Pro-Watch® Software Suite
Release 4.4

Web Client
User Guide
CONTENTS

Chapter 1  Overview
1.1 Purpose of this Document ................................................................. 2
1.2 Audience .......................................................................................... 3
1.3 Use of Symbols ................................................................................. 4
1.4 Pro-Watch ........................................................................................ 5
1.5 Pro-Watch Web Client ................................................................. 6

Chapter 2  Pro-Watch Web Client
2.1 Supported Web Browsers ............................................................... 8
  2.1.1 SigPlusWeb Plug-In for Google Chrome ........................................ 8
2.2 Recommended Screen Resolution and Size .................................. 8
2.3 Prerequisites for the Client Machine .......................................... 8
2.4 Prerequisites for the Web Server ................................................... 8
  2.4.1 For 1-tier System Architecture ................................................... 8
  2.4.2 For 2-tier System Architecture ................................................... 9
  2.4.3 For 3-tier System Architecture ................................................... 9
2.5 Supported Hardware .................................................................. 9
2.6 Security Certificate Requirement ............................................. 9
2.7 Security Settings for IE11 ............................................................. 9
  2.7.1 IE11 Advanced Settings ............................................................. 9
  2.7.2 IE11 Security Settings ............................................................... 12
2.8 Temporary Internet Files Setting for IE11 ................................. 17
2.9 Configuring the Browser Mode ....................................................... 18
2.10 Web Client User Account Prerequisites ..................................... 20
  2.10.1 Create a Valid Pro-Watch User Account ................................... 20
  2.10.2 Assign Web Client Workstation to the User Account................ 20
  2.10.3 Enable Your Web Password .................................................... 21
    2.10.3.1 Setting the Web Password .................................................. 22
  2.10.4 Grant Web Badge Maintenance Functions ................................ 22
2.11 Pro-Watch Web Client Login ...................................................... 24
  2.11.1 Login Troubleshooting Notes ................................................... 25
    2.11.1.1 Login and 3-Tier System Setup ....................................... 25
    2.11.1.2 Workaround Solution ..................................................... 25
2.12 Home Page ................................................................................ 26
  2.12.1 Home Navigation Links ......................................................... 27
  2.12.2 Time out for Session .............................................................. 31
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.13 Modules</td>
<td></td>
</tr>
<tr>
<td>2.14 Badging</td>
<td></td>
</tr>
<tr>
<td>2.14.1 Adding a Badge Record</td>
<td>34</td>
</tr>
<tr>
<td>2.14.1.1 Employee Tab</td>
<td>34</td>
</tr>
<tr>
<td>2.14.1.2 Address Tab</td>
<td>34</td>
</tr>
<tr>
<td>2.14.1.3 Credentials Tab</td>
<td>35</td>
</tr>
<tr>
<td>2.14.1.4 Assets Tab</td>
<td>39</td>
</tr>
<tr>
<td>2.14.1.5 Activity Log Tab</td>
<td>41</td>
</tr>
<tr>
<td>2.14.1.6 Notes Tab</td>
<td>41</td>
</tr>
<tr>
<td>2.14.2 Editing a Badge Record</td>
<td>41</td>
</tr>
<tr>
<td>2.14.3 Editing a Badge Image</td>
<td>42</td>
</tr>
<tr>
<td>2.14.4 Deleting a Badge Record</td>
<td>45</td>
</tr>
<tr>
<td>2.14.5 Searching for a Badge</td>
<td>45</td>
</tr>
<tr>
<td>2.14.6 Advanced Search Filters</td>
<td>46</td>
</tr>
<tr>
<td>2.14.7 Adding a New Custom Filter</td>
<td>46</td>
</tr>
<tr>
<td>2.14.8 Adding Badges in Bulk</td>
<td>48</td>
</tr>
<tr>
<td>2.14.9 Adding a New Credential</td>
<td>49</td>
</tr>
<tr>
<td>2.14.10 Dependencies Between PW Windows and Web Applications</td>
<td>54</td>
</tr>
<tr>
<td>2.15 Reporting</td>
<td>55</td>
</tr>
<tr>
<td>2.15.1 Report Terminology</td>
<td>55</td>
</tr>
<tr>
<td>2.15.2 Report Limitations</td>
<td>55</td>
</tr>
<tr>
<td>2.15.3 Add, Edit or Delete a Report</td>
<td>55</td>
</tr>
<tr>
<td>2.15.4 View or Run a Report</td>
<td>56</td>
</tr>
<tr>
<td>2.15.5 Printing a Report</td>
<td>57</td>
</tr>
<tr>
<td>2.15.6 Exporting a Report</td>
<td>57</td>
</tr>
<tr>
<td>2.16 Settings</td>
<td>59</td>
</tr>
<tr>
<td>2.16.1 Configuring People &amp; Group (Badging) Settings</td>
<td>59</td>
</tr>
<tr>
<td>2.16.2 Configuring Reports Settings</td>
<td>60</td>
</tr>
<tr>
<td>2.16.2.1 Reports General Settings</td>
<td>60</td>
</tr>
<tr>
<td>2.16.2.2 Reports Email Settings</td>
<td>61</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1 Internet Options Dialog Box ................................................................. 10
Figure 2 Internet Options - Advanced Tab ......................................................... 11
Figure 3 Internet Options - Settings Enable ..................................................... 11
Figure 4 Internet Options - Security Tab ............................................................ 12
Figure 5 Security Settings - Local Internet Zone Dialog box ................... 14
Figure 6 Compatibility View Settings window ............................................. 19
Figure 7 Pro-Watch Web Login Page ............................................................... 24
Figure 8 Pro-Watch Web Client Home Page ................................................... 25
Figure 9 Badge-Records Screen ................................................................. 33
Figure 10 Web Report Manager Screen ......................................................... 55
Overview

In this guide...

Purpose of this Document
Audience
Use of Symbols
Pro-Watch
Pro-Watch Web Client
1.1 Purpose of this Document

The Pro-Watch Web Client User’s Guide provides the procedures and information necessary to use the Pro-Watch 4.4 Web Client.
1.2 Audience

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

The following symbols appear in this guide:

**Danger:** Dangers provide information that you must follow to avoid the risk of physical injury.

**Warning:** Shock warnings provide information that you must follow to avoid physical injury by electrical shock.

**Caution:** Cautions provide information that you must follow to avoid damage to the hardware or software components of the system.

**Note:** Notes provide important information about a procedure or topic.

**Tip:** Tips provide information that maximizes the implementation of a feature.
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.

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 4.4 User Guide, 7-901071V15.
1.5 Pro-Watch Web Client

NOTE: After upgrading to PW 4.4, all users with web passwords must reset their passwords.

The Pro-Watch Web Client is a web based application that allows access to certain Pro-Watch functionalities remotely from any location.

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

1. The Pro-Watch Web Client 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 Web Client.
In this guide...

Supported Web Browsers
Recommended Screen Resolution and Size
Prerequisites for the Client Machine
Supported Hardware
Security Certificate Requirement
Security Settings for IE11
Temporary Internet Files Setting for IE11
Configuring the Browser Mode
Web Client User Account Prerequisites
Pro-Watch Web Client Login
Home Page
Modules
Badging
Reporting
Settings
2.1 Supported Web Browsers

The Pro-Watch Web Client supports

- **Recommended**: (Windows) Google Chrome Version 46 or above.
- (Windows) Internet Explorer 11 (IE11) and above.

**Note**: MS Edge does not support Badge Printing.

**Note**: If you are using IE11 browser, there may be a delay in page loading.

2.1.1 SigPlusWeb Plug-In for Google Chrome

1. In Google Chrome browser’s URL field, type `Chrome://plugins` 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.

2.2 Recommended Screen Resolution and Size

- Screen resolution: 1366 X 768 pixels and higher.
- Monitor size: 17 inches and larger.

2.3 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](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.

2. “Display internet sites in Compatibility View” option must be disabled.

2.4 Prerequisites for the Web Server

2.4.1 For 1-tier System Architecture

- Supports all of the following Windows Servers:
  - Windows Server 2016; 64-bit
  - Windows Server 2008/2012 R2; 64-bit
- Supports all of the following SQL Servers:
  - SQL SERVER 2012/2014/2016
- Must have all of the following components:
  - .NET Framework 4.6.1
  - Quad Core with 32 / 64 GB RAM
2.4.2 For 2-tier System Architecture

- Supports all of the following Windows Servers:
  - Windows Server 2016; 64-bit
  - Windows Server 2008/2012 R2; 64-bit
- Supports all of the following SQL Servers:
  - SQL SERVER 2012/2014/2016
- Must have all of the following components:
  - .NET Framework 4.6.1
  - Quad Core with 32 GB RAM

2.4.3 For 3-tier System Architecture

- Supports all of the following Windows Servers:
  - Windows Server 2016; 64-bit
  - Windows Server 2008/2012 R2; 64-bit
- Supports all of the following SQL Servers:
  - SQL SERVER 2012/2014/2016
- Must have all of the following components:
  - .NET Framework 4.6.1
  - Quad Core with 16 GB RAM

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 Security Settings for IE11

For the Pro-Watch Web Client to function properly, users are required to set security settings for Windows Internet Explorer.

**Note:** Enabling the security settings is a mandatory step that a user must do to receive the alarms/events/traces in the web page.

Security Settings can be enabled in two ways:

- **Using Advanced tab** - Refer to section IE11 Advanced Settings on page 9.
- **Using Security tab** - Refer to section IE11 Security Settings on page 12.

2.7.1 IE11 Advanced Settings

To enable the security settings for IE11 using Advanced tab:

1. Launch **Internet Explorer 11**.
2. In the **Internet Explorer** page, navigate to **Tools (Alt + X) > Internet Options** to display the **Internet Options** dialog box:

![Tools](image1)

*Figure 1  Internet Options Dialog Box*

3. Click the **Advanced** tab.
4. In the Settings list, scroll down until you see Use TLS 1.0, Use TLS 1.1 and Use TLS 1.2 options; select all three check boxes to enable them, as shown below.

**Figure 3  Internet Options - Settings Enable**

5. Click Apply and then click OK.

6. Restart the Internet Explorer to take effect.
Note: Make sure the "Do not save encrypted pages to disk" is NOT checked.

2.7.2 IE11 Security Settings

To enable the security settings for IE11 using Security tab:

1. Launch Internet Explorer 11.

2. In the Internet Explorer page, navigate to Tools (Alt + X) > Internet Options to display the Internet Options dialog box (See Figure 4):

3. Click and select the Security tab.

Figure 4  Internet Options - Security Tab

4. In the Select a zone to view or change security settings, select the Trusted Sites option.
5. Click the **Sites** command button to display the **Trusted Sites** dialog box:

![Internet Options screenshot]

6. Type in the **URL of your web server** and click the **Add** button.
7. Click the **Close** button to close the Trusted Sites dialog box.
8. Click the **Custom Level** button to display the **Security Settings - local Internet Zone** dialog box.
9. In Settings, scroll down and then select the following options.

**Table 1  IE11 Security Settings**

<table>
<thead>
<tr>
<th>IE11 Security Category</th>
<th>IE11 Security Component</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Framework</td>
<td>Loose XAML</td>
<td>Disable</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>XML browser applications</td>
<td>Enable</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>XPS documents</td>
<td>Enable</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>Permissions for components with manifests</td>
<td>Enable</td>
</tr>
<tr>
<td>.NET Framework-reliant components</td>
<td>Run components not signed with Authenticode</td>
<td>Enable</td>
</tr>
<tr>
<td>.NET Framework-reliant components</td>
<td>Run components signed with Authenticode</td>
<td>Enable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Allow ActiveX filtering</td>
<td>Enable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Allow previously unused ActiveX controls to run without prompt</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Allow scriplets</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Automatic prompting for ActiveX controls</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Binary and script behaviors</td>
<td>Enable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Display video and animation on a webpage that does not use external media player</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Download signed ActiveX controls</td>
<td>Prompt</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Download unsigned ActiveX controls</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Initialize and script ActiveX controls not marked as safe for scripting</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Only allow approved domains use ActiveX without prompt</td>
<td>Disable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Run ActiveX controls and plug-ins</td>
<td>Enable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Run antimalware software on ActiveX controls</td>
<td>Enable</td>
</tr>
<tr>
<td>ActiveX controls and plug-ins</td>
<td>Script ActiveX controls marked safe for scripting (takes effect after your estart Internet Explorer)</td>
<td>Enable</td>
</tr>
<tr>
<td>Downloads</td>
<td>File download</td>
<td>Enable</td>
</tr>
<tr>
<td>Downloads</td>
<td>Font download</td>
<td>Enable</td>
</tr>
<tr>
<td>Downloads</td>
<td>Enable .NET Framework setup</td>
<td>Enable</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Access data sources across domains</td>
<td>Disable</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Allow META REFRESH</td>
<td>Enable</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Allow scripting of Microsoft web browser control</td>
<td>Disable</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Allow script-initiated windows without size or position constraints</td>
<td>Disable</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Allow webpages to use restricted protocols for active content</td>
<td>Prompt</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Allow websites to open windows without address or status bars</td>
<td>Disable</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Display mixed content</td>
<td>Prompt</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Don't prompt for client certificate selection when only one certificate exists</td>
<td>Disable</td>
</tr>
</tbody>
</table>
### Table 1 IE11 Security Settings

<table>
<thead>
<tr>
<th>miscellaneous</th>
<th>Drag and drop or copy and paste files</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>miscellaneous</td>
<td>Enable MIME sniffing</td>
<td>Enable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Include local directory path when uploading files to a server</td>
<td>Disable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Launching applications and unsafe files</td>
<td>Prompt</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Launching programs and files in an IFRAME</td>
<td>Prompt</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Navigate windows and frames across different domains</td>
<td>Disable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Render legacy filters</td>
<td>Disabled</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Software channel permissions</td>
<td>Medium Safety</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Submit non-encrypted form data</td>
<td>Enable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Use Pop-up Blocker</td>
<td>Enable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Use SmartScreen filter</td>
<td>Enable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>User data persistence</td>
<td>Enable</td>
</tr>
<tr>
<td>miscellaneous</td>
<td>Websites in less privileged web content zone can navigate into this zone</td>
<td>Enable</td>
</tr>
<tr>
<td>script</td>
<td>Active scripting</td>
<td>Enable</td>
</tr>
<tr>
<td>script</td>
<td>Allow programmatic clipboard access</td>
<td>Prompt</td>
</tr>
<tr>
<td>script</td>
<td>Allow status bar updates via script</td>
<td>Disable</td>
</tr>
<tr>
<td>script</td>
<td>Allow websites to prompt for information using scripted windows</td>
<td>Disable</td>
</tr>
<tr>
<td>script</td>
<td>Enable XSS filter</td>
<td>Disable</td>
</tr>
<tr>
<td>script</td>
<td>Scripting of Java applets</td>
<td>Enable</td>
</tr>
<tr>
<td>user authentication</td>
<td>Logon</td>
<td>Automatic logon only in Intranet zone</td>
</tr>
</tbody>
</table>

10. After making all the correct selections as described in the above table, click OK.
11. If the system displays an "Are you sure you want to change the settings for this zone?" prompt, click Yes.
12. In Internet Options dialog box, click Apply and then click OK.
13. Restart the Internet Explorer to take effect.

2.8 Temporary Internet Files Setting for IE11

Make sure your IE11 browser has the following “Temporary Internet Files and History” setting to display the photo of searched badges properly:

1. Launch the Internet Explorer (IE) 11.
2. In the Internet Explorer page, navigate to Tools (Alt + X) > Internet Options to display the Internet Options dialog box:
3. In the **General** tab, click the **Settings** button to display the "**Temporary Internet Files and History Settings**" screen:

![Temporary Internet Files and History Settings](image)

4. Select the "**Every time I visit the webpage**" option button.

5. Click **OK** to close the "**Temporary Internet Files and History Settings**" screen.

6. Click **OK** once again to close the "**Internet Options**" screen.

### 2.9 Configuring the Browser Mode

Configuring the browser mode is a one time action that a user is required to do when setting up the Internet Explorer 9 to use with the Pro-Watch 4.4 Web Client.

To configure the browser mode for the Pro-Watch 4.4 Web Client:

1. Launch **Internet Explorer 11**.

2. Click **Tools** from Internet Explorer browser menu to display the **Tools** Menu. Or Press **Alt+T** if the browser menu is not displayed in Internet Explorer.

3. Select **Compatibility View Settings** from the **Tools** menu to display the **Compatibility View Settings** window as shown in Figure 6.
4. Clear the following two check box options from the Compatibility View Settings dialog box:
   a. Display intranet sites in Compatibility View.
   b. Display all websites in Compatibility View.
c. Add the Server Name (machine name) where the Pro-Watch Web Server is installed to the “Websites you’ve added to Compatibility View” list, as shown below:

![Compatibility View Settings](image)

Note: The server name may be different for each customer.

5. Click Close to close the dialog box.

2.10 Web Client User Account Prerequisites

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

2.10.1 Create a Valid Pro-Watch User Account

Refer to the Pro-Watch Software Suite 4.4 User Guide, 7-901071V15, Chapter 59 “DBC - Users.”

2.10.2 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.
2. Double click your user account to display the **Edit Users** screen:

![Edit Users Screen](image)

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.

For more information refer to the *Pro-Watch Software Suite 4.4 User Guide, 7-901071V15, Chapter 59 “DBC - Users” and Chapter 60 “DBC – Workstation.”*

### 2.10.3 Enable Your Web Password

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.

### 2.10.3.1 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**.

### 2.10.4 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**.
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 all the functions 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.
2.11 Pro-Watch Web Client Login

To access the Pro-Watch Web Client:

1. Open Windows Internet Explorer and navigate to
   https://prowatchlab05.cloudapp.net/ISPWebUI/Signin to display the login page.

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

   ![Figure 7  Pro-Watch Web Login Page](image)

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 4.4 User Guide, 7-901071V15 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 8 is displayed.

   **Note:** If you are using IE11 browser, there may be a delay in page loading.
2.11.1 Login Troubleshooting Notes

2.11.1.1 Login and 3-Tier System Setup
In a 3-tier system setup, you may have difficulty with logging in even when you present valid credentials. (PW-11234)

2.11.1.2 Workaround Solution
If you continue to get login error messages, try the following workaround solution:

1. Take backup of the existing web.config.
2. Modify the web.config and remove the following keys:
   
   <customErrors mode="Off" />

   <httpErrors errorMode="Custom"
   existingResponse="Replace">
   <remove statusCode="404" subStatusCode="-1" />  
   <remove statusCode="500" subStatusCode="-1" />  
   <error statusCode="404" path="Error.html" 
   responseMode="File" />
   <error statusCode="500" path="Error.html" 
   responseMode="File" />

---

**Figure 8** Pro-Watch Web Client Home Page
3. Application will now display .NET or IIS error page which will have detailed information.
4. Make changes in the configuration to prevent the error.
5. Restore the config file from the backup. (PW-11158)

2.12 Home Page
The Pro-Watch Web Client Home page is shown in Figure 8 on page 25. The following sections describe the features of the Pro-Watch Web Client Home page.
2.12.1 Home Navigation Links

![People & Group](image)

- **People**
- **Group**
- **Search**
### Table 2 Home Navigation Links

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Menu Icon](image.png) | Click to display the **Honeywell Menu** to display the following options:  
  ![Honeywell Menu](image2.png)  
  Click **People & Group** to display the Badging module.  
  Click **Report** to display the Report module.  
  Click **Settings** to display the Settings module.  
  Click **Logout** to log out of the web client.  
  **NOTE:** You can display this menu by clicking the “People & Group” title as well. |
### Table 2 Home Navigation Links

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Click <strong>People</strong> to display the list of badge-holders:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="People &amp; Group" /></td>
</tr>
<tr>
<td></td>
<td>Click a badge-holder name to display the respective badging record information on the right pane.</td>
</tr>
</tbody>
</table>
### Table 2 Home Navigation Links

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Click <strong>Group</strong> to display the list of groups available to assign to individual badge-holders:</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Group Image" /></td>
</tr>
<tr>
<td></td>
<td>Click a group name to display the respective group information on the right pane.</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Group Information" /></td>
</tr>
<tr>
<td></td>
<td>Click the <strong>ADD</strong> link to add a new badge record (displayed in the right pane):</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Add Badge Record" /></td>
</tr>
</tbody>
</table>
### Table 2 Home Navigation Links

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Actions" /></td>
<td>Click the <strong>Actions</strong> link to display badge-related links Refresh, Batch Modify, Delete, and <strong>Badge Profile &gt; General Fields</strong>:</td>
</tr>
<tr>
<td><img src="image" alt="Filter" /></td>
<td>Click the <strong>Filter</strong> link to display the list of <strong>predefined</strong> and <strong>user-defined custom</strong> filters. More about this in the Filtering section:</td>
</tr>
<tr>
<td><img src="image" alt="Search" /></td>
<td>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.</td>
</tr>
</tbody>
</table>

### 2.12.2 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 timeout in the `web.config` file located on the Pro-Watch Web Server Host, as shown below:

```xml
<sessionState mode="InProc" cookieless="false">
    <providers>
    </providers>
</sessionState>
```

### 2.13 Modules

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

- **Badging**: Refer to the Badging section.
- **Report**: Refer to the Reporting section.
- **Settings**: Refer to the Settings section.
2.14 Badging

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

Figure 9   Badge-Records Screen
2.14.1 Adding a Badge Record

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

2.14.1.1 Employee Tab

Note: The name of this tab, “Employee,” is configurable in PW Badge Builder module. It can be changed to anything else like “Profile,” for example.

1. Click the pencil icon to enter the editing mode.
2. Enter a First Name, Last Name (mandatory).
3. Select an Issue Date and Expire Date from the respective drop-down calendars.
4. Select a Badge Type, Clearance Code, and Partition from the respective drop-down lists.
5. Click Save.

2.14.1.2 Address Tab

1. Click the pencil icon to enter the editing mode.
2. Enter appropriate values for the Address 1, Address 2, City, State, and Zip Code fields.
3. Click Save.
2.14.1.3 Credentials Tab

**Note:** The name of this tab, in contrast to the other tab names, is not configurable. A credential can be a card or some other authorization token. All cards are credentials but not all credentials are cards.

**Credentials > Credential Details Sub-Tab**

Click the View More and View Less dynamic link to view all the credentials fields or only a subset of them.
1. Click the **Add New Credential** button ("+") to display the **Add New Credential** screen:

![Add New Credential Screen](image-url)

2. Enter an appropriate value for the **Card Number** field.
3. Select an appropriate value for **Card Status** and **Card Type** from their respective drop-down lists.
4. Type a **PIN** (Personal Identification Number) or generate a random one by click the generate icon. Enter the PIN to **PIN Verify** field to verify it.
5. Select an **Access Group** and **Additional Rights** from their respective dynamic side-popping lists.
6. Select **Activate** and **Deactivate** dates from their respective pop-up calendars.
7. Click **Add** to list the new credential in the left pane.
8. To edit, click the pen icon on the upper-right corner and edit the fields appropriately. When done, click **Save**.
**Credentials > Permissions Sub-Tab**

You can view all the permissions assigned to a credential in the Permissions sub-tab:

1. To view a summary of Additional Rights, click the filter icon on the upper-right:
2. To **schedule** any additional right, hover your cursor and click the **Calendar** icon to select a schedule from the pop-up **Start Date** and **End Date** fields:

3. To **delete** an additional right, click the **Delete** icon (which deletes without any further warning):
2.14.1.4 Assets Tab

An asset can be a certificate or a device. Click the Assets tab to view, add, or edit an asset:

1. To add a certificate, click the add button (“+”) on the upper-right and select Certificate to display the Add Certificate screen:

   ![Add Certificate Screen](image)

   - Certification
   - Issue Date
   - Expiry Date
   - Attempt
   - Score
   - Note
   - Translated

2. Select a certificate from the Certification drop-down list.

3. Select an issue date in the past from the Issue Date drop-down calendar.
4. Enter an **Expiry Date**.
5. Select a numeric value for **Attempt** from the drop-down list.
6. Enter appropriate values for the **Score**, **Supervisor** and **Note** fields.
7. Select **Translated** check-box if appropriate.
8. Click **Add**.
9. To add a device, click the **add button** ("+") on the upper-right and select **Device** to display the **Add Device** screen:

   ![Add Device](image)

   10. Select a device from the **Device** drop-down list.
   11. Enter an **Asset No**.
   12. Select a status from the **Status** drop-down list.
   13. Select an **Issue Date** from the pop-up calendar.
   14. Select a **Due Date** from the pop-up calendar.
   15. Select a **Date Returned** from the pop-up calendar.
   16. Enter notes, of any, in the **Note** field.
   17. Click **Add**.

**To Edit a Certification or Device**

1. Select the certificate or device.
2. Click the **Actions link** to display the drop-down menu:

![CERTIFICATIONS]

3. Select **View** to display the respective editing screen.
4. Click the **pencil icon** to activate the editing mode.
5. Make the necessary edits to the fields you want.
6. Click **Save**.

**To Delete a Certification or Device**

1. Select the certificate or device.
2. Click the **Actions link** to display the drop-down menu.
3. Click **Delete**. The system will prompt you with the following confirmation message:

   ![Confirm Delete]

   - **CANCEL**
   - **DELETE**

4. Click **Delete**.

**2.14.1.5 Activity Log Tab**

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

**2.14.1.6 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**.

**2.14.2 Editing a Badge Record**

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

![pencil icon]

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

See the sub-section below on **Editing a Badge Image**.
2.14.3 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 **AspectRatio** (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 display 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:

![Upload Identity screen]

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

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

**Note:** A BLOB type image can be saved either to a database or to a file location (if the “File System Storage” check-box is selected in BLOB properties screen). When a user saves an image to a shared file location, **ISPWebUIAppPool** should be given folder permission. To do that, go to the folder, right-click to select Properties, go to the Security tab and add the Application ID to the list with appropriate Read/Write permission.

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

### 2.14.4 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**.

### 2.14.5 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**, and **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.
2.14.6 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:

2.14.7 Adding a New Custom Filter
To add a custom filter click the Add (+) button to display the Select Filter list:
Select to expand the **Credentials** and/or **People** lists and select the filtering criteria you like:

The variables you’ve selected will be displayed on the Filter profile:
Click **Save** to save the custom filter(s) for future use.

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

### 2.14.8 Adding Badges in Bulk

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

   ![Add button](image)

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

   ![Add People: Bulk](image)

3. Enter the **Number of People** and the **Starting Card Number**.

4. Select appropriate values from the respective drop-down lists for **Employee Type**, **Partition**, and **Access Group**.

5. Toggle the **Validity** button to turn it **GREEN**.
   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:

```
Add People: Bulk

Badge with card number 8866 created successfully
Badge with card number 8867 created successfully
Badge with card number 8868 created successfully
Badge with card number 8869 created successfully

Added 4 of 4 cards successfully
```

8. Click **OK**

### 2.14.9 Adding a New Credential

**Note:** A card is one of the credentials types available in Pro-Watch.

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 **Credentials** tab.
5. Click the **Add New Credential** button to display the **Add New Credential** screen:

![Add New Credential Screen](image)

**Figure 10  Add New Credential Screen**

6. Enter the appropriate values into all the card fields displayed in the above figure. See Table 2-1 on page 53 for description of individual fields.
7. Scroll down to enter appropriate values for all the Permissions and Validity fields:

Add New Credential

Permissions
Access Group* Additional Rights

Or, Copy access from an existing card

Validity
Activate Deactivate
07/11/2017 00:00:01 07/11/2018 23:59:59

Set to profile expiry date

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

![Credential Fields](image)

10. Enter the appropriate values into all the card fields displayed in the above screens. See Table 2-1 on page 53 for description of individual fields.

11. Click **Save**.
### Table 2-1 Credential Fields Listed Alphabetically

<table>
<thead>
<tr>
<th>Credential Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADA</td>
<td>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. The “extended shunt time” needed is set up on the PW-5000 door configuration.</td>
</tr>
<tr>
<td>Card Number Extension</td>
<td>Enter an extended card number, if any.</td>
</tr>
<tr>
<td>Credential Number</td>
<td>Card number entered by the user.</td>
</tr>
<tr>
<td>Credential Status</td>
<td>Select one from the drop-down menu.</td>
</tr>
<tr>
<td>Credential Status</td>
<td>Select one of the following from the drop-down menu: Active, AutoDisable, Disabled, Expired, Lost, Stolen, Terminated, Unaccounted, Void.</td>
</tr>
<tr>
<td>Disable Card Days</td>
<td>Enter the number of days after which the card will be disabled automatically. Default maximum is 999.</td>
</tr>
<tr>
<td>Expire Date</td>
<td>Select from the drop-down menu. Select the “Never Expire” check-box for permanent cards that will never expire.</td>
</tr>
<tr>
<td>Group (Company)</td>
<td>Select one from the drop-down menu.</td>
</tr>
<tr>
<td>Guard</td>
<td>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.</td>
</tr>
<tr>
<td>Issue Date and Time</td>
<td>Select from the drop-down menus.</td>
</tr>
<tr>
<td>Issue Level</td>
<td>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</td>
</tr>
<tr>
<td>Parade Text</td>
<td>Enter the text that should parade through the LED window of the logical device when the card is presented.</td>
</tr>
<tr>
<td>PIN (Code)</td>
<td>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.</td>
</tr>
<tr>
<td>PIN Exempt</td>
<td>Select this option to allow the use of the card at a reader without entering PIN.</td>
</tr>
<tr>
<td>PIN Verify</td>
<td>Enter the PIN again to verify it.</td>
</tr>
<tr>
<td>Trace Card</td>
<td>Select this box to record in a log file every transaction generated by this card.</td>
</tr>
<tr>
<td>Type</td>
<td>Select a credential type from the drop-down menu.</td>
</tr>
</tbody>
</table>
12. Click the **Save Card** button to save the new card. Click **Cancel** not to save the new card.

### 2.14.10 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.

<table>
<thead>
<tr>
<th>Credential Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Count Attempts</td>
<td>Enter the maximum number of use attempts after which the card will be disabled automatically. Default maximum is 99.</td>
</tr>
<tr>
<td>User Level</td>
<td>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.</td>
</tr>
<tr>
<td>VIP</td>
<td>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.</td>
</tr>
</tbody>
</table>
2.15 Reporting

Click the Honeywell Menu button

Select Report to display the Web Report Manager screen:

Figure 10 Web Report Manager Screen

2.15.1 Report Terminology

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

2.15.2 Report Limitations

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

2.15.3 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.
2.15.4 View or Run a Report

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

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

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:**

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

### 2.15.5 Printing a Report

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

### 2.15.6 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:

Export Report

<table>
<thead>
<tr>
<th>Export Type</th>
<th>Row and Column Sizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF</td>
<td>None</td>
</tr>
</tbody>
</table>

- Display Report Title
- Display SSI Header & Footer
- Display Filter

Download FileName

Email Report. Requires SMTP information

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 None, 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.

Note: IE browser will not download the exported report if the “Disable” option is selected in the IE Options > Security tab.
2.16 Settings

You can configure two different types of settings:

1. People & Group (Badging)
2. Reports

2.16.1 Configuring People & Group (Badging) Settings

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 ink to display the General settings tab.
2. Click the **pencil icon** to activate editing mode.
3. Edit the setting fields.
4. Click **Save**.
### 2.16.2 Configuring Reports Settings

#### 2.16.2.1 Reports General Settings

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

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**.

**2.16.2.2 Reports Email Settings**

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

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 later.
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** ink to send yourself a test email.

8. Click **Save**.
Index

A
audience 3

B
badging 32
browser
configure 17
mode 18
support 8

C
configuring the browser 17

F
features 32

H
home page 26

I
IE9 security settings 14

L
login 24

M
modules 32

P
prerequisites 8
Pro-Watch
Web Client Login 24

R
reports 55
settings 60

S
screen
resolution 8
size 8
settings 59
advanced 9
badging 59
reports 60
security 9
security for IE8 9
temp Internet files 17
supported web browsers 8