specific card number.

1. Select “+” (Add Button) > Add People in Bulk to display the **Add People in Bulk** dialog box:

A screenshot of the 'Add People: Bulk' dialog box. It has several input fields and controls:

- Number of People:** A text input field containing the placeholder text 'Maximum no.of people allowed is 1000'.
- Card Number:** A text input field with the placeholder text 'Enter the starting card number'.
- Employee Type:** A dropdown menu currently set to 'Select'.
- Partition:** A dropdown menu with a grid icon.
- Access Group:** A dropdown menu with a grid icon and a checked checkbox next to the text 'Download Cards'.
- Validity:** A toggle switch that is turned off.
- Buttons:** At the bottom right are two buttons: 'CANCEL' and 'SAVE'.

2. Enter or select all the appropriate values and click **Save**.

2.11.3 Adding a Group

Profile

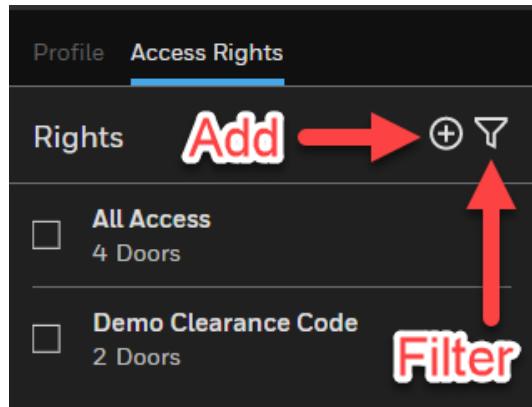
1. Select the **Group** tab. Then click the “+” (Add Button) to display the group **Profile** dialog box:

The screenshot shows the 'Profile' tab selected in the top navigation bar. The main area contains input fields for 'Name' (text box), 'Company Type' (dropdown menu), 'Partition' (dropdown menu with a grid icon), and 'Card Expiration Date Method' (radio buttons for 'FIRM EXPIRY DATE' and 'CARD EXPIRY DURATION'). Below these, there's a note about card deactivation after a duration. The 'Owner Info' section includes fields for 'Address1', 'Address2', 'City', 'State/Region/Province', and 'Zip Code/Postal Code'. To the right, the 'Notes' section displays a message about no notes added yet and a blue 'ADD NOTE' button. The 'Contacts' section also shows a message about no contacts added yet and a grey 'ADD CONTACT' button. At the bottom right are 'CANCEL' and 'SAVE' buttons.

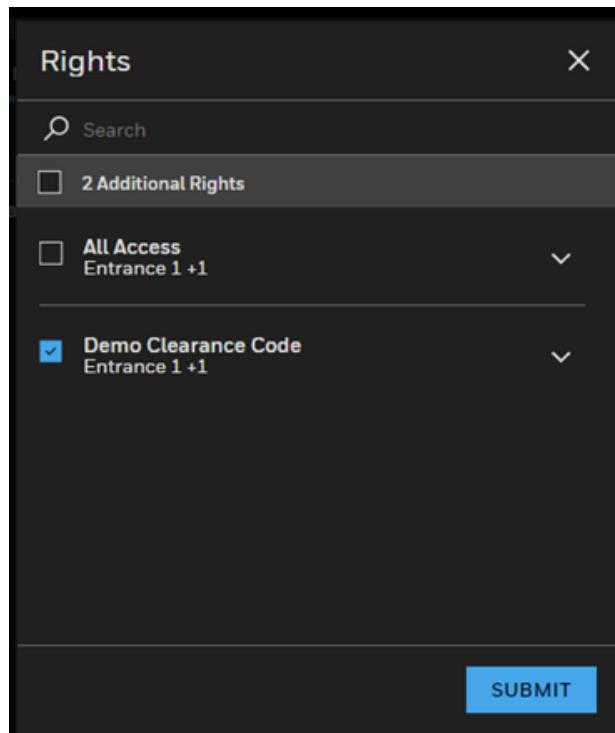
2. Enter or select the appropriate values for the fields.
3. Click **Save**.

Access Rights

1. Select the **Access Rights** tab:



2. To add a new access right, click the "+" (add) icon to display the **Rights** list:



3. Select the appropriate access right(s) from the list and click **Submit**.

Note: To filter and display access rights, click the funnel icon.

2.11.3.1 Notes Tab

To add a note to a badge record, click the **ADD NOTE** button. Select either the **Alarm** or **Critical** check-box. Type in your note in the text box. Click **Save**.

2.11.4 Editing a Badge Record

Select the badge record. Click the **PENCIL** icon on the upper-right corner to activate the editing mode:

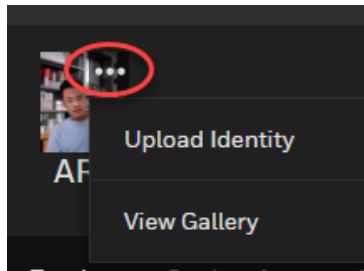


Edit all the fields you like; then click **Save**.

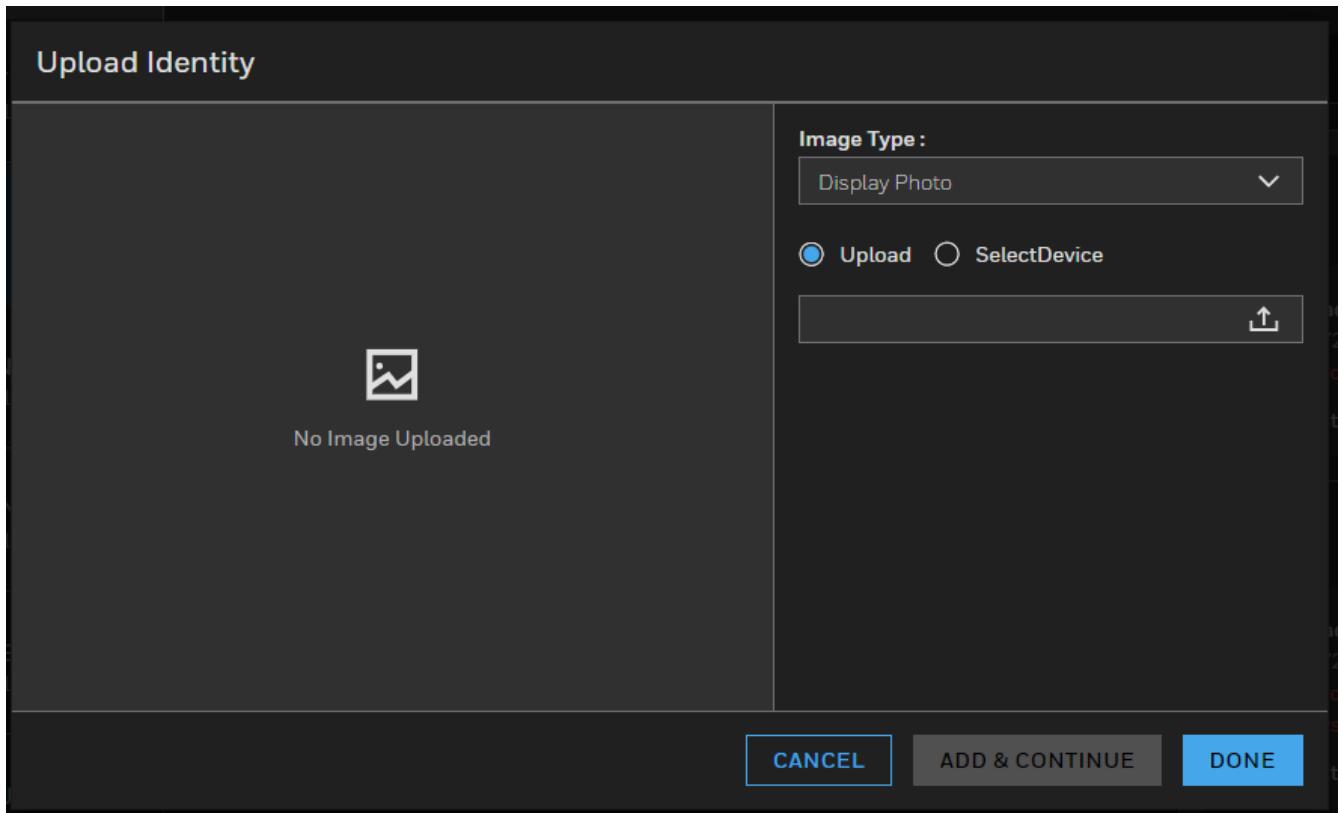
See the sub-section below on **Editing a Badge Image**.

2.11.5 Editing a Badge Image

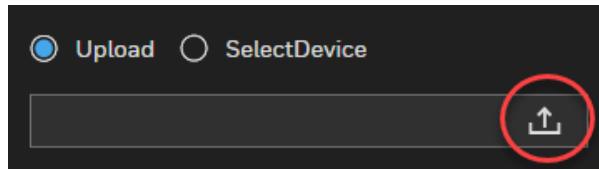
1. Select the badge record.
2. Click the **PENCIL** icon on the upper-right corner to activate the editing mode.
3. Click the **Actions link** on the image to display the pop-up menu.:



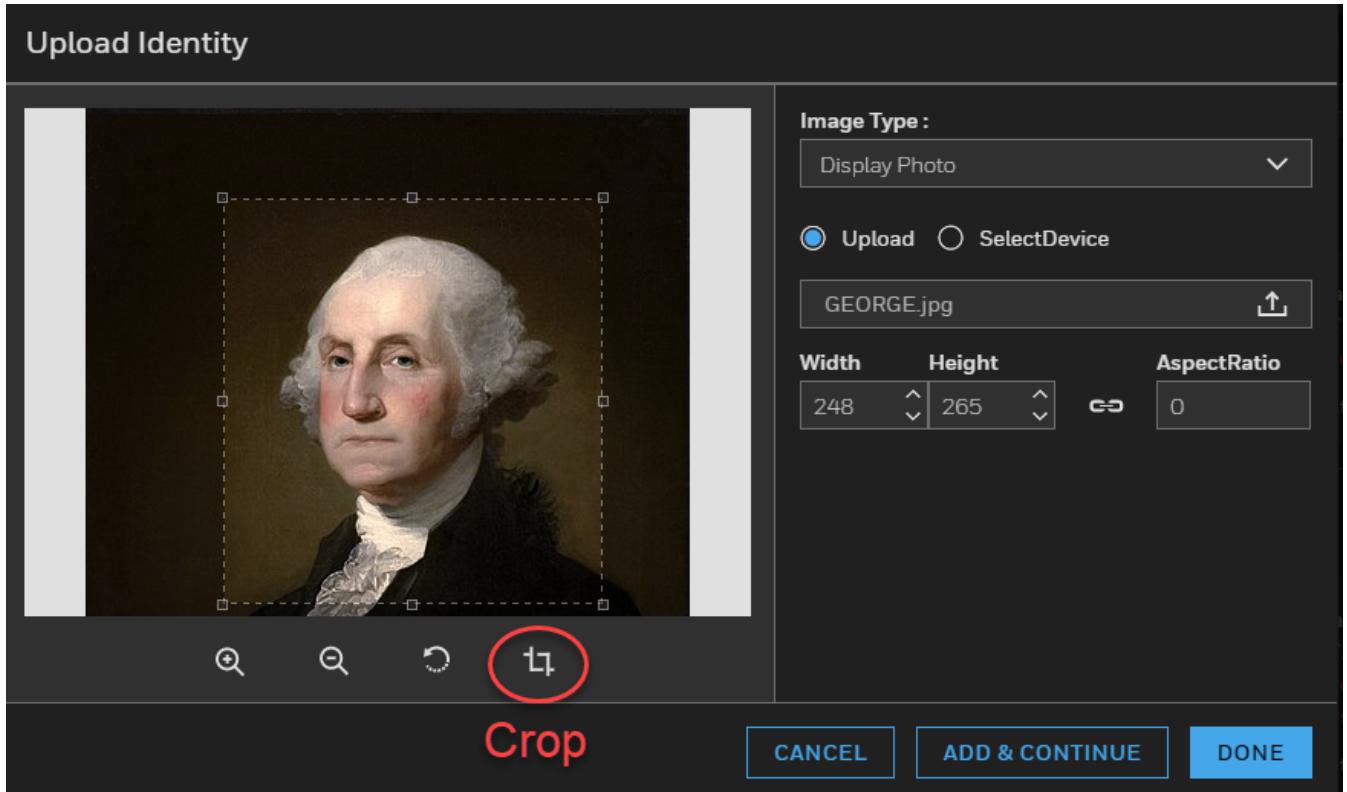
4. Select **Upload Identity** to launch the **Upload Identity** screen:



5. Select an **Image Type** from the drop-down menu.
6. Select **Upload** option-button. Then click the **Browse Button** to find the image you want to load:



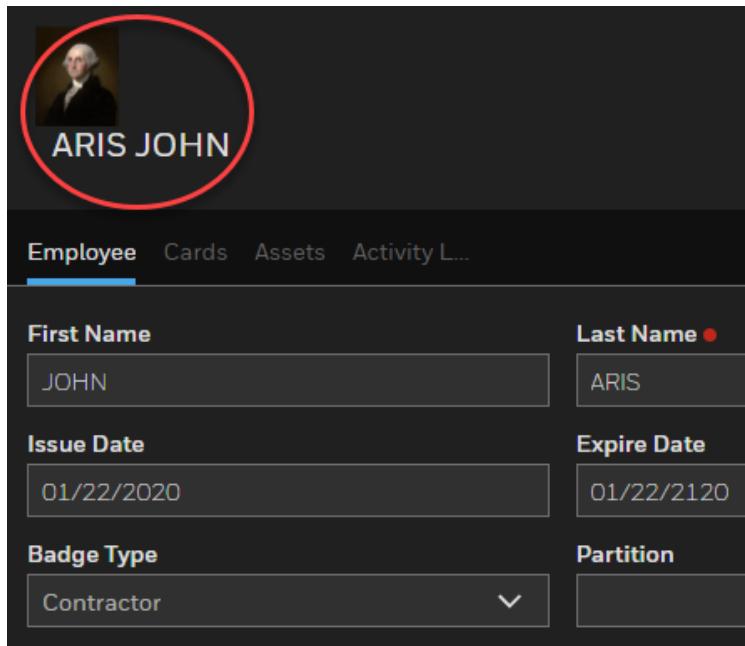
7. Browse and select an image. Click **Open** to upload the image to the **Upload Identity** page:



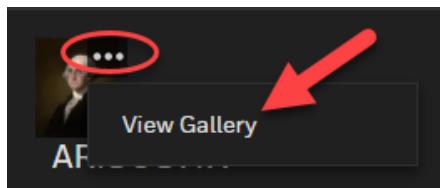
8. Crop the image before saving. Please note that the crop window size is as per the user-defined **Width**, **Height** (both in pixels) and **Aspect Ratio** (like 4:3 or 16:9) in the **Upload Identity Window**.
9. Click **Done** to return to the **EMPLOYEE tab**. Click **Save**. The image will be displayed in the badge record list:



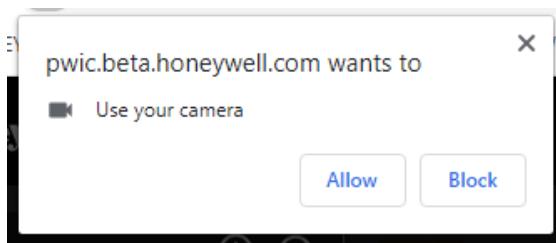
10. Select and double-click the badge record to have the new image display in the full badge record as well:



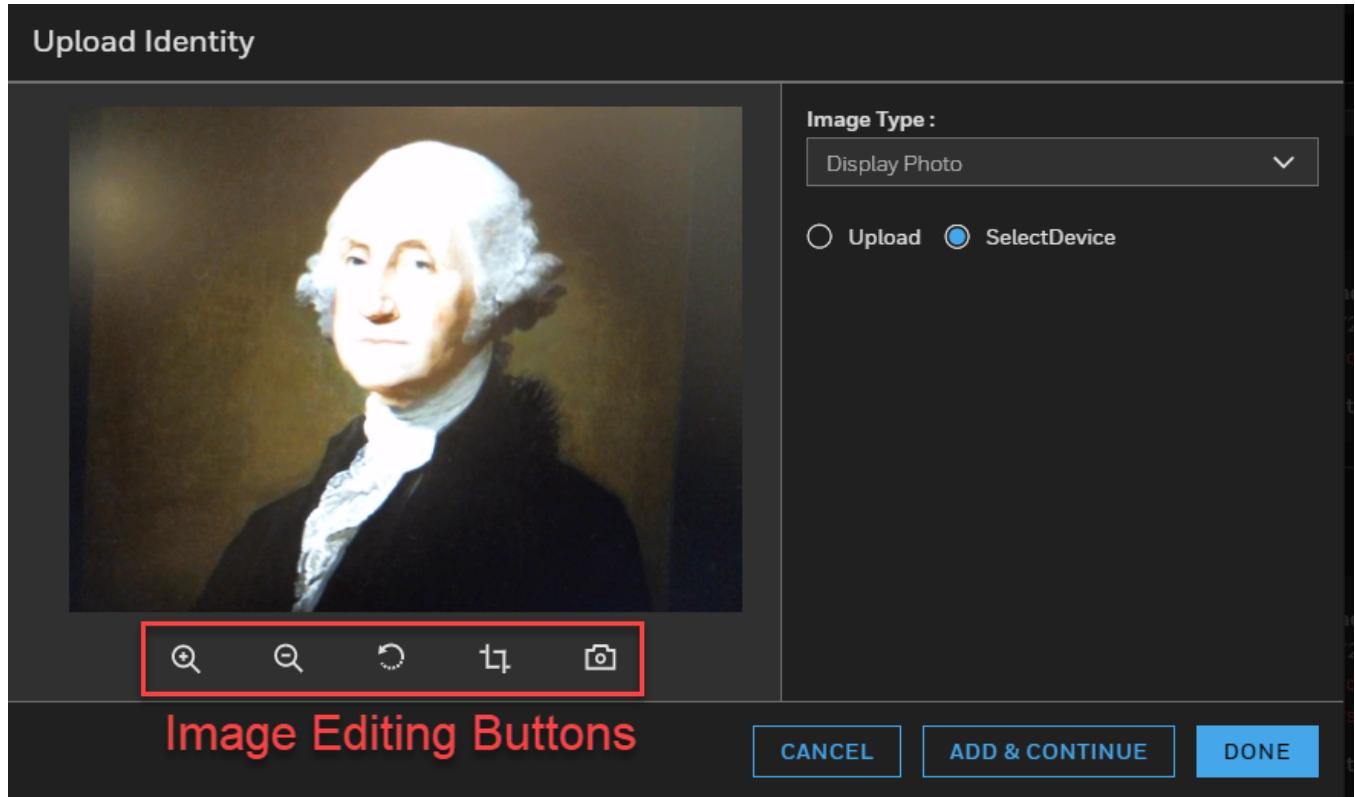
11. You can view an existing image from the image gallery by selecting the **View Gallery** option from the drop-down menu:



12. To capture an image from a device, select **Select Device** option-button in the **Upload Identity** screen. Pro-Watch will ask for your permission to use the camera. Click **Allow**:



13. Click **Allow** to display the image capture screen:



14. Rotate, crop and edit the image by using the **Image Editing Buttons** displaying underneath the image.

15. Click **Add & Continue** to save the image and continue.

16. Click **Done** to return to the **EMPLOYEE tab**. Click **Save**. The edited image will be display in the badge record.

2.11.6 Deleting a Badge Record

1. Select the badge record you want to delete.
2. Click the **Actions link** to display the drop-down menu.
3. Select **Delete**.

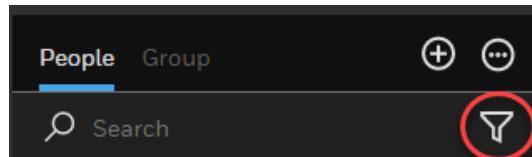
2.11.7 Searching for a Badge

In the **Search Badge** screen, enter any search value in the text field. Then, click the **Search** button. You can search by **First Name**, **Last Name**, **Company**, or **Card Number**.

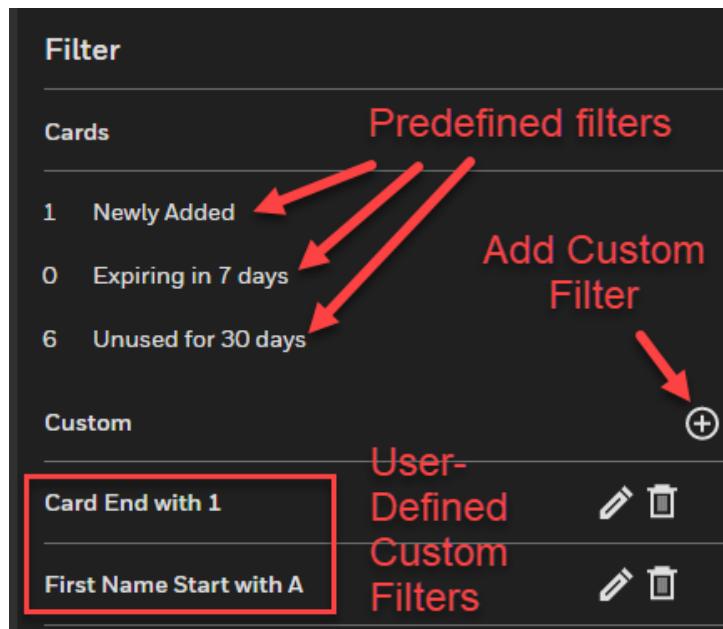
The system will either return the badge you are searching for, or, if there are more than one badges that satisfy the search criteria, it will return multiple results. You can select the one you like.

2.11.8 Advanced Search Filters

You can perform an advanced search for badges by clicking the **filter** (funnel) icon:

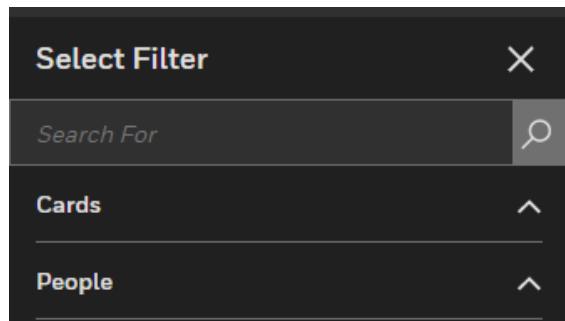


Clicking the filter icon will display a list of **predefined** (but configurable) and **user-defined custom filters**:

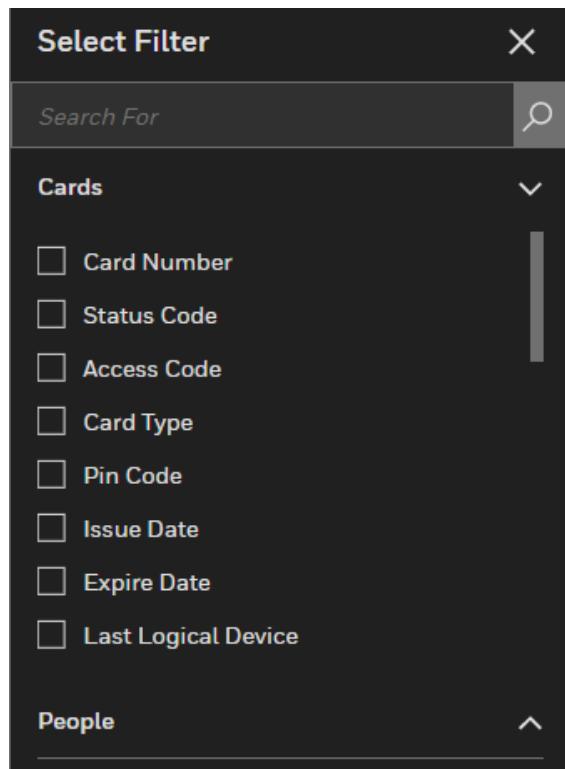


2.11.9 Adding a New Custom Filter

To add a custom filter click the **Add ("+" button)** to display the **Select Filter** list:



Select to expand the **Cards** and/or **People** lists and select the filtering criteria you like:



The variables you select will be displayed on the **Filter profile**:

Filter

Select Filter

Search For

Cards

- Card Number
- Status Code
- Access Code
- Card Type
- Pin Code
- Issue Date
- Expire Date
- Last Logical Device

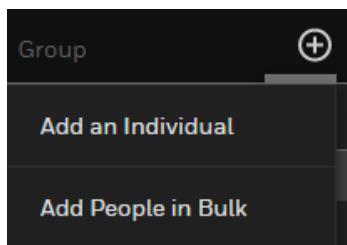
People

Click **Save** to save the custom filter(s) for future use.

Click **Apply** to generate the filtered results.

2.11.10 Adding Badges in Bulk

1. Click **Add button (“+”)** to display the drop-down add-functions list:



2. Select **Add People in Bulk** to display the **Add People: Bulk** add screen:

Add People: Bulk

Number of People • Maximum no.of people allowed is 1000

Card Number • Enter the starting card number

Employee Type • Select

Partition

Access Group

Validity

Download Cards

CANCEL **SAVE**

3. Enter the **Number of People** and the **Starting Card Number**. You can add a maximum of 1000 (one thousand) people.
4. Select appropriate values from the respective drop-down lists for **Employee Type**, **Partition**, and **Access Group**.
5. OPTIONAL: Toggle the **Validity** button to turn it **GREEN**.

Validity

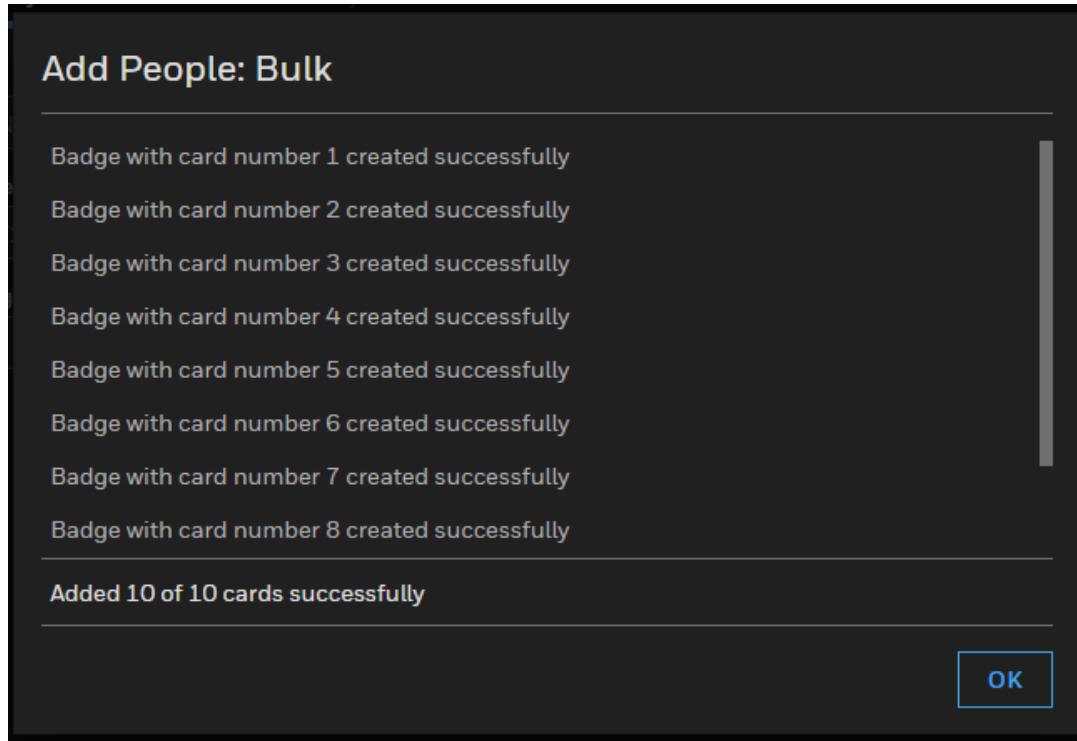
Activate • 03/05/2020 00:00:01

Deactivate • Duration Date 03/05/2021 23:59:59

People & cards belonging to this group will expire on the date mentioned above

- a. Select an **Activate** date and time from the pop-up calendar and clock to activate the badge(s).
- b. Select **Duration** and specific number of **Weeks**, **Months** or **Years** after which to **Deactivate** the badge(s).
- c. Select **Date** and a date and time from the pop-up calendar and clock on which to Deactivate the badge(s).
6. Select **Download Cards** check-box to download the card immediately.

7. Click **Save** to add badges in bulk. When all cards are created successfully, the system will display a message similar to this:



8. Click **OK**.

2.11.11 Adding a New Card

Note: The terms “card” and “credential” are synonymous.

1. Click the **People & Group** button on the main menu bar to display the **Search Badge** screen
2. Search and find the badge you’d like to edit. The system will display the **View Badge** screen.
3. In the **View Badge** screen, click the **Edit Badge** button to display the **Edit Badge** screen.
4. Select **Cards** tab.

5. Click the **Edit icon (Pencil)** and then **ADD NEW CARD** button to display the **Add New Card** screen:

The screenshot shows the 'Add New Card' interface. It consists of two main sections: 'Badge Detail' and 'Permissions'.
Badge Detail:

- Card Number** (Required): A text input field.
- Card Status**: A dropdown menu showing 'Active'.
- Card Type**: A dropdown menu with a downward arrow.
- PIN**: A section containing a text input field labeled 'Type' and a double-headed arrow icon.
- PIN Verify**: A text input field.

Permissions:

- Access Group**: A dropdown menu with a downward arrow.
- Additional Rights**: A dropdown menu with a downward arrow.

At the bottom right are two buttons: **CANCEL** and **ADD**.

Figure 3 Add New Card Screen

6. Enter the appropriate values into all the card fields displayed in the above figure. “PIN” and “PIN Verify” fields are optional. See Table 2-1 on page 48 for description of individual fields.

7. Scroll down to enter appropriate values for all the **Permissions** and **Validity** fields:

Add New Card

Permissions

Access Group ●	Additional Rights
[Empty input field]	[Empty input field]

Or ,Copy access from an existing card

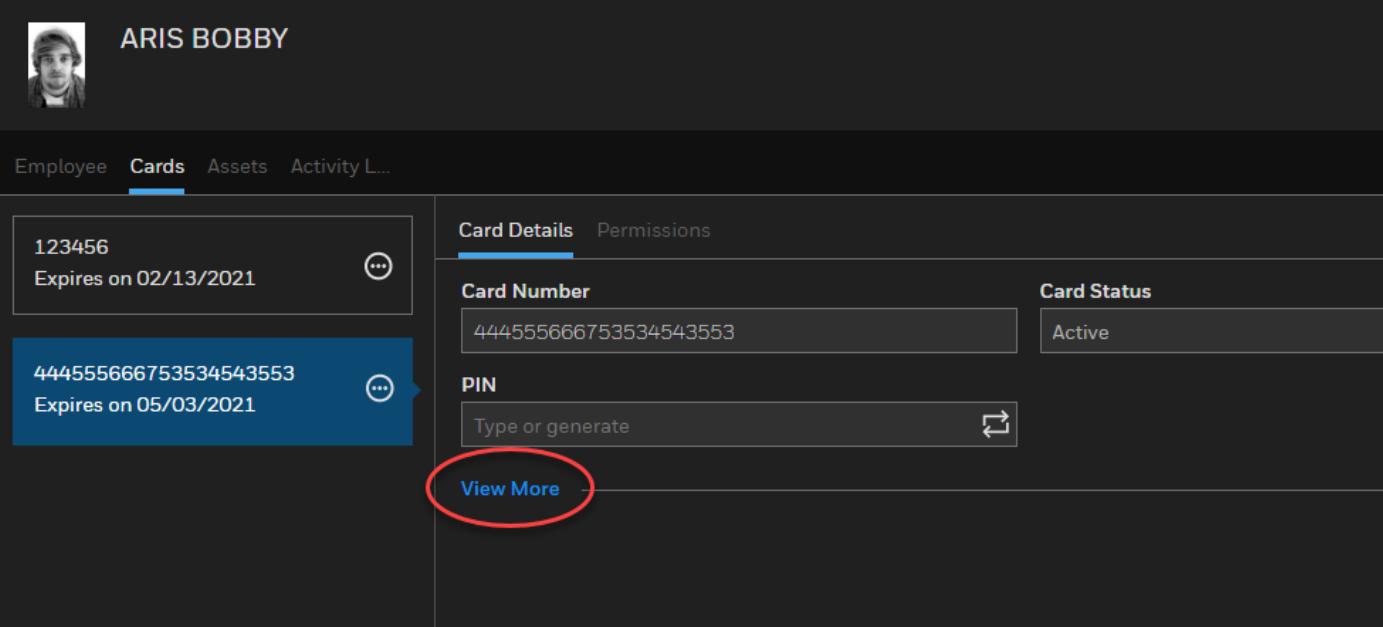
Validity

Activate	Deactivate
05/03/2020 00:00:01 	05/03/2021 23:59:59 

Set to profile expiry date

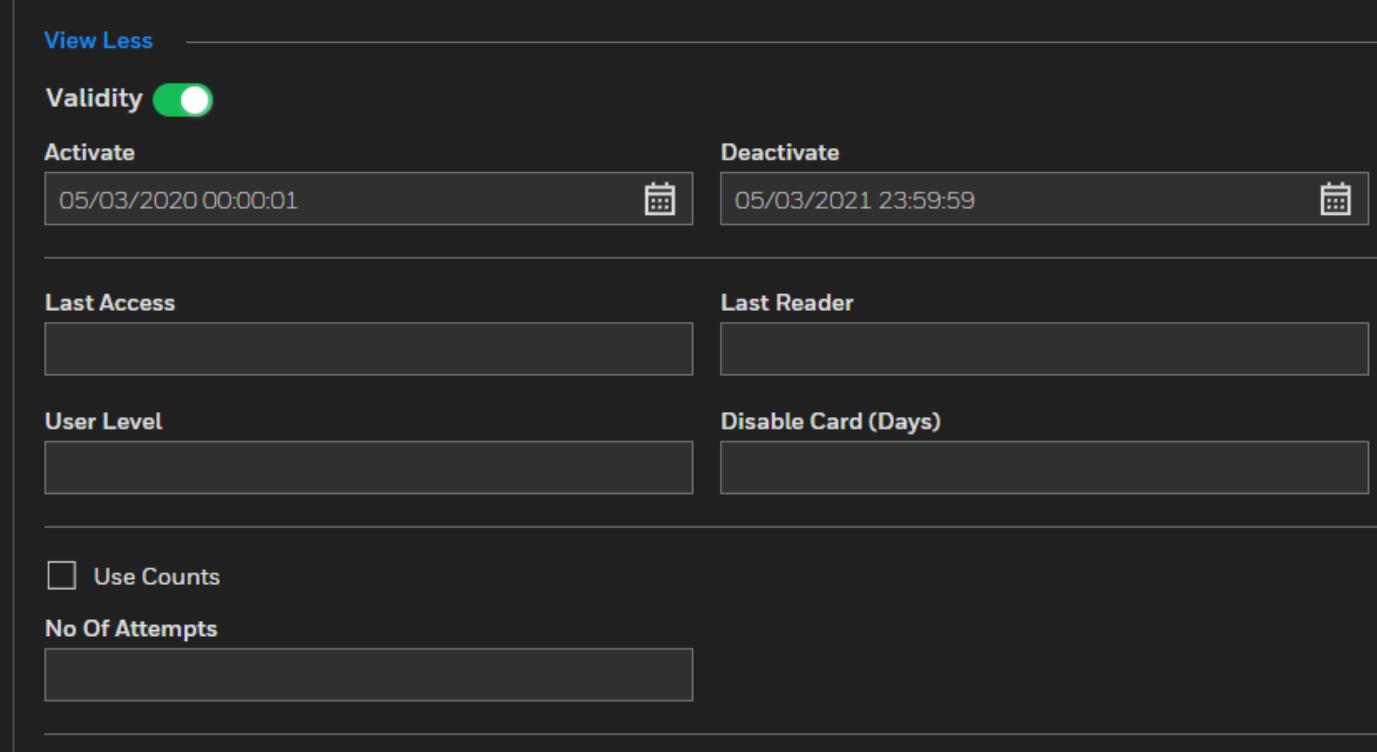
CANCEL **ADD**

8. Click **Add** to go back to the **Card Details** screen where the new credential will be listed:



The screenshot shows the 'Cards' tab selected in the navigation bar. Two credentials are listed. The second credential, which has a blue background, is expanded to show its details. The 'View More' link at the bottom of this expanded section is highlighted with a red oval.

9. Click **View More** link to display additional credential fields. Click the **Edit** (pencil) icon to activate the editing mode. Scroll down to view all the variable fields:



This screenshot shows the 'Card Details' screen for a specific credential. It includes sections for Activation/Deactivation dates, Last Access, Last Reader, User Level, Disable Card (Days), and other settings like Use Counts and No Of Attempts. A 'View Less' button is visible on the left.

Activation		Deactivation	
05/03/2020 00:00:01	<input type="button" value="Edit"/>	05/03/2021 23:59:59	<input type="button" value="Edit"/>

Last Access	Last Reader

User Level	Disable Card (Days)

Use Counts

No Of Attempts

Parade Text

Card Notes

ADA Trace Card PIN Exempt VIP Guard

Create Date
Return Date Select  **Card Number Extension**

Last Print Date

Print Count

10. In the above screen, enter the appropriate values into the card fields you want. See Table 2-1 on page 48 for description of individual fields.

11. Click **Save**.

Table 2-1 Credential Fields Listed Alphabetically

Credential Field	Description
ADA	ADA refers to "Americans with Disabilities Act." Select this check box to allow for extended shunt time on a door so that someone in a wheelchair, for example, has enough time to get through the door without generating an alarm.
Card Number Extension	Enter an extended card number, if any.
Card Number	Card number entered by the user.
Card Type	Select one from the drop-down menu.
Credential Status	Select one of the following from the drop-down menu: Active, AutoDisable, Disabled, Expired, Lost, Stolen, Terminated, Unaccounted, Void.
Disable Card Days	Enter the number of days after which the card will be disabled automatically. Default maximum is 999.

Credential Field	Description
Expire Date	Select from the drop-down menu. Select the “ Never Expire ” check-box for permanent cards that will never expire.
Group (Company)	Select one from the drop-down menu.
Guard	Check this option to enforce for the guards a specific ordered trail from one selected reader to another or to enable the cardholder to participate in the Guard Tour.
Issue Date and Time	Select from the drop-down menus.
Issue Level	Denotes the number of times the card has been issued. For brand new cards the number should be one (“1”). If, for example, the card has been lost and is reissued, the number should be two (“2”), etc
Parade Text	Enter the text that should parade through the LED window of the logical device when the card is presented.
PIN (Code)	Personal Identification Number (PIN) entered by the user. Click “ Generate Random PIN ” link to generate a random PIN. Also see Dependencies Between PW Windows and Web Applications .
PIN Exempt	Select this option to allow the use of the card at a reader without entering PIN.
PIN Verify	Enter the PIN again to verify it.
Trace Card	Select this box to record in a log file every transaction generated by this card.
Type	Select a credential type from the drop-down menu.
Use Count Attempts	Enter the maximum number of use attempts after which the card will be disabled automatically. Default maximum is 99.
User Level	The user level is often used to make some cards accomplish special tasks. For example, a manager may want to use such a card to automatically unlock the lobby doors at the beginning of a shift. Panel-level triggers and procedures can be written to trigger only on valid card accesses where the cardholder user level is equal to the user level set in the trigger. Allowed user level values range between 0 (zero) and 255. If a user enters anything out of this range Pro-Watch displays a validation error message and prompts the user to enter a proper value.
VIP	Select this check box to exempt the cardholder from anti-passback restrictions. A cardholder with VIP privileges can pass his/her card to the next person to swipe and pass through a reader.

12.Click the **Save Card** button to save the new card. Click **Cancel** not to save the new card.

2.11.12 Dependencies Between PW Windows and Web Applications

1. In Pro-Watch windows application , if “**Require All cards to have a PIN code**” is selected in badge profile, the PW web application will display the **PINCode textbox** as mandatory and won’t allow the user to save a card (add/edit) without pin code.
2. In Pro-Watch windows application , if the “**Required All Pin codes to be length**” set to one of the given length(4-20) in badge profile, the PW Web application will check for the entered pin code length to the configured length otherwise won’t allow to save the card (add/edit).
3. In Pro-Watch Windows application, if “**Display two text boxes for pincode**” is selected in badge profile, the PW Web application will display “**Confirm Pincode**” text box to validate the pincode match while saving a card.

2.12 Alarms

- See “**Acknowledging and Clearing Alarms**” on page 51.
- See “**Masking and Unmasking**” on page 57.

2.12.1 Alarm Management

2.12.1.1 New features

The user can:

- View video on alarm page.
- Locally change the columns listed on alarm monitoring page.
- Associate a workflow with alarm at system and device level.
- Acknowledge alarm and trigger incident automatically.

2.12.2 Acknowledging and Clearing Alarms

Note: Alarm Page Must contain one or more columns for the Web Alarm Page to work properly.

1. Click the **Alarms** link in the Honeywell Hamburger Menu to display the **Alarms** table:

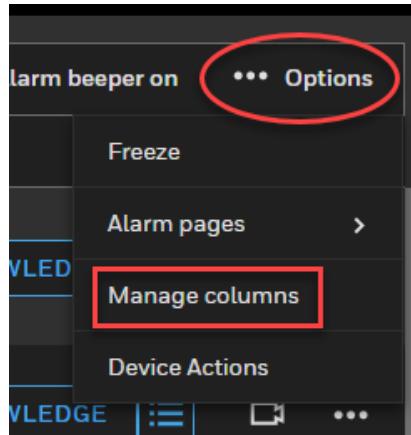
The screenshot shows the Honeywell Pro-Watch Web Client interface. On the left, there's a sidebar with a menu icon and the text "Honeywell Pro-Watch | Alarms". Below it, it says "6 UnAcknowledged" and "27 Acknowledged". On the right, there's a table titled "ALARMS" with columns for "COMPANY", "EVENT & SYSTEM TIME", and "ACTIONS". The table lists three unacknowledged alarms:

COMPANY	EVENT & SYSTEM TIME	ACTIONS
Door Held Open HC-T1-Entrance1 GFloor	01/22/2020 07:22:45 01/22/2020 07:22:45	ACKNOWLEDGE
Forced Door HC-T1-Entrance1- S2-SFloor	01/22/2020 07:22:39 01/22/2020 07:22:39	ACKNOWLEDGE
Door Held Open HC-T1-Entrance1 GFloor	01/22/2020 07:20:47 01/22/2020 07:20:47	ACKNOWLEDGE

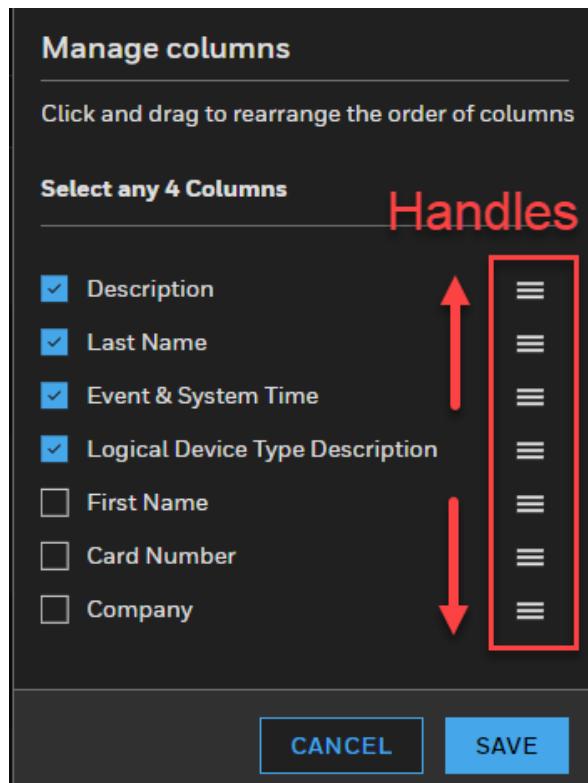
2.12.3 Managing the Columns of the Alarms Table

You can configure and reposition of the alarms table by editing its columns.

1. Click the **Options** menu on the upper-right to display the options:



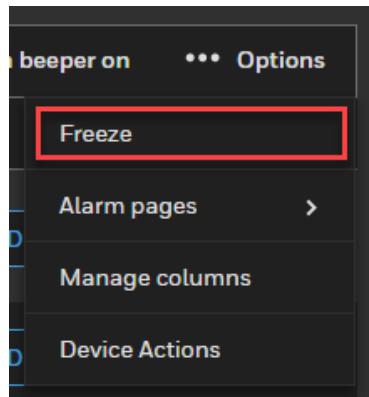
2. Select **Manage Columns** option to display the **Manage Columns** screen:



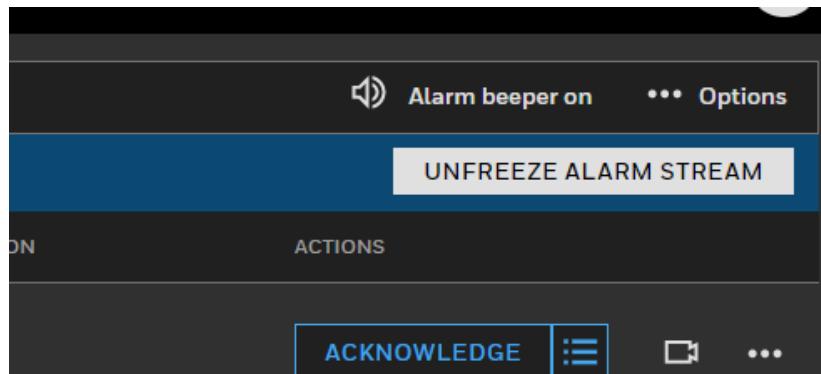
3. Select or unselect, and drag by the handles to rearrange the order of columns.

2.12.4 Freezing and Unfreezing Alarms

To freeze alarm reporting, click the **Options** link and select **Freeze**:



To unfreeze alarm reporting, click the “UNFREEZE ALARM STREAM” button:

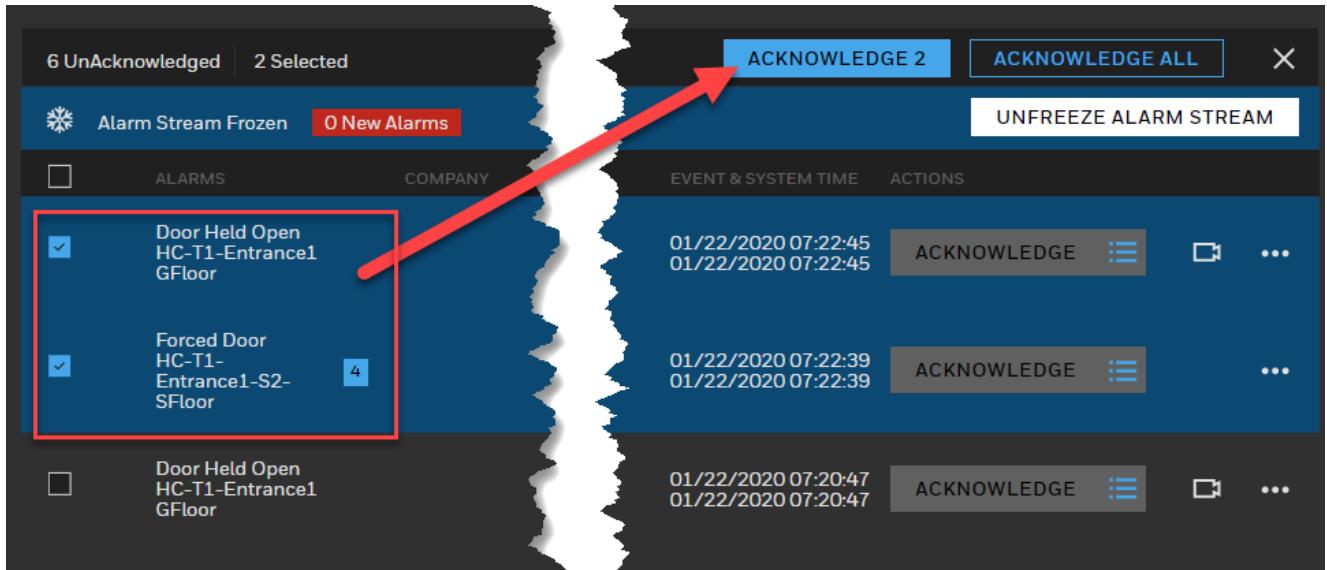


2.12.5 Acknowledging an Unacknowledged Alarm

To acknowledge an unacknowledged alarm:

1. Display the list of unacknowledged alarms by selecting the **Alarms** option from the **Honeywell Hamburger Menu** (Figure 4).
2. Click the **Acknowledge** button on each alarm’s row.

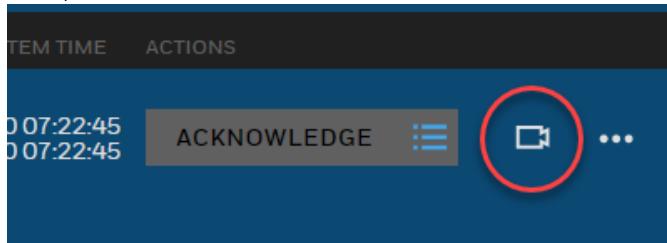
3. Or, first select the unacknowledged alarm's **check-box** and then click the **Acknowledge link** on the menu bar.



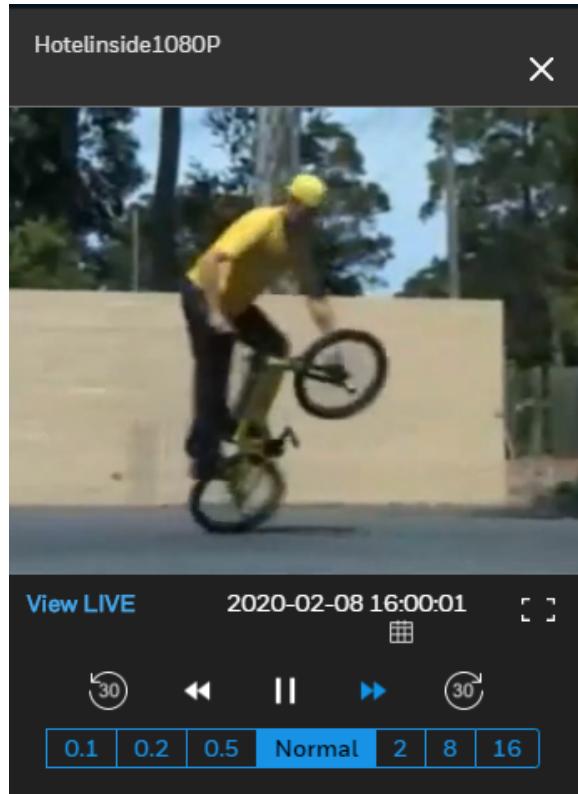
4. To acknowledge all alarms, click the **Acknowledge All** button.

2.12.6 Alarm Camera View

Click the respective **camera icon**  to view the camera view associated with that specific alarm:

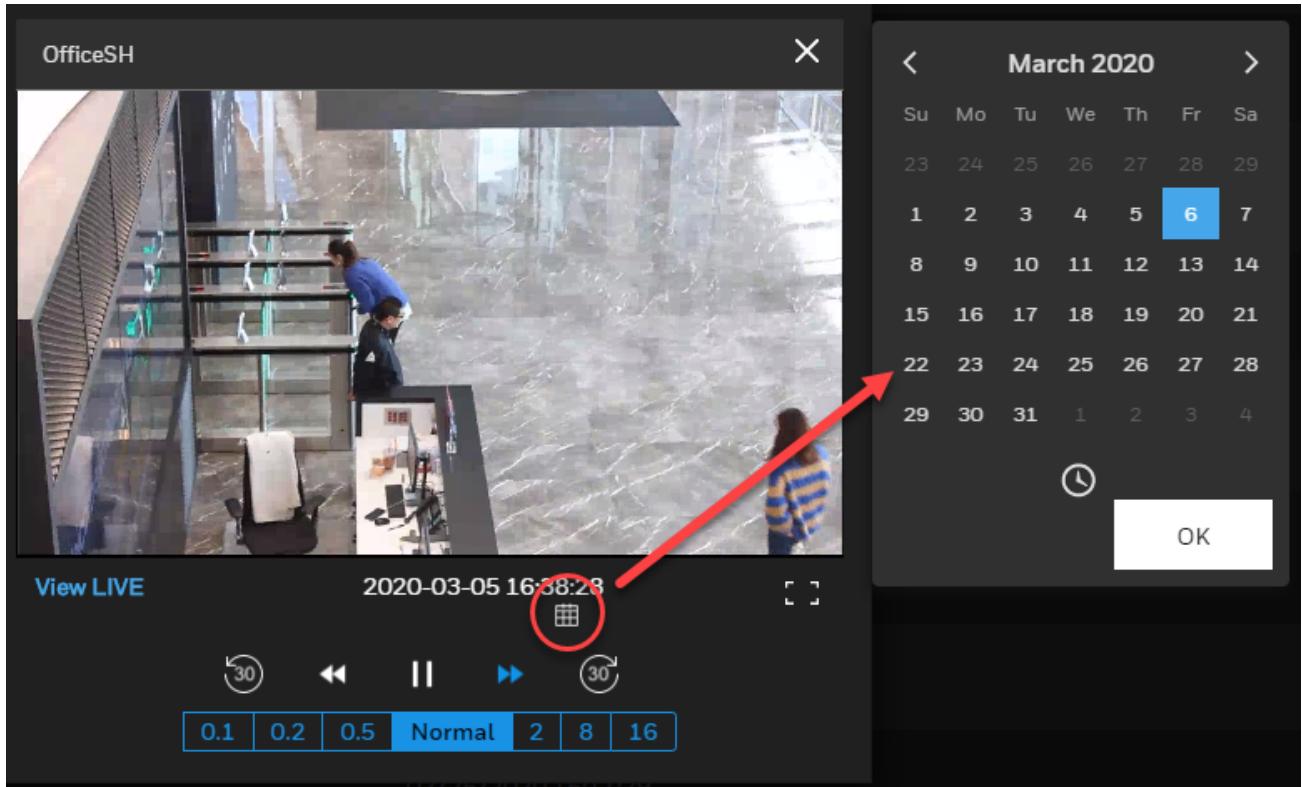


View the video play in the video screen:



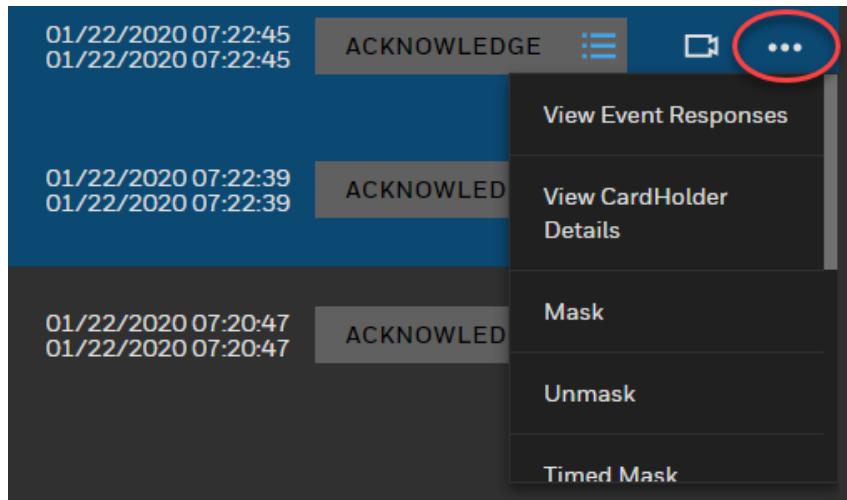
- **Normal** replays the video clip at its original recording speed.
- **To slow down** the replay, select **0.1, 0.2, or 0.5** speed settings.
- **To speed up** the replay, select **2, 8, or 16** speed settings.
- **To jump back or forward for 30 seconds**, click one of the 30-second links.

- To view the same camera recording at a specific date, click the **calendar** icon, browse the calendar and select a date:



2.12.7 Actions

- To select from available responses to an alarm event, click the **ellipsis link (action menu)** on the right of the alarm row to display the respective drop-down list:



- From the drop-down list, select an action option:

- View Cardholder Details**

- **Mask.** See [Masking and Unmasking](#).
- **Unmask.** See [Masking and Unmasking](#).
- **Timed Mask.** See [Masking and Unmasking](#).
- **Activate.** Activates the output.
- **Deactivate.** Deactivates the output.
- **Pulse.** Pulses the output.
- **Timed Activate.** Activates the output for a specified period of time.
- **Lock** - locks an unlocked door. Until the operator unlocks it again, the door remains locked.
- **Unlock** - unlocks a locked door. Until the operator locks it again, the door remains unlocked.
- **Momentary Unlock** - momentarily unlocks a locked door for the duration of the **Strike Time**, as configured in the device settings. Used by the operators to let someone in quickly, after which the door reverts to the locked state.
- **Reenable** - reverts a disabled door back to its original time values set in its access code.
- **Time Override** - allows the operator to manually override the device's time settings for a configurable Time Interval, after which the door reverts back to its original settings. When this option is selected, the system displays a configurable Time Interval field in minutes. This shunts the DPS and subsequent alarms, thereby for period of time overrides the default operational mode.

2.12.7.1 Masking and Unmasking

Masking and **unmasking** allows the operator to remove (mask) a device from the access system or restore (unmask) a device to the access system.

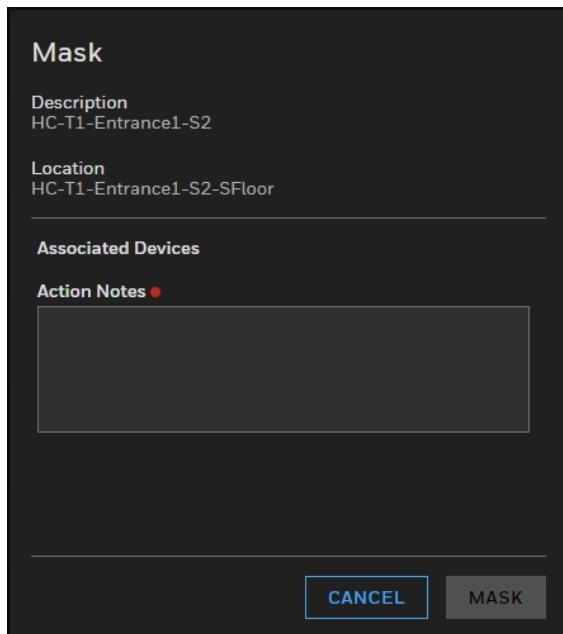
An alarm may indicate a problem with a specific logical device that requires action. For example, a broken door may be causing a forced door alarm. You can initiate a mask action to temporarily remove the door from the access system in order to prevent continuous alarms during the repair of the door.

You can initiate a **Timed Mask** action to temporarily remove the door from the access system in order to prevent continuous alarms during the repair of the door.

Caution: If someone masks a door or unlocks a door and a shift change happens, the new operator may not realize that a door was unlocked or masked.

To Mask

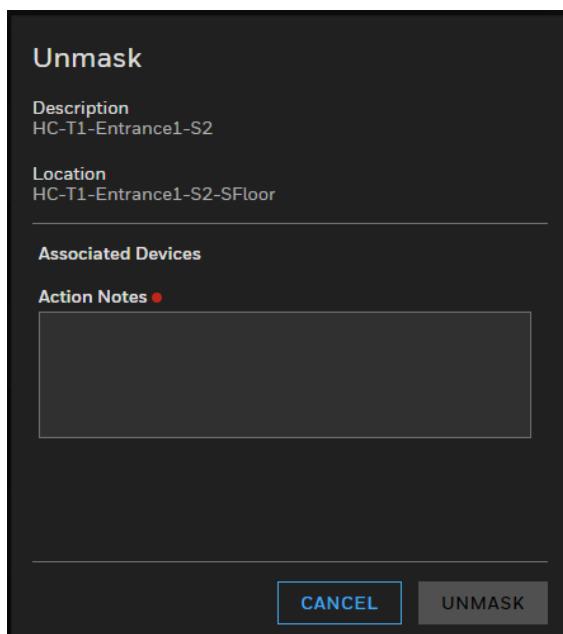
Select the **Mask** action from the Actions drop-down menu of optional actions.



Enter an **Action Note** and click **Mask**.

To Unmask

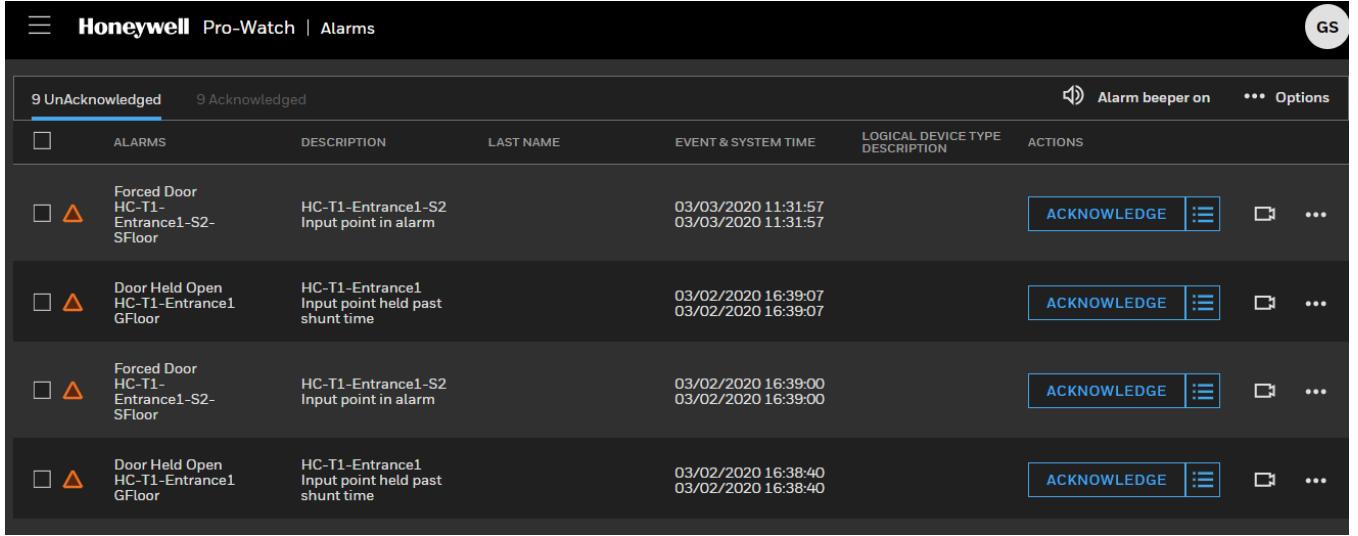
Select the **Unmask** action from the Actions drop-down menu of optional actions.



Enter an **Action Note** and click **Unmask**.

2.12.7.2 Alarm Landing Screen

Select **Alarms** to display the Alarms Landing Screen. [Figure 4](#) displays the list of unacknowledged alarms by default:

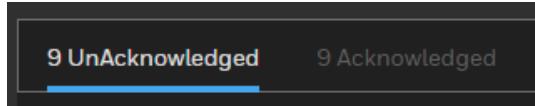


The screenshot shows the Honeywell Pro-Watch Web Client interface with the 'Alarms' tab selected. At the top, it displays '9 UnAcknowledged' and '9 Acknowledged'. Below this is a table with columns: ALARMS, DESCRIPTION, LAST NAME, EVENT & SYSTEM TIME, LOGICAL DEVICE TYPE DESCRIPTION, and ACTIONS. The table lists four unacknowledged alarms, each with an orange triangle icon and a blue 'ACKNOWLEDGE' button.

ALARMS	DESCRIPTION	LAST NAME	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE DESCRIPTION	ACTIONS
<input type="checkbox"/> △	Forced Door HC-T1- Entrance1-S2- SFloor	HC-T1-Entrance1-S2 Input point in alarm	03/03/2020 11:31:57 03/03/2020 11:31:57		ACKNOWLEDGE ≡ ... <input type="checkbox"/>
<input type="checkbox"/> △	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time	03/02/2020 16:39:07 03/02/2020 16:39:07		ACKNOWLEDGE ≡ ... <input type="checkbox"/>
<input type="checkbox"/> △	Forced Door HC-T1- Entrance1-S2- SFloor	HC-T1-Entrance1-S2 Input point in alarm	03/02/2020 16:39:00 03/02/2020 16:39:00		ACKNOWLEDGE ≡ ... <input type="checkbox"/>
<input type="checkbox"/> △	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time	03/02/2020 16:38:40 03/02/2020 16:38:40		ACKNOWLEDGE ≡ ... <input type="checkbox"/>

Figure 4 Alarm Landing Screen with Unacknowledged Alarms

The number of **unacknowledged** and **acknowledged** alarms are displayed on the top of the screen:



Pro-Watch Web Client

Alarms

To view the list of acknowledged alarms, click the **Acknowledged** link:

9 UnAcknowledged		9 Acknowledged		
<input type="checkbox"/>	ALARMS	DESCRIPTION	LAST NAME	EVENT & SYSTEM TIME
<input type="checkbox"/>	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time		03/03/2020 11:31:57 03/03/2020 11:31:57
<input type="checkbox"/>	Forced Door HC-T1- Entrance1-S2- SFloor	HC-T1-Entrance1-S2 Input point in alarm RTN		03/03/2020 16:39:07 03/03/2020 16:39:07
<input type="checkbox"/>	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time		03/03/2020 16:39:00 03/03/2020 16:39:00
<input type="checkbox"/>	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time		02/25/2020 16:38:40 02/25/2020 16:38:40

Acknowledging Alarms

To acknowledge one or more alarms, select them in the list of unacknowledged alarms and then click **Acknowledge [Number]**:

9 UnAcknowledged		3 Selected	ACKNOWLEDGE 3		
		Alarm Stream Frozen	0 New Alarms		
<input type="checkbox"/>	ALARMS	DESCRIPTION	LAST NAME	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE DESCRIPTION
<input checked="" type="checkbox"/>	Forced Door HC-T1- Entrance1-S2- SFloor	HC-T1-Entrance1-S2 Input point in alarm		03/03/2020 11:31:57 03/03/2020 11:31:57	ACKNO
<input checked="" type="checkbox"/>	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time		03/02/2020 16:39:07 03/02/2020 16:39:07	ACKNO
<input checked="" type="checkbox"/>	Forced Door HC-T1- Entrance1-S2- SFloor	HC-T1-Entrance1-S2 Input point in alarm		03/02/2020 16:39:00 03/02/2020 16:39:00	ACKNO
<input type="checkbox"/>	Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time		03/02/2020 16:38:40 03/02/2020 16:38:40	ACKNO

To acknowledge all alarms, click **Acknowledge All**:



You can also acknowledge individual alarms by clicking their respective **Acknowledge** button:

<input checked="" type="checkbox"/>	ALARMS	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE DESCRIPTION	DESCRIPTION	ADDRESS	ACTIONS
<input checked="" type="checkbox"/>	Video Server Status Blre_VMS	05/14/2020 15:32:36 05/14/2020 15:32:36		Blre_VMS Communication Break	100	ACKNOWLEDGE
<input checked="" type="checkbox"/>	Recorder Event	05/13/2020 19:43:11 05/13/2020 19:43:11		Hybrid NVR R6.5 IP22 Low Disk Space	5235	ACKNOWLEDGE
<input checked="" type="checkbox"/>	Recorder Event	05/13/2020 19:39:41 05/13/2020 19:39:41		Hybrid NVR R6.5 IP22 Low Disk Space	5235	ACKNOWLEDGE
<input checked="" type="checkbox"/>	Recorder Event	05/13/2020 19:36:51 05/13/2020 19:36:51		Hybrid NVR R6.5 IP22 Low Disk Space	5235	ACKNOWLEDGE
<input checked="" type="checkbox"/>	Recorder Event	05/13/2020 19:33:38 05/13/2020 19:33:38		Hybrid NVR R6.5 IP22 Low Disk Space	5235	ACKNOWLEDGE

When you select to acknowledge all unacknowledged selected alarms, a prompt will ask you if you'd really like to do that:

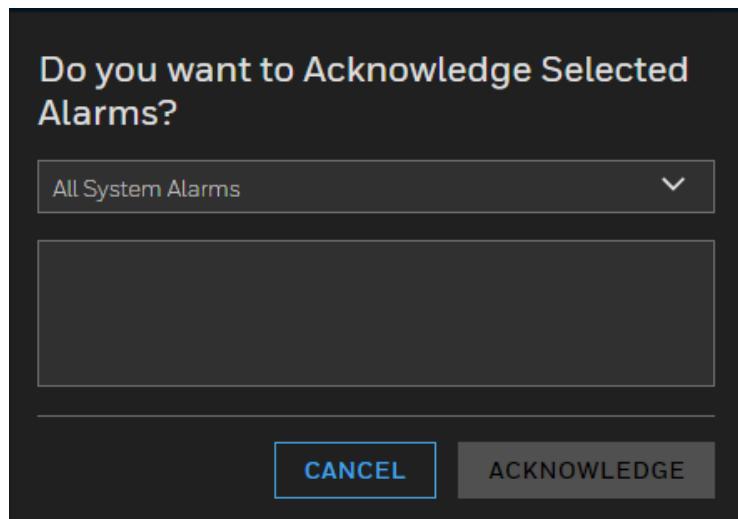
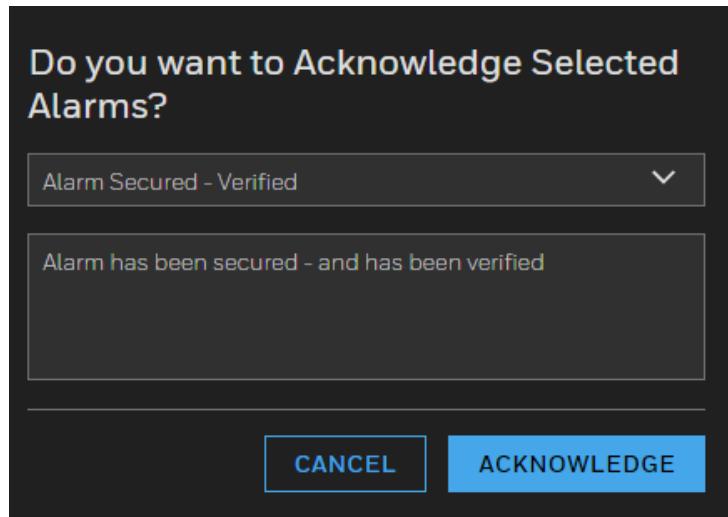


Figure 5 Acknowledge All Alarms Prompt Message

Select one from the drop-down list which enables the **Acknowledge** button or type in your own note:



When you click **Acknowledge**, Pro-Watch will acknowledge all selected alarms (3 in number in [Figure 5](#) but can be any other number, depending on the case).

2.12.8 Acknowledging Workflow-Associated Alarm(s)

On acknowledging an alarm, if (at Event Type or Point level) a workflow is associated, corresponding incident will be created.

2.12.8.1 Acknowledging a Workflow-Associated Alarm

1. Acknowledge a workflow-associated alarm by clicking the ACKNOWLEDGE button link:

The screenshot shows a list of alarms. At the top, it says "2 UnAcknowledged" and "20 Acknowledged". There are two rows of data:

ALARMS	DESCRIPTION	LAST NAME	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE DESCRIPTION	ACTIONS
<input type="checkbox"/> △ Door Held Open HC-T1-Entrance1 GFloor	HC-T1-Entrance1 Input point held past shunt time		04/10/2020 12:00:01 04/10/2020 12:00:01	Door Position	ACKNOWLEDGE ☰ ...
<input type="checkbox"/> △ Forced Door HC-T1-Entrance1-S2-SFloor	HC-T1-Entrance1-S2 Input point in alarm		04/10/2020 11:59:52 04/10/2020 11:59:52	Door Position	ACKNOWLEDGE ☰ ...

2. The user will be taken to the newly created Incident:

The screenshot shows a mobile-style interface for the Honeywell Pro-Watch Web Client. At the top, there's a navigation bar with three horizontal lines on the left, the text "Honeywell Pro-Watch | Incidents" in the center, and a circular icon with "AA" on the right. Below the navigation is a back arrow labeled "← Back". The main content area has a dark header with the text "Door3" and some status counts: "12 unassigned", "4 in progress", and "1 completed". The main body contains a card for an incident with the following details:

- ID 514
- Type: **Void Card**
- Date: 2020-05-15 02:43:31
- Location: Door3
- Workflow Name: Max step_TC_1
- Description: TEST STEP ADDING
- User: --
- Activity: Administrator 02:43:31 - Created an incident.

A blue button at the bottom of the card says "RESPOND NOW".

Note: Consider the case when a workflow is associated with the same event type at a Point and Event level. When the alarm from that point is acknowledged, the **workflow associated with the Point takes precedence** over the workflow that is associated at the Event Type while creating the incident.

2.12.8.2 Acknowledging a Workflow-Associated Rolled-Up Alarm

On acknowledging a Rolled-Up alarm, equal number of incidents per alarm will be created.

Pro-Watch Web Client

Alarms

Here is an example where 2 Void Card Alarms are rolled up into 1, as shown below:

The screenshot shows the Honeywell Pro-Watch Alarms interface. At the top, it displays '5 UnAcknowledged' and '1 Acknowledged'. The main table lists alarms with columns for ALARMS, COMPANY, LAST NAME, FIRST NAME, and EVENT & SYSTEM TIME. One specific alarm is highlighted with a red border and a green status bubble containing the text 'Returned to Normal'.

ALARMS	COMPANY	LAST NAME	FIRST NAME	EVENT & SYSTEM TIME
□	Porter Comm Not Responding ApplicationModule			05/03/2020 20:58:18 05/03/2020 20:58:18
□	Video Server Status VMS			05/03/2020 22:49:53 05/03/2020 22:49:53
□	Video Server Status VMS			05/03/2020 20:58:55 05/03/2020 20:58:55
□	Void Card PW-5000 Demo Case 2 Rollups			05/03/2020 23:03:32 05/03/2020 23:03:32

Two incident are created for each alarm, as shown below:

The screenshot shows the Honeywell Pro-Watch Incidents interface. It displays a table with 43 incidents, each row containing a workflow name, ID, creation date, owner, and progress bar. Two specific incidents are highlighted with a red border.

WORKFLOW NAME	ID	CREATED ON	OWNER	PROGRESS
Event Prep Fire/Fire6	87	2020-05-03 23:04:35		0 of 1
Event Prep Fire/Fire6	86	2020-05-03 23:04:35		0 of 1
Event Prep Fire/Fire6	85	2020-05-03 23:01:44		0 of 1
Test Sop6	84	2020-05-03 14:26:13		0 of 1
Test Sop6	83	2020-05-03 14:24:01		0 of 1
Event Prep Fire/Fire6	82	2020-05-03 11:42:19		0 of 1

Here is the created incident for reference:

The screenshot shows a single incident entry titled "Void Card". The incident details are as follows:

- ID: 87 • Void Card
- Date: 2020-05-03 23:04:35
- Case: PW-5000 Demo Case
- Workflow Name: Event Prep Fire/Fire6
- Description: This procedure shall be completed 48hours before any events.
- Activity: mely 23:04:35 - Created an incident.

A blue button labeled "RESPOND NOW" is visible at the bottom left. A red box highlights the entire incident entry.

2.12.8.3 Acknowledging Multiple Alarms With or Without a Workflow Associated

Workflow-associated alarms will be skipped when acknowledging all alarms or acknowledging multiple alarms. Such alarms need to be acknowledged individually by the user.

Refer to the below screen shots.

Example: User Selected 5 Alarms

The screenshot shows a list of 5 selected alarms. The top navigation bar indicates "5 UnAcknowledged" and "5 Selected". The toolbar includes "ACKNOWLEDGE 5", "ACKNOWLEDGE ALL" (which is highlighted with a red box), and "UNFREEZE ALARM STREAM".

ALARMS	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE	PRIORITY	DESCRIPTION	ACTIONS
<input checked="" type="checkbox"/> Operator Action	05/03/2020 22:11:02 05/03/2020 22:11:02		1	Operator has logged in	<button>ACKNOWLEDGE</button> <button>⋮</button> <button>...</button>
<input checked="" type="checkbox"/> Void Card Testing The Location	05/03/2020 22:09:21 05/03/2020 22:09:21	Reader	2	Entrance 1 Void Card	<button>ACKNOWLEDGE</button> <button>⋮</button> <button>...</button>
<input checked="" type="checkbox"/> Void Card Testing The Location	05/03/2020 22:09:19 05/03/2020 22:09:19	Reader	2	Entrance 1 Void Card	<button>ACKNOWLEDGE</button> <button>⋮</button> <button>...</button>
<input checked="" type="checkbox"/> Stolen Badge PW-5000 Demo Case	05/03/2020 22:10:07 05/03/2020 22:10:07	Reader	30	Entrance 2 Stolen Card Attempt	<button>ACKNOWLEDGE</button> <button>⋮</button> <button>...</button>
<input checked="" type="checkbox"/> Stolen Badge PW-5000 Demo Case	05/03/2020 22:10:07 05/03/2020 22:10:07	Reader	30	Entrance 2 Stolen Card Attempt	<button>ACKNOWLEDGE</button> <button>⋮</button> <button>...</button>

Two among the 5 Alarms have workflow associated. Thus those 2 are skipped, and the 3 remaining alarms are acknowledged:

Pro-Watch Web Client

Alarms

The screenshot shows the Honeywell Pro-Watch Alarms interface. At the top, there are two tabs: "2 UnAcknowledged" (highlighted in blue) and "5 Acknowledged". Below the tabs is a table with the following columns: ALARMS, EVENT & SYSTEM TIME, LOGICAL DEVICE TYPE DESCRIPTION, PRIORITY, and DESCRIPTION.

ALARMS	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE DESCRIPTION	PRIORITY	DESCRIPTION
<input type="checkbox"/> ◆ Void Card Testing The Location	05/03/2020 21:39:24 05/03/2020 21:39:24	Reader	2	Entrance Void Card
<input type="checkbox"/> ◆ Void Card Testing The Location	05/03/2020 21:39:24 05/03/2020 21:39:24			Incident arc

A modal dialog box is overlaid on the page, containing the following text:

Create Incident

2 of 5 alarms remain unacknowledged because they have incident workflows associated

OK

2.12.9 Clearing Incident Associated Alarm(s)

On clearing an alarm, the alarm service checks if the alarm has an open incident associated to it. If yes, the alarm will not be allowed to clear until the incident is completed or closed.

2.12.9.1 Clearing an Alarm Which Has an Open Incident Ticket

- Recently created incident after a Force Door Alarm acknowledgment:

The screenshot shows the Honeywell Pro-Watch interface for incidents. The title bar says "Honeywell Pro-Watch | Incidents". Below it, "Reader1_TEST" is selected. The main area shows an unacknowledged alarm for "Forced Door" at 2020-05-03 23:21:33, located at "Maitra Main door". The workflow name is "Force Door open". The description is "Force Door open". There is a "RESPOND NOW" button. To the right, the "Activity" section shows an entry for "e570970" at 23:21:33: "Created an incident."

- User trying to **Clear** the alarm from **Acknowledged Alarm Pane**:

The screenshot shows the Honeywell Pro-Watch interface for alarms. The title bar says "Honeywell Pro-Watch | Alarms". The "ALARMS" tab is selected, showing 1 acknowledged alarm. The details for the acknowledged alarm are: "Forced Door" at "Maitra Main door", event time "05/03/2020 23:21:00", system time "05/03/2020 23:21:00", priority 0, address 900. The "ACTIONS" column contains a "CLEAR" button and a more options icon. A red box highlights the "CLEAR" button.

- Clear action failed since the associated incident is still open:

The screenshot shows the Honeywell Pro-Watch interface for alarms again. The "ALARMS" tab is selected, showing 1 acknowledged alarm. The details for the acknowledged alarm are the same as before. The "ACTIONS" column now shows a grayed-out "CLEAR" button and the more options icon.

2.12.9.2 Clearing a Rolled-Up Alarm with Associated Incidents

In case of a rolled-up alarm if one of those alarms respective incident is open, the Clear action will still fail. It requires all the related Incident ticket to be closed. Refer below image

Pro-Watch Web Client

Alarms

1. Clear action failed because at least one associated incident is still open:

<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 21:39:24 05/03/2020 21:39:24	Reader	2	Entrance 1 Void Card	<button>CLEAR</button> <button>☰</button>	<button>...</button>
<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 21:39:24 05/03/2020 21:39:24	Reader	2	Entrance 1 Void Card	<button>CLEAR</button> <button>☰</button>	<button>...</button>
<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 20:56:48 05/03/2020 20:56:48	Reader	2	Entrance 1 Void Card	<button>CLEAR</button> <button>☰</button>	<button>...</button>
<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 20:56:47 05/03/2020 20:56:47	Reader	2	Entrance 1 Void Card	<button>CLEAR</button> <button>☰</button>	<button>...</button>
<input type="checkbox"/>	<input checked="" type="radio"/>	Unknown Badge READER_1 3 Rollups	05/03/2020 21:46:54 05/03/2020 21:46:55	Reader	8	READER_1 Unknown Card	<button>CLEAR</button> <button>☰</button>	<button>...</button>

2.12.9.3 Clearing Multiple Acknowledged Alarms or All Alarms

When user Clear all, if there are open Incident associated to those acknowledged alarms then those alarms will be skipped without clearing.

Honeywell Pro-Watch Alarms					
1 UnAcknowledged		3 Acknowledged			
<input type="checkbox"/>	ALARMS	EVENT & SYSTEM TIME	LOGICAL DEVICE TYPE DESCRIPTION	PRIORITY	DESCRIPTION
<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 21:39:24 05/03/2020 21:39:24	Reader	2
<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 20:56:48 05/03/2020 20:56:48		
<input type="checkbox"/>	<input checked="" type="radio"/>	Void Card Testing The Location	05/03/2020 20:56:47 05/03/2020 20:56:47		

Complete Incident

3 of 6 Alarm(s) remains uncleared because there are associated incident(s).

OK

2.12.10 View Rollup Details

Note: Video is not supported in the Rollup function.

Alarm Rollup function displays multiple events for a single logical device in a single line. A counter field in that line indicates the total number of events received.

Events assigned to an event type are subject to alarm rollup under the following conditions:

- Rollup Events check-box must be selected in the **Event Type** configuration dialog box.

- Rollup number must be selected on the alarm page. You can view rolled-up events on the alarm page.

The screenshot shows a dark-themed user interface titled "Roll up details". At the top, it displays "Void Card | PW-5000 Demo Case". Below this, a circular badge indicates "14" events. The main area is divided into two columns: "EVENT & SYSTEM TIME" and "ACTIONS". The "EVENT & SYSTEM TIME" column lists four pairs of dates/times, each followed by a small "copy" icon. The "ACTIONS" column contains four "OK" buttons, one corresponding to each row. The entire interface has a clean, modern design with a focus on readability and ease of use.

EVENT & SYSTEM TIME	ACTIONS
04/26/2020 16:28:00	OK
04/26/2020 16:27:59	OK

Figure 6 View Rollup Details

2.13 Events

- See “**Pausing Events**” on page 71.
- See “**Filtering Events**” on page 72.
- See “**Clearing Events**” on page 73.

Display the main **Honeywell Hamburger Menu**.

Select **Events** to display the Events Landing Screen:

EVENT TYPE & DESCRIPTION	LOGICAL DEVICE DESCRIPTION	EVENT & SYSTEM TIME	FULL NAME	LOCATION	COMPANY
Stolen Badge	Entrance 2	04/26/2020 16:24:21 04/26/2020 16:24:21		PW-5000 Demo Case	
Stolen Badge	Entrance 2	04/26/2020 16:24:20 04/26/2020 16:24:20		PW-5000 Demo Case	
Operator Action		04/26/2020 16:24:19 04/26/2020 16:24:19			
Stolen Badge	Entrance 2	04/26/2020 16:24:19 04/26/2020 16:24:19		PW-5000 Demo Case	
Operator Action		04/26/2020 16:08:36 04/26/2020 16:08:36			
Operator Action		04/26/2020 16:07:39 04/26/2020 16:07:39			

Figure 7 Events Landing Screen

The events will be displayed in rows, with the following properties, each represented by a separate column:

- Event System & Time
- Event Type Description
- Logical Device Description
- Full Name
- Company
- Point Description
- Card Number
- Card Status

Note: Operator Logon /Logoff event will be reported as **Event Occurred** from web.

2.13.1 Pausing Events

You can click the **Pause Event Stream** button on the upper-right to temporarily stop event reporting.

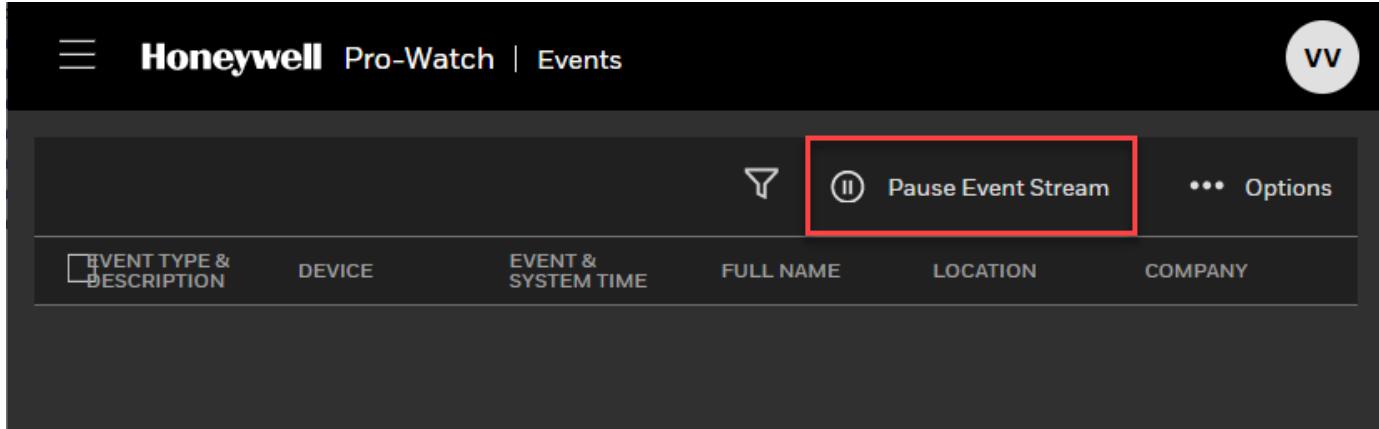


Figure 8 Pause Events

The system will display an “**Resume Event Stream Paused**” message when you click the **Pause Event Stream** button.

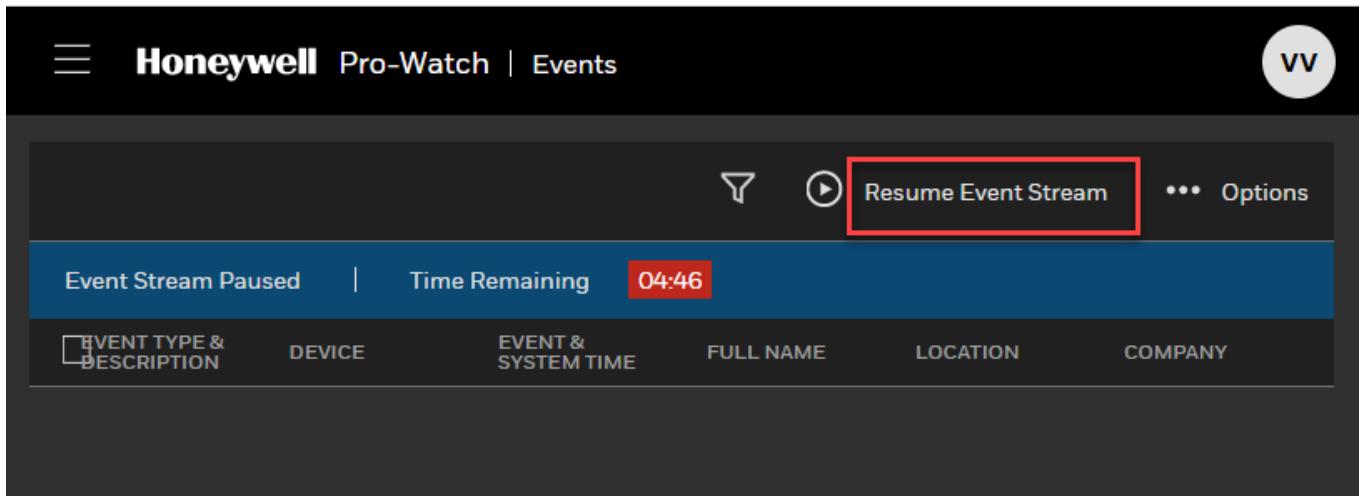


Figure 9 Event Stream Paused

A count-down timer will display how much pause time is left, before the system automatically unpausing following the countdown.

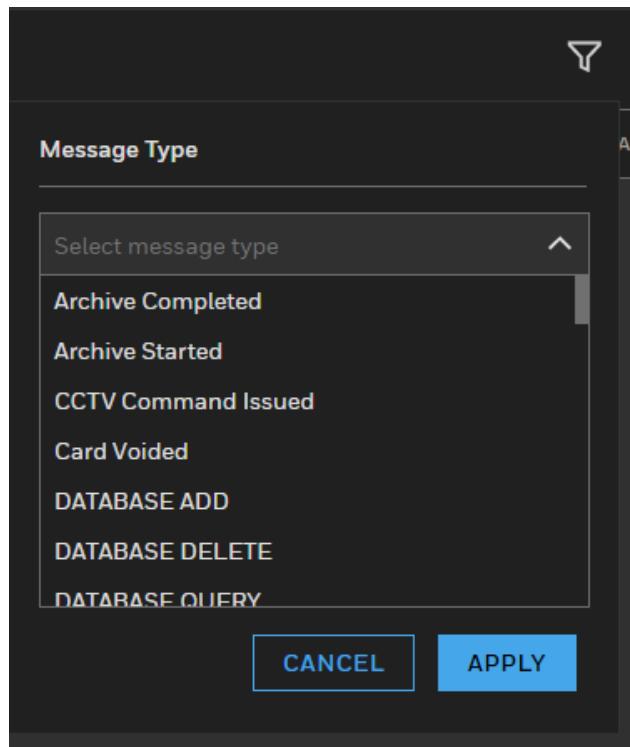
See “**Events**” on page 70.

2.13.2 Filtering Events

Click the **Filter** button on the upper-right to display the filtering options.

2.13.2.1 Filtering by Message Type

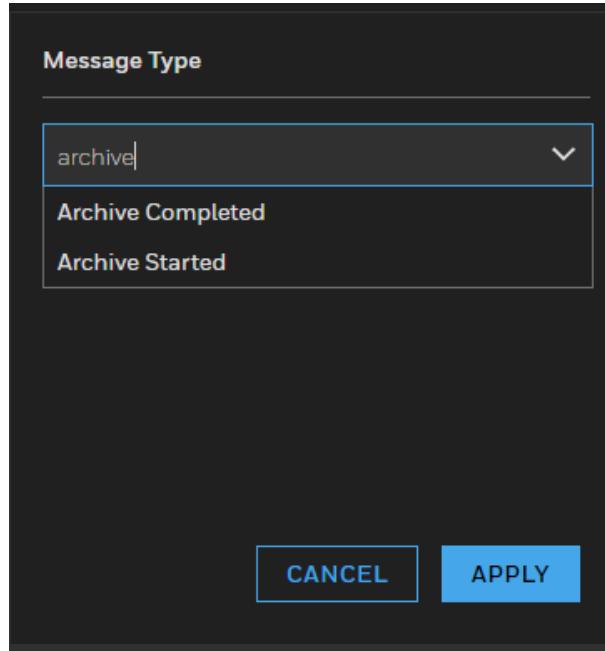
You can filter by **Message Type** by clicking the Search drop-down list and then selecting a type from the list:



When done, click **Apply**.

2.13.2.2 Filtering by Text Search

You can also filter events by entering a text string into the search box to display the message types that contain the search keyword(s):



See “**Events**” on page 70.

2.13.3 Clearing Events

To clear events, do one of the following:

1. Select one or more individual events by checking their check-boxes and then click the **Clear** button.

Pro-Watch Web Client

Events

2. Click **Clear All** button to clear all the alarm events displayed.

<input checked="" type="checkbox"/> EVENT TYPE & DESCRIPTION	LOGICAL DEVICE DESCRIPTION	EVENT & SYSTEM TIME	FULL NAME	LOCATION	COMPANY
<input checked="" type="checkbox"/> Stolen Badge	Entrance 2	04/27/2020 17:19:23 04/27/2020 17:19:23		PW-5000 Demo Case	
<input checked="" type="checkbox"/> Stolen Badge	Entrance 2	04/27/2020 17:19:23 04/27/2020 17:19:23		PW-5000 Demo Case	
<input checked="" type="checkbox"/> Stolen Badge	Entrance 2	04/27/2020 17:19:22 04/27/2020 17:19:22		PW-5000 Demo Case	
<input checked="" type="checkbox"/> Stolen Badge	Entrance 2	04/27/2020 17:19:22 04/27/2020 17:19:22		PW-5000 Demo Case	
<input checked="" type="checkbox"/> Stolen Badge	Entrance 2	04/27/2020 17:19:22 04/27/2020 17:19:22		PW-5000 Demo Case	
<input checked="" type="checkbox"/> Stolen Badge	Entrance 2	04/27/2020 17:19:22 04/27/2020 17:19:22		PW-5000 Demo Case	

Figure 10 Clearing Alarm Events

See “**Events**” on page 70.

2.13.4 FAQs - Troubleshooting and Functional Workarounds

1. PROBLEM: Events and Live alarms not coming in 3-Tier Installation.

SOLUTION: Add Webserver workstation in Pro-Watch Thick client to get events and live alarms.

2. PROBLEM: Live alarms or Events not coming either with or without Redbanner error message.

SOLUTION: Try one of the following, one at a time:

- a. Refresh the web page.
- b. Logout and Login.
- c. Restart the Event Service .
- d. Reset IIS.

3. PROBLEM: Unable to logout/Internal Server error.

SOLUTION:

- a. Clear your browser cookies.
- b. Logout and Login

4. PROBLEM: Logical device description for alarm is not shown for Panel Comm Not responding events in web client.

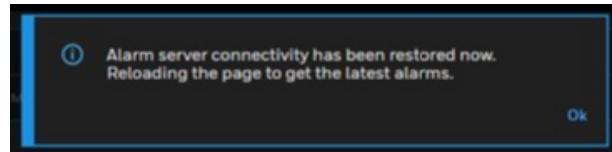
SOLUTION:

- a. See the logical device description on Alarm detail page.

5. **PROBLEM:** Disconnection between:

- Browser & Live Alarm Service
- Live Alarm Service & Alarm Processor
- Alarm Processor & Mic Service

SOLUTION: Users will be informed with the error message and upon successful re-connection the error message will be hidden and "Alarm Page Reload" pop-up will be prompted to re-fetch the latest alarms from the server.



2.14 Reports

- See "**Report Terminology**" on page 76.
- See "**Report Limitations**" on page 76.
- See "**Add, Edit or Delete a Report**" on page 76.
- See "**View or Run a Report**" on page 77.
- See "**Printing a Report**" on page 78.
- See "**Exporting a Report**" on page 78.
- See "**People & Group (Badging) Settings**" on page 81.
- See "**Workflow Settings**" on page 82.

Display the main **Honeywell Hamburger Menu**:

Select **Report** to display the My Reports screen:

Figure 10 Web Report Manager Screen

The screenshot shows a grid of six report cards under the heading ': Access Reports'. Each card has a title, a star icon, and a 'GENERATE' button.

- Badge Holder Access to Logical Device**: Type Badge, Status Shared, Owner Administrator, Last Run 05/14/2020 08:43:00. Description: This report will display badge holders who have acce... [More](#). Buttons: GENERATE.
- Badge Holders in Clearance Code**: Type Badge, Status Shared, Owner Administrator, Last Run 05/14/2020 08:43:00. Description: This report will display all active badge holder car... [More](#). Buttons: GENERATE.
- Badge Holders in Clearance Codes - Select by Compa...**: Type Badge, Status Shared, Owner Administrator, Last Run 07/12/2017 09:47:00. Description: This report will display all badge holders and their... [More](#). Buttons: GENERATE.
- Badge Only Transactions1234**: Type Transaction, Status Shared, Owner Administrator, Last Run 04/30/2020 01:24:00. Description: This report will display card only transactions for ... [More](#). Buttons: GENERATE.
- Card not used in the Last X Days**: Type Badge, Status Shared, Owner Administrator, Last Run 05/14/2020 08:41:00. Description: This report will display active badge holder cards t... [More](#). Buttons: GENERATE.
- Card Status - Select by Card Company**: Type Badge, Status Shared, Owner Administrator, Last Run 06/26/2017 01:58:00. Description: Go to System in Control Panel to activate Windows. This report is a card status report filtered by comp... [More](#). Buttons: GENERATE.

2.14.1 Report Terminology

“Viewing” and “running” a report are used interchangeably since they mean the same thing.

2.14.2 Report Limitations

If you have more than 20,000 rows per report, the report export behavior may change depending on your system setup.

2.14.3 Add, Edit or Delete a Report

You cannot create a new report, edit or delete an existing report from inside the thin web client. However, you can view the sample reports created in Pro-Watch thick client.

See “**Reports**” on page 75.

2.14.4 View or Run a Report

- In the Reports module, select a **Sample Report Category** to display the individual reports of that category in the right pane:

Honeywell Pro-Watch | Reports

Sample Report Category

Individual Reports

Suggested

Access Reports

Others

Badge Holder Access to Logical Device

Type Badge
Status
Owner prowatch madurai
Last Run

This report will display badge holders who have acce... [More](#)

GENERATE

Badge Holders in Clearance Code

Type Badge
Status
Owner prowatch madurai
Last Run

This report will display all active badge holder car... [More](#)

GENERATE

Badge Holders in Clearance Codes - Select by Compa...

Type Badge
Status
Owner prowatch madurai

Card not used in the Last 7 Days

Type Badge
Status
Owner prowatch madurai

- Click the **Favorites** star icon to save the individual report in the Favorites folder:

Badge Holder Access to Logical Device

Type Badge
Status
Owner prowatch madurai
Last Run

This report will display badge holders who have acce... [More](#)

GENERATE

3. Click the **Actions** ellipsis link and select **View** to display the **Runtime Filters** screen.
4. Enter appropriate values for all the filter fields that apply to that specific report. For example, in the below sample screen, enter appropriate values for one, several, or all of the following fields: **Last Name, First Name, Card Number, Company, Logical Device, and/or Clearance Code:**

The screenshot shows a web-based reporting interface titled "Badge Holder Access to Logical Device". At the top, it displays "Type: Badge", "Owner: prowatch madurai", and "Last Run:". Below this, the section "Runtime Filters - Enter Values" contains six input fields, each with a number (1 through 6) and a dropdown menu. The fields are: 1. Last Name (Begins With %), 2. First Name (Begins With %), 3. Card Number (Begins With %), 4. Company (Begins With %), 5. Logical Device (Begins With %), and 6. Clearance Code (Begins With %). Each dropdown menu has a downward arrow icon.

5. Click **Generate** to run your report. The above sample screen will generate a "Badge Holder Access to Logical Device" report.

See "**Reports**" on page 75.

2.14.5 Printing a Report

1. Generate your report as described in the section [View or Run a Report](#).
2. Click **Print** to print your report.

2.14.6 Exporting a Report

Note: If your report has more than 20,000 (twenty thousand) rows, the export behavior may vary, depending on the specific system setup and resources.

1. Generate your report as described in the section [View or Run a Report](#).

2. Click **Export** to display the **Export Report** screen:

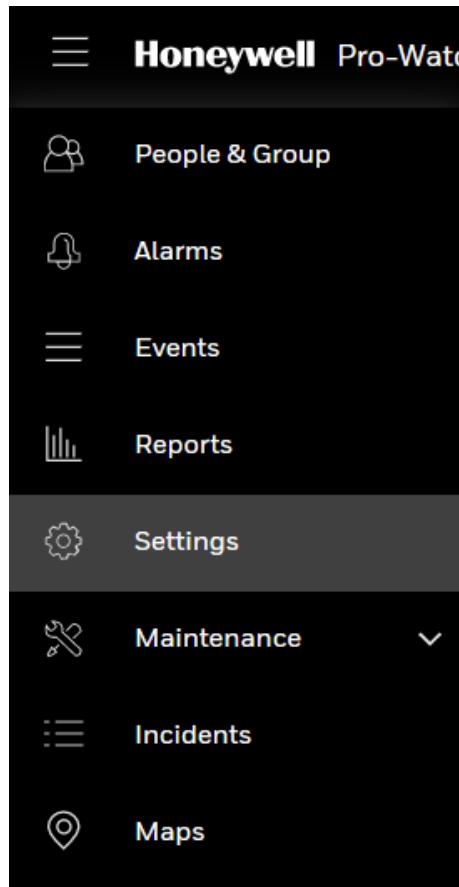
The screenshot shows the 'Export Report' configuration interface. At the top left is the title 'Export Report'. Below it is a section labeled 'Export Type' with a dropdown menu set to 'PDF'. To the right are two dropdown menus: 'Row and Column Sizing' set to 'None' and 'Delimiter' set to 'Vertical Bar'. Below these are three checked checkboxes: 'Display Report Title', 'Display SSI Header & Footer', and 'Display Filter'. A 'Download File Name' input field is present. An 'Email Report. Requires SMTP information' toggle switch is turned off. At the bottom right are 'CANCEL' and 'EXPORT' buttons.

3. Select an **Export Type** from the drop-down menu. Choices are PDF, EXCEL, TXT, XML.
4. Select **Row and Column Sizing** from the drop-down menu. Choices are Size Columns to Contents, Size Rows to Contents, Size Columns and Rows to Contents.
5. Fill in all the necessary fields and make all the appropriate selections.
6. Click **Export** to export your report.

See “**Reports**” on page 75.

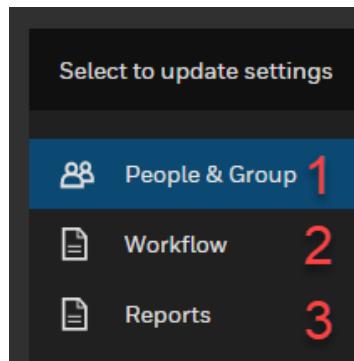
2.15 Settings

Display the main Honeywell Hamburger Menu:



You can configure three different types of settings:

1. People & Group (Badging)
2. Workflow
3. Reports:



2.15.1 People & Group (Badging) Settings

The screenshot shows the Honeywell Pro-Watch Settings interface. On the left, there's a sidebar with options: 'Select to update settings' (highlighted), 'People & Group' (selected and highlighted in blue), 'Workflow', and 'Reports'. The main content area has a 'General' tab selected. Under 'Card Activity Log (Days)', the value '30' is entered. Below that is a section titled 'Define Card Usage Filters' with two columns: 'Fields' and 'Show Data for'. Under 'Fields', three filters are checked: 'Newly Added' (In the last 5 days), 'Expiring' (In 7 Days), and 'Unused' (In the last 30 days). To the right of these fields are input boxes: '5 Days' for Newly Added, 'Today' for Expiring, and '30 Days' for Unused.

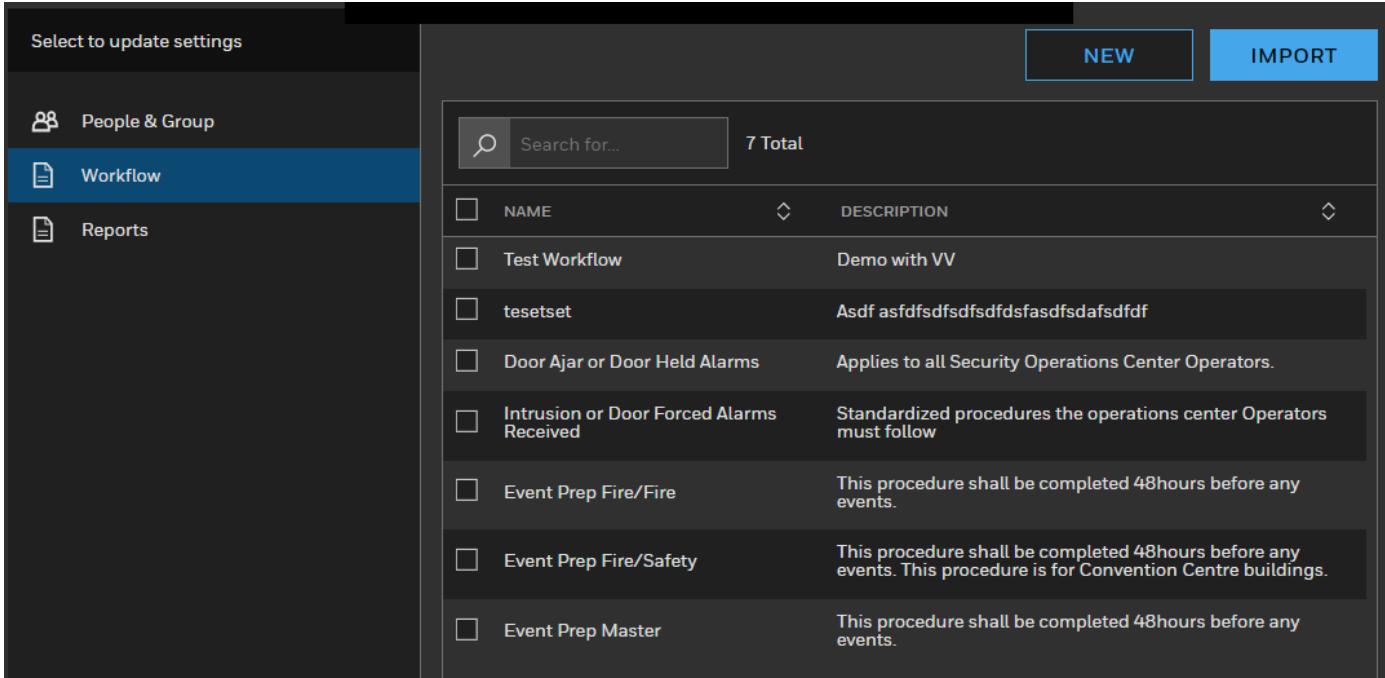
You can filter your badging results by configuring the following fields:

- **Card Activity Log (in X days)**
- **Newly Added in the Last X Days**
- **Expiring in X Days**
- **Unused in the Last X Days**

1. Click **Settings > People & Group** navigation link to display the **General** settings tab.
2. Click the **pencil icon** to activate editing mode.
3. Edit the setting fields.
4. Click **Save**.

2.15.2 Workflow Settings

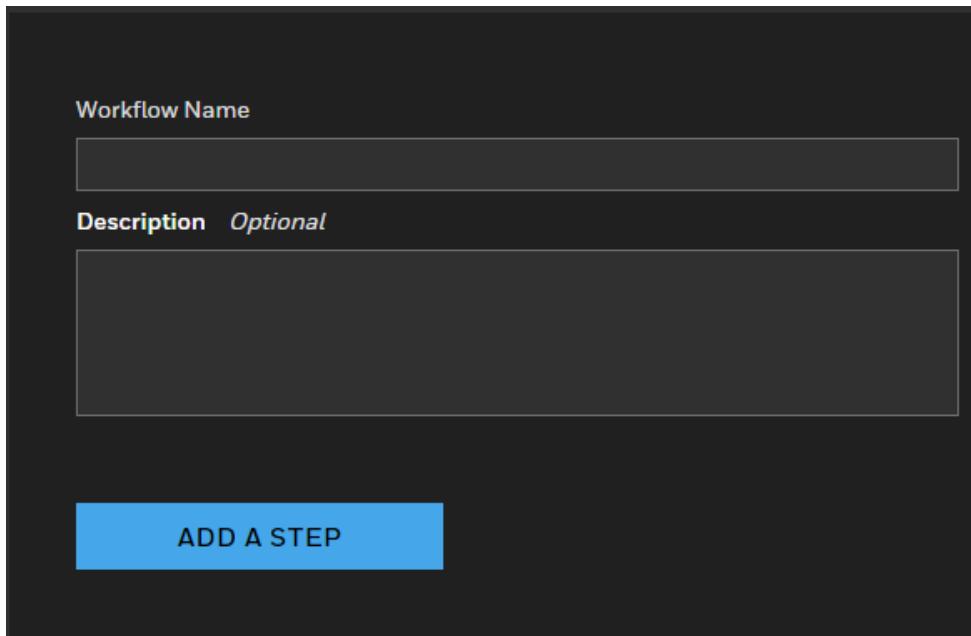
1. Click **Settings > Workflow** navigation link to display the **Workflow** screen:



NAME	DESCRIPTION
Test Workflow	Demo with VV
tesetset	Asdf asfdfdsfsdfsdfsfasdfsdafsdfdf
Door Ajar or Door Held Alarms	Applies to all Security Operations Center Operators.
Intrusion or Door Forced Alarms Received	Standardized procedures the operations center Operators must follow
Event Prep Fire/Fire	This procedure shall be completed 48hours before any events.
Event Prep Fire/Safety	This procedure shall be completed 48hours before any events. This procedure is for Convention Centre buildings.
Event Prep Master	This procedure shall be completed 48hours before any events.

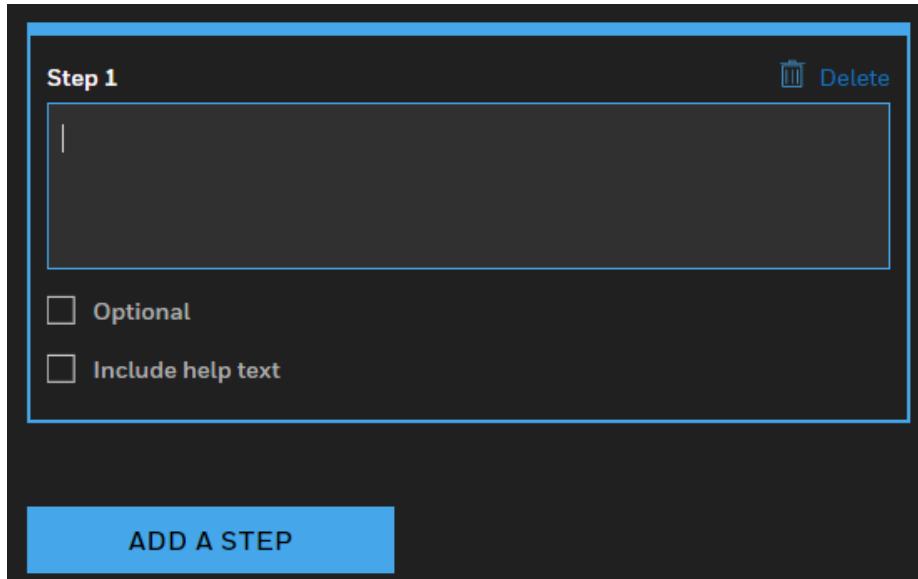
2.15.2.1 Creating a New Workflow

1. Click **New** to display the **New Workflow** screen:



2. Enter a **Workflow Name** and **Description**.

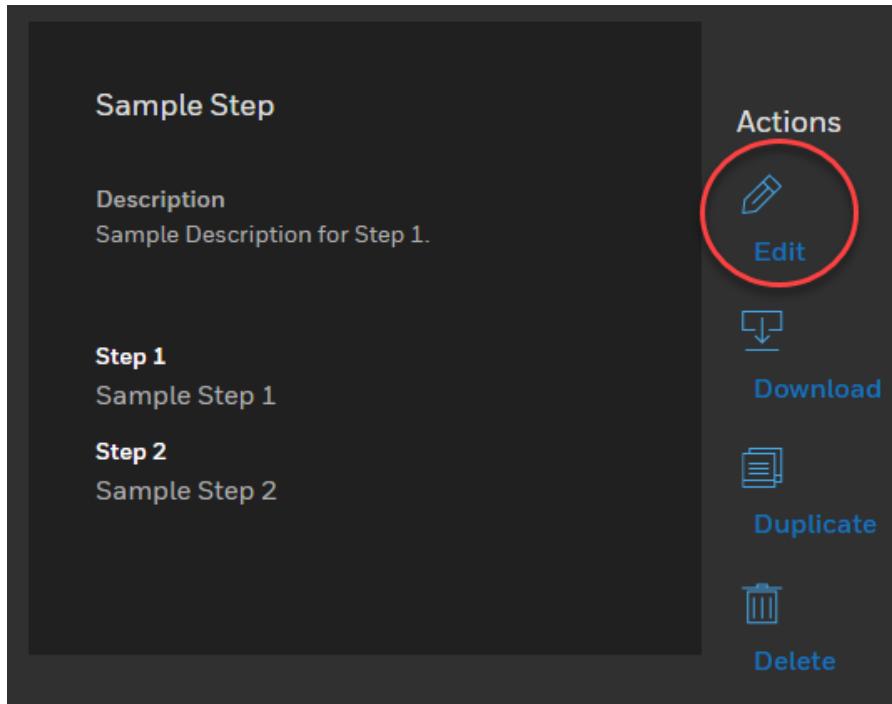
3. Click **Add a Step** to display the **Add a Step** screen:



4. Fill in the necessary information.
5. To add another step, again click the **Add a Step** button and repeat step 4 above.
6. When you added all the steps, click **Save**.

2.15.2.2 Editing a Workflow

1. Double-click it in the workflow list.
2. In the **Actions** list, click **Edit** to display the editing screen:



3. Make the necessary edits and click **Save**.
4. To duplicate a workflow, click the **Duplicate** link.
5. To download a workflow, click the **Download** link.

2.15.2.3 Deleting a Workflow

Select it in the workflow list or the editing screen and click **Delete**.

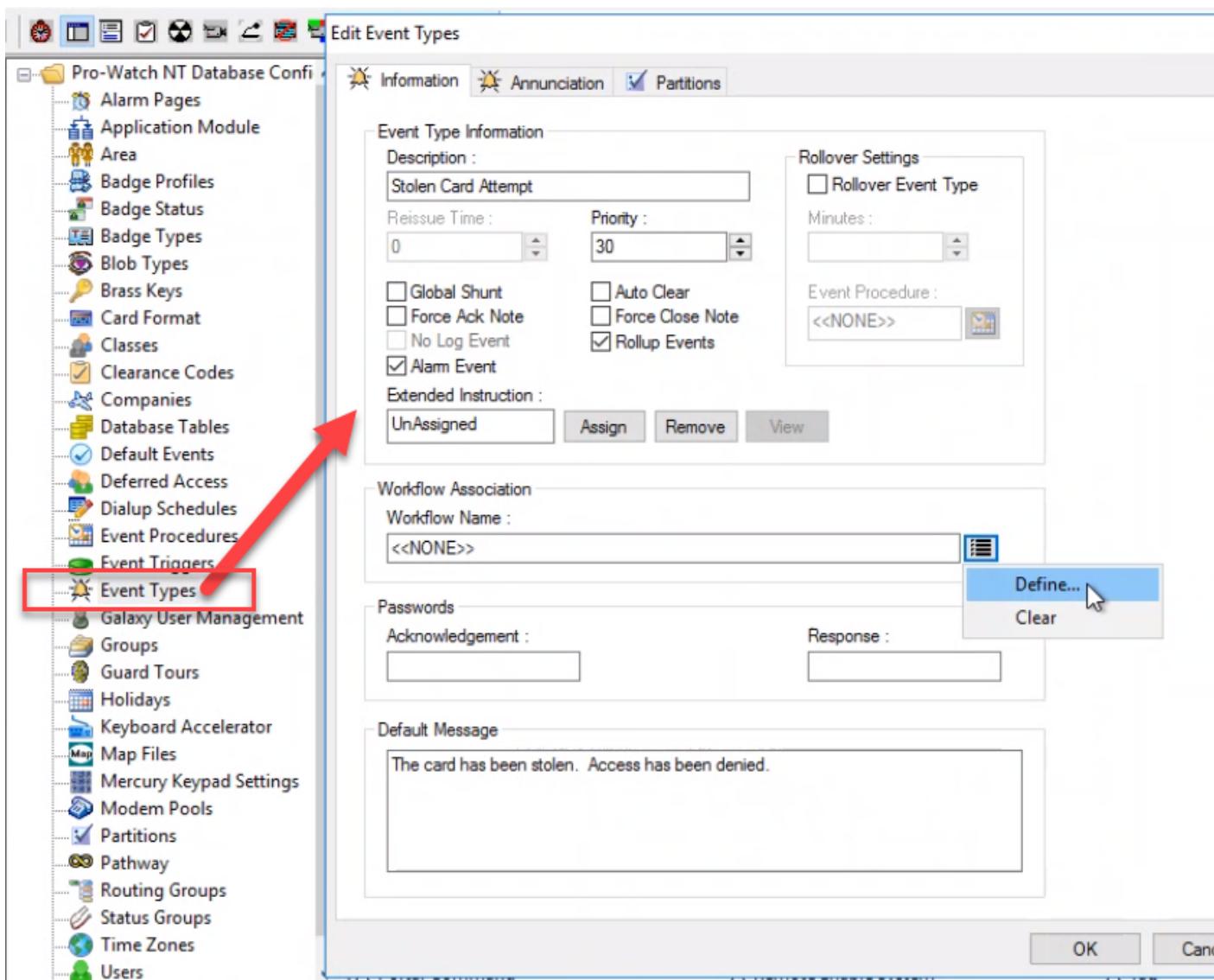
2.15.2.4 Importing a Workflow

1. In the workflow list screen, click the **Import** button.
2. Browse and find the workflow file and click **Open**.

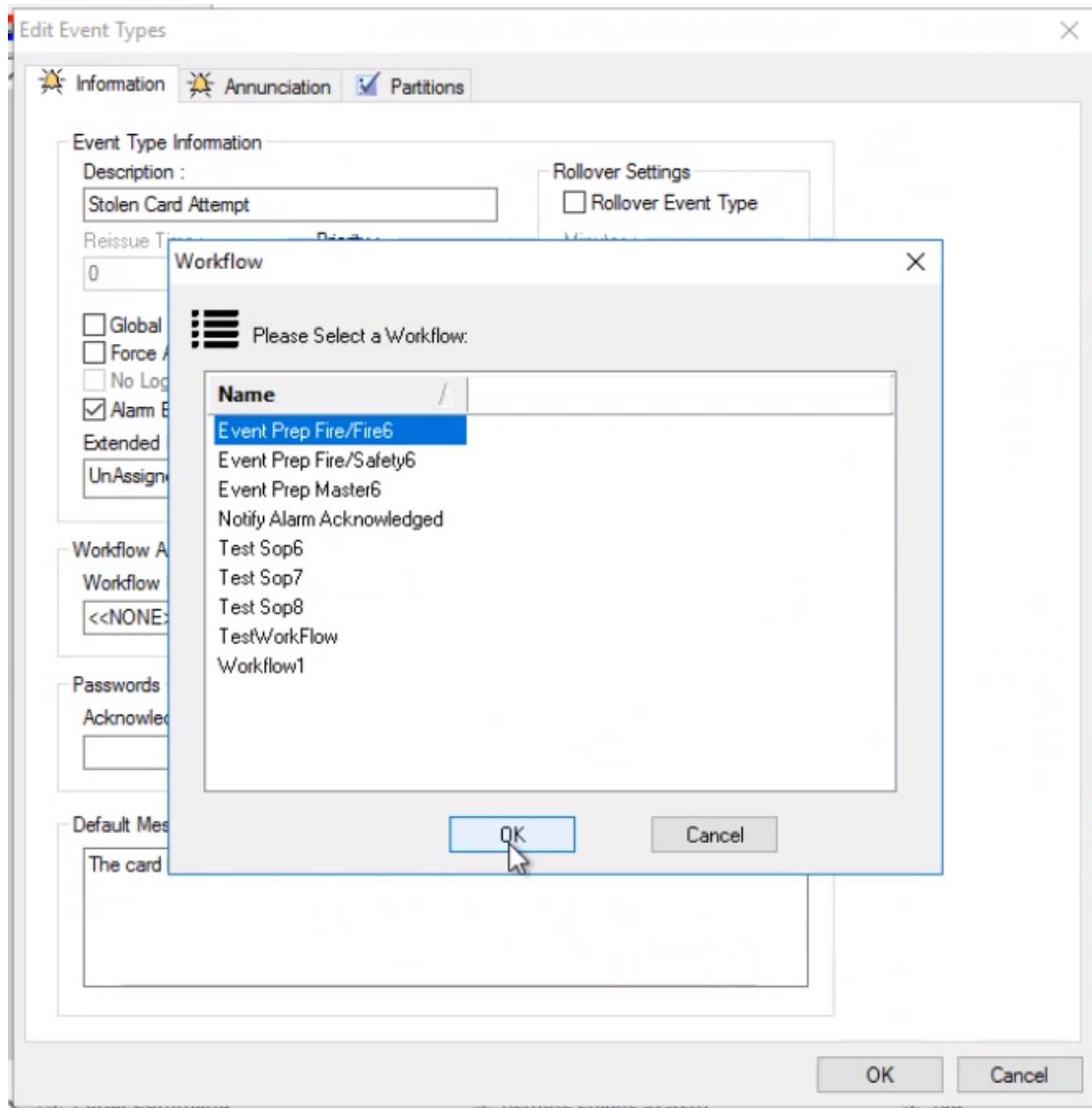
2.15.2.5 Associating Workflows at the Event Level

Note: Pro-Watch supports a maximum number of 500 workflows.

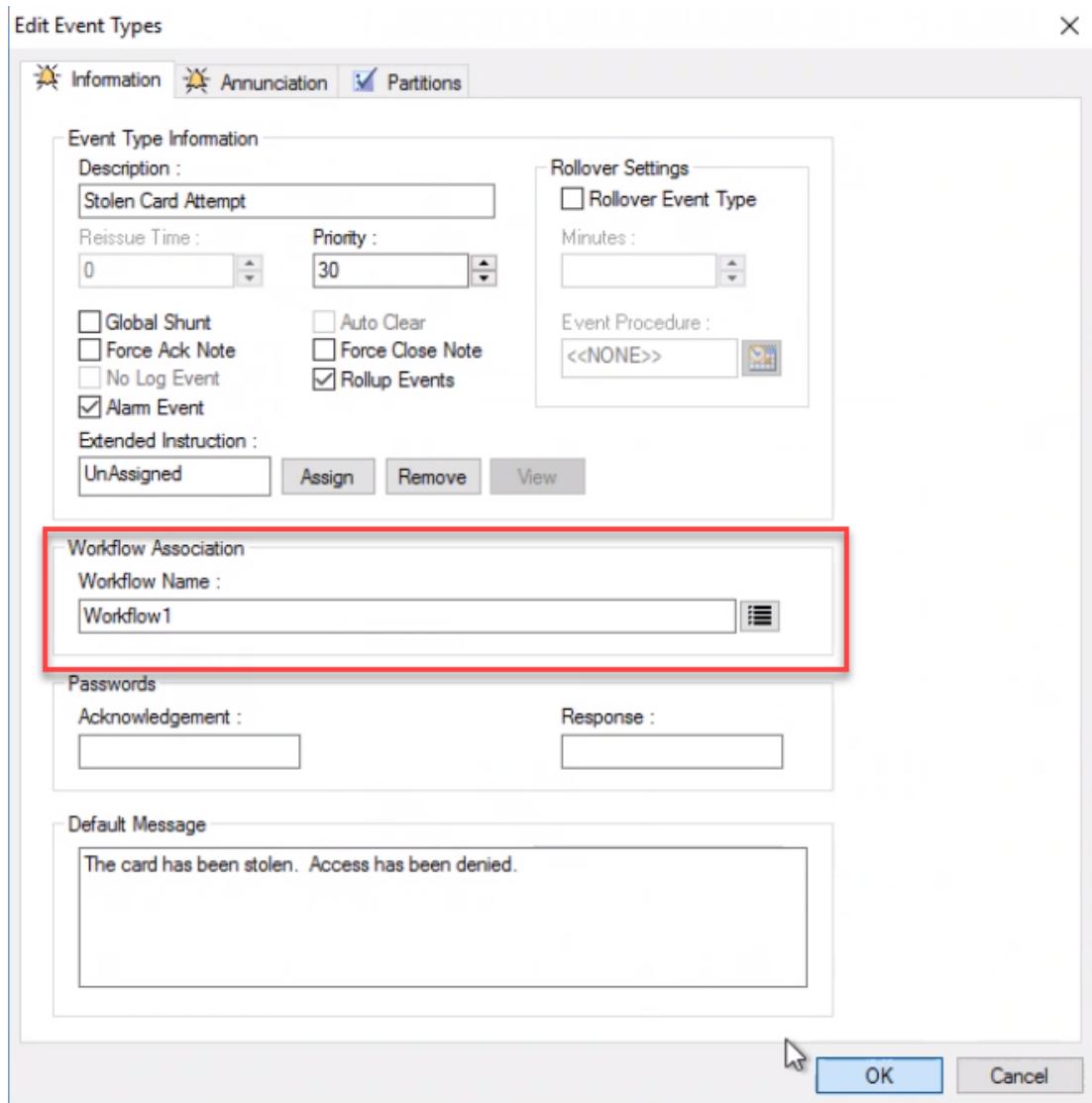
1. In Pro-Watch thick-client **Database Configuration** menu, select **Event Types** to display the **Edit Event Types** screen:



2. Click the **Workflow Association** drop-down menu and from the pop-up menu select **Define** to display the **Workflow screen**:



3. Select a **Workflow** and click **OK**:

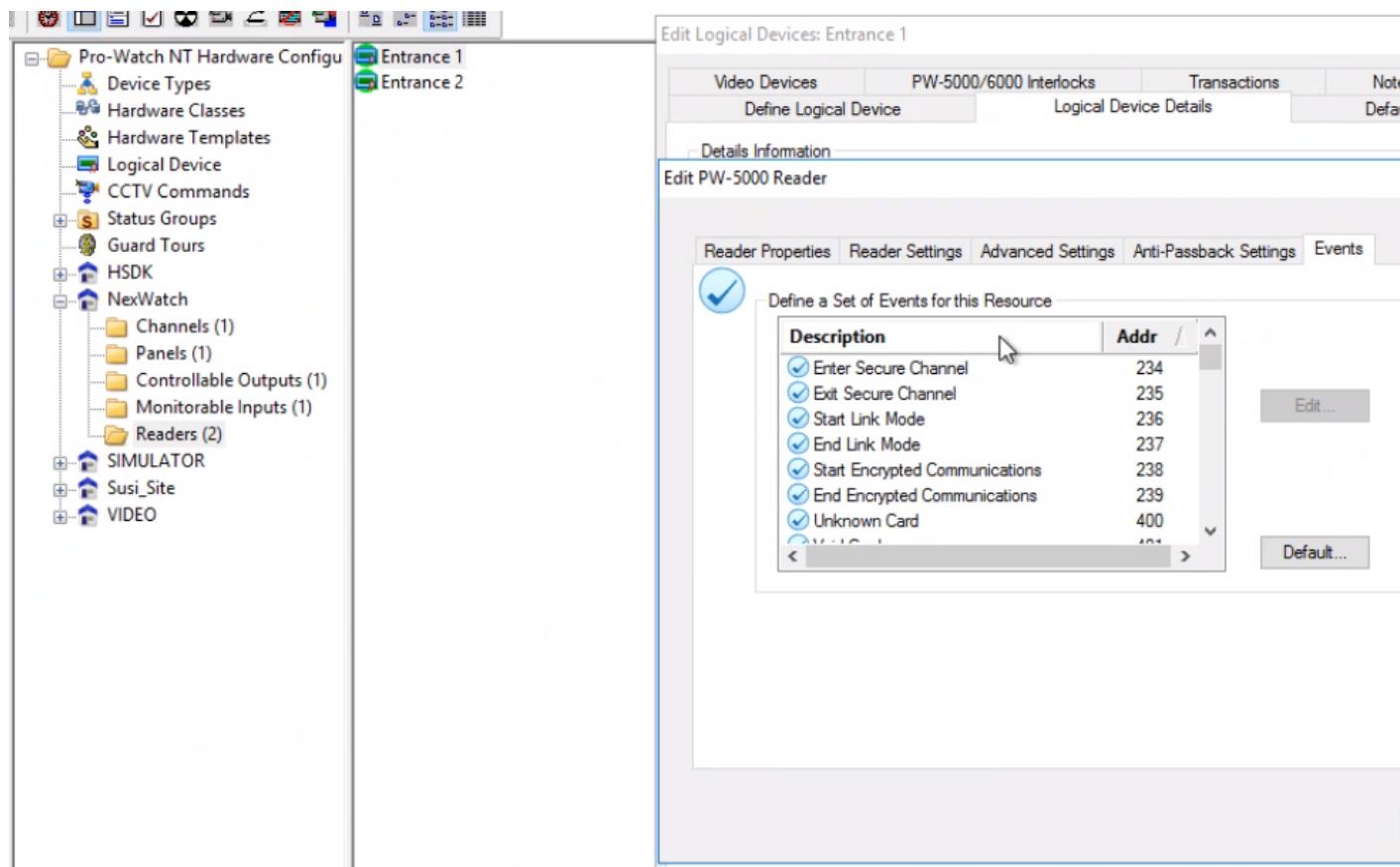


4. In the **Edit Event Types** screen click **OK** again to finish associating the selected workflow to an event.

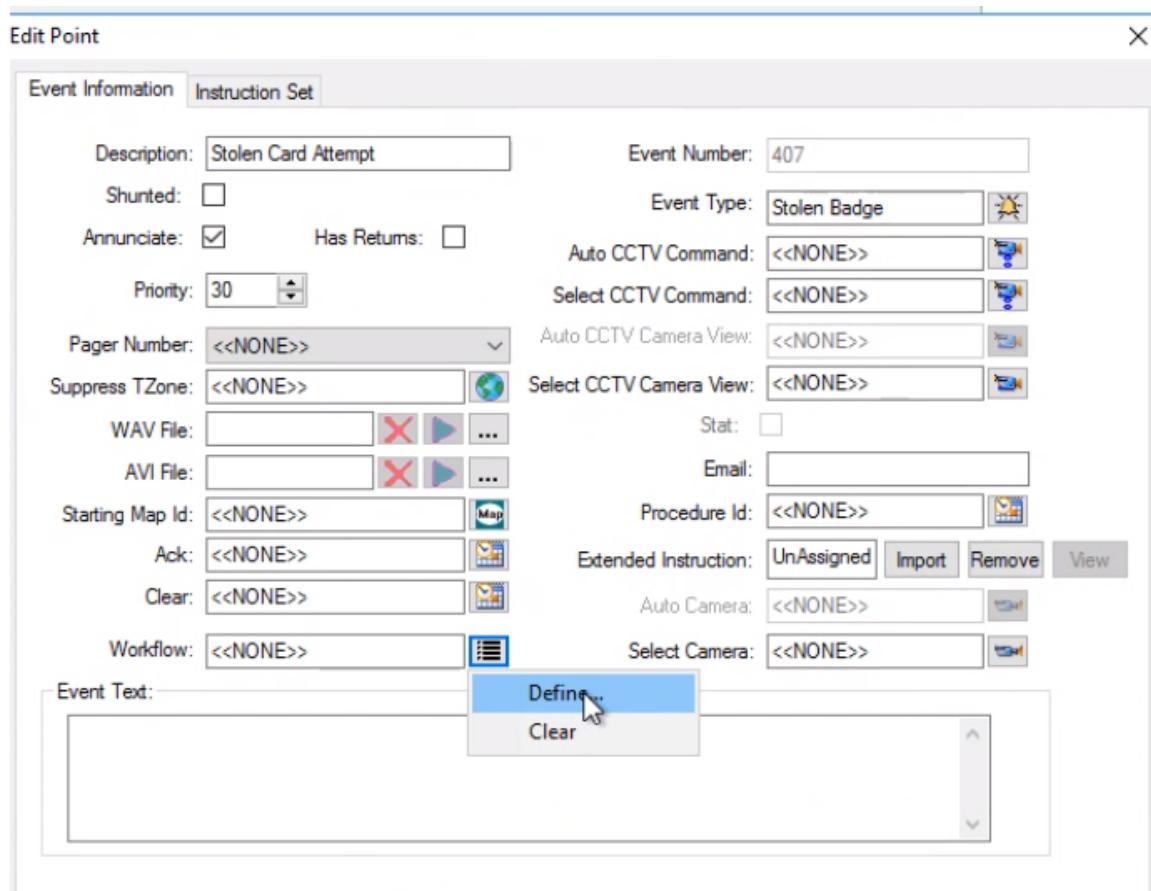
2.15.2.6 Associating Workflows at the Point Level

Note: Pro-Watch supports a maximum number of 500 workflows.

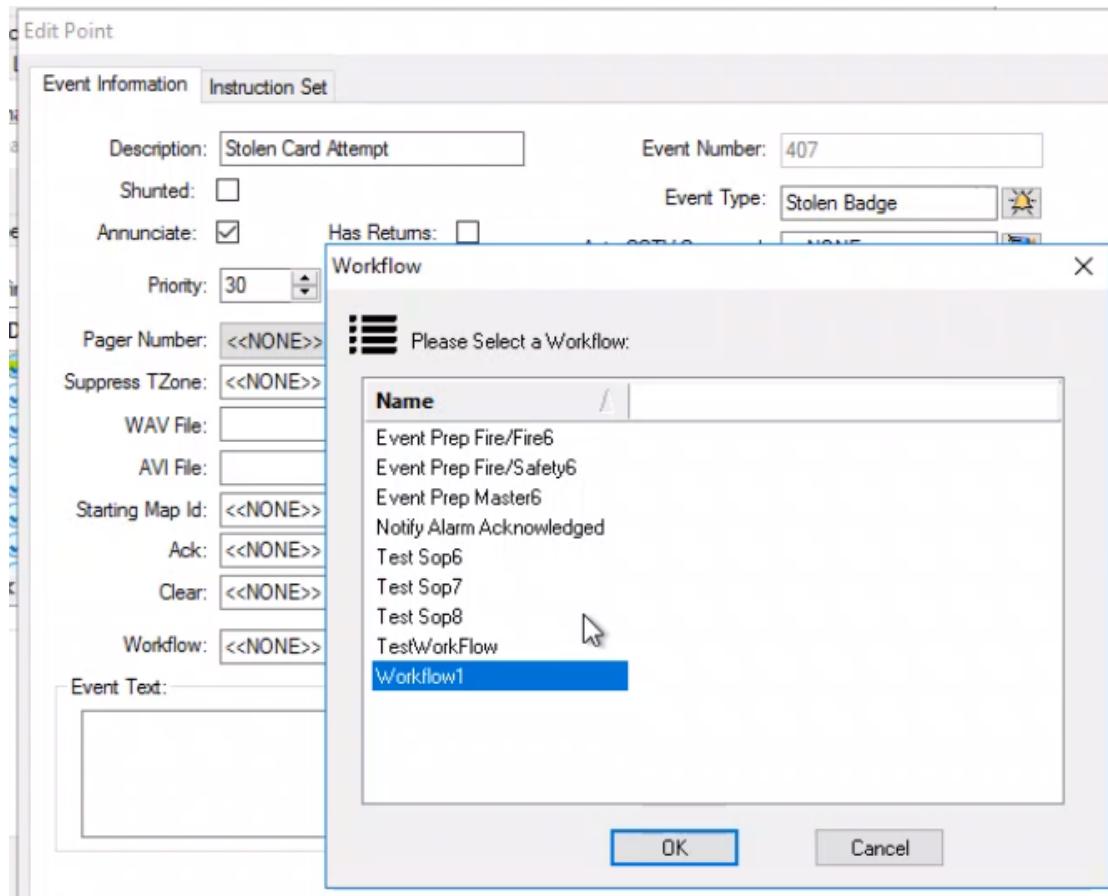
1. From Pro-Watch thick client's **Hardware Configuration** menu, select a **logical device** to display its editing screen:



2. In the **Edit Point** screen's **Event Information** tab, click **Workflow** drop-down menu and from the pop-up menu select **Define**:



3. Select a workflow and click **OK**:



4. In the **Edit Point** screen click **OK** again to finish associating the selected workflow to a logical device.

2.15.3 Reports Settings

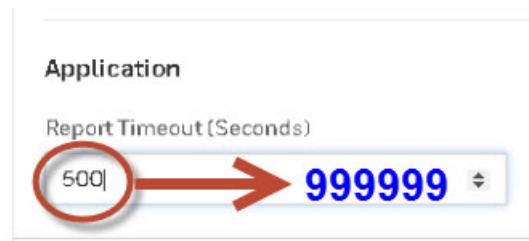
2.15.3.1 Reports General Settings

1. Click **Settings > Reports** navigation link to display the **General** settings tab:

The screenshot shows the 'Reports General Settings' page. On the left, a sidebar lists 'People & Group', 'Workflow', and 'Reports' (which is selected and highlighted in blue). The main content area has tabs for 'General' (selected) and 'Email'. Under 'General', there are sections for 'Branding' (with 'ADD WATERMARK' and 'ADD LOGO' buttons), 'Output Settings' (with 'Print' options like Report Header, Footer, Filter, and layout choices for Portrait or Landscape), 'Functional' (with check-boxes for Fixed Row, Column, and Row Summaries), and 'Application' (with a 'Report Timeout (Seconds)' input set to 240). In the bottom right corner, there are 'CANCEL' and 'SAVE' buttons. A red circle with a white pencil icon is drawn around the 'SAVE' button.

2. Click the **pencil icon** on the upper-right to launch the edit mode.
3. Click **ADD WATERMARK** to add a watermark to your reports.
4. Click **ADD LOGO** to add a logo to your reports.
5. Select one or more of the following **Output Settings** check-boxes: **Report Header**, **Report Footer**, **Report Filter**.
6. Select either the **Portrait** or **Landscape** to display layout option button.
7. Select **Row Number** and/or **Alternate Row Color** check-box.

8. For **Application >Report Timeout (Seconds)** field enter the value of "999999" for successful export of reports with a lot of data.



9. Click Save.

2.15.3.2 Reports Email Settings

1. Click **Settings > Reports >Email** navigation link to display the **Email** settings:

SMTP Server	Port	Send Timeout(Seconds)
smtp.gmail.com	0	0

SSL

Credentials

Use Default Credentials

Username	Password
Admin	

Email Address(Sender)
tyrion@gmail.com

SEND TEST E-MAIL

2. Click the **pencil icon** on the upper-right to launch the edit mode.
3. Enter the appropriate values for **SMTP Server**, **Port**, **Send Timeout (Seconds)** fields.
4. Select the **SSL** check-box for **Secure Socket Layer**.
5. Select the **Use Default Credentials** check-box to use the default credentials.
6. Enter the appropriate values for **User Name**, **Password**, **Email Address (Sender)** fields.
7. Click the **SEND TEST MAIL** link to send yourself a test email.

8. Click **Save**.

2.16 Simplified Device Maintenance

Display the main **Honeywell Hamburger Menu**.

Note: Prerequisite for Firmware & Password Update to work from NVR 6.5 onwards and VMS 650 onwards:

VMS web configurator and NVR web configurator should be configured with administrator credentials, before triggering the firmware and password update from Pro-Watch thin client.

Unique System Number of camera is mandated for feature to work.

Please refer to the list of models supported for firmware update and password update in [Section 2.22 Honeywell Camera Models Supported for Simplified Device Maintenance](#).

2.16.1 Recommendations for Firmware and Password Updates

1. Use Chrome latest version for best experience.
2. Firmware upgrade and password change may fail in many scenarios which user doesn't know if
 - DM service is stopped/hanged in NVR
 - Make sure PW / NVR Host names are pingable from both Pro-Watch and NVR.
 - Make sure Pro-Watch IC web interface is accessible from NVR system.
 - VMS web configurator and NVR web configurator should be configured with administrator credentials, before triggering the firmware and password update from Pro-Watch thin client
 - Unique System Number of camera is mandated for feature to work.
 - NVR is not discovered with unique number as call up number in Maxpro VMS
 - Uploaded wrong inventory file with wrong model and wrong version
 - Camera account is locked due to any reason
 - Camera's internal parameter is not synced from VMS to Pro-Watch
 - TLS and E2E are not enabled in all systems
 - The user must manually change the version number of NVR in VMS from older version to 6.5.

2.16.2 Firmware Update

2.16.2.1 Camera Hardware Configuration

Before you can update your firmware in the thin (web) client, you need to configure your hardware permission settings in Pro-Watch thick client (that is, the Main Application).

1. In Pro-Watch thick client, go to **Database > Users**.
2. Create or select the root-level Admin user.

3. Right-click and open the **Edit Users** screen..
4. Select **Programs** tab.
5. Go to **Hardware Configuration > Cameras**.
6. Set the **Query** method to **GRANT**. This setting will allow you to upgrade your camera firmware and update passwords.

Edit Users

The screenshot shows the 'Edit Users' interface with the 'Programs' tab selected. The main area displays a tree view titled 'Define User Programs and Functions'. Under the 'Hardware Configuration' node, the 'Cameras' node is expanded, showing four items: 'add - GRANT', 'delete - GRANT', 'query - GRANT' (which is highlighted with a blue selection box), and 'update - GRANT'. Other nodes like 'CCTV', 'Card Format', etc., are also listed.

7. Go to **Hardware Configuration > Video Firmware Update**.
8. Set the **Modify** method to **GRANT**. This setting will allow you to update the firmware files. Set the **View Devices** method also to **GRANT** which will enable you to view the camera list.

9. Set the **Cancel Upgrade** method to **GRANT**. This setting will attempt to cancel the pending Firmware Updates.

Edit Users

The screenshot shows the 'Edit Users' interface in the Pro-Watch Web Client. At the top, there is a navigation bar with tabs: Badge Profiles, Event Procedures, Eventview Columns, User Information, Device Status Filtering, Programs, and a fourth tab which is partially visible. Below the navigation bar, the title 'Define User Programs and Functions' is displayed. A tree view lists various program categories and their sub-functions. The 'Video Firmware Upgrade' category is expanded, showing three sub-functions: 'Cancel Upgrade - GRANT', 'Modify - GRANT' (which is highlighted with a blue selection box), and 'View Devices - GRANT'. Other categories listed include Status Groups, Subpanel Maintenance, Time Zone Def, Video Firmware Inventory, Videosystems, Zone Group/Partition maintenance, Zone List maintenance, Zone maintenance, Incident Workflow, and Maps.

10. Go to **Hardware Configuration > Video Firmware Inventory**.

11. Set the **Modify** method to **GRANT** which will enable you to upload the firmware files. Set the **View** method also to **GRANT** which will enable you to view the inventory..

Edit Users

The screenshot shows the 'Edit Users' interface in the Pro-Watch Web Client. At the top, there is a navigation bar with several tabs: 'Badge Profiles', 'Event Procedures', 'Eventview Columns', 'User Information' (which is currently selected), 'Device Status Filtering', 'Programs', and a few others partially visible. Below the navigation bar, the main area is titled 'Define User Programs and Functions'. A tree view displays various system components and their associated methods:

- Status Groups
- Subpanel Maintenance
- Time Zone Def
- Video Firmware Inventory
 - Modify - GRANT (highlighted with a blue border)
 - View - GRANT
- Video Firmware Upgrade
- Videosystems
- Zone Group/Partition maintenance
- Zone List maintenance
- Zone maintenance
- Incident Workflow
- Maps
- Mustering Tracking

12. Go to Hardware Configuration > Device Password Management

13. Set the **Change Password** method to **GRANT**. Set the **View** method also to **GRANT**. Both of these granted methods will allow you to view and manage the passwords in the thin (web) client.

Edit Users

The screenshot shows the 'Edit Users' interface in the Pro-Watch Web Client. At the top, there is a navigation bar with icons and labels for 'Badge Profiles', 'Event Procedures', 'Eventview Columns', 'User Information' (which is selected), 'Device Status Filtering', 'Programs', and a gear icon. Below the navigation bar is a title 'Define User Programs and Functions'. The main area contains a tree view of user programs and functions. The tree structure is as follows:

- Hardware Configuration
 - CCTV
 - CCTV Cameras
 - CCTV Commands
 - CCTV Monitors
 - Cameras
 - Card Format
 - Channel Maintenance
 - Device Password Management
 - Change Password - GRANT
 - View Devices - GRANT
 - Device Types
 - Dialup Schedule Maintenance
 - Enable Codes

The 'Change Password - GRANT' and 'View Devices - GRANT' items under 'Device Password Management' are highlighted with a blue selection box. To the right of the tree view, there is a vertical scroll bar and a status bar at the bottom with arrows and text.

2.16.2.2 Not Supported

1. When recorder is in fail-over mode, Firmware upgrade and Password change are not supported.
2. Multicast camera password change is not supported.
3. VMS in VMS deployment model is not supported for camera Firmware update and Password Update.
4. The user must update the camera firmware or must change the camera Password only with VMS 650 and above and Honeywell NVR 6.5 and above.

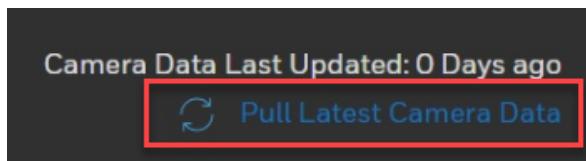
2.16.2.3 NVR and Pro-Watch Upgrade Notes

- When NVR is upgraded from 6.0 to 6.5 and above, you must also update the Honeywell NVR version in VMS-650. Go to Maxpro VMS configuration page and select recorder version as 6.5 + to get this feature working for upgrade deployments.
- If Pro-Watch core is upgraded from 4.5 or below version to 5.0, then the user has to manually trigger the download of VMS in PW thick client, in order to sync the new fields required for firmware and password update to work.

2.16.2.4 Displaying Current Versions

This is a must step to get the count of available cameras.

When the web client is first launched, the Current Version of the cameras will not be displayed. To populate the **Current Version** column, click the “**Pull Latest Camera Data**” link on the upper-right corner of the **Cameras** tab:



2.16.2.5 Cameras

Notes:

- If user is changing camera's Unique System Number, then he may lose Firmware or Password update history on Pro-Watch Intelligent Command.
- Firmware update jobs will be canceled, when redundant NVR is online.

In the Honeywell Hamburger Menu bar, click the **Firmware** link to display the **Firmware** landing page and to see a list of all cameras which belong to that user:

Click to see a list of all cameras

81 All Cameras

1 Available for Honeywell cameras 5 Updated Last 20 days

DEVICE STATUS NAME MANUFACTURER/MODEL TYPE IP ADDRESS

DEVICE STATUS	NAME	MANUFACTURER/MODEL	TYPE	IP ADDRESS
<input type="checkbox"/>	saturn-NVR1	Honeywell / HCW2GV	NTSC	10.78.157.166

List of Cameras Available for Update



Caution: Only Honeywell ONVIF cameras with Honeywell NVR recorder version 6.5 onwards, and VMS version 650 onwards will be listed as available for a firmware update.

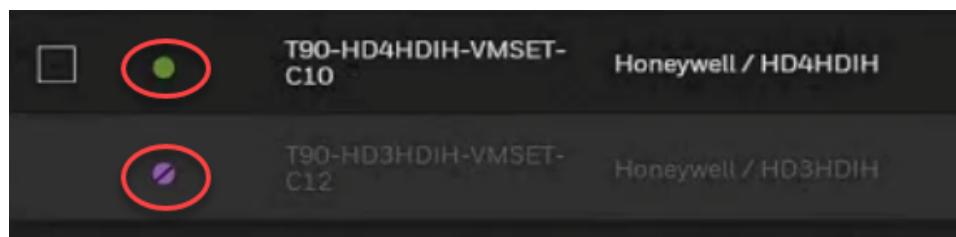
Caution: A firmware **update** can be an **upgrade** as well as a **downgrade**. Firmware update feature is available only for cameras with a single firmware file.

2.16.2.6 Display All Cameras

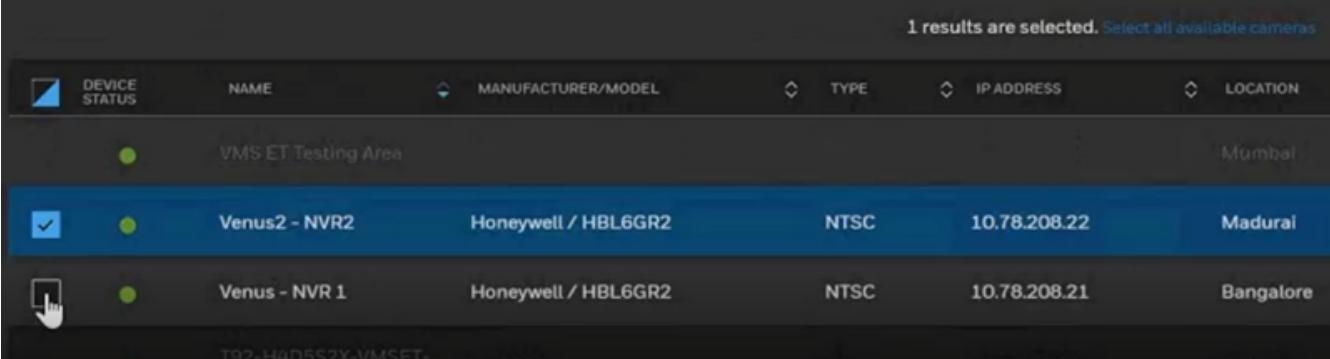
Click the **All Cameras** link to view all the available cameras from both Honeywell and non-Honeywell recorders:

The screenshot shows the 'Firmware' section of the Pro-Watch Web Client. At the top, there are three tabs: 'Cameras' (which is selected), 'Firmware File Repository', and 'File Management'. Below the tabs, the 'Camera Firmware Overview' is displayed with three status indicators: '1 Available for Honeywell cameras', '5 Updated Last 20 days', and '81 All Cameras'. The 'All Cameras' indicator is circled in red. A large white arrow points from this red circle down to a detailed list of cameras. The list is titled 'Honeywell Cameras' and contains two entries: 'Venus2 - NVR2' and 'Venus - NVR 1'. Both entries have a green dot next to them, indicating they are enabled and available. Below this section is another titled 'Non-6.5 or Non-Honeywell Cameras', which lists two entries: 'T92-H4D5S2X-VMSET-C21_1080_20F_10G' and 'T92-H3D3SR2X-VM5ET-C19_1080_20F_5G'. These entries have grayed-out text and are preceded by a purple dot with a diagonal line, indicating they are disabled.

- **Only Honeywell cameras** capable of receiving a firmware upgrade are highlighted and displayed in WHITE letters.
- **Non-Honeywell recorder or Non-Honeywell cameras** are not highlighted. They are grayed out and firmware update is not available for them.
- **GREEN** dot means the camera is enabled and available.
- **PURPLE DOT WITH DIAGONAL LINE** means the camera is disabled.



To select a camera to update, click and select its check-box:



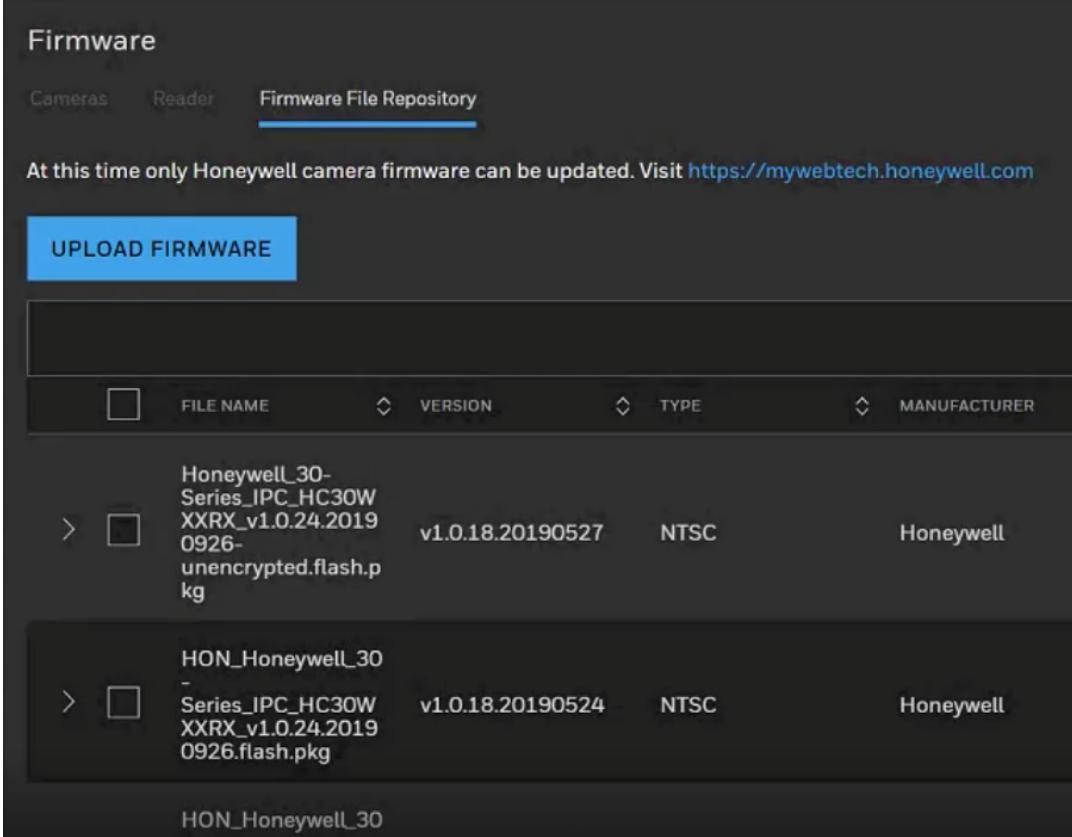
1 results are selected. Select all available cameras

DEVICE STATUS	NAME	MANUFACTURER/MODEL	TYPE	IP ADDRESS	LOCATION
●	VMS ET Testing Area				Mumbai
<input checked="" type="checkbox"/>	Venus2 - NVR2	Honeywell / HBL6GR2	NTSC	10.78.208.22	Madurai
<input type="checkbox"/>	Venus - NVR 1	Honeywell / HBL6GR2	NTSC	10.78.208.21	Bangalore

By clicking a check-box, the user can select the firmware version available for a specific selected camera model and firmware type.

2.16.3 Uploading a Camera's Firmware

Click the **Firmware File Repository** link to display the list of firmwares uploaded to Pro-Watch:



Firmware

Cameras Reader **Firmware File Repository**

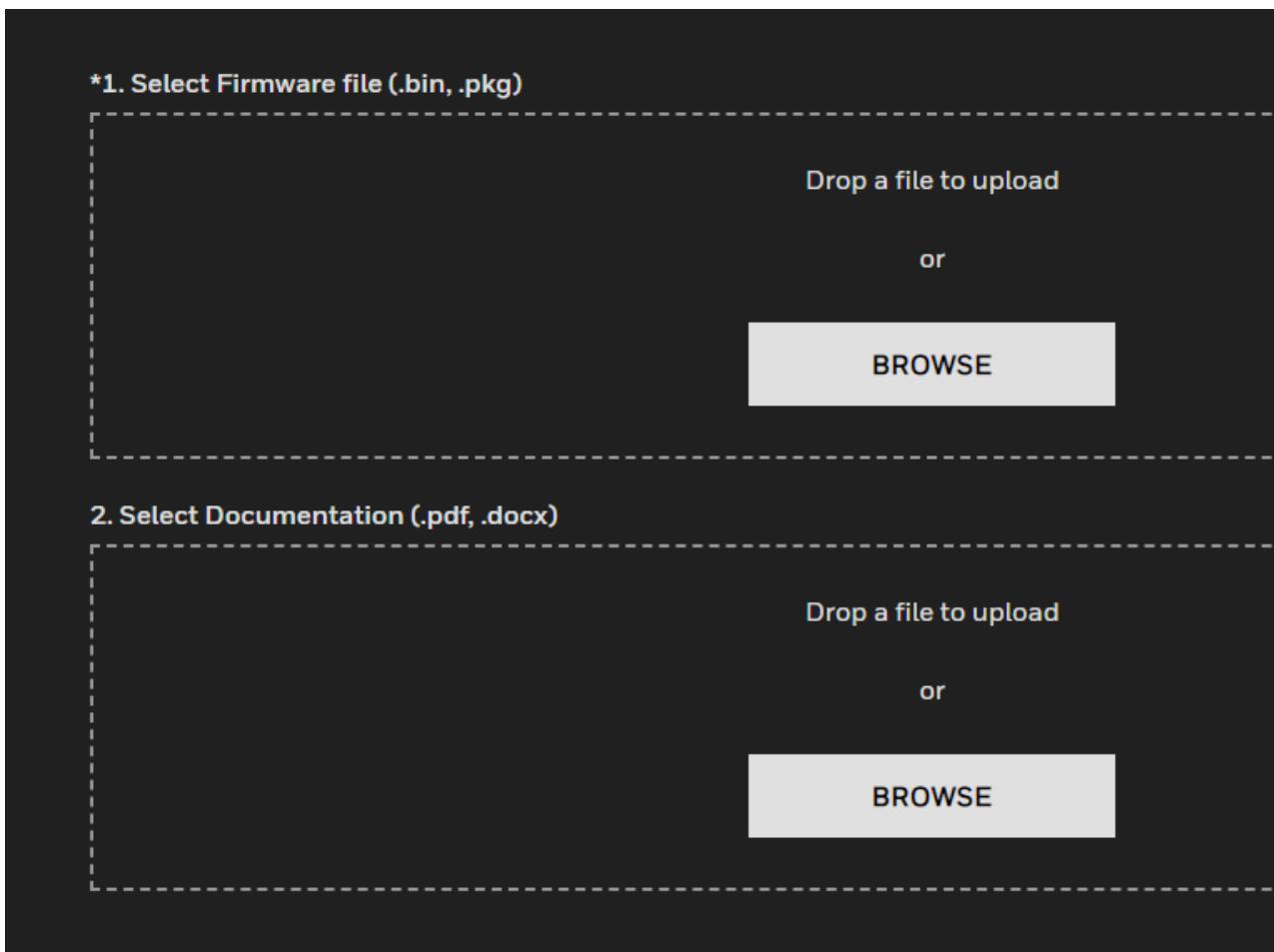
At this time only Honeywell camera firmware can be updated. Visit <https://mywebtech.honeywell.com>

UPLOAD FIRMWARE

<input type="checkbox"/>	FILE NAME	VERSION	TYPE	MANUFACTURER
> <input type="checkbox"/>	Honeywell_30-Series_IPC_HC30W_XXRX_v1.0.24.20190926-unencrypted.flash.pkg	v1.0.18.20190527	NTSC	Honeywell
> <input type="checkbox"/>	HON_Honeywell_30-Series_IPC_HC30W_XXRX_v1.0.24.20190926.flash.pkg	v1.0.18.20190524	NTSC	Honeywell

Let's say we'd like to update the HCD8G camera.

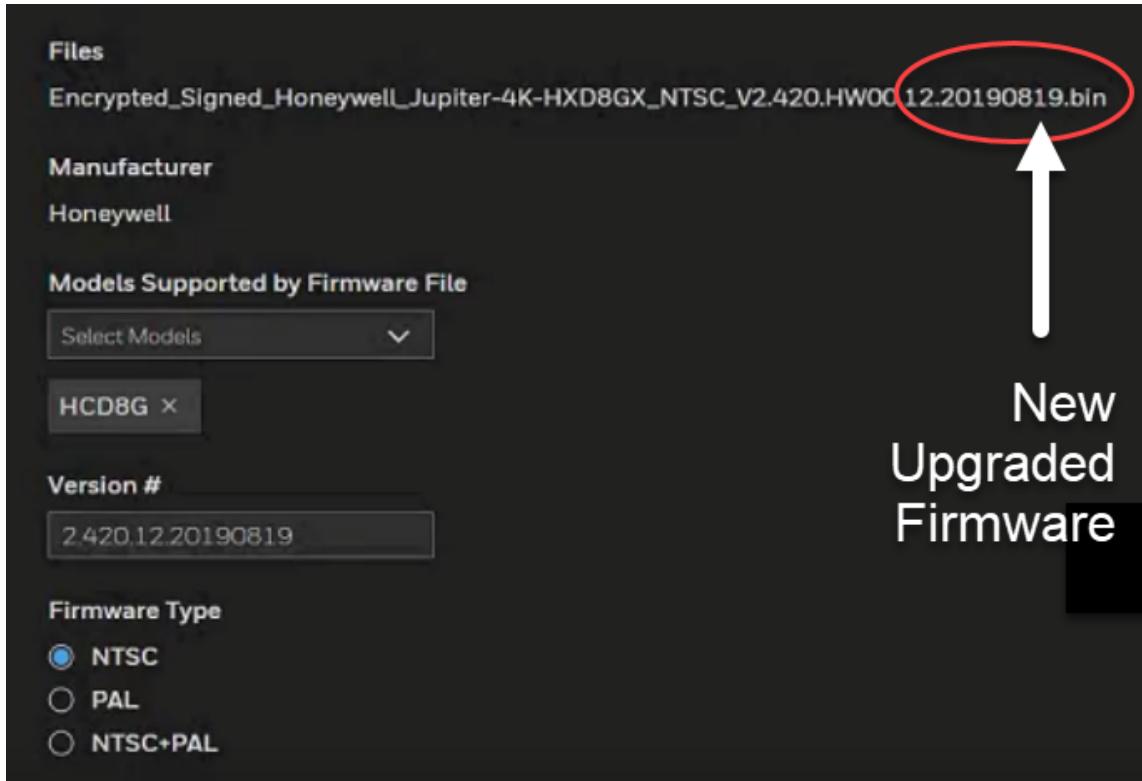
Click **Upload Firmware button** to display the firmware upload screen:



- Click **Browse** to find the **firmware file** to upload. Select the **.bin** or **.pkg** file and click **Open** to upload the file.
- Click **Browse** to find the firmware documentation file to upload. Select the **.pdf** or **.docx** file and click **Open** to upload the file.

Note: Max firmware size is 100 MB. Max doc size is 5 MB.

After uploading the updated firmware, the screen will look similar to this:



All the available models (based on model selected in NVR) populate here. The user can select more than one model also for the same firmware.

- Select the **camera model**(s) supported by the firmware.
- Select the **firmware type** (NTSC, PAL, or NTSC-PAL). Once the firmware are uploaded you cannot edit – you need to delete and add or override the existing files. If the firmware type and version format are wrong, then those cameras cannot be upgraded.
- The **latest firmware version number display format** (displayed under the “**Latest Version**” column) is **YYYYMMDD**. Camera version format examples are provided in the below table to illustrate how to extract the firmware version number to upload inventory:

	Camera Version Format Example	Version Number to Upload Inventory
1	V2.460. HW00 .5.R.20190827	20190827
2	v 1.0.18.20190523	20190523
3	1.0. HW0 .001, Build date: 2019-07-13	20190713
4	1.000. HW01 .1.190814	190814
5	1.0.18.20190523	20190523
6	5.5.52 build 181108	181108
7	1.000. 0034 .0 build: 2017 - 11 - 01	20171101
8	2.420. HW00 .9, Build Date: 2018 - 12 - 17	20181217

- Click **Complete** to upload the updated firmware.

Note: If user is uninstalling and reinstalling the inventory, then he or she must ensure that the inventory network path remain the same. If the user chooses to change the inventory path during reinstallation, then he or she must manually delete all the old entries from Pro-Watch Intelligent Command before adding any new inventory entries.

The uploaded firmware and camera is displayed in the updated list:

<input type="checkbox"/>	FILE NAME	VERSION	TYPE
<input type="checkbox"/>	Encrypted_Signed_Honeywell_Jupiter-4K-HXD8GX_NTSC_V2.420.HW00.12.20190819.bin	2.420.12.20190819	NTSC
CAMERA MODELS SUPPORTED BY THIS FIRMWARE:			
1. HCD8G			

When we click and switch to the **Cameras** view, TWO cameras are listed including the newly updated HCD8G camera:

The screenshot shows the Pro-Watch Web Client interface. At the top, there's a navigation bar with 'Firmware' and 'Cameras' tabs. The 'Cameras' tab is highlighted and circled in red. Below it, the 'Camera Firmware Overview' section shows '2 Available for Honeywell cameras' (circled in red), '5 Updated Last 20 days', and '81 All Cameras'. The main area is titled 'New Firmware' and displays a table of devices. The table has columns: DEVICE STATUS, NAME, MANUFACTURER/MODEL, TYPE, and IP ADDRESS. Two rows are visible: 'saturn-NVR1' (Honeywell / HCW2GV, NTSC, 10.78.157.166) and 'Jupiter - HCD8G- NVR3' (Honeywell / HCD8G, NTSC, 10.78.208.224). A red box highlights the second row, and a large white arrow points from the '2 Available' count in the overview to this row.

DEVICE STATUS	NAME	MANUFACTURER/MODEL	TYPE	IP ADDRESS
●	saturn-NVR1	Honeywell / HCW2GV	NTSC	10.78.157.166
●	Jupiter - HCD8G- NVR3	Honeywell / HCD8G	NTSC	10.78.208.224

The list displays both the **CURRENT version** of the firmware running on camera and the **LATEST uploaded version** of the firmware.



DEVICE STATUS	NAME	MANUFACTURER/MODEL	CURRENT VERSION	LATEST VERSION
<input type="checkbox"/>	saturn-NVR1	Honeywell / HCW2GV	1.000.18.20190409	20190819
<input checked="" type="checkbox"/>	Jupiter - HCD8G- NVR3	Honeywell / HCD8G	2.420.9.20181217	20190819

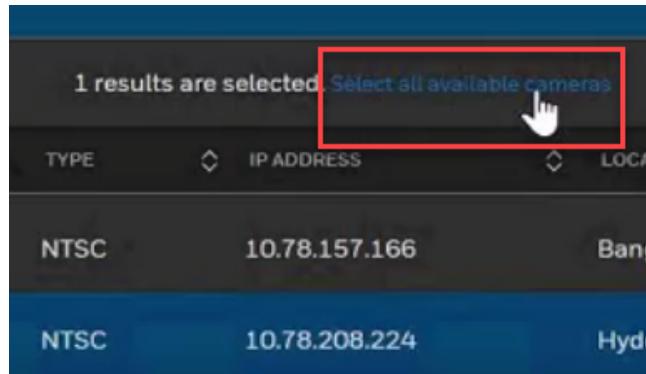
Note: During the firmware inventory upload if Model, Type, and Version are not selected properly, available logic will fail.

Select the camera for the update, which activates the “**UPDATE FIRMWARE FOR 1**” button since only one camera is selected:



DEVICE STATUS	NAME	MANUFACTURER/MODEL	CURRENT VERSION	LATEST VERSION
<input type="checkbox"/>	saturn-NVR1	Honeywell / HCW2GV	1.000.18.20190409	20190819
<input checked="" type="checkbox"/>	Jupiter - HCD8G- NVR3	Honeywell / HCD8G	2.420.9.20181217	20190819

There can be hundreds of cameras at a site that require upgrading. To update multiple cameras at the same time, click the “**Select all available cameras**” link:



TYPE	IP ADDRESS	LOCATION
NTSC	10.78.157.166	Bangor
NTSC	10.78.208.224	Hyde

In this case, since we have two cameras, both will be selected when we click the “Select all available cameras” link:

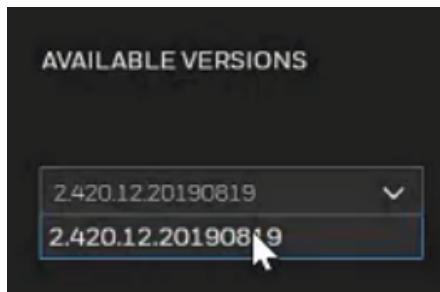
The screenshot shows a table of cameras with columns for DEVICE STATUS, NAME, MANUFACTURER/MODEL, CURRENT VERSION, LATEST VERSION, and NOTES. Two checkboxes in the DEVICE STATUS column are checked. A red box highlights these two checkboxes. To the right, a modal window titled "UPDATE FIRMWARE FOR 2" displays the selected cameras and their latest versions.

Since in this example we want to update just one camera, we select the HCD8G camera and click the UPDATE FIRMWARE button to display the update screen:

The screenshot shows a table with a single row for "Model # HCD8G". The "# OF CAMERAS" column has a dropdown set to "1 Camera". The "CURRENT VERSION" column shows "2.420.9.20181217". The "AVAILABLE VERSIONS" column has a dropdown menu open, showing "2.420.12.20190819" as the selected option. The "FIRMWARE TYPE" column shows "NTSC". At the bottom are "INSTALL & UPDATE" and "CANCEL" buttons.

Note: Cameras on this screen are grouped by MODEL names, firmware version, and firmware type. If for example we had two HCD8G model cameras that needed updating, we would see TWO cameras listed under the “Model # HCD8G” category.

Available Versions drop-down list will list all the available firmware uploaded for that specific camera. In this case, since we've uploaded only one updated firmware, only one firmware is listed:



Note: The Available Versions list can be used to **downgrade** the firmware as well. This may happen when, for example, we'd like to revert back to a previously released firmware. To do that, select the previously released version from the drop-down list to downgrade the firmware.

Click the **INSTALL & UPDATE** button to display the **Updates in Progress** banner in the **Updated** tab of the **Cameras** screen. The updated camera

record will also display an “In Progress” message:

The screenshot shows the 'Firmware' section of the Pro-Watch Web Client. In the top left, there's a summary bar with three sections: '1 Available for Honeywell cameras', '5 Updated Last 20 days' (with a yellow 'Updates in Progress' button highlighted by a red oval), and '81 All Cameras'. Below this is a table listing five cameras with their details: Venus2 - NVR2, Venus - NVR 1, Series30 - NVR2, saturn-NVR1, and Jupiter - HCD8G- NVR3. To the right of the table is a sidebar with a search bar and a list of update statuses: 2020-02-21, 2020-02-21, 2020-02-21, Job Failed In DM, and In Progress (also highlighted by a red oval). A red arrow points from the 'Updates in Progress' button in the summary bar to the 'In Progress' status in the sidebar.

Note: User can perform firmware update operations from "All Camera" tab as well. When the update is in progress, the check-box for the updated camera will not be available for selection. **The user can choose to cancel the firmware updates only from the Update tab when the jobs are in “pending” state. The cancellation request will be performed if jobs are not picked up by the backend-system for the update.** This prevents accidental updates while the update is still in progress. Click the **All Cameras** link to verify that no check-box is available:

<input type="checkbox"/> DEVICE STATUS	NAME	MANUFACTURER/MODEL
<input type="checkbox"/>	Mercury - NVR1	Honeywell / HBL2GR1
<input type="checkbox"/>	LPR_1	HBL6GR2
<input type="checkbox"/>	Jupiter - HCD8G- NVR3	Honeywell / HCD8G

If the update is successful:

- If the update is successful, a **success feedback message** will display with the date of the update. That camera will no longer be listed under the cameras available for an update:

The screenshot shows the 'Camera Firmware Overview' section. At the top, there are two summary boxes: '1 Available for Honeywell cameras' with a hand cursor icon over it, and '4 Updated Last 20 days'. Below this, a large message states 'HCD8G camera is no longer listed as available for an update'. A red box highlights the row for 'saturn-NVR1', which is listed under 'NAME' and 'MANUFACTURER/MODEL' as 'Honeywell / HCW2GV'. A red arrow points from the 'Available' box down to the highlighted row.

The updated firmware can be viewed in the camera's web page as well:

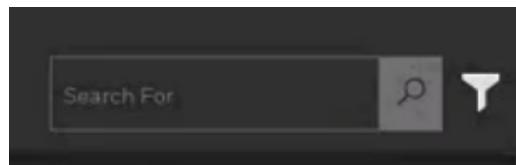
The screenshot shows the 'Setup' tab of the Honeywell HCD8G camera configuration interface. On the left is a sidebar with links: Camera Setup, Compression Setup, Zoom and Focus, Audio Setup, and Network Setup. On the right, under the 'Version' heading, is a table of information. The table includes: Firmware Version (2.420.HW00.12, Build Date 2019-08-19), Web Version (3.2.1.691512), ONVIF Version (16.12), and Serial Number (Z363601293). At the bottom right of the table area, it says 'Copyright 2018. All rights reserved.' A red box highlights the 'Build Date' cell.

If the update is not successful:

- If the update is **not successful**, a failure message will display with the reason for the failure. If the user tries to upload the same firmware once again after the first failure, it will revert back to the last available stable version.

2.16.3.1 Search Function

You can use the search field to search for any alphanumerical value in the columns in the **Camera** screen:



Note: The only fields you cannot search for are the **Device** and **Update Status** columns.

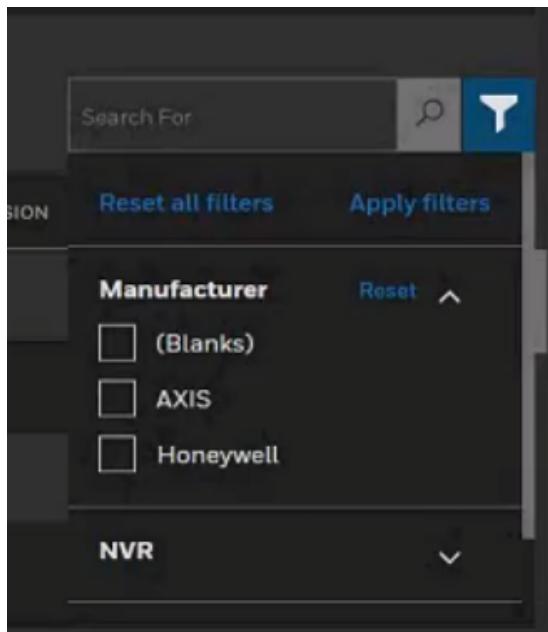
For example, searching for the keyword “bangalore” selects and displays all the cameras with the value “Bangalore” in the LOCATION field/column:

A screenshot of a table search results for cameras. The search term "bangalore" is entered in the search bar at the top right, circled in red. The results table has columns: LOCATION, CURRENT VERSION, LATEST VERSION, and UPDATE STATUS. The first three rows have the LOCATION column highlighted with a red box, and the first two rows have the LOCATION value "Bangalore" circled in red. The fourth row shows the full value "Bangalore".

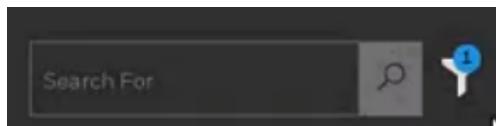
LOCATION	CURRENT VERSION	LATEST VERSION	UPDATE STATUS
Bangalore	1.000.1.20190617		2020-02-21
Bangalore			
Bangalore			
Bangalore			

2.16.3.2 Dynamic Filtering

You can search for cameras by using the **Manufacturer** and **NVR** drop-down filter lists and by location.

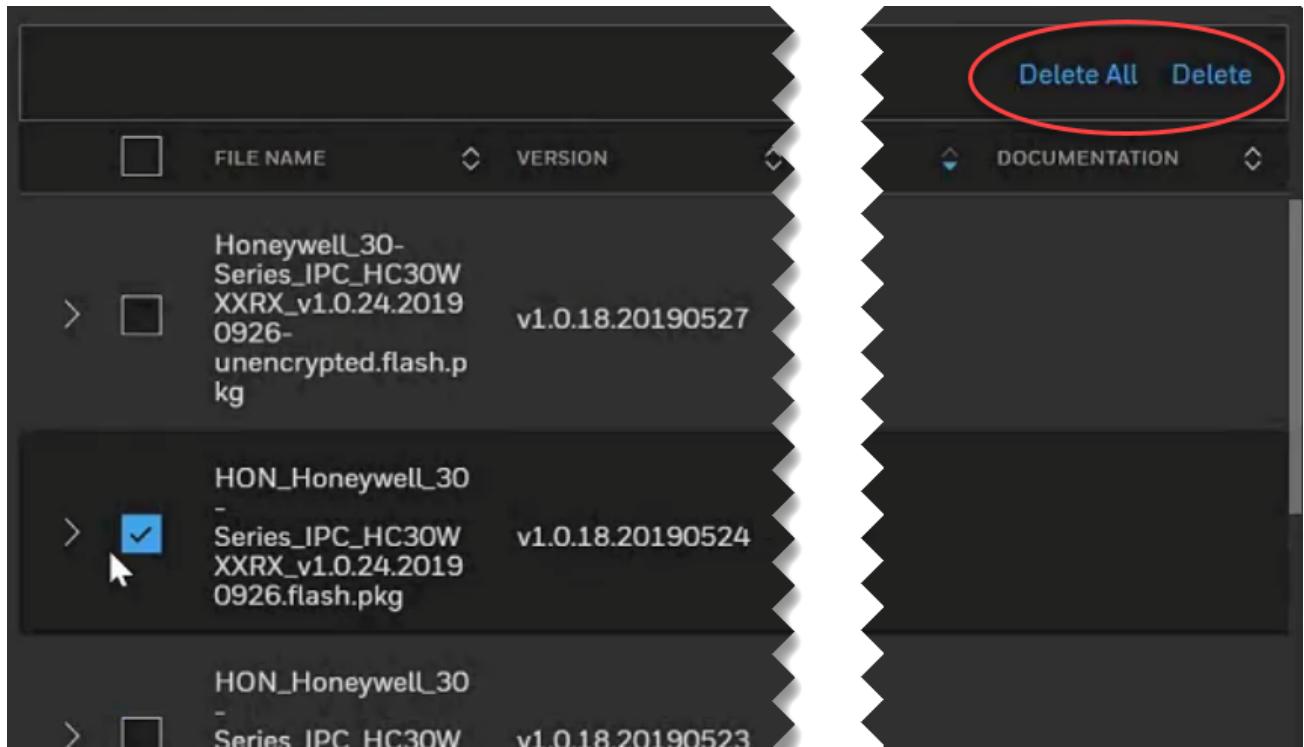


A blue numerator will display the number of filters applied:

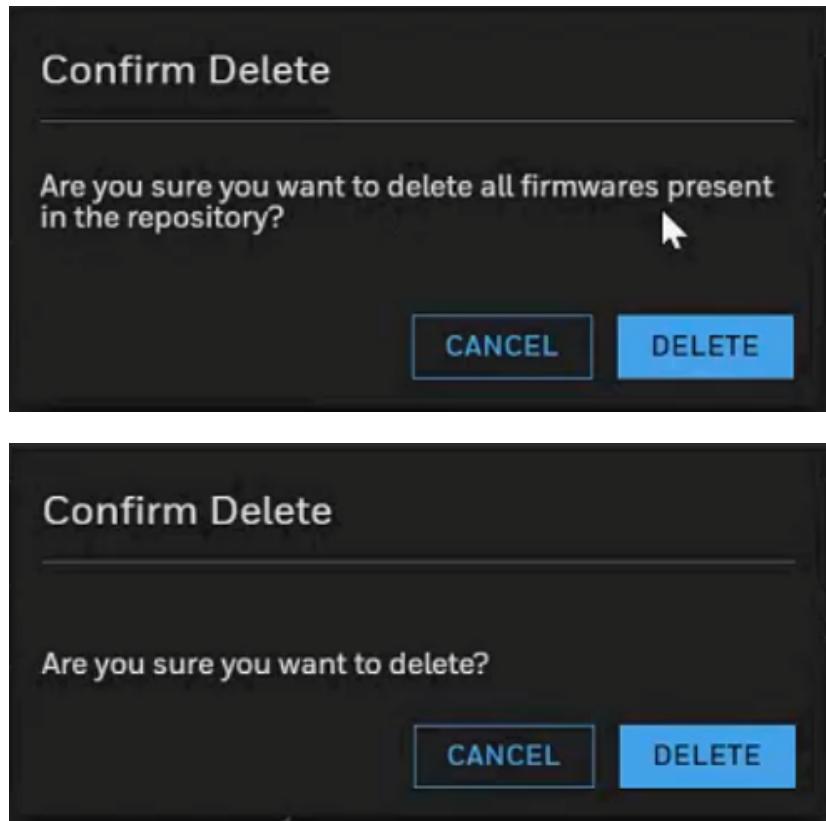


2.16.4 To Delete Firmware

To delete one or more firmware, select them in the list and then click either the **Delete All** or **Delete** link on the upper-right corner of the firmware screen:



Pro-Watch will display a prompt asking if you really want to delete one or all the firmware:



Click **Delete**.

2.16.5 Multi-User Known Issue

When multiple users are using the thin (web) client, the firmware updates performed by one user will not be displayed automatically in the second user's firmware list.

Note: Make sure a pull request is done if a new camera is added to Maxpro. The pull request will take time depending on the number of cameras. For 2000 cameras it will approximately take 4 to 7 Min. Sometimes the pull request will not complete; it will get stuck and there will be no progress. When that happens, the user needs to close the browser and reopen it.

Note: The user needs to go to different pages and come back to get the right status of the upgrade and camera count across the tabs.

PROBLEM: The first user will have the update display in the **Available** tab but the update will not display automatically on the second user's **Available** tab.

SOLUTION: The second user can see the updated firmware status, by selecting either **All Camera** or **Updated** tab -- if the Camera is either loaded on the grid or is present in UI cache for these 2 tabs. Multi-user status update will be inconsistent since those will not change unless otherwise the user switch the tabs.

When the firmware upgrade is in progress, search and filter operations will not work for the cameras that are not part of the ongoing patch update.

2.16.6 Passwords

Make sure cameras are not configured in two different NVR or different head-end systems.

The total count is overall number of cameras in the system, irrespective of what type of cameras are counted from any type of recorders.

Select all that need to be updated in Firmware and Password page.

First it will select only the first X number. If we want, we can select all after the first selection.

Status of the camera will not get live update. That is, if the camera is on-line during download it will remain in enabled state in IC even when camera goes off-line or is disabled in Maxpro - this is applicable for both Firmware and Password.

The user will be able to select those cameras for Firmware and Password update but it will fail at the end.

Caution: Make sure that the camera is not connected to non-NVR clients and other systems during password update. This is to ensure that the camera does not lock out due to wrong password when the systems try to reconnect with the old password.

Note: Password update is not supported for multicast camera's. Hence password update jobs initiated for multicast camera's will be cancelled.

Note: Password update jobs will also be canceled when redundant NVR is online.

In the Honeywell Hamburger Menu bar, click the **Passwords** link to display the **Passwords** screen:

The screenshot shows the 'Password Camera Overview' section of the Pro-Watch Web Client. At the top, it displays '21 Total Cameras' and '0 Updated Last 20 Days'. Below this is a table with columns: DEVICE STATUS, NAME, and MANUFACTURER/MODEL. The table lists four cameras:

DEVICE STATUS	NAME	MANUFACTURER/MODEL
●	Camera15_5	AXISM7010
□	Dummy Honeywell Saturn	Honeywell / HCL2GV
□	FWSimulator	Honeywell / HDZ20HDEX
●	HospitalTank1080P	Generic-RTSP

- **GREEN DOT** means the camera is enabled (which can be online or offline).
- **PURPLE DOT WITH SLASH** means the camera is not enabled.
- **DIMMED GRAY** rows designate cameras that are not available for password update.
- **WHITE** rows designate cameras that are available for password update.

2.16.6.1 Updating a Password

Update tab will show last 30 days history.

Either password update pass or fail update count will increase.

1. Select the camera the password of which you'd like to update:

Camera password overview

DEVICE STATUS	NAME	MANUFACTURER/MODEL	IP ADDRESS	LOCATION	UPDATE STATUS
<input type="checkbox"/>	Series 30	HONEYWELL / HC30W45R2	10.78.208.30	BLR	2020-04-28
<input type="checkbox"/>	Venus - Nabin	Honeywell / HBL6GR2	10.78.208.23	BLR	
<input type="checkbox"/>	Jupiter	Honeywell / HCD8G	10.78.208.224	BLR	2020-04-28
<input type="checkbox"/>	Venus - Chandan	Honeywell / HBL6GR2	10.78.208.22	BLR	2020-04-28
<input type="checkbox"/>	Venus - Jensen	Honeywell / HBL6GR2	10.78.208.21	BLR	2020-04-28

Showing 1- 9 of 9 Results

Activate Windows
Go to Settings to activate Windows.

This screen will display the **total number of cameras** available and the **number of passwords updated** within the last 30 days.

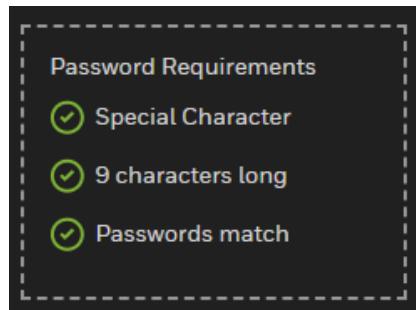
2. Click the “**CHANGE PASSWORD FOR 2**” button to display the password changing screen:

The screenshot shows a dark-themed dialog box titled "Change Password For 2 Camera(s)". It contains fields for "New Password" and "Confirm Password", both represented by masked input boxes. To the right of these fields is a dashed box labeled "Password Requirements" containing five checked items: "Uppercase & Lowercase letters", "Numeric Character", "Special Character" (with a note about allowed symbols: "@_!%^.~?#\$=-+*;,&"), "10 characters long", and "Passwords match". Below the input fields is a note: "Note: In case, NVR redundancy is configured then corresponding NVR needs to be re-discovered again in VMS post the successful password update." At the bottom are two buttons: "CANCEL" and "SAVE & APPLY CHANGES".

3. Enter a password which satisfies all the five requirements:

- Uppercase and Lowercase Letters
- Numeric Character
- Special Character
- 10 Characters Long
- Password Match

4. Reenter the password to confirm it. When you satisfy all three requirements, the requirements list will display green check-marks:



5. Click the "**SAVE & APPLY CHANGES**" button.

2.16.6.2 Filtering Cameras for Password Updates

You can filter cameras for password updates by using two methods.

Filtering by Keyword

1. Enter a keyword into the search box.
2. Click the magnifying glass icon:

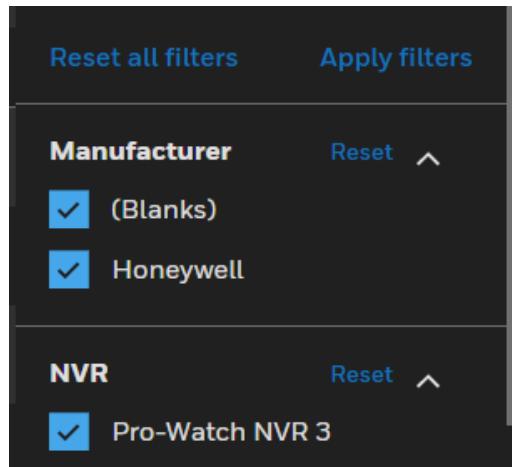
The screenshot shows a search interface. On the left, a table displays search results for 'Honeywell'. The columns are 'DEVICE STATUS' (checkbox), 'NAME' (dropdown), and 'MANUFACTURER/MODEL'. Two rows are shown: 'Dummy Honeywell Saturn' (status: off, name: dropdown, model: Honeywell / HCL2GV) and 'FWSimulator' (status: off, name: dropdown, model: Honeywell / HDZ20HDEX). On the right, there is a search bar with the text 'Honeywell' and a magnifying glass icon. Below the search bar, there is a dropdown menu labeled 'UPDATE STATUS'.

Filtering by Preset Lists

1. Click the filter icon.
2. Select a preset filter from any of the drop-down lists to filter the cameras by **Manufacturer**, **NVR** (recorder), or **Location**:

The screenshot shows a filter configuration interface. At the top, there is a search bar with the text 'salesdemo' and a magnifying glass icon. Below the search bar are two buttons: 'Reset all filters' and 'Apply filters'. The main area contains three dropdown menus with arrows: 'Manufacturer', 'NVR', and 'Location'.

3. If you wish, you can select more than one filter:



4. Click **Apply Filters**.

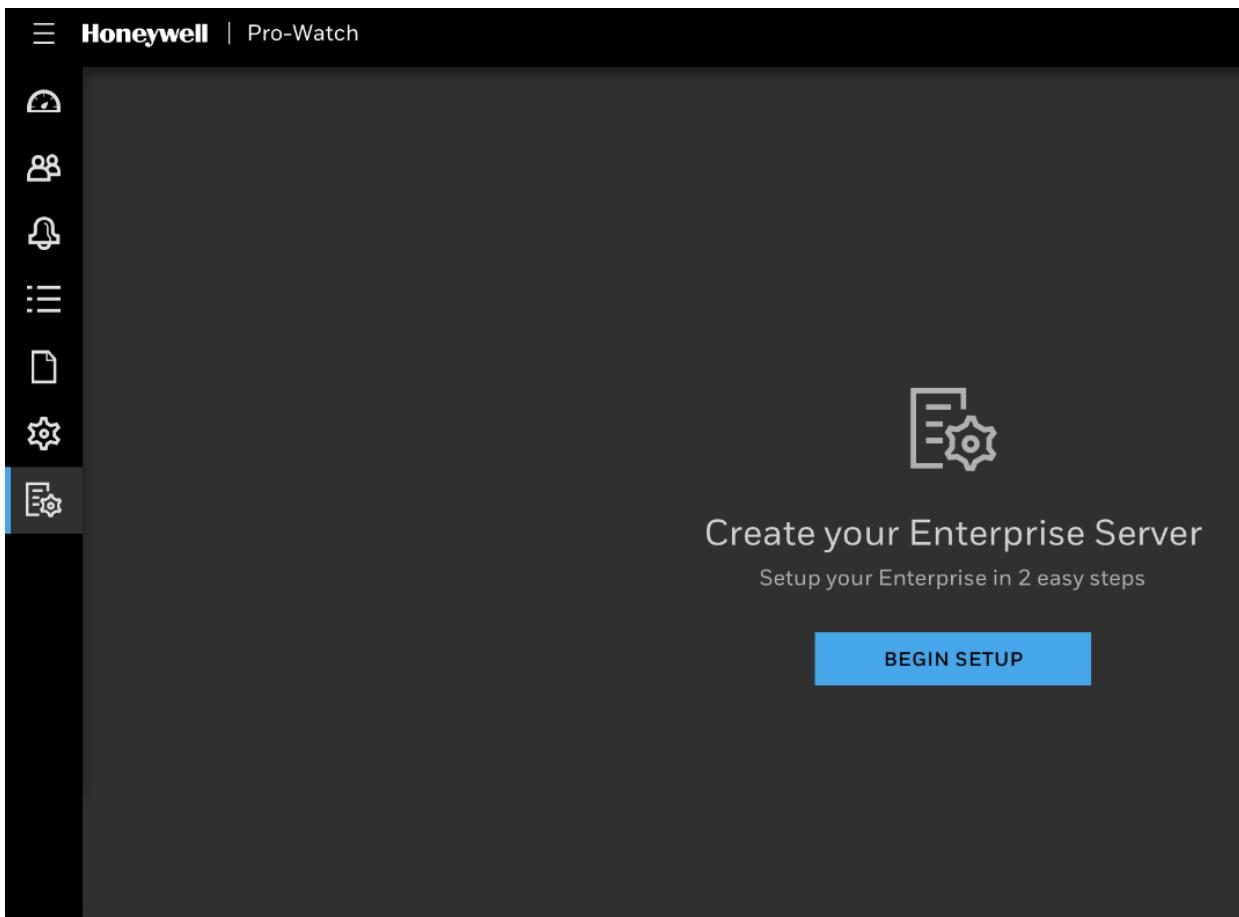
Note: You cannot filter last 24 hours, yesterday etc. updated history.

2.16.7 Events Under Simplified Maintenance

- Firmware upgrade success
- Firmware upgrade failed
- Firmware upgrade started
- Password upgrade started
- Password upgrade failed

2.17 Enterprise Manager

Select **Enterprise Manager** to display the first **Enterprise** screen:



2.17.1 Creating an Enterprise Server

1. Click Begin Setup button to display the **Create Enterprise Server** screen:

The screenshot shows the 'Create Enterprise Server' interface. At the top, there are two tabs: '1 ENTERPRISE DETAILS' (which is active) and '2 SELECT TABLE GROUPS'. Below the tabs, there are fields for 'Server Name/Instance Name' and 'Database', both of which are currently empty. A 'View less' link is located below the 'Server Name/Instance Name' field. Under 'Authentication Type', there are three radio buttons: 'Windows Authentication' (selected), 'SQL Authentication', and 'Custom'. Below these are fields for 'TimeOut (in seconds)' and 'Data Retention Period in day(s)', both of which are empty. A checked checkbox labeled 'Encryption' is present. At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

2. In the **Enterprise tab**, enter the following information:
 - Server Name/Instance Name
 - Database
3. Select one of the following **Authentication Types**:
 - Windows Authentication
 - SQL Authentication
 - Custom
4. Enter a time value in seconds into the **TimeOut** field.
5. Enter an appropriate number of days into the **Data Retention Period** field.
6. Click **Cancel** to cancel adding the new Enterprise Server.
7. Click **Next** to display the **Table Group** tab.

2.17.2 Selecting Table Groups

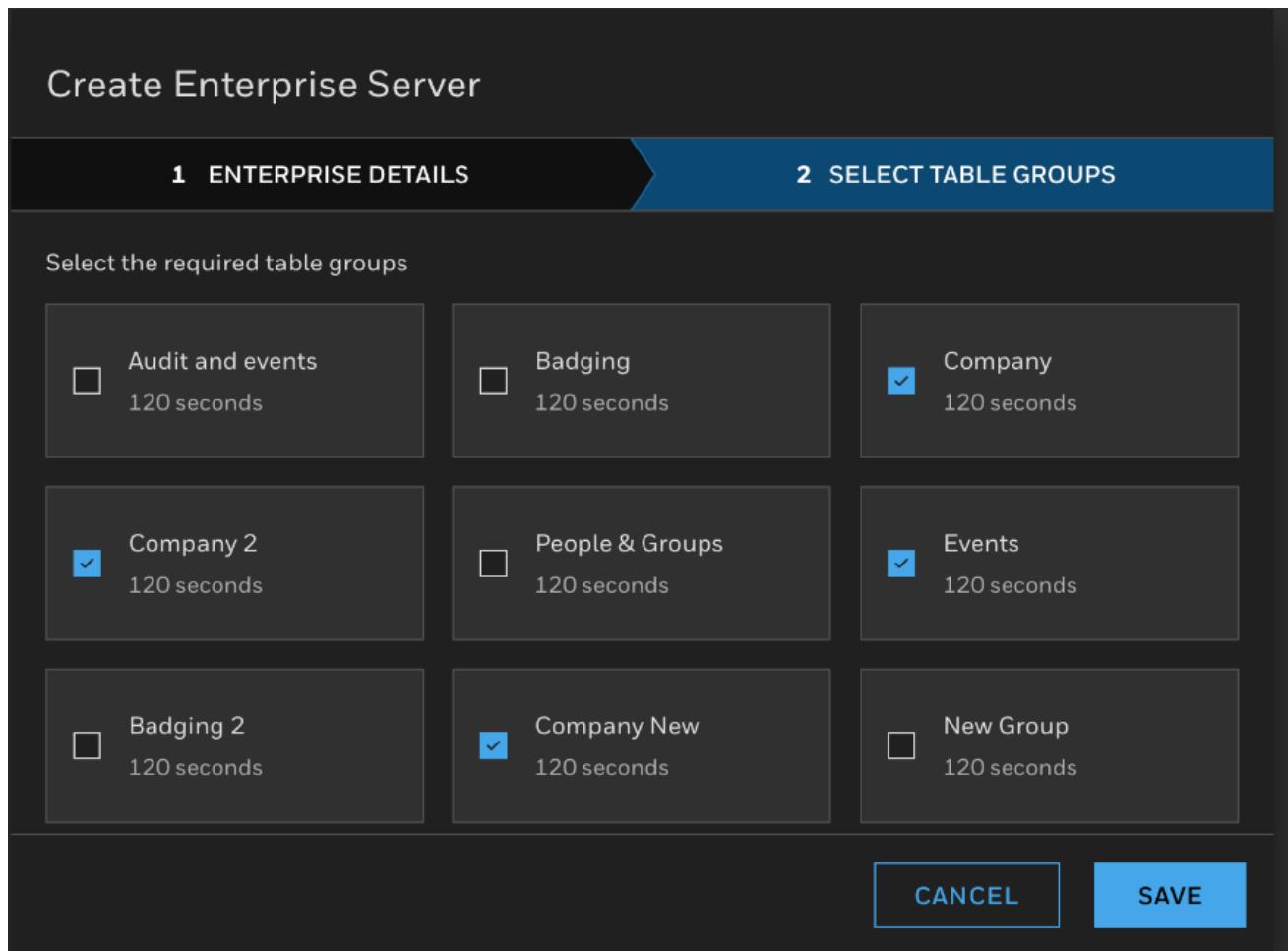
Create Enterprise Server

1 ENTERPRISE DETAILS 2 SELECT TABLE GROUPS

Select the required table groups

<input type="checkbox"/> Audit and events 120 seconds	<input type="checkbox"/> Badging 120 seconds	<input checked="" type="checkbox"/> Company 120 seconds
<input checked="" type="checkbox"/> Company 2 120 seconds	<input type="checkbox"/> People & Groups 120 seconds	<input checked="" type="checkbox"/> Events 120 seconds
<input type="checkbox"/> Badging 2 120 seconds	<input checked="" type="checkbox"/> Company New 120 seconds	<input type="checkbox"/> New Group 120 seconds

CANCEL **SAVE**

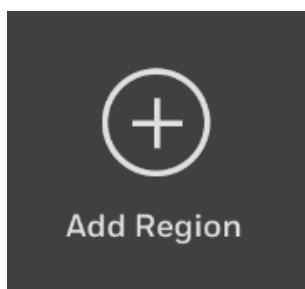


Pro-Watch will display tables from the database address you've entered earlier.
Select one or more tables as appropriate and click **Save**.

Note: Refer to *Pro-Watch 5.0 Enterprise Configuration Guide* for more details on Table Groups.

2.17.3 Creating a Region Server

1. To add a region, click the **PLUS button** on the upper-right corner of the Enterprise screen:



This action will display the **Create Region Server** screen:

The screenshot shows the 'Create Region Server' interface. At the top, it says 'Create Region Server'. Below that, there are two tabs: '1 ENTERPRISE DETAILS' (which is selected) and '2 SELECT TABLE GROUPS'. The 'ENTERPRISE DETAILS' tab contains the following fields:

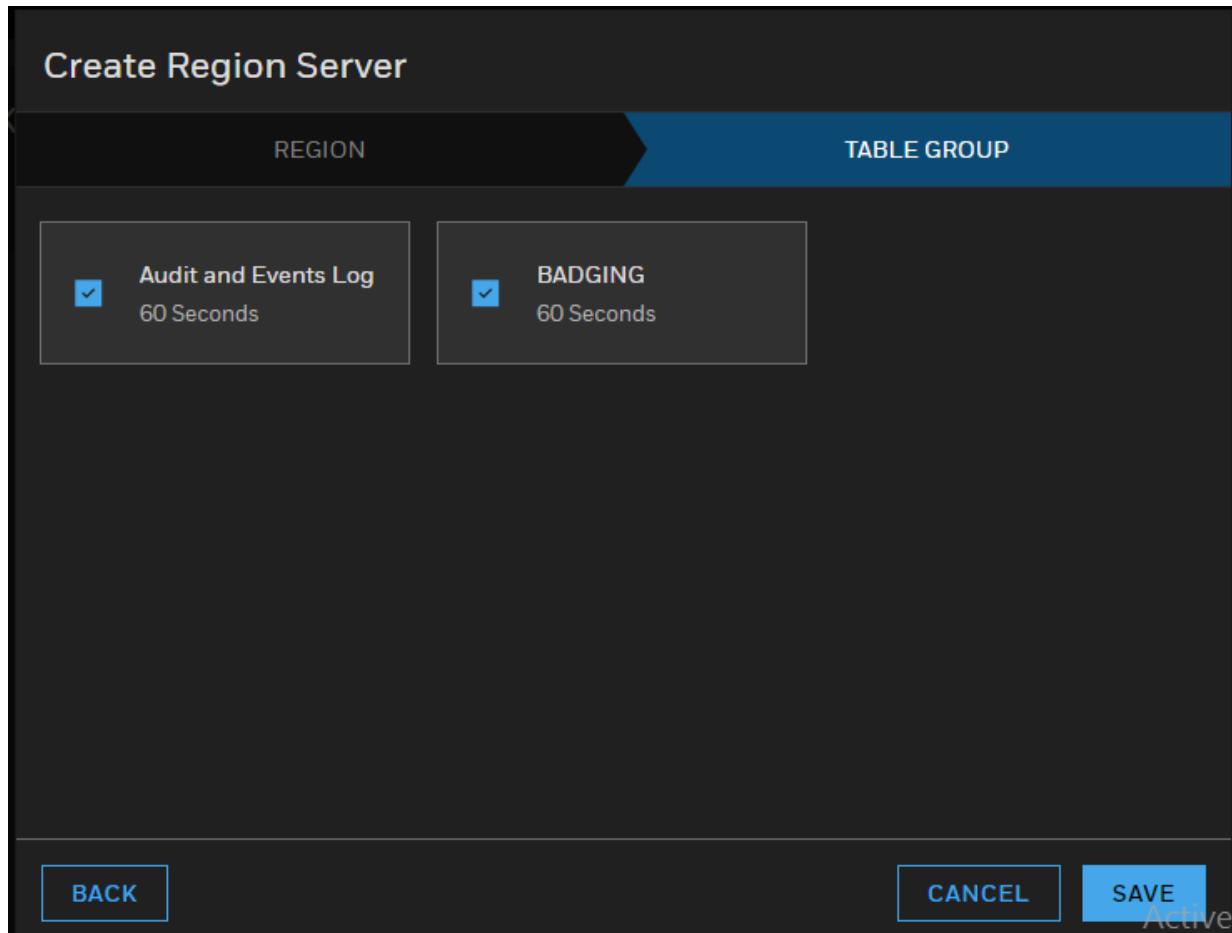
- Server Name/Instance Name:** IE3PLNTGRK5S2
- Database:** PWNT
- View less** (link)
- Authentication Type:** A group of three radio buttons: Windows Authentication (selected), SQL Authentication, and Custom.
- TimeOut (in seconds):** A text input field containing '20'.
- Data Retention Period in day(s):** A text input field containing '1'.
- Encryption:** A checked checkbox.

At the bottom right are two buttons: 'CANCEL' and 'NEXT' (highlighted in blue).

2. In the **Region tab**, enter the following information:
 - Server Name/Instance Name
 - Database
3. Select one of the following **Authentication Types**:
 - Windows Authentication
 - SQL Authentication
 - Custom
4. Enter a time value in seconds into the **TimeOut** field.
5. Enter an appropriate number of days into the **Data Retention Period** field.
6. Click **Cancel** to cancel adding the new region.
7. Click **Next** to display the **Table Group** tab.

2.17.4 Selecting Table Groups

To select a table, click and select the **Table Group tab**:



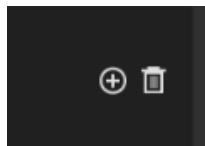
Pro-Watch will display tables from the database address you've entered earlier.
Select one or more tables as appropriate and click **Save**.

Note: Refer to *Pro-Watch 5.0 Enterprise Configuration Guide* for more details on Table Groups.

2.17.5 Deleting the Enterprise

Warning: **Deleting the Enterprise will delete the whole configurations, including the configured Regions.**

To **delete** a region, select it from the list of regions and then click the **TRASH CAN icon** on the upper-right corner of the Enterprise screen:



Note: More specific details of Enterprise configuration is available in the *Pro-Watch 5.0 Enterprise Configuration Guide*.

2.17.6 Updated Enterprise Screen

After you create your regions and select your tables, the Enterprise screen will list them as shown in the below screen:

The screenshot shows the 'Server Details' section with the server name 'IE3P-LNTGR-K5S2' and status 'ENTERPRISE ONLINE'. It displays metrics: 04 Regions, 06 Groups, and 10 Tables. A green banner at the top right indicates a 'New Region Added' with the ID 'BRUSS / 1911-098'. A 'DELETE SERVER' button is visible. Below this, a section titled '4 Regions' lists four entries: 'IUYRTHNN-790 ONLINE' (Last Sync: Yesterday Jun 27th, 4:20 PM, Table Count: 04, Fault(s) Detected: 02), 'Phil-117-XCVF ONLINE' (Last Sync: Yesterday Jun 27th, 4:25 PM, Table Count: 04), 'SGHLL-110189-UIR... ONLINE' (Last Sync: Yesterday Jun 27th, 3:20 PM, Table Count: 04), and 'BRUSS / 1911-098 ONLINE' (Last Sync: Yesterday Jun 27th, 4:55 PM, Table Count: 04). At the bottom left is a large 'Add Region' button with a plus sign.

This screen displays the overall status of both the Enterprise and the Regions, including the following:

1. The ONLINE or OFFLINE status.
2. The last time the synch occurred successfully.
3. The number of Regions.
4. The total number of Tables.
5. Total number of synching Faults.

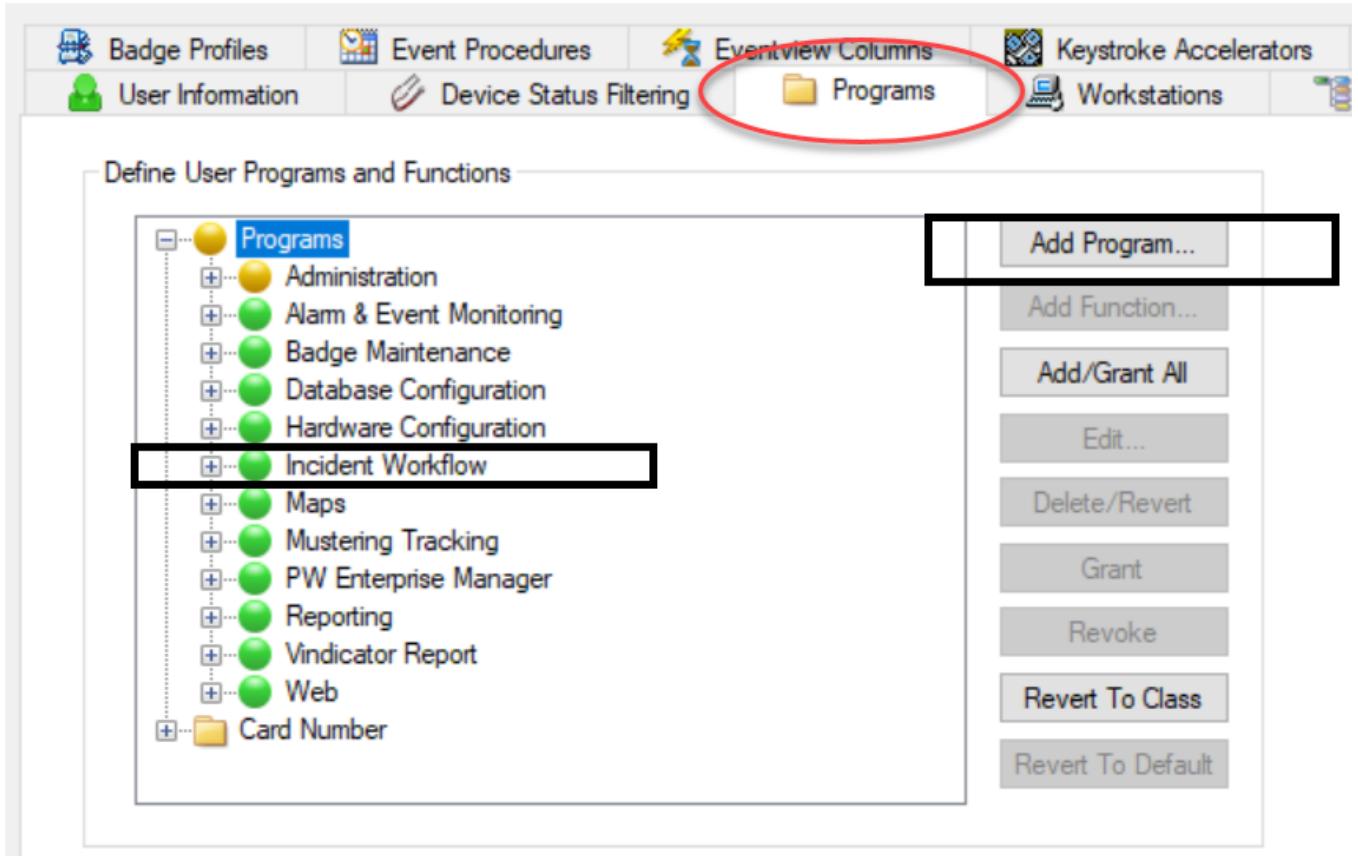
Note: Refer to *Pro-Watch 5.0 Enterprise Configuration Guide* for more details on configuring the Enterprise and the Regions.

2.18 Incidents

2.18.1 Incident Permissions

Make sure you first set the incident permissions in the Pro-Watch thick client as shown below:

Edit Users



2.18.2 Incidents Landing Page

Display the main **Honeywell Hamburger Menu**.

In the Honeywell Hamburger Menu bar, click the **Incidents** link to display the **Incidents** landing page:

The screenshot shows a table titled "18 Incidents" with columns: ID, WORKFLOW NAME, CREATED ON, OWNER, and PROGRESS. Each incident row contains a small icon representing the workflow type (e.g., red hexagon for Door Ajar or Door Held Alarms, yellow triangle for Event Prep Fire/Fire), the incident ID, the workflow name, the creation date, the owner's name (if applicable), and a progress bar indicating the number of steps completed.

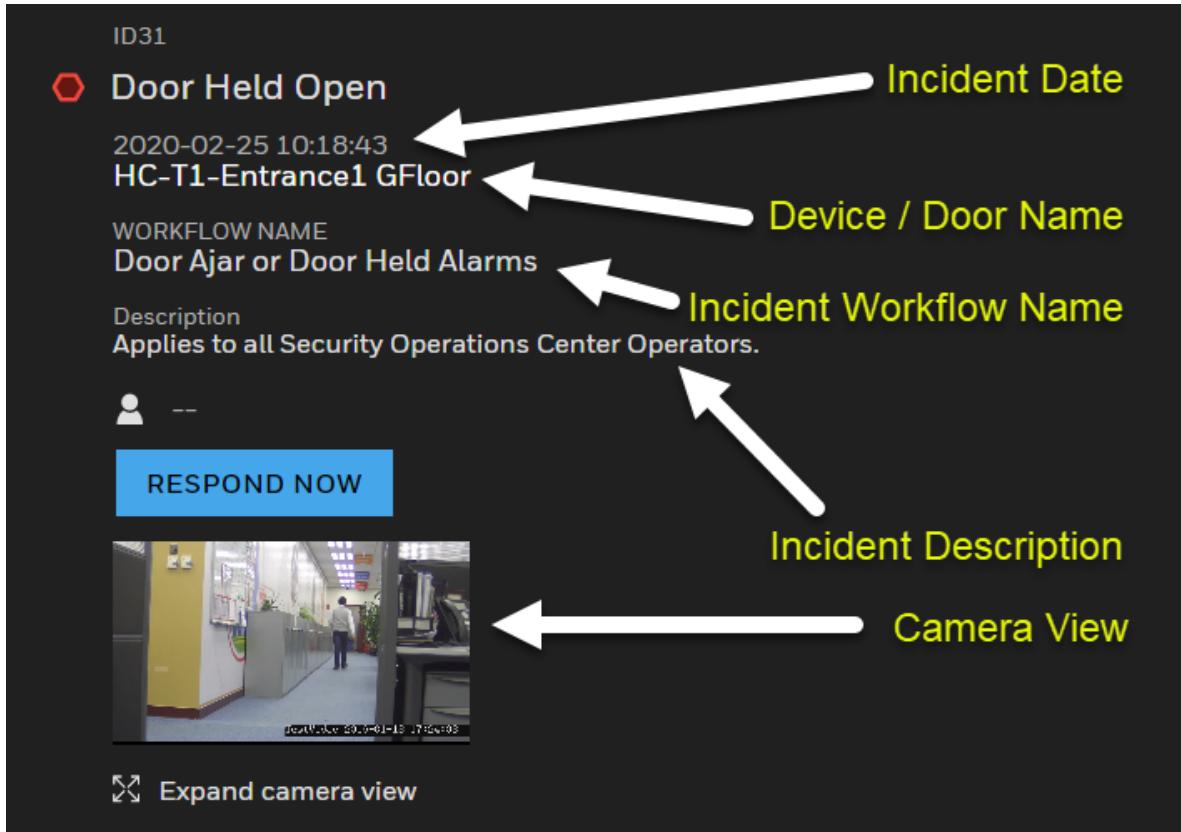
18 Incidents				
ID	WORKFLOW NAME	CREATED ON	OWNER	PROGRESS
32	Door Ajar or Door Held Alarms	2020-02-25 10:30:08		0 of 8
31	Door Ajar or Door Held Alarms	2020-02-25 10:18:43		0 of 8
29	Door Ajar or Door Held Alarms	2020-02-25 04:53:32		0 of 8
28	Intrusion or Door Forced Alarms Received	2020-02-24 07:15:53		0 of 8
27	Door Ajar or Door Held Alarms	2020-02-24 06:57:26		0 of 8
26	Intrusion or Door Forced Alarms Received	2020-02-21 12:29:17	venkatesh	0 of 8
24	Door Ajar or Door Held Alarms	2020-02-20 09:54:01		0 of 8
18	Door Ajar or Door Held Alarms	2020-02-12 14:24:24	ronda	2 of 8
17	Door Ajar or Door Held Alarms	2020-02-12 13:50:50	ronda	0 of 8
15	Door Ajar or Door Held Alarms	2020-02-11 13:59:45	venkatesh	4 of 8
13	Event Prep Fire/Fire	2020-01-30 19:14:03	vijay	0 of 1

Incidents are listed with:

- **ID Number** – the system number assigned to the incident.
- **Workflow Name** – the system name given to the incident.
- **Date of Creation** – date of the incident.
- **Owner** – the name of the person who assumes the responsibility of responding to an incident by following the automatically-populated number of steps.
- **Percentage of Progress** – displays how many of the steps necessary to respond to an incident have been taken by the **Owner** of the incident.

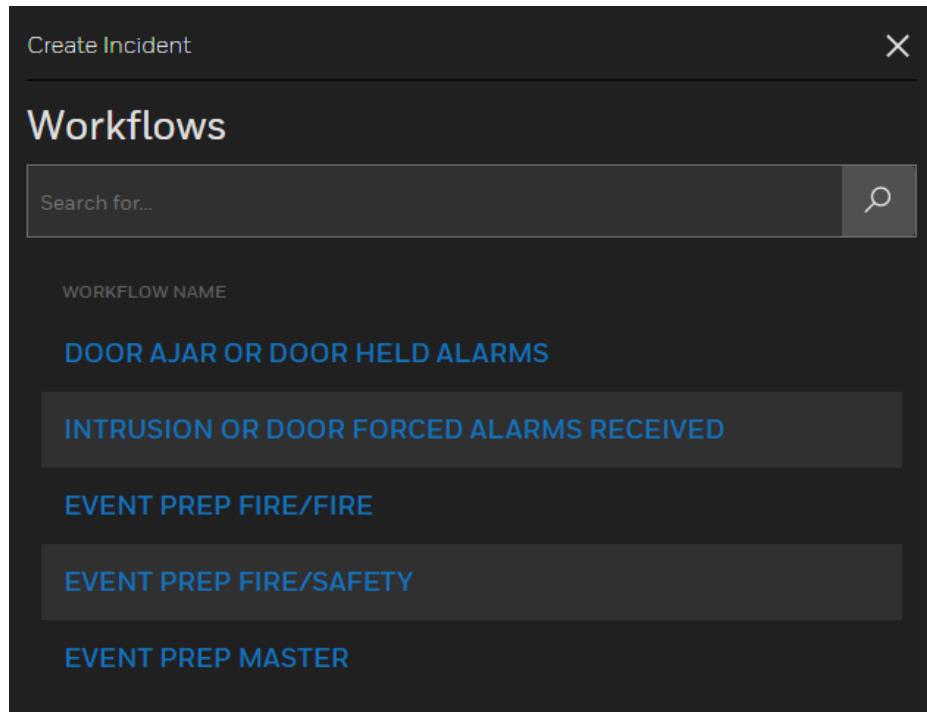
2.18.3 Incident Management Screen

Click on an incident on the **Incident Landing Page** to display its management screen:



2.18.4 Creating an Incident

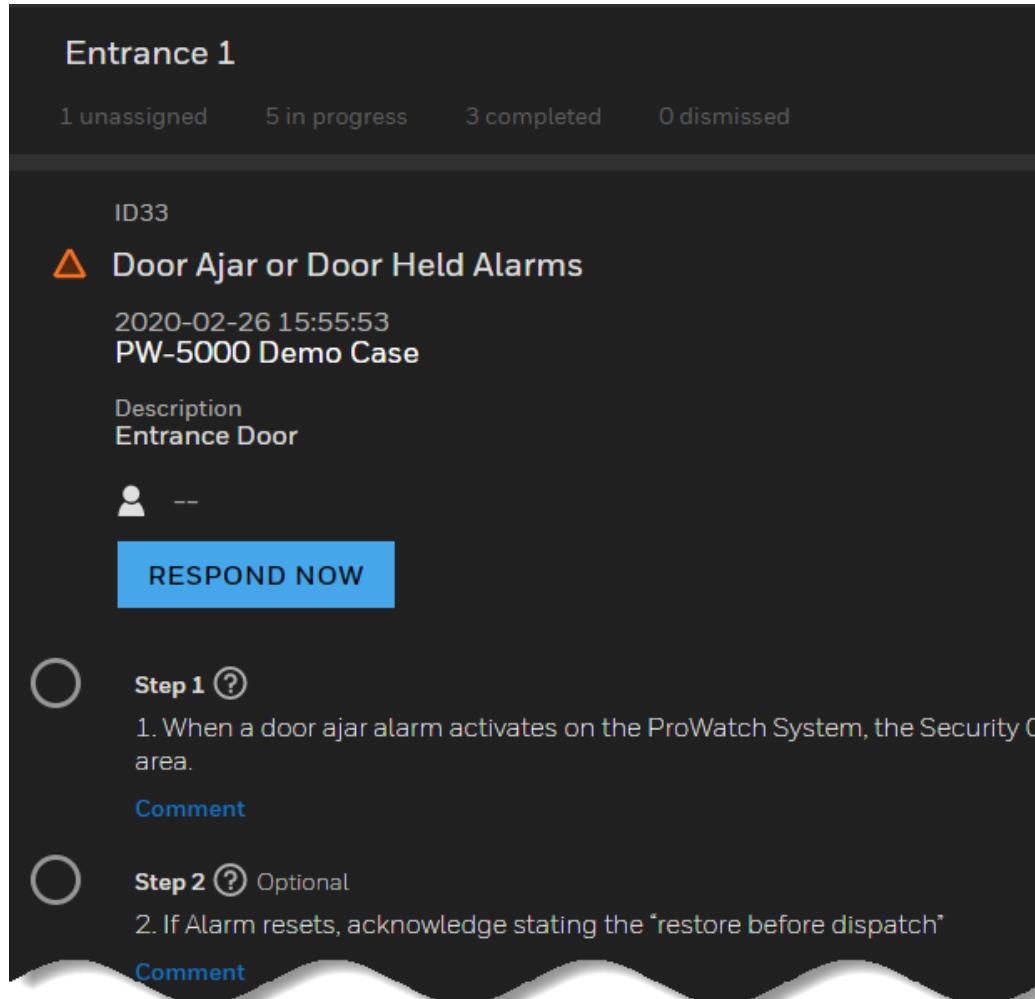
1. To create an incident, click the **CREATE** button on the **Incident Landing Page** to display the **Create Incident** screen:



2. Select a workflow to display the **Workflow** screen:

The screenshot shows the 'Door Ajar or Door Held Alarms' workflow screen. It includes fields for 'Priority' (with options 'URGENT', 'HIGH', and 'LOW', where 'HIGH' is selected), 'Device Name or Location' (set to 'Entrance 1'), and 'Description' (set to 'Entrance Door'). At the bottom are 'BACK' and 'CREATE' buttons.

3. Search for a workflow by using the search field.
4. Select an incident **Priority, Device Name or Location** (optional), and/or **Description** (optional).
5. Click **Create** to display the new incident management screen with auto-populated response steps:



2.18.5 Responding to an Incident

1. To respond to an incident click the **RESPOND NOW** command button.
2. Follow the procedural steps displayed for the incident and place a check mark after each completed step:

The screenshot shows a list of steps for responding to a door ajar alarm. Step 1 is completed (marked with a green checkmark). Step 2 is optional (marked with a green checkmark). Step 3 is optional (marked with an empty circle). Step 4 is optional (marked with an empty circle). Each step includes a 'Comment' link.

- Step 1** ⓘ
1. When a door ajar alarm activates on the ProWatch System, the Security Operations C area.
[Comment](#)
- Step 2** ⓘ Optional
2. If Alarm resets, acknowledge stating the "restore before dispatch"
[Comment](#)
- Step 3** ⓘ Optional
3. If the operator resets the door alarm, the SOC operator will acknowledge the alarm w
[Comment](#)
- Step 4** ⓘ Optional
4. If repeatedly activating ESO dispatch is still required
[Comment](#)

3. The PROGRESS bars will display how many of the necessary steps have been taken by the operator:

The screenshot shows a detailed view of a specific alarm. The alarm ID is ID15. It is a Door Ajar or Door Held Alarm, occurring on 2020-02-11 at 13:59:45. The description is --. The operator assigned is venkatesh. There is a blue 'TAKE OVER' button at the bottom.

ID15

Door Ajar or Door Held Alarms

2020-02-11 13:59:45

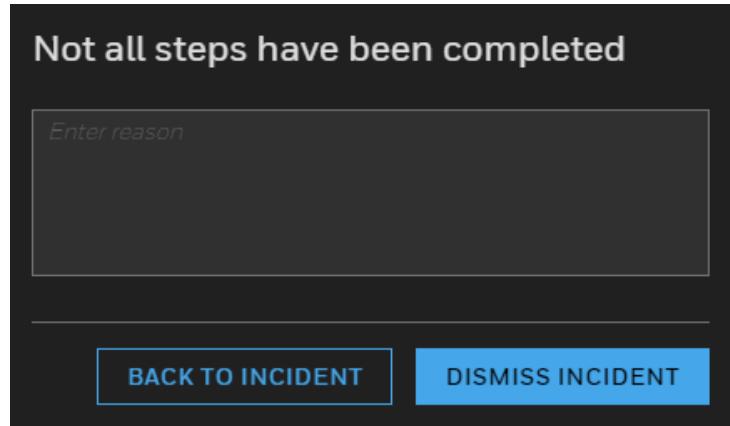
Description

--

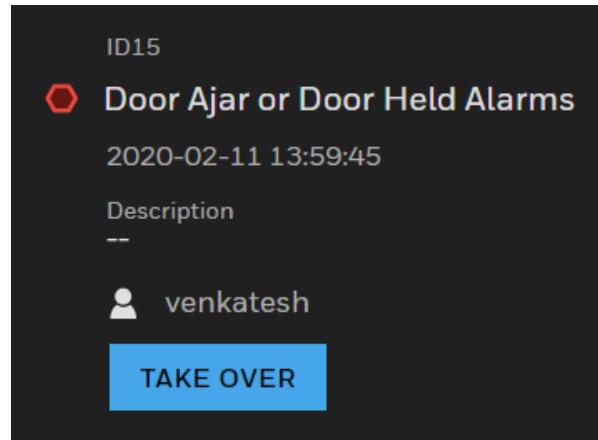
venkatesh

TAKE OVER

4. To dismiss an incident, click the **DISMISS** command button. If not all completion steps are completed, Pro-Watch will display a **NOT ALL STEPS HAVE BEEN COMPLETED** warning message:



5. Enter the reason why all steps are not completed. Then click the **DISMISS INCIDENT** button.
6. To return to the incident, click the **BACK TO INCIDENT** button.
7. To take over the responsibility of responding to an incident, click the **TAKE OVER** button:



2.18.6 Activity Log

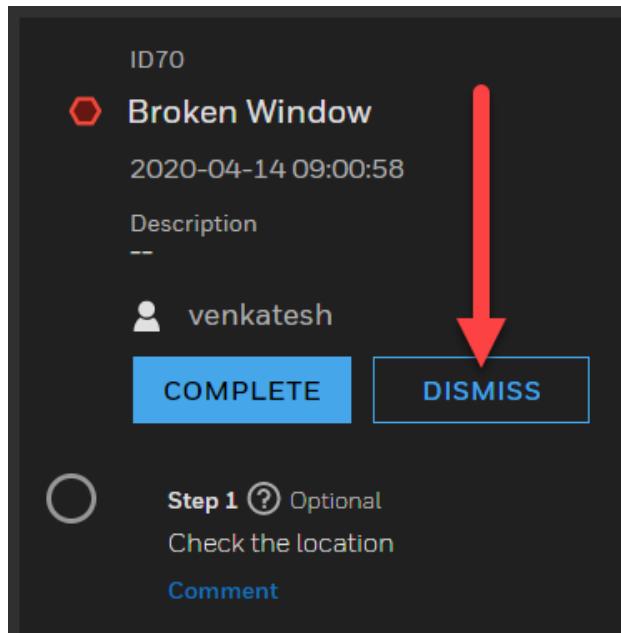
The Activity Log will display a history of the actions taken for the incident, with the first action at the bottom of the list, the latest at the top:

Activity	
venkatesh	2020-02-24
Last Activity	
Took over the incident.	
marcus	2020-02-11
Marked Step4 as complete.	
marcus	2020-02-11
Marked Step3 as complete.	
marcus	2020-02-11
Marked Step2 as complete.	
marcus	2020-02-11
Added a comment in step1.	
marcus	2020-02-11
Marked Step1 as complete.	
marcus	2020-02-11
Started responding to the incident.	
marcus	2020-02-11
First Activity	
Created an incident.	

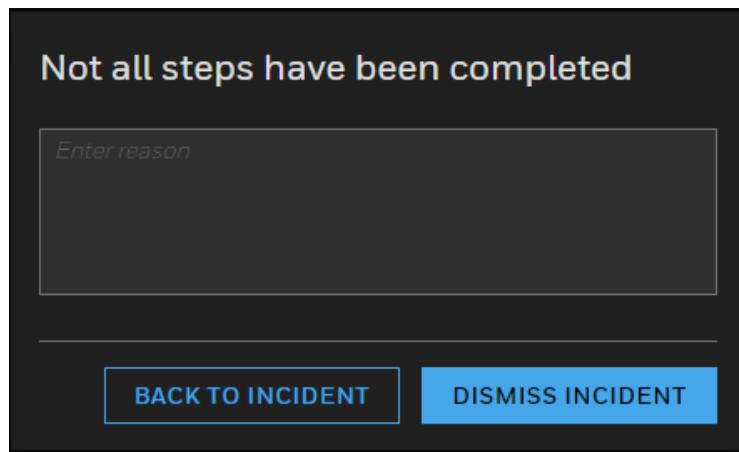
2.18.7 Dismissing an Incident

To dismiss an incident:

1. Click and select the incident in the Incidents screen to display the incident detail screen:



2. Click the **DISMISS** button. If you are dismissing the incident without completing all the steps, a warning message will display:

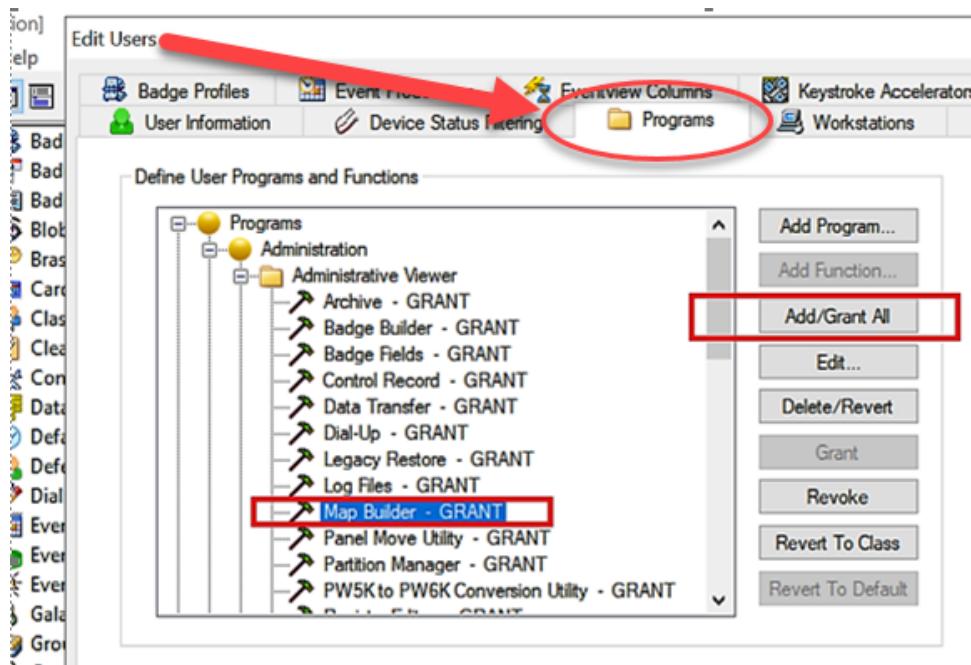


3. Either click the **BACK TO INCIDENT** button and complete all the necessary steps, or click the **DISMISS INCIDENT** button to dismiss the incident.

2.19 Maps

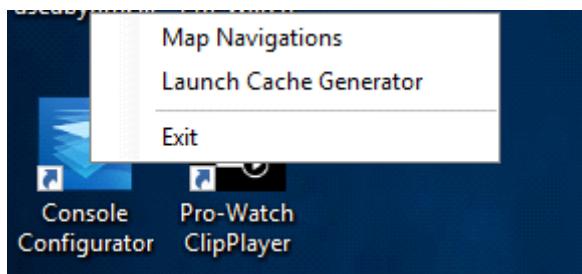
2.19.1 Map Permissions

Maps View Can be edited only with the below permission:

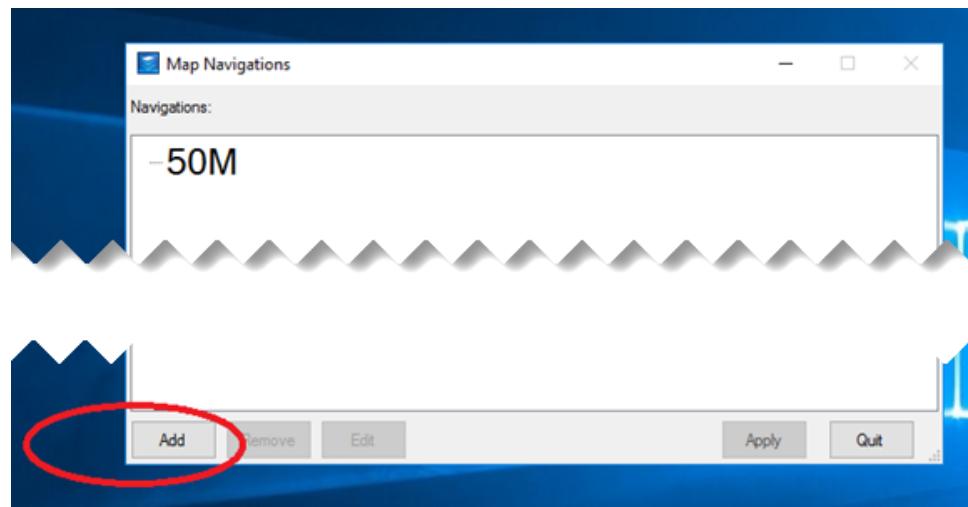


2.19.2 Adding (Level) Maps to Pro-Watch Intelligent Command

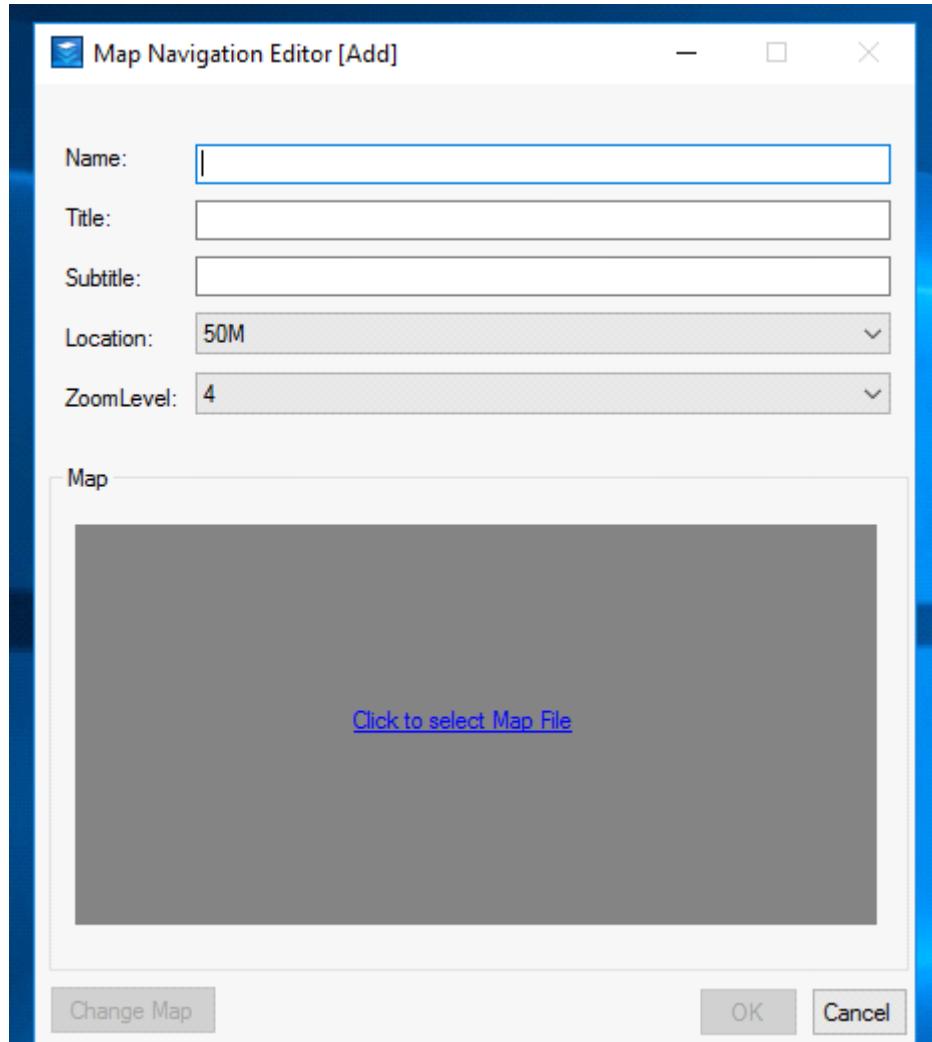
1. Click "Console Generator" and click "Map Navigations":



2. Click "Add" to select a root:



3. After filling the information:

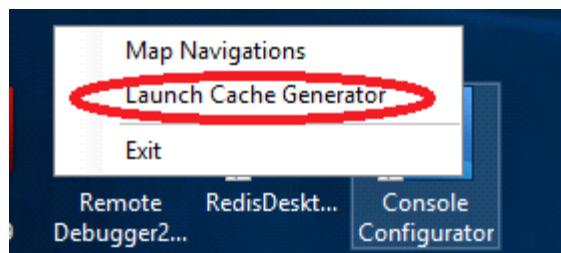


4. Add **Name** and **Title**.
5. Select the map image file and upload.
6. Then, click "**OK**" to complete adding the map.

2.19.3 Generating Maps

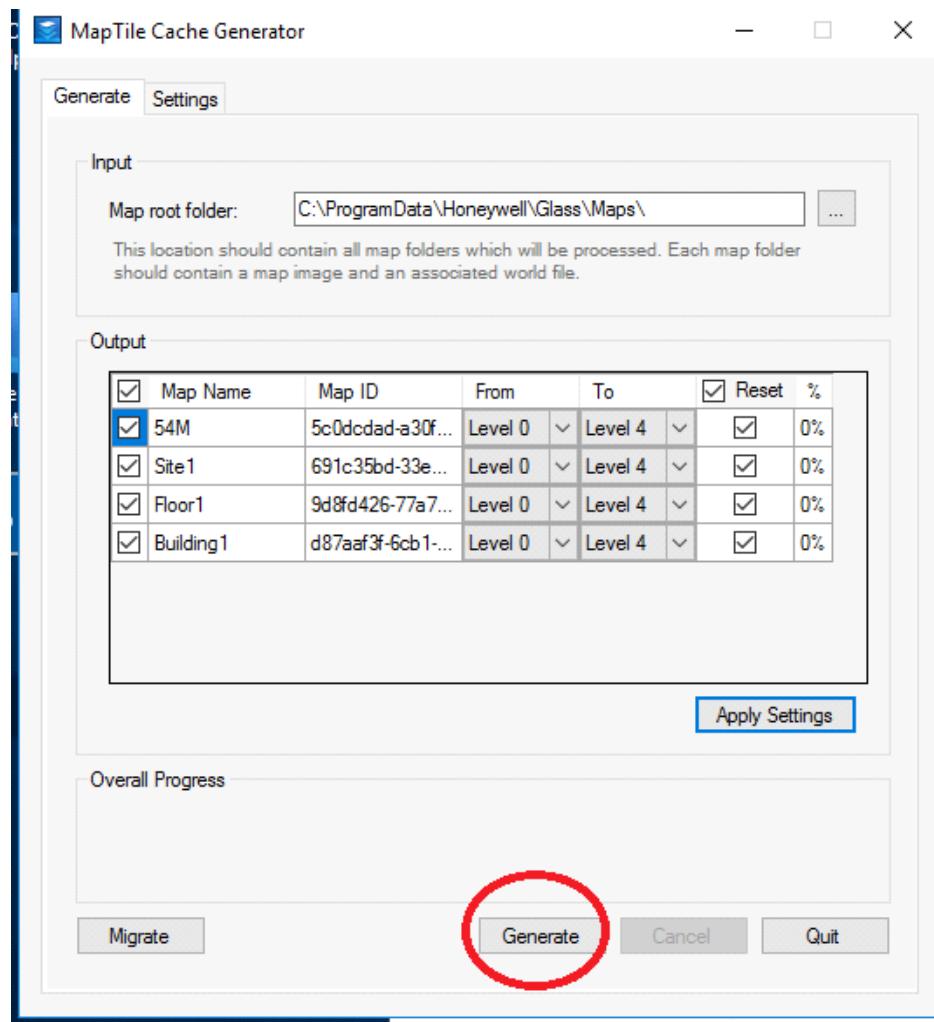
(Continuing from [Adding \(Level\) Maps to Pro-Watch Intelligent Command](#) above)

1. Click "**Console Generator**" and then click "**Launch Cache Generator**".



2. Select the recently uploaded map images, and then click "Generate."

Note: If there are many maps to generate, it may take some time. Please upload and generate a small number of maps in Map Tile cache generator to save time. There might be file/folder memory growth expected after generating maps in the Map Tile cache generator tool.)



3. After generating the map(s), you can go to the below address to check:

C:\ProgramData\Honeywell\Glass\Maps\7db93780-b90b-41ee-8943-ba405ca8d133

- If there is the file "tilecache", it means map-generation has been successful:

The screenshots show the following directory structure:

- Top Screenshot (File Explorer):**
 - Path: This PC > Local Disk (C:) > ProgramData > Honeywell > Glass > Maps > 5c0dcdad-a30f-4d2e-9081-24f69114b5b1
 - File: tilecache (highlighted with a red circle)
 - Subfolders: ReferenceFile, 未标题-1.jgw, 未标题-1
 - File: 未标题-1.jpg
- Bottom Screenshot (File Explorer):**
 - Path: Local Disk (C:) > ProgramData > Honeywell > Glass > Maps > 5c0dcdad-a30f-4d2e-9081-24f69114b5b1 > tilecache
 - Files: 2306999.1796875, 4613998.359375, 9227996.71875, 36911986.875, 73823973.75, 295295895, 590591790

- Drag the camera onto the map:

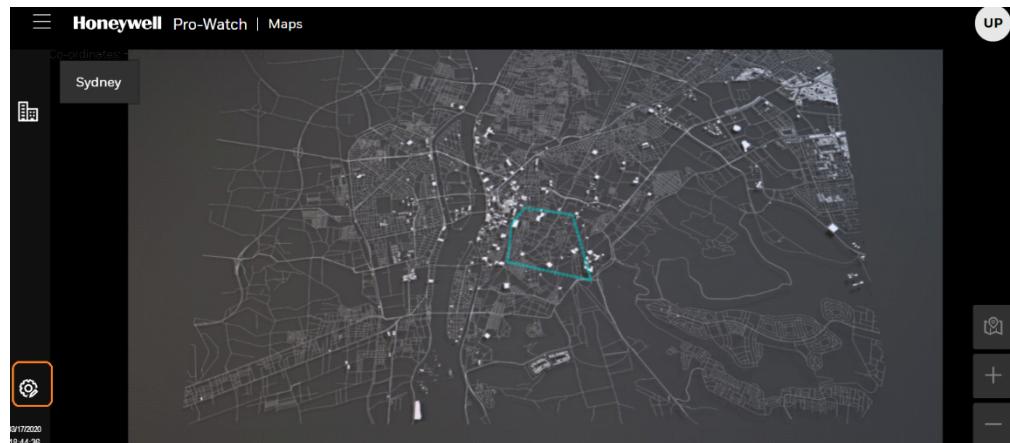
The screenshot shows the Honeywell Pro-Watch Maps interface with the following elements:

- Object Browser:** On the left, it lists objects including Camera1, Camera6, Default Controllable Obj., Default Monitorable In..., Entrance1, Entrance2, secure, secure_3, secure_4, and secure_5.
- Map View:** The central area shows a map with several camera icons (represented by surveillance cameras) and their corresponding live feeds in a grid format.
- Live Feeds:** The feeds are arranged in a grid:
 - Top-left: Camera1 (labeled 'secure')
 - Top-right: Entrance 1
 - Middle-left: Camera1 (labeled '359')
 - Middle-right: Entrance 2
 - Bottom-left: Camera6
 - Bottom-right: An empty feed slot.

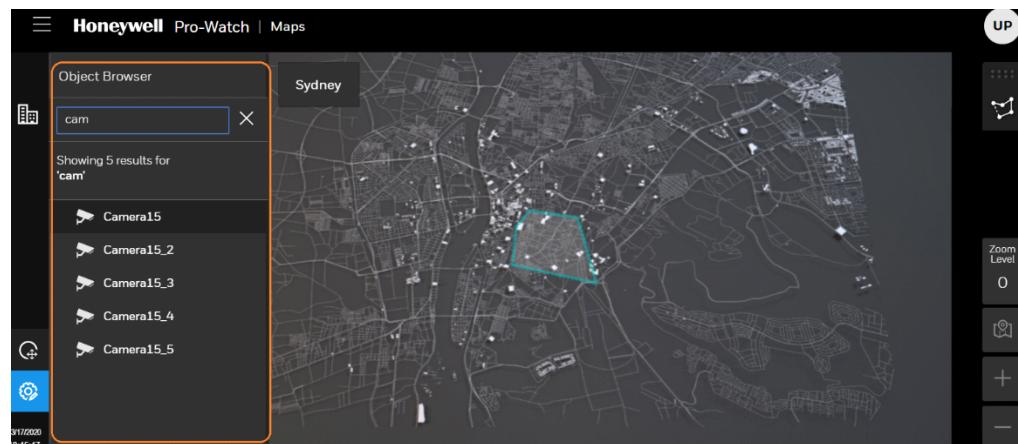
2.19.4 Configuring Devices on the Map

Note: Device configuration and icon locations in Map can be backed up from path "C:\Program data\Honeywell\Glass\Store" in Pro-Watch Intelligent Command -Web Tier.

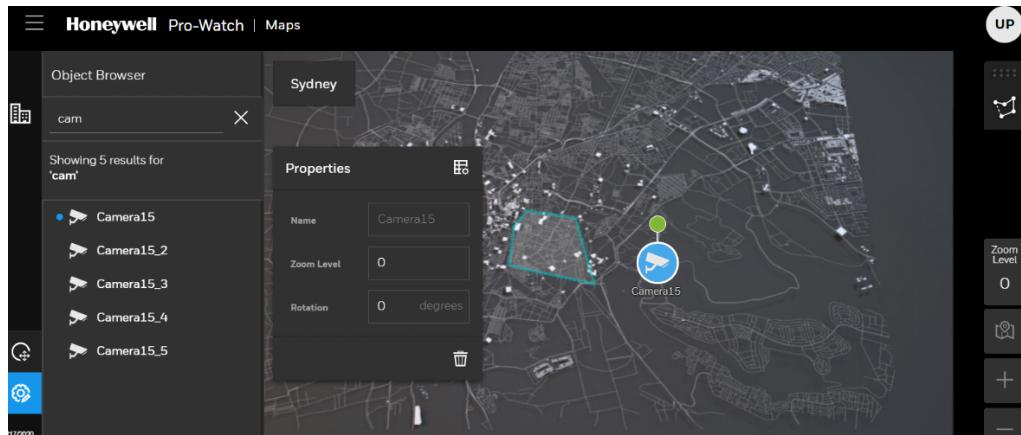
1. Start device configuration list by clicking the config tool:



2. From the device list, user can select a device and drag and drop on to the map image:

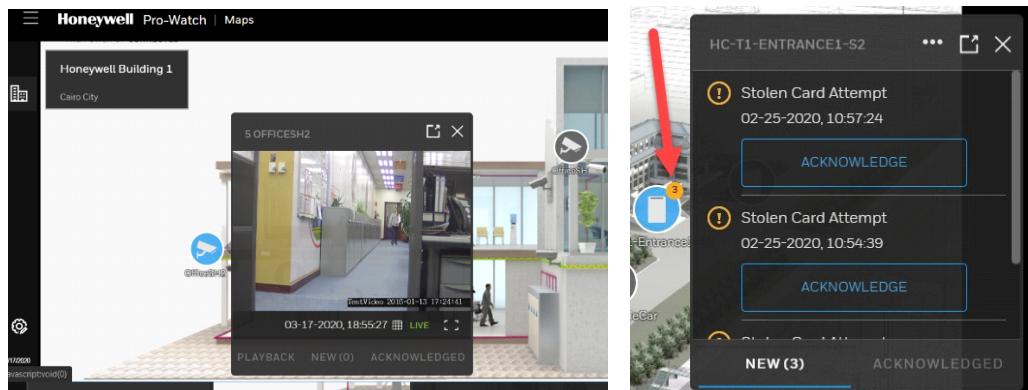


3. User can use free text search feature to search for device:



4. Clicking on the config tool icon closes the configuration session.

2.19.5 Viewing Video and Alarms on Maps Device Popup



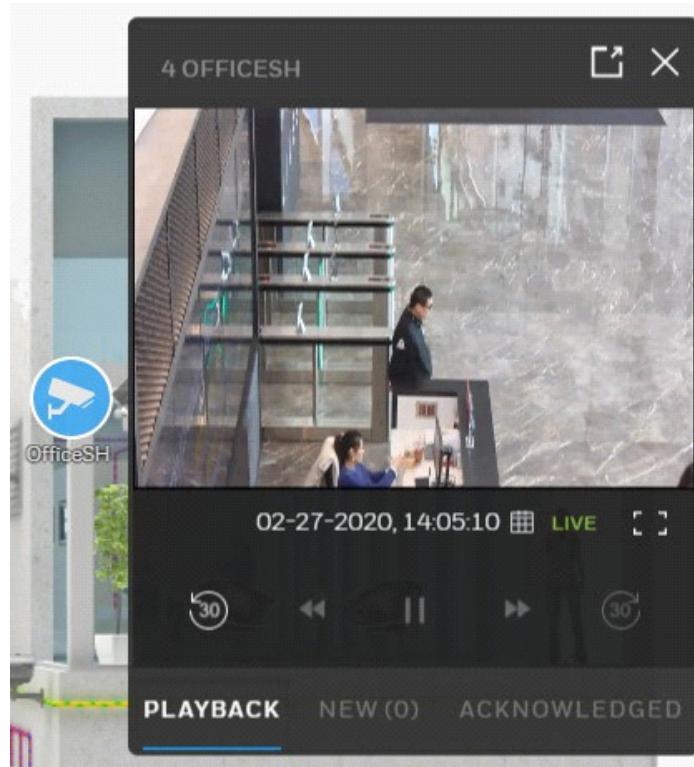
2.19.6 Controlling Zoom Level

To increase the zoom level, click the + (plus) sign on the lower-right corner.

To decrease the zoom level, click the - (minus) sign on the lower right corner.

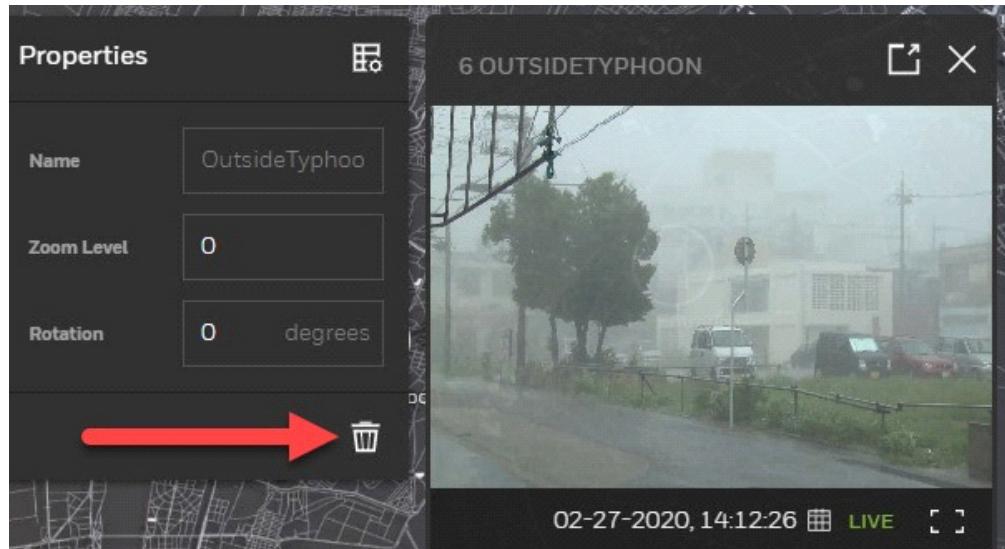


2.19.7 Controlling the Video Playback Using Standard Playback Controls as Well Calendar Control



2.19.8 Removing a Device from the Map

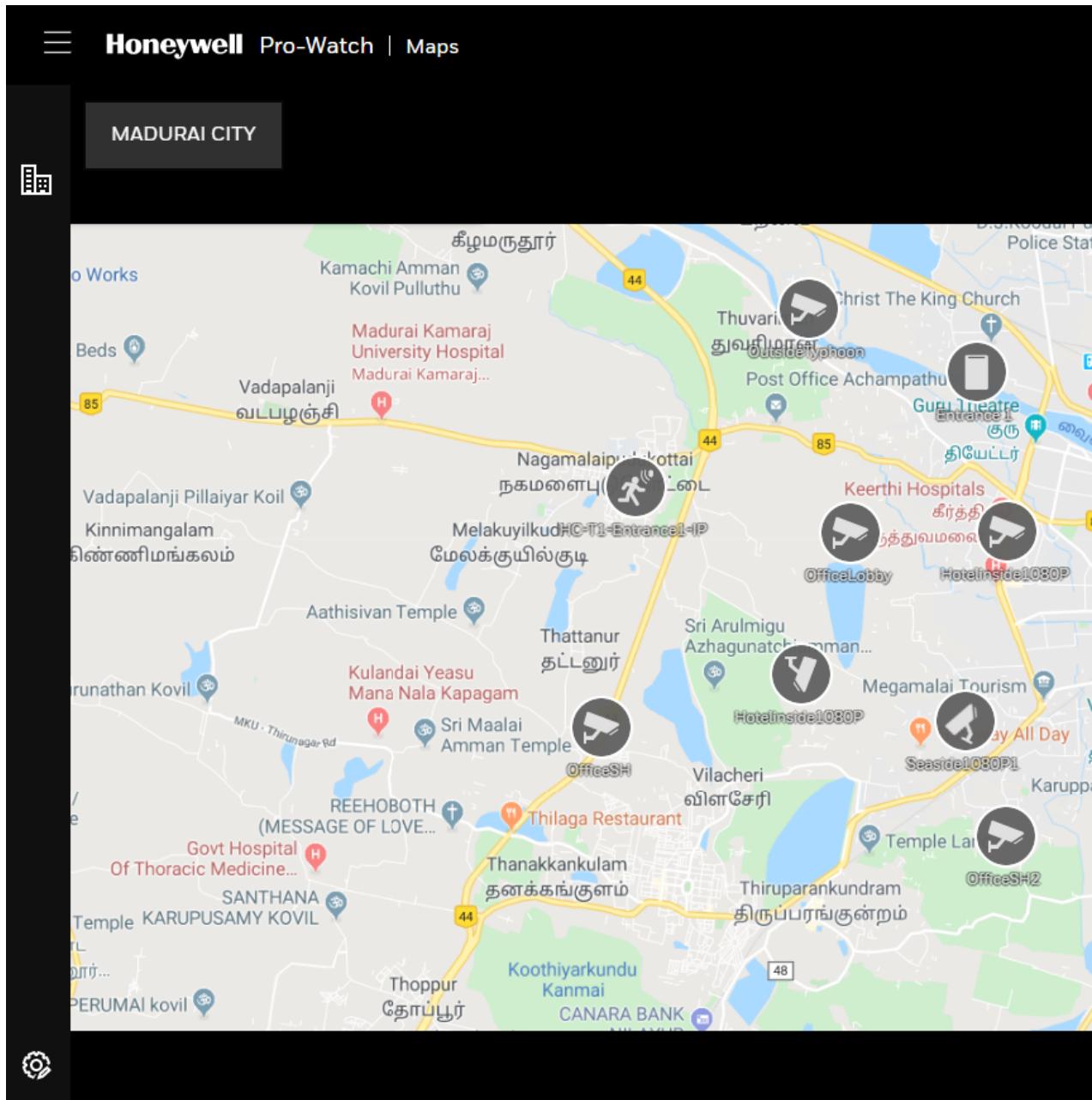
1. Click config tool to lunch map configuration. See [Configuring Devices on the Map](#).
2. Select target device on the map.
3. Click the Delete icon:



2.19.9 Displaying Maps in Web Client

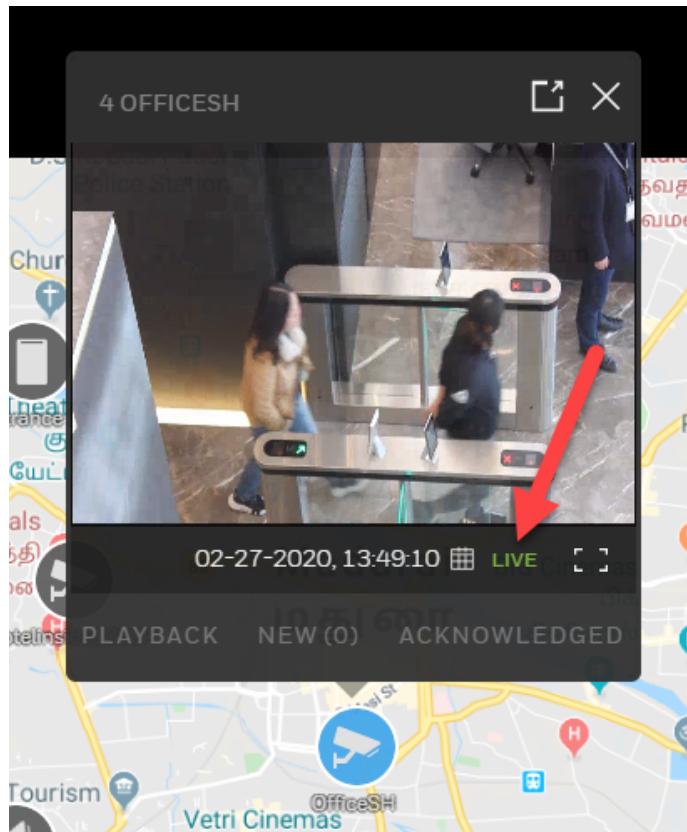
Display the main Honeywell Hamburger Menu.

In the Honeywell Hamburger Menu bar, click the **Maps** link to display the **Maps** landing page:



2.19.10 Live Camera View

To view a camera, click on the camera icon to display a live view:



2.19.11 Zoom Level

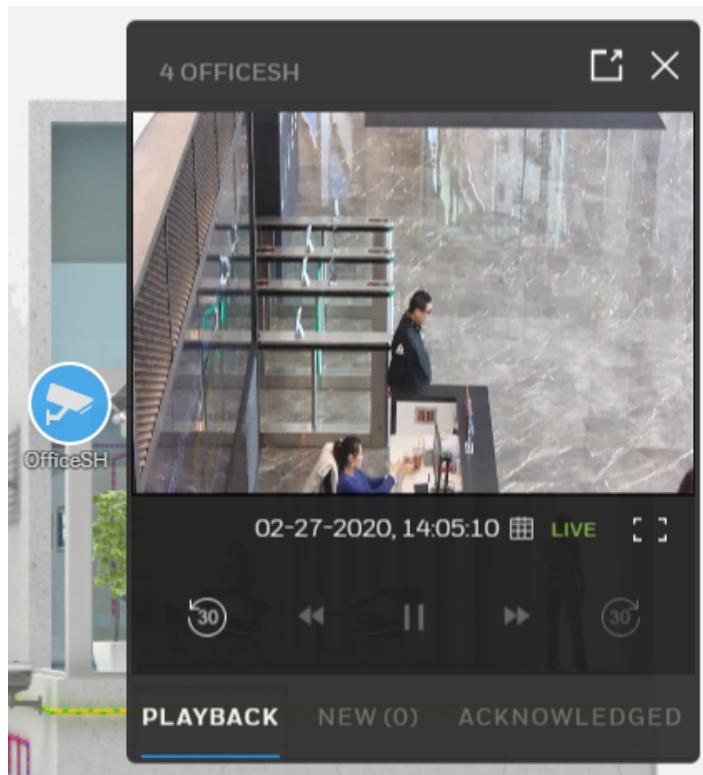
To increase the zoom level, click the + (plus) sign on the lower-right corner.

To decrease the zoom level, click the - (minus) sign on the lower-right corner.

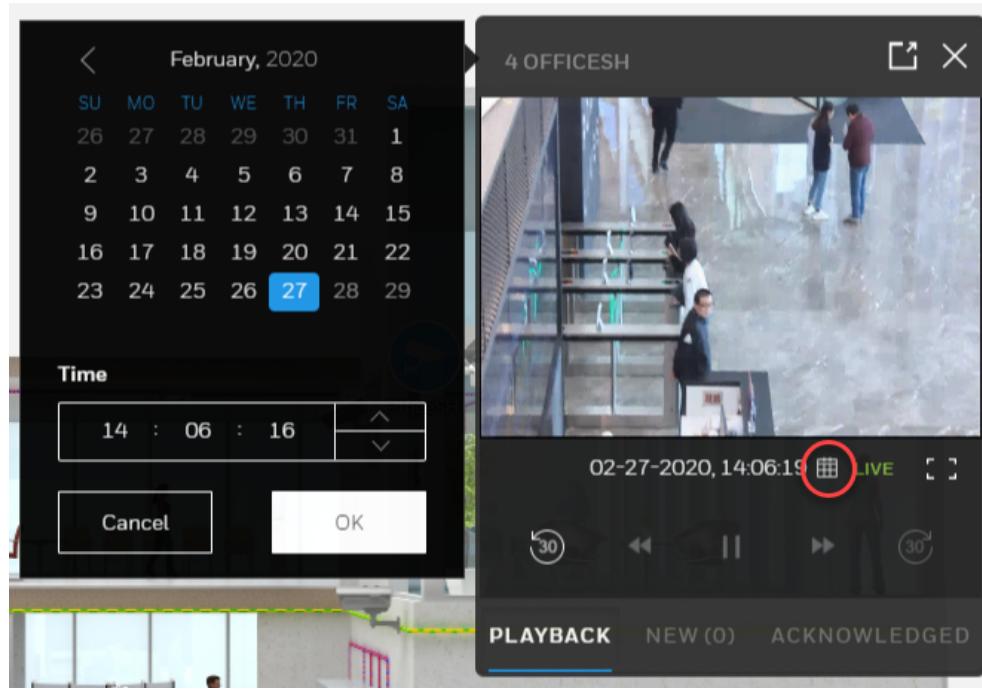


2.19.12 Playback

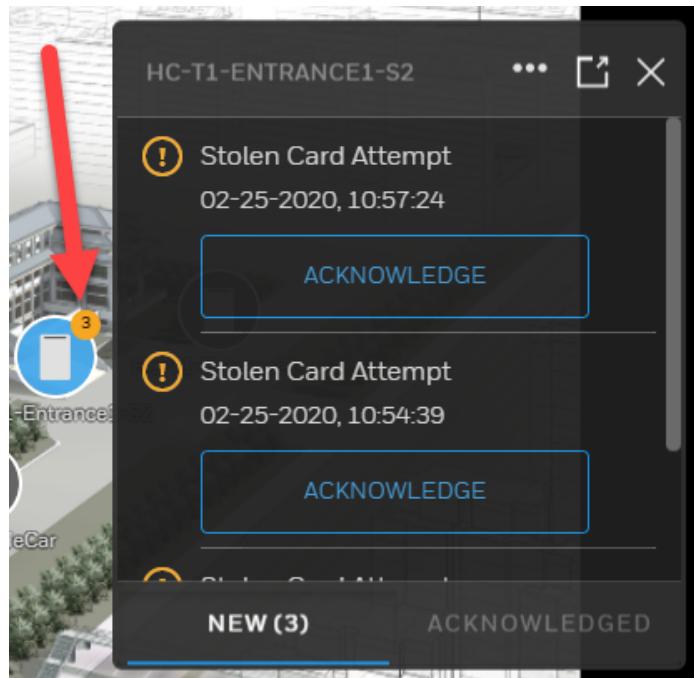
To playback, click the PLAYBACK link:



Click the CALENDAR icon to select a date for video playback:



2.19.13 Acknowledging the Alarms in Map



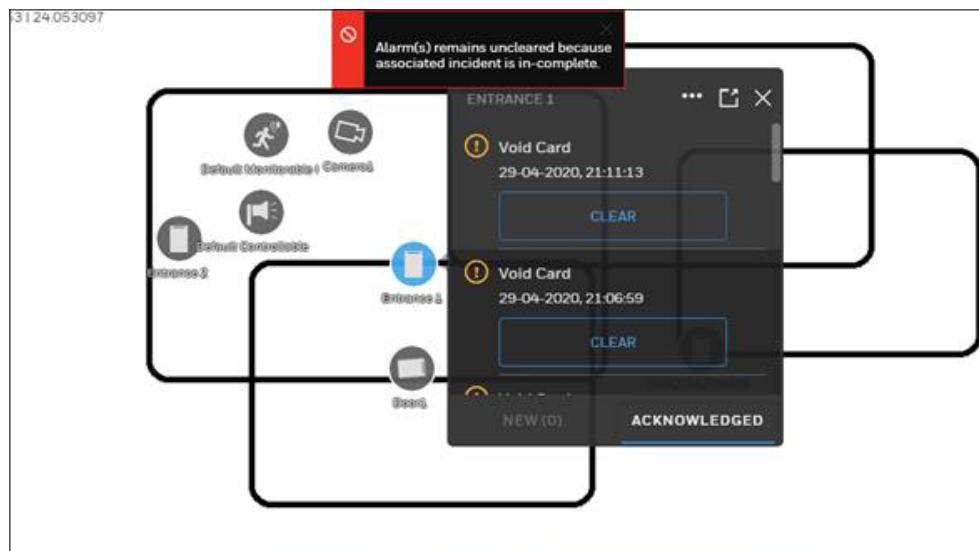
The number circle on the icon will display the number of alarms recorded. To acknowledge the alarm, click the ACKNOWLEDGE button.

A workflow-associated alarm, when acknowledged, will not automatically navigate the user to the Incidents page. The user must navigate manually to the Incidents page in order to view the incident.

2.19.14 Clearing the Alarms in Maps

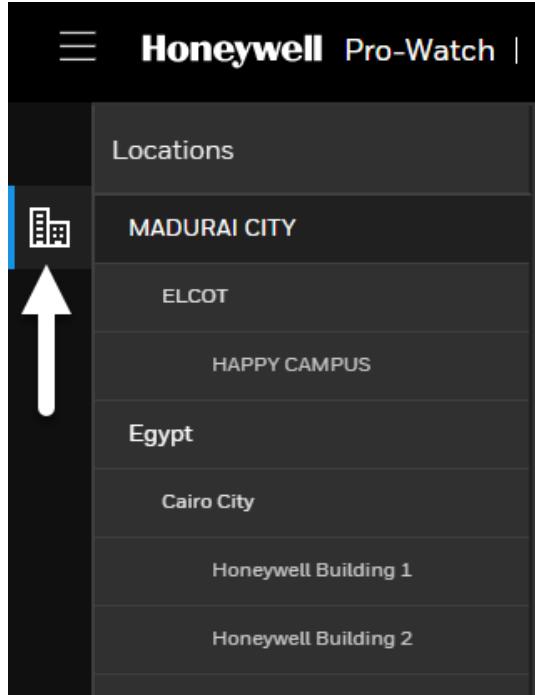
If there is any incident associated with the alarm, clearing the alarm will fail and display the following **error message**:

“Alarm(s) remains uncleared because associated incident is in-complete.”



2.19.15 Browsing by Location

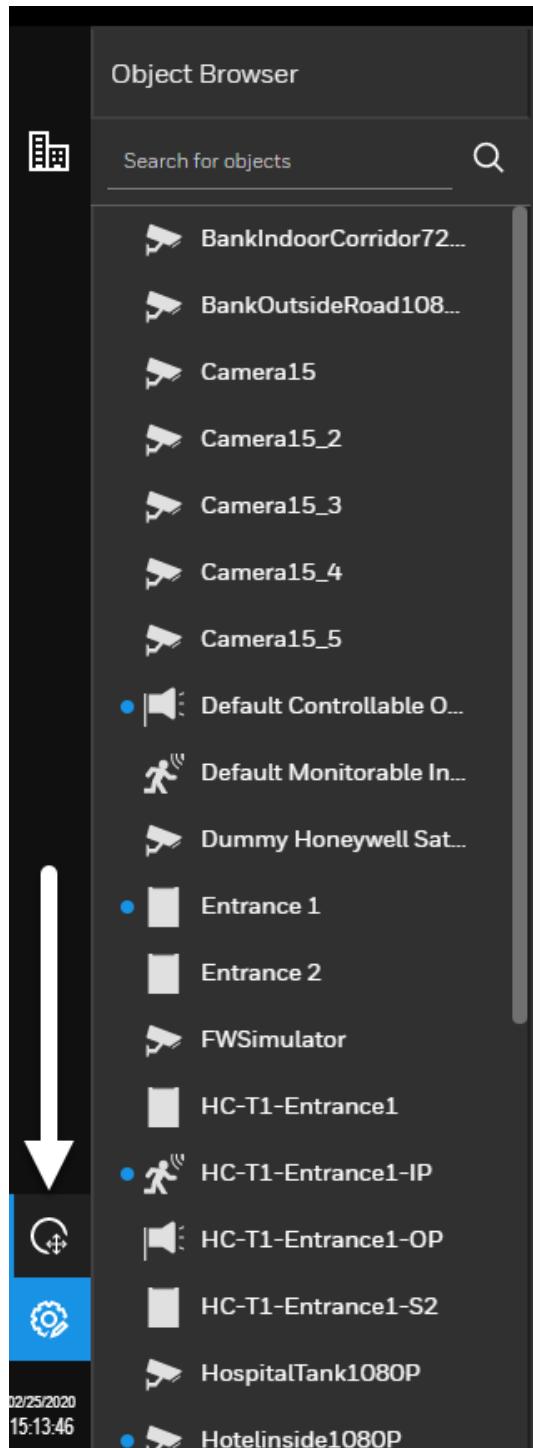
To browse different locations, click the **Building** icon to display the **Locations** list:



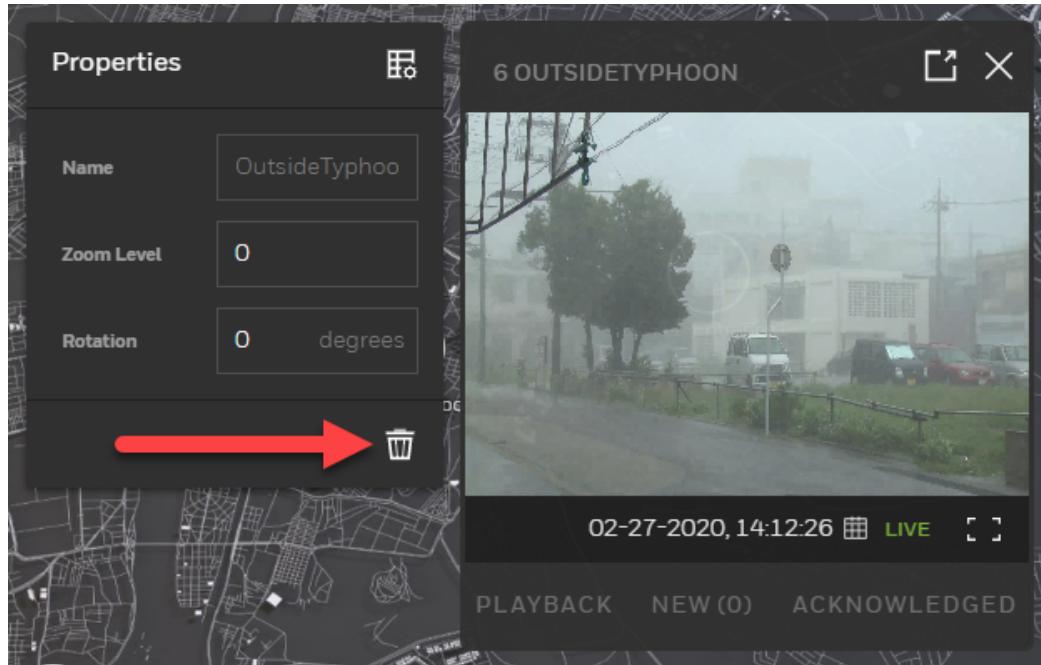
Select a location to display its map on the right pane.

2.19.16 Browsing by Map Objects

To browse by different map objects, click the **Wheel** icon to display the **Objects** list:



Select an object from the list to display it on the right pane:



To delete the camera view, click the TRASH icon in the Properties screen.

2.20 Known Issues and Recommendations, System Settings

2.20.1 Installation

1. Run "Pro-Watch Intelligent Command.exe" as administrator.
2. Make sure the Windows updates are completed.
3. Make sure installer (user) has Admin privileges.

2.20.2 Firmware Inventory file store

1. Ensure a file path (location) is preset for firmware files to be stored, locally or on a network path.
2. If network path is used, we recommend using "Map Network Drive" to map this folder locally.
3. Ensure this path is available as inventory storage path during installation.
4. Ensure the user (credential given in installer) has the write access to this path.

2.20.3 If you face any Login issues:

1. Run "cmd" as administrator and do "iisreset".
2. Do "ctrl + F5" in the Pro-Watch sign in page.
3. If in any case, the "Pro-Watch Server" was restarted, complete steps 2 and 3 above.

2.20.3.1 Possible resolutions:

- The client workstation and Web Server workstation should be added for the Web to work.
- The client workstation and Web Server workstation should be added to the web user.
- User's web password should be set in advance. But please note that a user's web password is needed ONLY for Basic Authentication, not for Windows Authentication.
- Pro-Watch Server service should be running.

2.20.4 If you get a "Certificate Error" at Login:

1. Manually create the certificate and sign in.

2.20.5 If VMS and Pro-Watch data are out of sync:

1. Go to video channel properties, turn OFF "is installed" press OK. Then, open video channel properties turn ON "is installed."
2. Or, go to services.msc. Restart "Pro-Watch Server" and try download.
3. Or, go to specific recorder in VMS and update description and save (this will initiate the auto sync).

2.20.6 Unable to add firmware inventory file from few machines and the progress indicator is always showing 0% progress

1. Go to the machine, where Pro-Watch web UI is installed.
2. Open powershell in admin mode and go to path: C:\Program Files (x86)\Honeywell\UnifiedSecurityPlatform\Web\LiveAlarm\Util
3. Type \export.ps1 and press enter.
4. Above command will generate "Honeywell_Certificate" certificate at this location:C:\Program Files (x86)\Honeywell\UnifiedSecurityPlatform\Web\LiveAlarm\Util. Now copy this certificate to machine from where the user is seeing this problem of uploading the inventory file.
5. Install this certificate under "Local machine," with password as "HON123well," and place this certificate at "Trusted Root Certification Authority."
6. Open Chrome browser and clear all the browsing and cache history. Then, open PWIC in Chrome browser, log in and again try uploading inventory. This time it should succeed.

2.20.7 Other Issues and Recommendations:

1. Firmware Update cancel operation may show error occurred even though operation is successful.
2. Camera data last updated may show "0 days ago", even after pulling data several days earlier.
3. Sometimes the Firmware Update status notification will be delayed, even though camera is upgraded and stated streaming in VMS.

4. The user may be able to upload firmware for camera models for which Firmware Update is not supported. The user cannot perform Firmware Update for those models even when firmware is available.
5. Add NVR 6.5 only after installing all PWIC components for the sync to work.
6. Camera USN should be a unique number across NVRs for Firmware Update feature to work.
7. To make the camera-pull-request to work in PWIC, user should make sure web configurator is configured with appropriate user credential in NVR and VMS.
8. When installed in intranet, Ping using Hostname to ensure PW IC (services) and NVR boxes communicate to each other.
9. Install VMS 650 and PW 5.0 on separate machines.

2.21 Honeywell Camera Models Supported for Simplified Device Maintenance

SERIALID	MANUFACTURER	MODEL
1	Honeywell	H4D3PRV3
2	Honeywell	HED3PR3
3	Honeywell	H4D3PRV2
4	Honeywell	HBD3PR1
5	Honeywell	HBD3PR2
6	Honeywell	HBW4PR2
7	Honeywell	H4W4PRV2
8	Honeywell	HEW4PR2
9	Honeywell	HEW2PR2
10	Honeywell	H4W2PRV2
11	Honeywell	HBW2PR2
12	Honeywell	HBW4PR1
13	Honeywell	H4W4PRV3
14	Honeywell	HEW4PR3
15	Honeywell	HEW4PRW3
16	Honeywell	HBW2PR1
17	Honeywell	HBW2PR1
18	Honeywell	HEW2PRW1
19	Honeywell	H2W4PRV3
20	Honeywell	H2W2PRV3
21	Honeywell	H4D8PR1
22	Honeywell	HBD8PR1
23	Honeywell	HED8PR1
24	Honeywell	HFD5PR1
25	Honeywell	HDZP252DI
26	Honeywell	HED2PER3
27	Honeywell	H4W4PER3

Pro-Watch Web Client*Honeywell Camera Models Supported for Simplified Device Maintenance*

28	Honeywell	HEW4PER3
29	Honeywell	H4W4PER2
30	Honeywell	HBD2PER1
31	Honeywell	HBW4PER1
32	Honeywell	HBW4PER2
33	Honeywell	HDZP304DI
34	Honeywell	HBW4PGR1
35	Honeywell	H4W8PR2
36	Honeywell	HBW8PR2
37	Honeywell	H2W2PC1M
38	Honeywell	H2W4PER3
39	Honeywell	H2W2PER3
40	Honeywell	HEW2PER3
41	Honeywell	HEW4PER3B
42	Honeywell	HBW2PER1
43	Honeywell	HEW4PER2
44	Honeywell	HEW4PER2B
45	Honeywell	HEW2PER2
46	Honeywell	H4W2PER2
47	Honeywell	HBW2PER2
48	Honeywell	H4W2PER3
49	Honeywell	HPW2P1
50	Honeywell	HC30W42R3
51	Honeywell	HC30W45R3
52	Honeywell	HC30W45R2
53	Honeywell	HC30WB2R1
54	Honeywell	HC30WB5R1
55	Honeywell	HC30WB5R2
56	Honeywell	HC30WE2R3
57	Honeywell	HC30WE5R3
58	Honeywell	HC30WE5R2

59	Honeywell	HC30WF5R1
60	Honeywell	HCD8G
61	Honeywell	HC60W35R2
62	Honeywell	HC60W35R4
63	Honeywell	HC60W45R2
64	Honeywell	HC60W45R4
65	Honeywell	HC60WB5R2
66	Honeywell	HC60WB5R5
67	Honeywell	HC60WZ2E30
68	Honeywell	H3W2GR1
69	Honeywell	H3W2GR2
70	Honeywell	H3W4GR1
71	Honeywell	H4W2GR1
72	Honeywell	H4W2GR2
73	Honeywell	H4W4GR1
74	Honeywell	HBW2GR1
75	Honeywell	HBW2GR3
76	Honeywell	HBW4GR1
77	Honeywell	HCW2G
78	Honeywell	HCW4G
79	Honeywell	H4L2GR1
80	Honeywell	HBL2GR1
81	Honeywell	HCL2G
82	Honeywell	HDZ302LIK
83	Honeywell	HDZ302LIW
84	Honeywell	H4D8GR1
85	Honeywell	HBD8GR1
86	Honeywell	HFD6GR1
87	Honeywell	HFD8GR1
88	Honeywell	HSW2G1
89	Honeywell	HSWB2G1

Pro-Watch Web Client*Honeywell Camera Models Supported for Simplified Device Maintenance*

90	Honeywell	HDZ302DE
91	Honeywell	HDZ302D
92	Honeywell	HDZ302DIN
93	Honeywell	HTMZ160T302W
94	Honeywell	HEPZ302W0
95	Honeywell	HM4L8GR1
96	Honeywell	HMBL8GR1
97	Honeywell	H4L6GR2
98	Honeywell	HBL6GR2
99	Honeywell	H4W2GR1V
100	Honeywell	H4W4GR1V
101	Honeywell	H3W2GR1V
102	Honeywell	H3W4GR1V
103	Honeywell	HBW2GR1V
104	Honeywell	HBW2GR3V
105	Honeywell	HCW2GV
106	Honeywell	H2W2GR1
107	Honeywell	HCL2GV
108	Honeywell	HBL2GR1V
109	Honeywell	H4L2GR1V

Copyright Honeywell Inc. 2020

Index

A

account prerequisites 13
activity log 133
alarms 51
 acknowledging 51
 clearing 67
 clearing a rolled-up 67
 clearing multiple 68
 incident-associated 67
 landing screen 59
 masking, unmasking 57
 multiple 65
 rolled-up 63
 rollup, details 68
 unacknowledging 51
 workflow-associated 62, 65
audience 2

B

badging 26
 advanced searching 40
 bulk, adding 42
 images 35
 record, adding 26
 record, deleting 39
 record, editing 35
 searching 39
browser
 configure 13
 support 12
browsing
 by location 148
 by objects 149

C

camera 98
 display all 100
 filtering 118
 granting 93
 latest data 98
 live view 144, 145
 models 153
 permissions 93
 search function 109
 uploading firmware 101
 video playback 146
 zoom level 145
cameras
 version format 103
configuring the browser 13
custom filter
 adding 40

D

dependencies
 Windows and Web 50
dynamic filtering 110

E

Enterprise Manager
 creating, Enterprise 121
 creating, region 122
 deleting, region 124
 selecting a table 122, 124
 updated Enterprise screen 125
events 70
 clearing 73

filtering 72
pausing 71

F

features 25
filtering
 by preset 118
filters
 advanced searching 40
 custom, adding 40
firmware 93
 deleting 111
 not supported 97
 NVR 98
 search function 109
 updating 93
 uploading 101

H

hardware
 supported 13
home page 19
Honeywell cameras 153
Honeywell Hamburger Menu 21

I

incidents 126
 activity log 133
 creating 129
 dismissing 134
 landing page 127
 management 128
 reporting 131

L

live camera view 144, 145
login 17

M

maintenance 93
maps 135
 adding 135
 browsing
 by location 148
 by objects 149
 configuring devices 140
 displaying 144
 generating 137
 live camera view 145
 removing a device 143
 video playback 143
 viewing video and alarms 141
 zoom level 141

masking 57

menu
 hamburger 21

modules 25

N

NVR upgrade 98

P

passwords 113
 updating 115
prerequisites 13
 account 13
 client machine 13

Pro-Watch

 Web Client 3
 Web Client Login 17

R

region

adding 122

reports 75

adding, editing, deleting 76

email settings 92

exporting 78

limitations 76

printing 78

running 77

settings 91

terminology 76

rolled-up alarms 63

S

settings

badging 81

reports 91

security for IE8 13

supported

hardware 13

web browsers 12

U

unmasking 57

W

workflow

associated alarms, acknowledging 62

associated multiple alarms 65

associated rolled-up alarms 63

associating with events 85

associating with logical device 88

deleting 84

editing 84

importing 84

settings 82

(This page is left blank intentionally.)

Honeywell
135 West Forest Hill Avenue
Oak Creek, WI 53154
(414) 766-1700 Ph
(414) 766-1798 Fax
www.honeywellintegrated.com

Honeywell – Europe
Boeblingerstrasse 17
71101 Schonaich
Germany
Tel +49-7031-637-782
Fax +49-7031-637-769

Specifications subject to change without notice.
© Honeywell. All rights reserved.

Honeywell