



Pro-Watch® Software Suite Release 4.3.5

Web Client User Guide

Copyright © 2017 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.

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
1.6 Pro-Watch WEBUI Installation	7
1.6.1 Problem	9
1.6.2 Solution	9
1.7 Workstation Permissions	10
1.7.1 Asterisk (“*”) for Workstation Name	10
1.8 Windows Authentication	11
1.8.1 Troubleshooting - Inability to Log In	18
1.8.2 Troubleshooting - Validate the Auth and Auth Service	18
1.8.3 Troubleshooting - “Your connection is not private” Warning	19
1.9 Token-Based Authentication	20
1.9.1 (Optional) Validate the Auth and Auth Service	24
1.9.2 To rollback to Basic Authentication	25
1.10 Moving Pro-Watch Components to Non-Default Website	26
1.10.1 THINKTECHURE Identity Service	27
1.10.2 AUTHENTICATION Identity Service	29
1.10.3 PW Web API	30
1.10.4 4.ISP Web UI	31
1.11 Dynamic IP Restriction Configuration	34
1.11.1 Introduction	34
1.11.2 Installation of IP and Domain Restrictions	34
1.11.3 Pro-Watch Single-Tier and Two-Tier Deployment	34
1.11.4 Pro-Watch Three Tier Deployment	35

Chapter 2 Pro-Watch Web Client

2.1 Supported Web Browsers	38
2.1.1 SigPlusWeb Plug-In for Google Chrome	38
2.2 Recommended Screen Resolution and Size	38
2.3 Prerequisites for the Client Machine	38
2.4 Prerequisites for the Web Server	38
2.4.1 For 1-tier System Architecture	38
2.4.2 For 2-tier System Architecture	39

2.4.3 For 3-tier System Architecture	39
2.5 Supported Hardware.....	39
2.6 Security Certificate Requirement.....	39
2.7 Security Settings for IE11.....	39
2.7.1 IE11 Advanced Settings	39
2.7.2 IE11 Security Settings	42
2.8 Temporary Internet Files Setting for IE11.....	47
2.9 Configuring the Browser Mode.....	48
2.10 Web Client User Account Prerequisites.....	50
2.10.1 Create a Valid Pro-Watch User Account.....	50
2.10.2 Assign Web Client Workstation to the User Account.....	50
2.10.3 Enable Your Web Password.....	51
2.10.3.1 Setting the Web Password.....	52
2.10.4 Grant Web Badge Maintenance Functions.....	52
2.11 Pro-Watch Web Client Login.....	54
2.11.1 Login Troubleshooting Notes.....	55
2.11.1.1 Login and 3-Tier System Setup.....	55
2.11.1.2 Workaround Solution	55
2.12 Home Page.....	56
2.12.1 Home Navigation Links	57
2.12.2 Time out for Session.....	61
2.13 Modules.....	62
2.14 Badging.....	62
2.14.1 Adding a Badge Record.....	64
2.14.1.1 Employee Tab	64
2.14.1.2 Address Tab.....	64
2.14.1.3 Credentials Tab	65
2.14.1.4 Assets Tab	69
2.14.1.5 Activity Log Tab	71
2.14.1.6 Notes Tab	71
2.14.2 Editing a Badge Record.....	71
2.14.3 Editing a Badge Image	72
2.14.4 Deleting a Badge Record.....	75
2.14.5 Searching for a Badge	75
2.14.6 Advanced Search Filters.....	76
2.14.7 Adding a New Custom Filter.....	76
2.14.8 Adding Badges in Bulk	78
2.14.9 Adding a New Credential	79
2.14.10 Dependencies Between PW Windows and Web Applications.....	84
2.15 Reporting.....	85
2.15.1 Report Terminology	85
2.15.2 Report Limitations.....	85
2.15.3 Add, Edit or Delete a Report	85
2.15.4 View or Run a Report.....	86
2.15.5 Printing a Report.....	87
2.15.6 Exporting a Report	87
2.16 Settings.....	89
2.16.1 Configuring People & Group (Badging) Settings	89

2.16.2 Configuring Reports Settings	90
2.16.2.1 Reports General Settings	90
2.16.2.2 Reports Email Settings	91

Appendix

Troubleshooting

A.1 Introduction	94
A.2 Steps to Follow	95

(This page is left blank intentionally for double-sided printing.)

LIST OF FIGURES

Figure 1 Internet Options Dialog Box	38
Figure 2 Internet Options - Advanced Tab	39
Figure 3 Internet Options - Settings Enable	39
Figure 4 Internet Options - Security Tab	40
Figure 5 Security Settings - Local Internet Zone Dialog box	42
Figure 6 Compatibility View Settings window	47
Figure 7 Pro-Watch Web Login Page	52
Figure 8 Pro-Watch Web Client Home Page	53
Figure 9 Badge-Records Screen	61
Figure 10 Web Report Manager Screen	83

(This page is left blank intentionally for double-sided printing.)

Overview



1

In this guide...

[Purpose of this Document](#)

[Audience](#)

[Use of Symbols](#)

[Pro-Watch](#)

[Pro-Watch Web Client](#)

[Pro-Watch WEBUI Installation](#)

[Workstation Permissions](#)

[Windows Authentication](#)

[Token-Based AuthenticationToken-Based Authentication](#)

[Moving Pro-Watch Components to Non-Default Website](#)

[Dynamic IP Restriction Configuration](#)

Overview

Purpose of this Document

1.1 Purpose of this Document

The Pro-Watch Web Client User's Guide provides the procedures and information necessary to install and use the Pro-Watch 4.3.5 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 4.3.5 User Guide, 7-901071V13.

1.5 Pro-Watch Web Client



NOTE: After upgrading to PW 4.3.5 MVO-2, 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.

1.6 Pro-Watch WEBUI Installation

1. Click the installation wizard to display the Welcome screen:



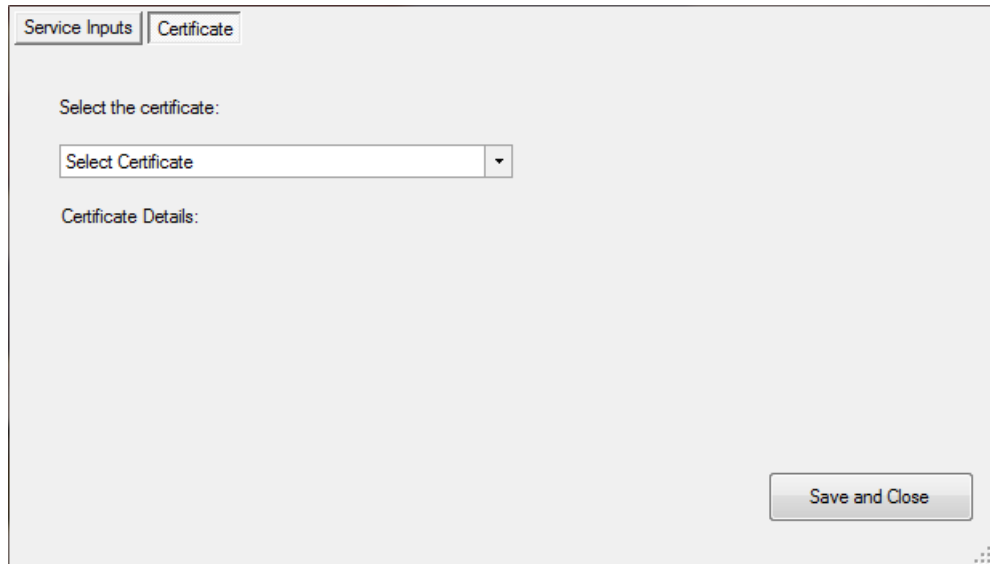
2. Click **Next** to display the **Service Inputs** tab:

The screenshot shows the "Service Inputs" tab of the installation wizard. It has two tabs at the top: "Service Inputs" (selected) and "Certificate". Below the tabs are several input fields with labels and asterisks indicating required fields: "Enter the DTU Server *:" with "localhost" entered; "Enter the DTU Port no *:" with "8733" entered; "Installed DTU as IIS (YES or NO) *?" with "NO" entered; "Enter the Auth Server Name *:" with "localhost" entered; "Enter Auth Port No :(Leave Empty if default Port)" which is empty; "Enter the Session Time out (in Sec) *:" with "20" entered; and "Enable Windows Authentication (YES or NO) *?" with "NO" entered. A "Save and Close" button is located at the bottom right.

3. Enter the following values into the respective fields:
- **DTU Server:** The Hostname of the DTU Server.
 - **DTU Port No:** The port number for DTU if running on self-hosted environment.
 - **Installed DTU as IIS:** Enter YES or NO if DTU has been hosted in IIS Service.
 - **Auth Server Name:** The Hostname of the Authentication server if the token based authentication has been installed.
 - **Auth Port No:** The port No if any for the authentication server.

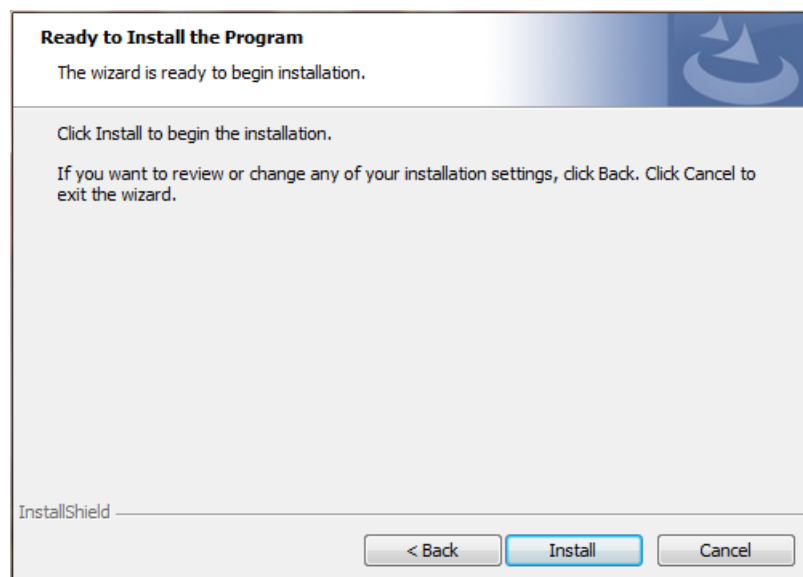
- **SessionTimeout:** The time duration in seconds for the application needs to be active before signing out the user.
- **Windows Authentication:** Enter YES or NO if Windows Authentication has to be enabled for the Users instead of forms authentication.

4. Click and select the **Certificate** tab:



The screenshot shows a window with two tabs: 'Service Inputs' and 'Certificate'. The 'Certificate' tab is active. It contains a label 'Select the certificate:' followed by a drop-down menu with the text 'Select Certificate'. Below this is a label 'Certificate Details:' followed by a large empty text area. In the bottom right corner, there is a button labeled 'Save and Close'.

5. From the drop-down list, select the appropriate **Certificate** to be installed.
6. Click **Save and Close** to display the next screen:



7. Click **Install** to finish the installation process.

1.6.1 Problem

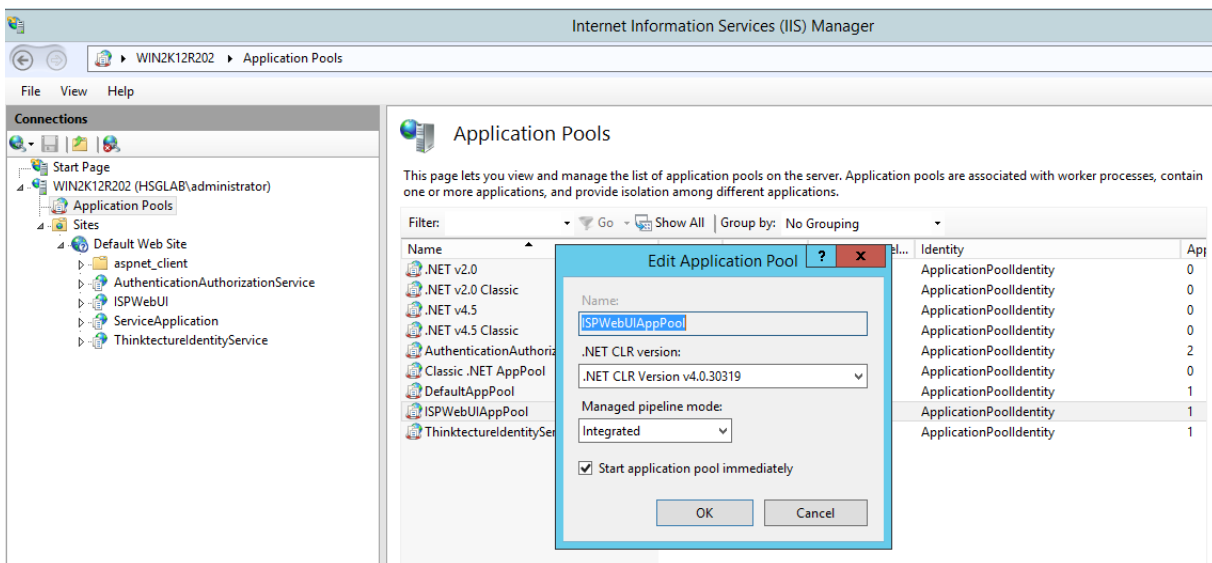
When installing PW 4.3.5 Web Component, sometimes ASP.NET will not register correctly with IIS. When trying to bring up the Login page, user will see the following error message:

"HTTP Error 500.21 **Internal Server Error**: Handler 'PageHandlerFactory-Integrated' has a bad module 'ManagedPipelineHandler' in its module list".

Reason for the error: ASP.NET may not be registered properly with Internet Information Services (IIS). User must register ASP.NET with IIS to enable the handlers required to run .NET pages.

1.6.2 Solution

1. Open the **Command Prompt** under an **Administrator** account.
2. Navigate to "C:\Windows\Microsoft.NET\Framework\v4.0.30319".
3. Run the command "**aspnet_regiis.exe -i**".
4. Launch your **Internet Information Services (IIS) Manager**. Double-click the **Application Pools** link in the navigation sidebar. Make sure the **Pro-Watch 4.3.5 Application Pools** listed in the **Application Pools** pane display **4.6.1** version of the **.NET Framework**:



Close the **Internet Information Services (IIS) Manager** screen.

1.7 Workstation Permissions

1.7.1 Asterisk (“*”) for Workstation Name

A workstation named “*” (one asterisk only) has to be added to the list of workstations for the Pro-Watch web user to access the web client from any workstation in the network.



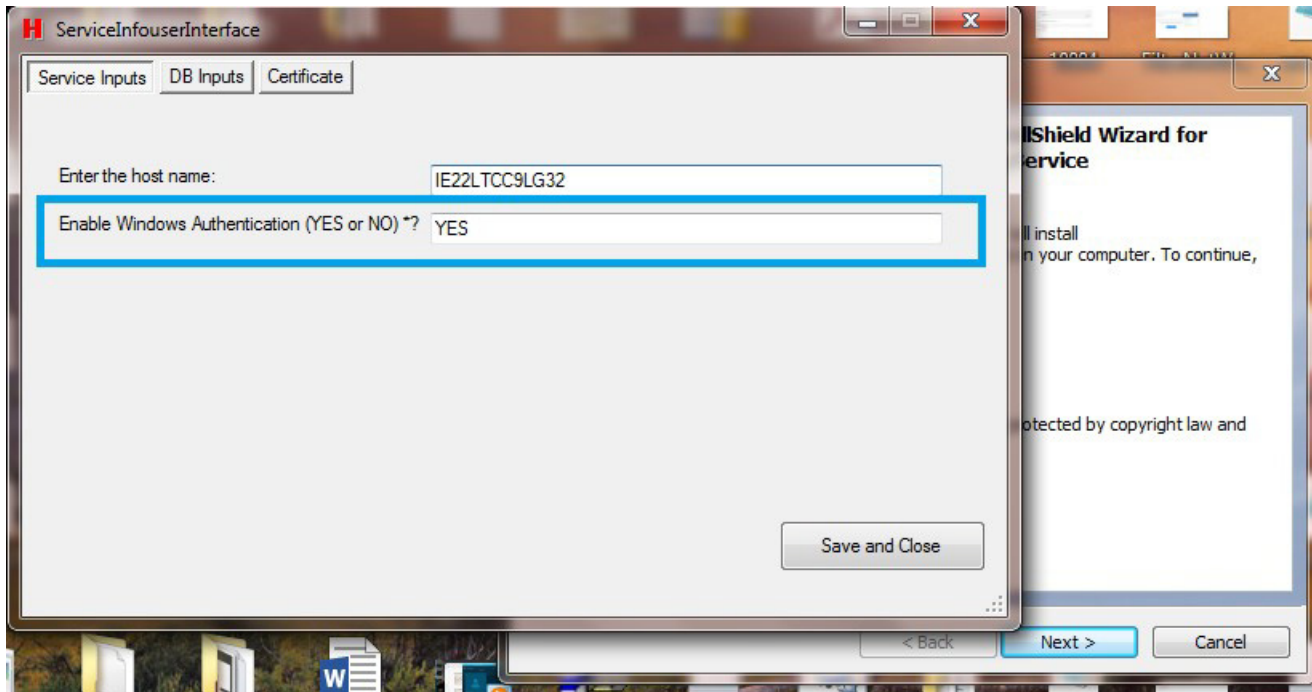
Caution: The user account used to install the Web Server must also have the Web Server workstation added to the list of user workstations. Failure to do this will result in all web users losing access to the web client.

1.8 Windows Authentication

The web client login requires Windows authentication.

Follow these steps to set up Windows authentication:

1. Install **thinktecture.service.msi** to display the **Service Info User Interface** screen:



2. In the **Enable Windows Authentication** field, enter YES.
3. Configure the **web.config** settings for the **ThinktectureIdentityService.exe** as shown below:

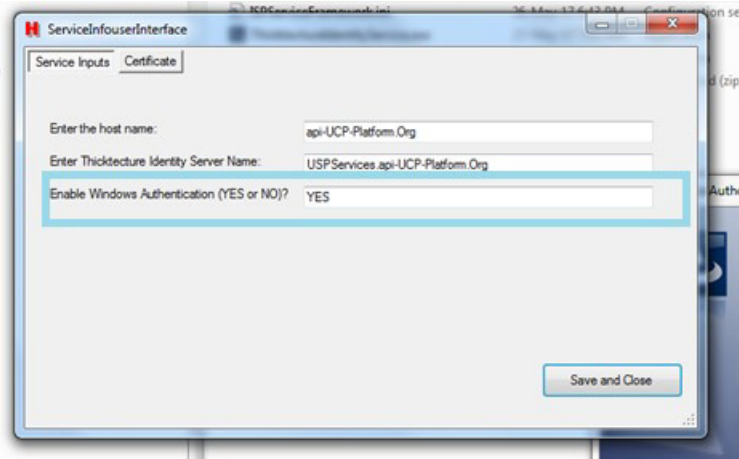
```
<!--GetUserPrivileges validate for this scope in the token-->
<add key="userprevscopes" value="prowatch" />
<!-- AccessTokenLifetime set to 10 hours-->
<add key="AccessTokenLifetime" value="60" />
<add key="AbsoluteRefreshTokenLifetime" value="86400" />
<add key="SlidingRefreshTokenLifetime" value="43200" />
<!-- Pre Watch Database connection information -->
<add key="PWDatabaseServer" value="IE3PLT3308T72" />
<add key="PWDatabase" value="PWNT" />
<add key="EncryptDBConnection" value="1" />
<add key="EncryptTrustServerCertificate" value="1" />
<add key="UseIntegratedSecurity" value="1" />
<!--0-Form and 1-Windows-->
<add key="UseWindowsAuthentication" value="false" />
<add key="MaxLoginAttempts" value="3"></add>
<add key="ResetLockDuration" value="1"></add>
</appSettings>
```

Note:



Note: Ignore this step if the above-mentioned configuration settings are correctly updated as a part of the installation process.

4. Install **AuthenticationAuthorizationService.exe** to display the **Service Info User Interface** screen:



5. In the **Enable Windows Authentication** field, enter YES.
6. Configure the **web.config** settings for the **AuthenticationAuthorizationService** as shown below:

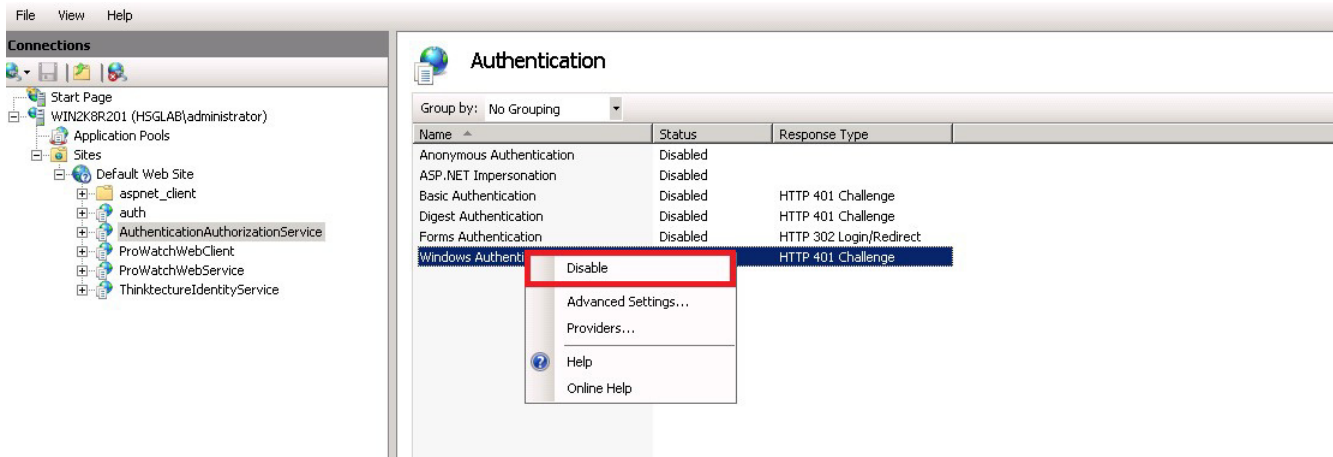
```
<section name="unity" type=
"Microsoft.Practices.Unity.Configuration.UnityConfigurationSection,Microsoft.Practices.Unity.Configuration" />
<section name="ispInfrastructure" type="Honeywell.ISP.Framework.ISPInfrastructure,
Honeywell.ISP.Framework.Common.Configuration.ISPConfigurationProvider" />
<section name="logging" type="Honeywell.ISP.Framework.Logging.Configuration.LoggingConfiguration,
Honeywell.ISP.Framework.Logging" />
</configSections>
<ispInfrastructure>
  <providers>
    <add name="ThinkTectureProvider" appName="AzAndAnServer" endpoint="https://localhost/ThinktectureIdentityService"
      faultRetry="5" initialInterval="2" increment="2" />
  </providers>
</ispInfrastructure>
<appSettings>
  <add key="UseWindowsAuthentication" value="false" />
</appSettings>
<unity>
```



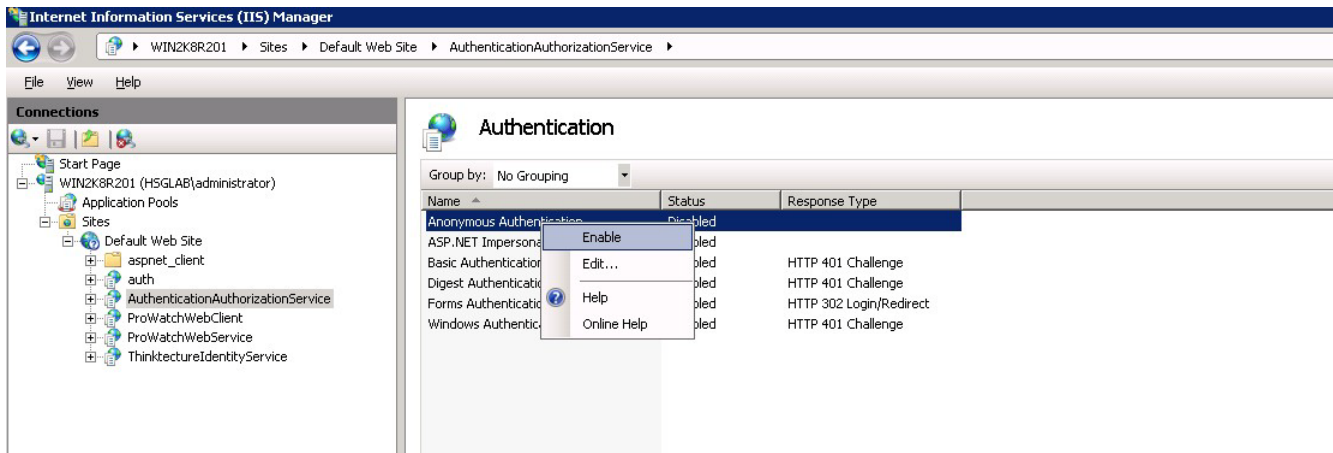
Note: You must provide URL of the ThinktectureIdentityService for **Auth** and **Auth web.config** to communicate to Thinktecture service. URL format should be same as displayed in the above screen-shot.

7. If you have selected the option for Windows Authentication, you must follow the following steps.
 - a. Select **AuthenticationAuthorizationService** from the **inetmgr** and select **Authentication** option.

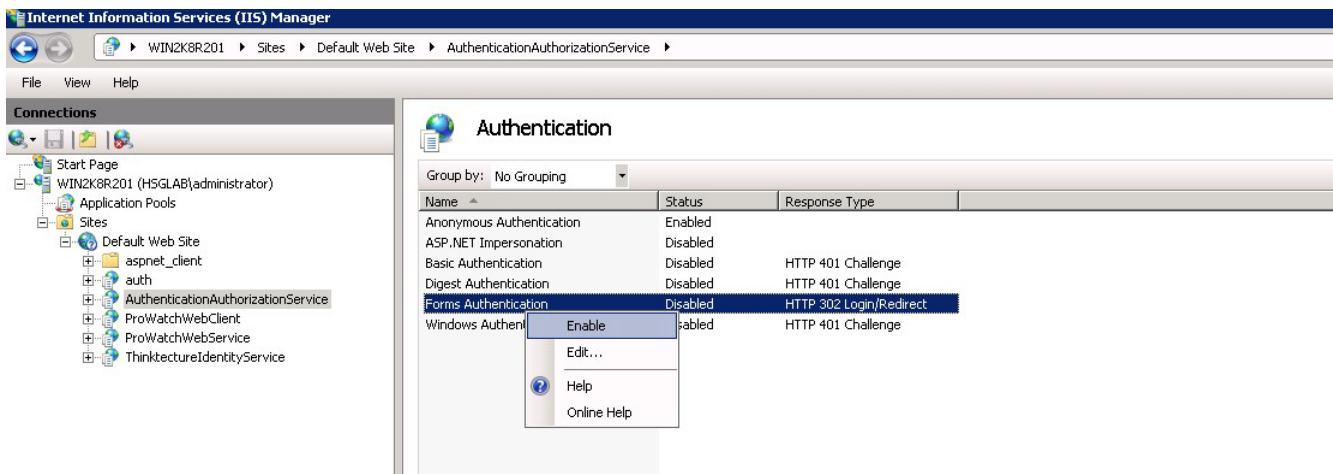
- b. Right click on **Windows Authentication** and select **Disable**:



- c. Right click on **Anonymous Authentication** and select **Enable**:



- d. Right click on **Forms Authentication** and select **Enable**:

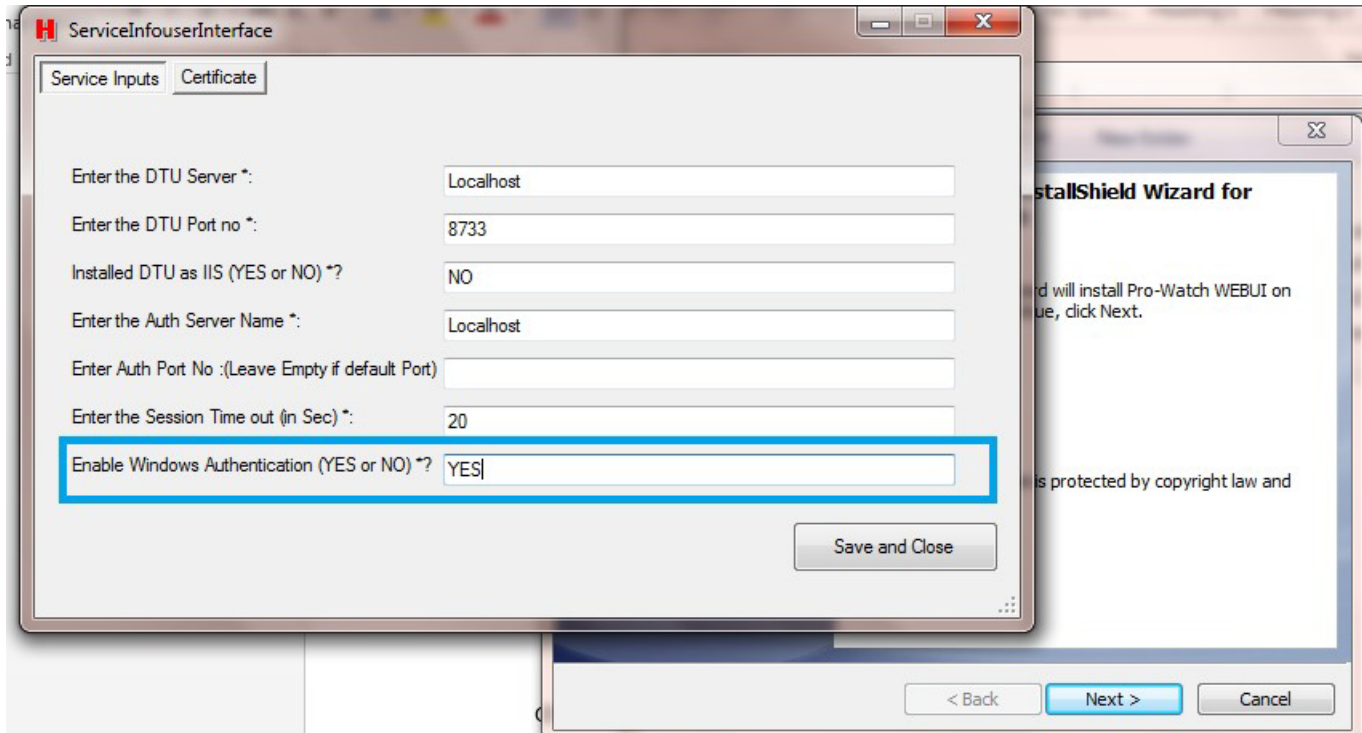


- e. Check if the folder path has '**C:\ISPLogs**' has the required permission for the users of thinktexture and auth and auth.



Note: Ignore this step if the above-mentioned configuration settings are correctly updated as a part of the installation process.

8. On Installing WebUI, enter YES in the **Enable Windows Authentication** field:



9. Configure the **web.config** settings for the WebUI in order to communicate to **AuthenticationAuthorizationService** by following the below steps:



Note: You must provide URL of the Auth and Auth for the webui to communicate to auth and auth service. URL format should be same as displayed in the below screen-shot:

```
<add key="UseTokenBasedAuthentication" value="1"/>
<add key="ISPAuthEndPoint" value="https://atlantic/AuthenticationAuthorizationService/api/AuthenticationAuthorization"/>
```

- a. Set **UseTokenBasedAuthentication** to 1.



Note: Ignore this step if the above-mentioned configuration setting is correctly updated as a part of the installation process.

- b. Run the below command in command prompt:



Important Note: While running the below command, provide the correct Web application and Web site name in which Pro-Watch web UI is deployed.

C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis" -pe secureAppSettings -app /ISPWebUI -site "Default Web Site

10. Configure the **PW DTU** config settings in order to communicate to **AuthenticationAuthorizationService** by following the steps below.



Important Note: DTU can be hosted in IIS or Windows Service.

- If it is IIS hosted, make below mentioned changes in "Program Files (x86)\Honeywell\UnifiedSecurityPlatform\DTU\Web.config"
- If it is Windows Service hosted, make below mentioned changes in "Program Files (x86)\Honeywell\UnifiedSecurityPlatform\DTU\Bin\PW-DTU-WinService.exe.config"



Note: You must provide URL of the Auth and Auth for the DTU to communicate to auth and auth service. URL format should be same as displayed in the below screen-shot.



Note: Set **ISOMAuthenticationScheme** to Bearer:

```
<add key="ThumbnailHeight" value="100"/>
<add key="CompanyClearCodeModificationTimeout" value="600"/>
<!--Image path for Badge Print -->
<add key="DefaultImagePath" value="C:\Program Files (x86)\ProWatch\Bin"/>
<add key="BadgePhotoCustomField" value="BADGE_DISPPHOTO"/>
<!--Report page size limit-->
<add key="PageSize_Min" value="10"/>
<add key="PageSize_Max" value="1000"/>
<add key="License_Expiry_TimeOut" value="60"/>
<!--Minutes-->
<!-- ISOMAuthenticationScheme - Basic/Bearer -->
<add key="ISOMAuthenticationScheme" value="Bearer"/>
<add key="BaseAnAURL" value="https://<<Please type the host name>>/AuthenticationAuthorizationService/" />
<!--PWServerConnectTimeout in milliseconds-->
<add key="PWServerConnectTimeout" value="30000"/>
<!--
```

- 1) ISOM Authentication Scheme should be Bearer
- 2) BaseAnAURL should be https://machinename//AuthenticationAuthorization/



Note: Ignore this step if the above-mentioned configuration setting is correctly updated as a part of the installation process.

- a. Change **ThinktectureURL** as shown in the below screen-shot:

The screenshot displays two Notepad++ windows side-by-side. The left window, titled 'Auth & Auth Web.Config file', shows an XML configuration with a red box highlighting the 'ThinkTectureURL' property, which is set to 'https://ATLANTIC/ThinktectureIdentityService/'. The right window, titled 'DTU Web.Config file', also shows an XML configuration with a red box highlighting the 'ThinkTectureURL' property, which is set to 'https://ATLANTIC/ThinktectureIdentityService/'. Both windows show various other configuration properties like 'ThumbnailHeight', 'CompanyClearCodeModificationTimeout', 'DefaultImagePath', 'BadgePhotoCustomField', 'PageSize_Min', 'PageSize_Max', 'License_Expiry_TimeOut', 'ISOMAuthenticationScheme', 'BaseAnAURL', 'PWServerConnectTimeout', 'TelosStartMinute', 'TelosUser ID', 'TelosSponsorID', 'TelosPassCode', 'DefaultImagePath', 'Report page size limit', 'CertificateName', and 'CertificatePassword'.

b.

Service Name	Key	Example Settings
Auth and Auth (Web.config)	ThinkTectureProvider	https://atlantic/ThinktectureIdentityService https://<MachineName>/ThinktectureIdentity Service
DTU (Web.config) for IIS PW-DTU-WinService.e xe.config - windows service	ThinktectureURL	https://atlantic/ThinktectureIdentityService https://<MachineName in LOWER CASE >/ThinktectureIdentityService



Important Note: If token based authentication is used, then it is essential to set up Dynamic IP Restrictions.

c. Restart IIS and log in.

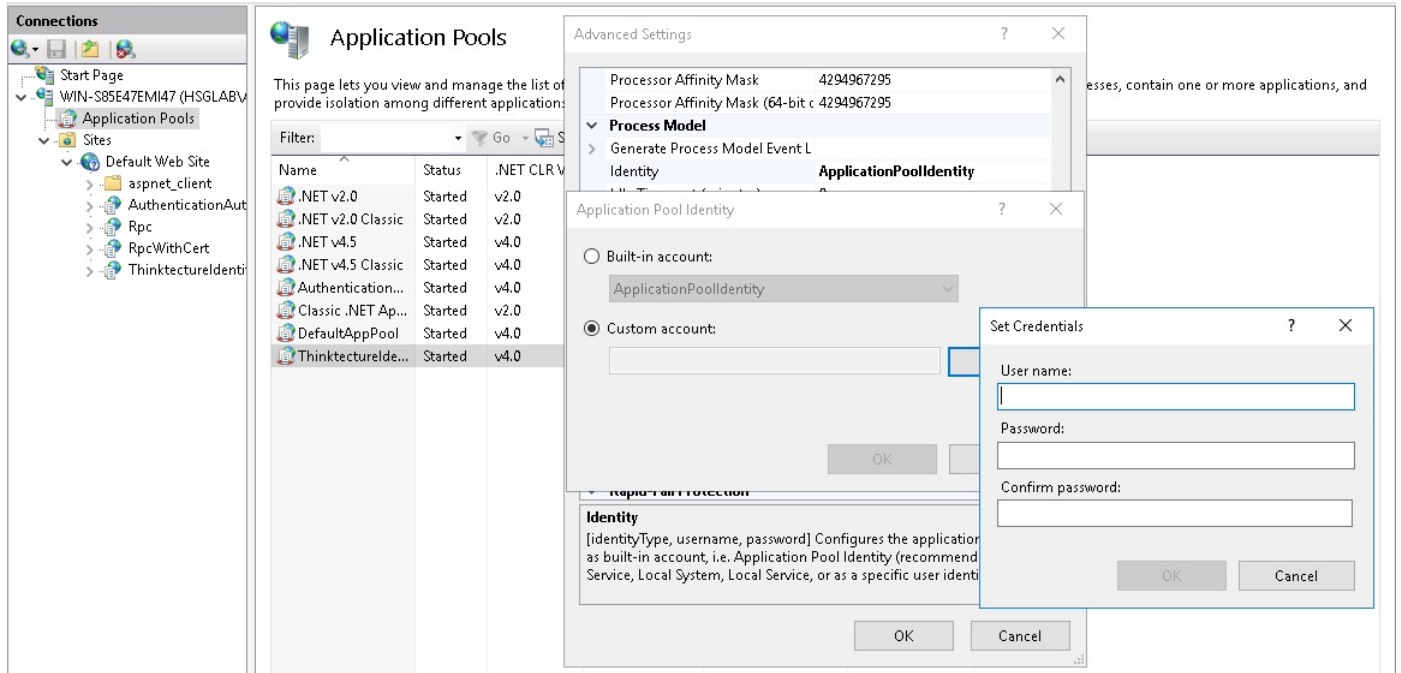
11. **OPTIONAL:** After configuring the end to end setup, confirm that the sql server is added with IIS Application pool identity login.

```
USE master
GO
/*
* Add login or apppool to Server Role
*/
sp_addsrvrolemember @loginame = [IIS
APPPool\ThinktectureIdentityService], @rolename =
[sysadmin]
GO
/*
* Add login or apppool to Server Role
*/
sp_dropsrvrolemember @loginame = [IIS
APPPool\ThinktectureIdentityService], @rolename =
[sysadmin]
GO
```

12. Sometimes Thinktecture Identity Service cannot connect to SQL with built-in account user, hence we may need to set the Custom account as below.

a. i) Go to **Application Pool Identity** of "ThinktectureIdentityService"

b. ii) Set the **Required User** credentials under **Custom** account:



1.8.1 Troubleshooting - Inability to Log In

Try the following if you are not able to log in.

1. Refer to the file site.log in the Web.UI directory example.

Example : C:\Program Files

(x86)\HONEYWELL\UnifiedSecurityPlatform\Web\WEBUI

2. If you get the error

"Response status code does not indicate success: 401 (Unauthorized)"

DTU has not been configured properly revisit Point 10.

3. Check if you have updated the config file web.config when IIS has been deployed in IIS mode and PW-DTU-WinService.exe.config if dtu has been deployed in windows Service mode.
4. Make sure the url key - ThinktectureURL the machine name is mentioned in lower host.
5. In case in site.log you do not get a token then please check the web.config file of Web.UI look at the key

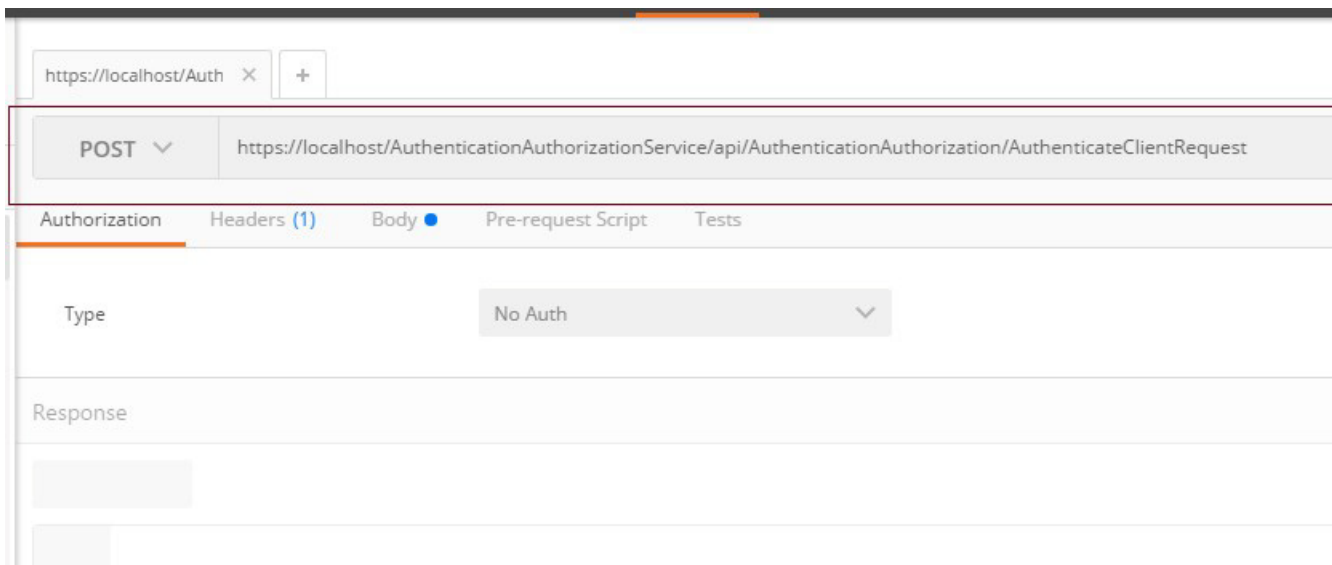
web.config ISPAuthEndPoint if it is mentioned in step 9 above, in section [Windows Authentication](#), page 11.

1.8.2 Troubleshooting - Validate the Auth and Auth Service

This is required only if you have issues with the installation.

Postman can be used to validate the Auth and Auth service.

1. Select appropriate request type and type Auth & Auth url as shown below:



2. Enter the header details as shown below:

Key	Value
<input checked="" type="checkbox"/> Content-Type	application/json
New key	value

3. Enter the payload details and click **Send**:

```

1 {"ClientID":"ProWatchWebClient","ClientSecret":"secret","Username":"e451847","Password":"1","Scope":"prowatch offline_access"}
2
3

```

1.8.3 Troubleshooting - “Your connection is not private” Warning Message

If you get the warning message “Your connection is not private” and you are not able to proceed, see [Appendix A, Troubleshooting](#), page 93.

1.9 Token-Based Authentication

Token-based authentication uses the same user name and web password set in Pro-Watch. This mode is not supported if the mobile app is using the DTU.



Note: Token-based authentication can be used separately, independent of the window-based authentication.

1. Install **thinktecture.service.msi**.
2. Enter “YES” to **Enable Windows Authentication** or ‘NO’ not to use windows integrated authentication.
3. Configure the **web.config** settings for the **ThinktectureIdentityService.exe** as shown below:

```
<!--GetUserPrivileges validate for this scope in the token-->
<add key="userprevscopes" value="prowatch" />
<!-- AccessTokenLifetime set to 10 hours-->
<add key="AccessTokenLifetime" value="60" />
<add key="AbsoluteRefreshTokenLifetime" value="86400" />
<add key="SlidingRefreshTokenLifetime" value="43200" />
<!-- Pro Watch Database connection information -->
<add key="PWDatabaseServer" value="IE3PLT3308T72" />
<add key="PWDatabase" value="PWNT" />
<add key="EncryptDBConnection" value="1" />
<add key="EncryptTrustServerCertificate" value="1" />
<add key="UseIntegratedSecurity" value="1" />
<!--0-Form and 1-Windows-->
<add key="UseWindowsAuthentication" value="false" />
<add key="MaxLoginAttempts" value="3"></add>
<add key="ResetLockDuration" value="1"></add>
</appSettings>
```



Note: Ignore the above step if the above-mentioned configuration setting is correctly updated as a part of the installation process.

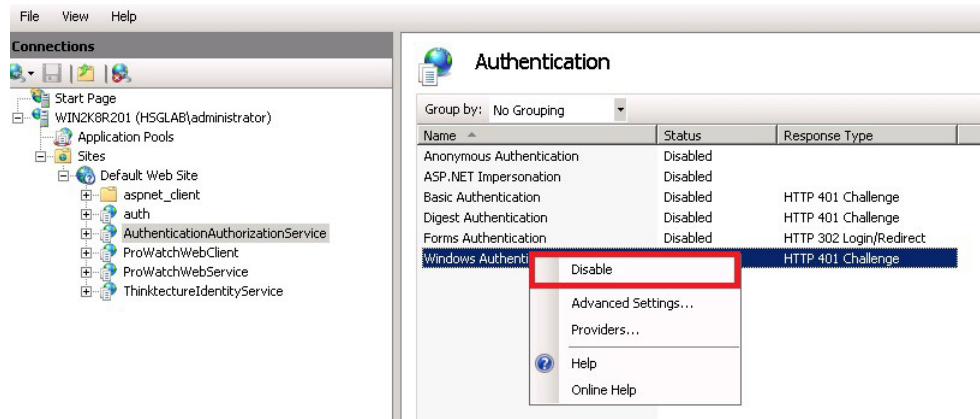


Note: You must provide URL of the ThinktectureIdentityService for Auth and Auth to communicate to Thinktecture service. URL format should be same as displayed in the below screen-shot.:

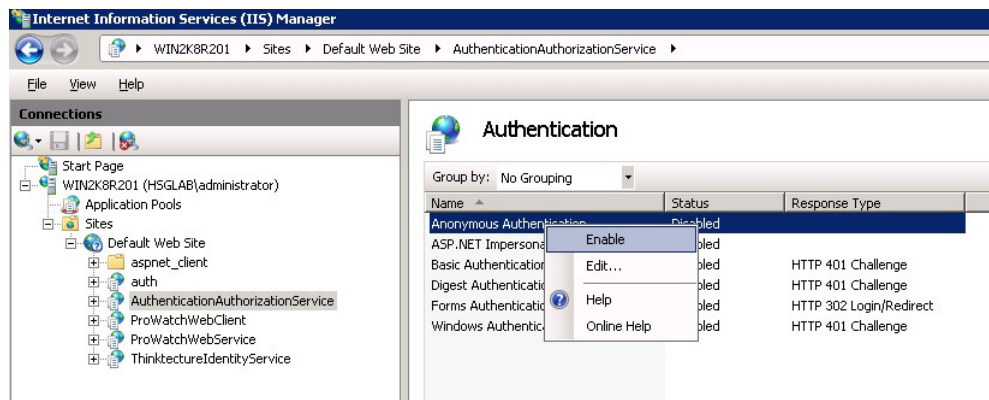
```
<section name="unity" type=
"Microsoft.Practices.Unity.Configuration.UnityConfigurationSection,Microsoft.Practices.Unity.Configuration" />
<section name="iSPInfrastructure" type="Honeywell.ISP.Framework.ISPInfrastructure,
Honeywell.ISP.Framework.Common.Configuration.ISPConfigurationProvider" />
<section name="logging" type="Honeywell.ISP.Framework.Logging.Configuration.LoggingConfiguration,
Honeywell.ISP.Framework.Logging" />
</configSections>
<iSPInfrastructure>
  <providers>
    <add name="ThinkTectureProvider" appName="AzAndAnServer" endpoint="https://localhost/ThinktectureIdentityService"
      faultRetry="5" initialInterval="2" increment="2" />
  </providers>
</iSPInfrastructure>
<appSettings>
  <add key="UseWindowsAuthentication" value="false" />
</appSettings>
<unity>
```

4. If the option for Windows Authentication has been selected, follow the following steps:

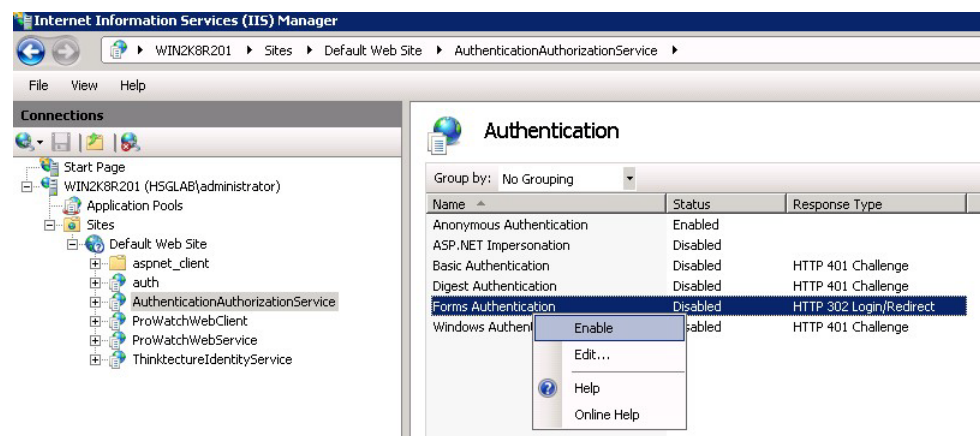
- Select **AuthenticationAuthorizationService** from the **inetmgr** and select **Authentication** option.
- Right click on **Windows Authentication** and select **Disable**:



- Right click on **Anonymous Authentication** and select **Disable**:



- Right click on **Forms Authentication** and select **Enable**:



- Check if the Folder path "**C:\ISPLogs**" has the required permission.



Note: Ignore the above-mentioned configuration settings if they are correctly updated as a part of the installation process.

5. Configure the web.config settings for the **WebUI** in order to communicate to **AuthenticationAuthorizationService**. Below are the details,
 - Need to provide URL of the Auth and Auth for the webui to communicate to auth and auth service. Note that, URL format should be same as mentioned in the below screen-shot.
 - Set **TokenBasedAuthentication** to **1**.

```
<add key="UseTokenBasedAuthentication" value="1"/>
<add key="ISPAuthEndPoint" value="https://atlantic/AuthenticationAuthorizationService/api/AuthenticationAuthorization"/>
```



Note: Ignore the above-mentioned configuration setting if it is correctly updated as a part of the installation process.

- a. Run the below command in command prompt.



Important Note: While running the below command, provide the correct Web application and Web site name in which Pro-Watch web UI is deployed.

```
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis" -pe secureAppSettings -app /ISPWebUI -site "Default Web Site"
```



Important Note:

DTU can be hosted in IIS or Windows Service.

If it is IIS hosted, make below mentioned changes in "Program Files (x86)\Honeywell\UnifiedSecurityPlatform\DTU\Web.config"

If it is Windows Service hosted, make below mentioned changes in "Program Files (x86)\Honeywell\UnifiedSecurityPlatform\DTU\Bin\PW-DTU-WinService.exe.config"

6. Configure the PW DTU config settings in order to communicate to **AuthenticationAuthorizationService**. Below are the details,:
 - Need to provide URL of the Auth and Auth for the DTU to communicate to auth and auth service. Note that, URL format should be same as mentioned in the below screenshot.
 - Set **ISOMAuthenticationScheme** to Bearer.

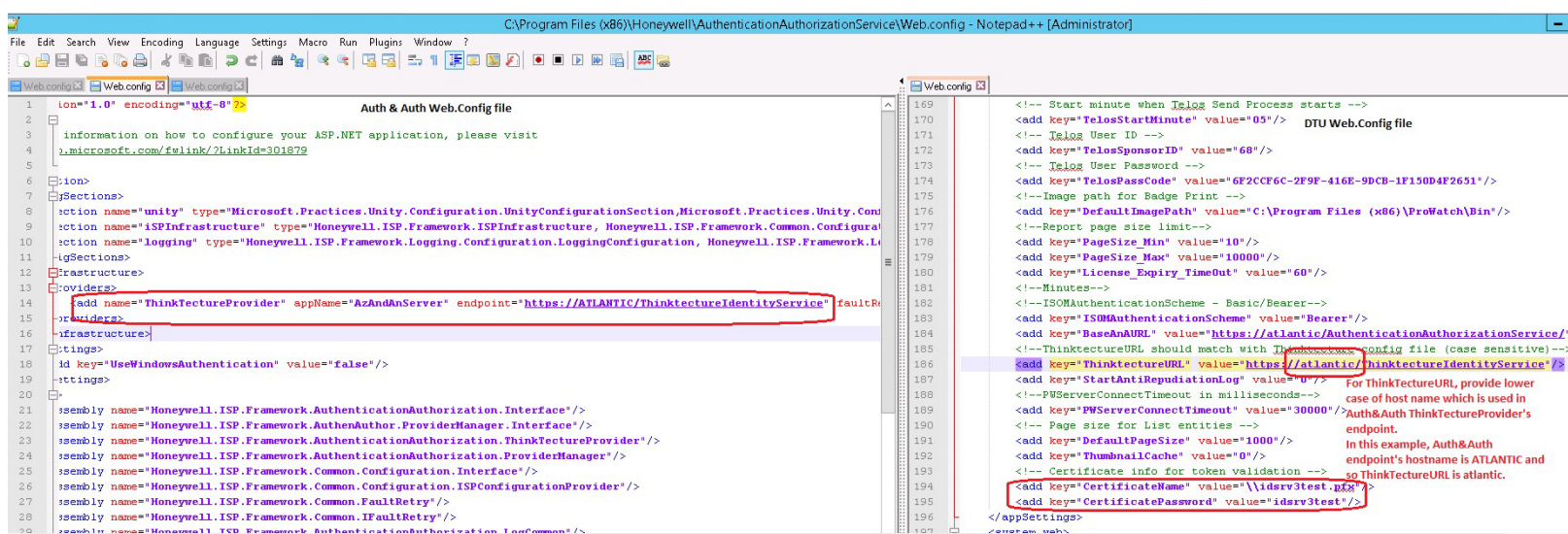
```
<add key="ThumbnailHeight" value="100"/>
<add key="CompanyClearCodeModificationTimeout" value="600"/>
<!--Image path for Badge Print -->
<add key="DefaultImagePath" value="C:\Program Files (x86)\ProWatch\Bin"/>
<add key="BadgePhotoCustomField" value="BADGE_DISPPHOTO"/>
<!--Report page size limit-->
<add key="PageSize_Min" value="10"/>
<add key="PageSize_Max" value="1000"/>
<add key="License_Expiry_TimeOut" value="60"/>
<!--Minutes-->
<!--ISMAuthenticationScheme Basic/Bearer -->
<add key="ISMAuthenticationScheme" value="Bearer"/>
<add key="BaseAnAURL" value="https://<<Please type the host name>>/AuthenticationAuthorizationService/" />
<!--PWServerConnectTimeout in milliseconds-->
<add key="PWServerConnectTimeout" value="30000"/>
<!--
```

1) ISOM Authentication Scheme should be Bearer
2) BaseAnAURL should be
https://machinename//AuthenticationAuthorization/



Note: Ignore the above-mentioned configuration setting if it is correctly updated as a part of the installation process.

a. Change **ThinktectureURL** as shown in the below screen-shot:



Important Note: If token based authentication is used, you must set up **Dynamic IP Restrictions**.

b. Restart IIS and log in.

7. (Optional) After configuring the end to end setup, confirm that the sql server is added with IIS Application pool identity login.

USE master

GO

/*

*** Add login or apppool to Server Role**

***/**

**sp_addsrvrolemember @loginame = [IIS
APPPool\ThinktectureIdentityService], @rolename = [sysadmin]**

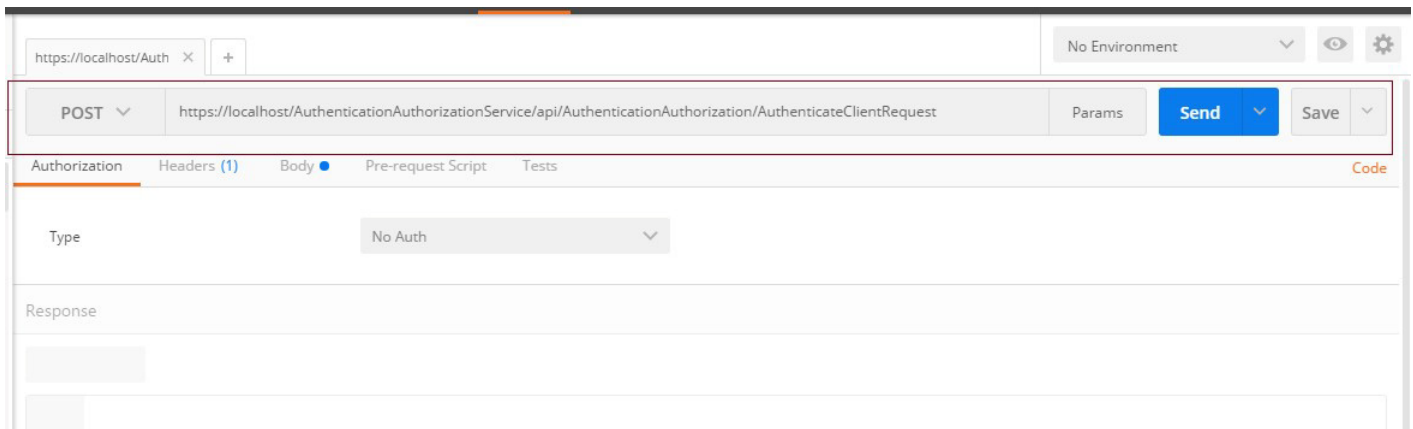
GO

```
/*  
* Add login or apppool to Server Role  
*/  
  
sp_dropsrvrolemember @loginame = [IIS  
APPPOOL\ThinktectureIdentityService], @rolename = [sysadmin]  
  
GO
```

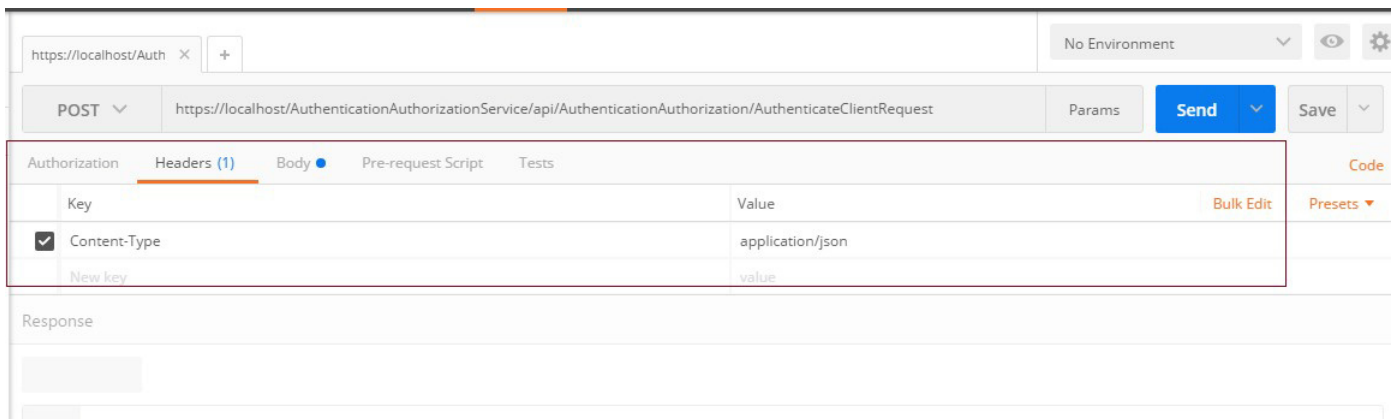
1.9.1 (Optional) Validate the Auth and Auth Service

Postman can be used to validate the Auth and Auth service.

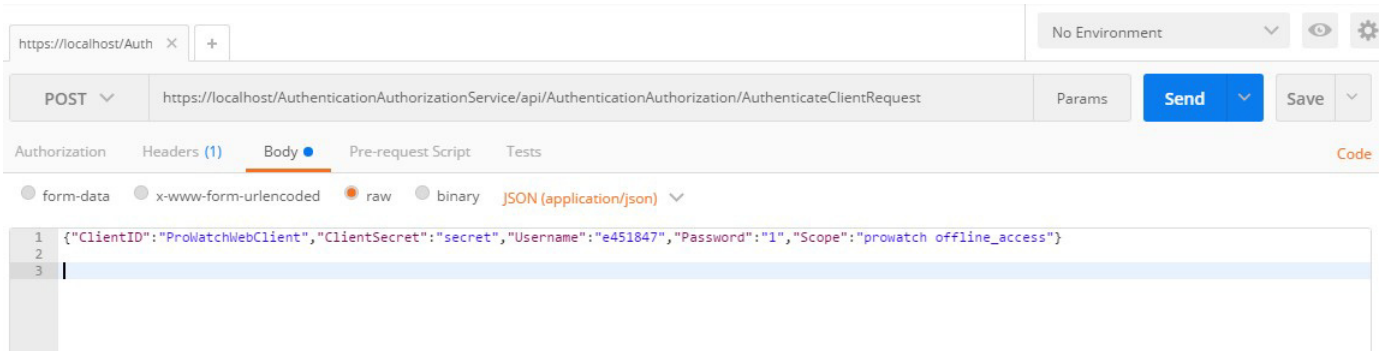
1. Select appropriate request type and type Auth & Auth url as shown below:



2. Enter the header details as shown below:



3. Enter the payload details and click **Send**.



1.9.2 To rollback to Basic Authentication

1. In DTU Config file, Set **ISOMAuthenticationScheme** app setting to "Basic".
2. In ISPWebUI web config file, set **UseTokenBasedAuthentication** app setting to "0".

1.10 Moving Pro-Watch Components to Non-Default Website

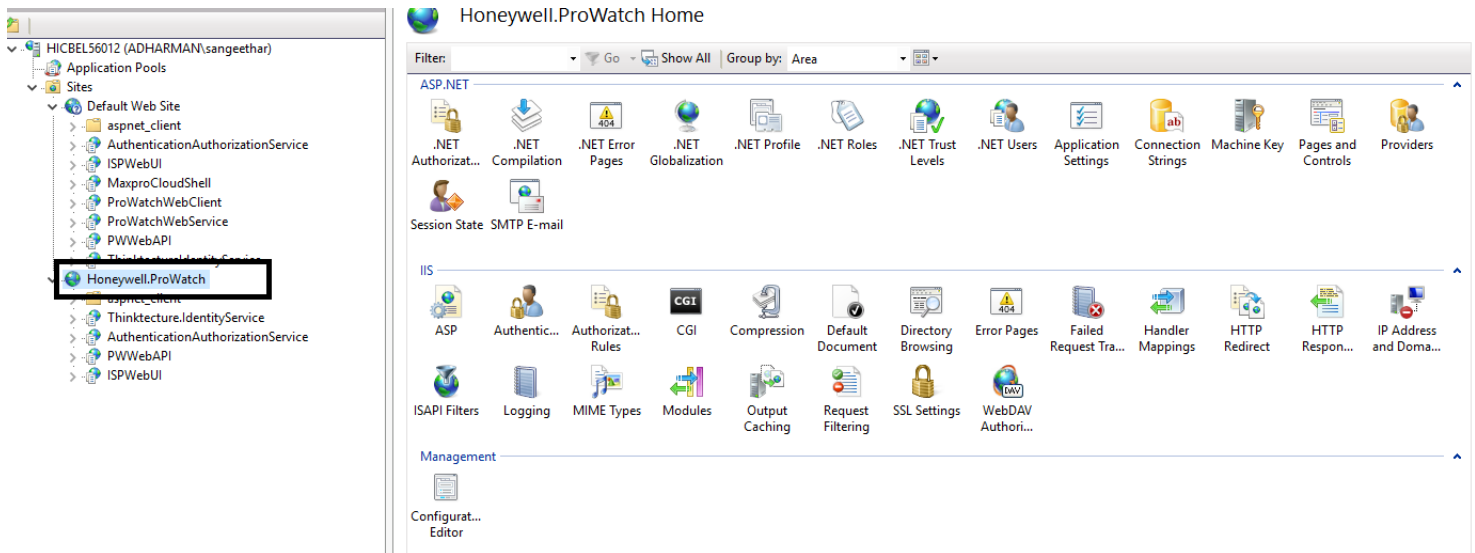


Note: You should be able to log in to the application before performing the steps described in this section.

This section describes how to move the below sites manually from Default web site to any other web site.

1. Thinktecture Identity Service
2. Authentication Authorization Service
3. PW Web API
4. ISP Web UI

For demonstration purposes, a new website has been created in IIS - **Honeywell.ProWatch**. All applications will be moved to this web site.



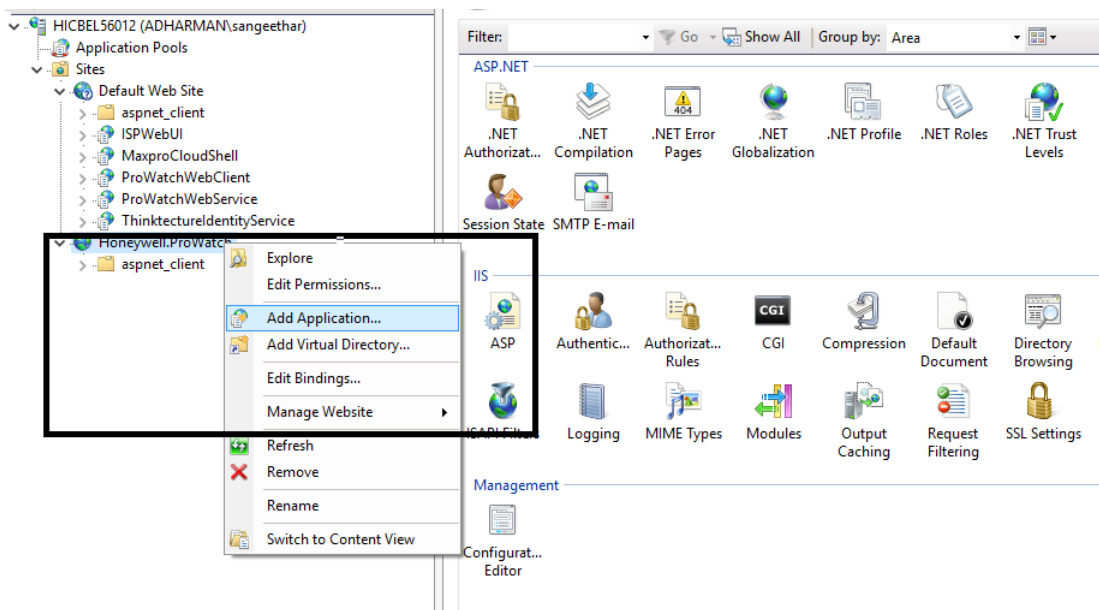
Create bindings same as Default Web Site.

For https binding, use the same certificate used by Default Web Site.

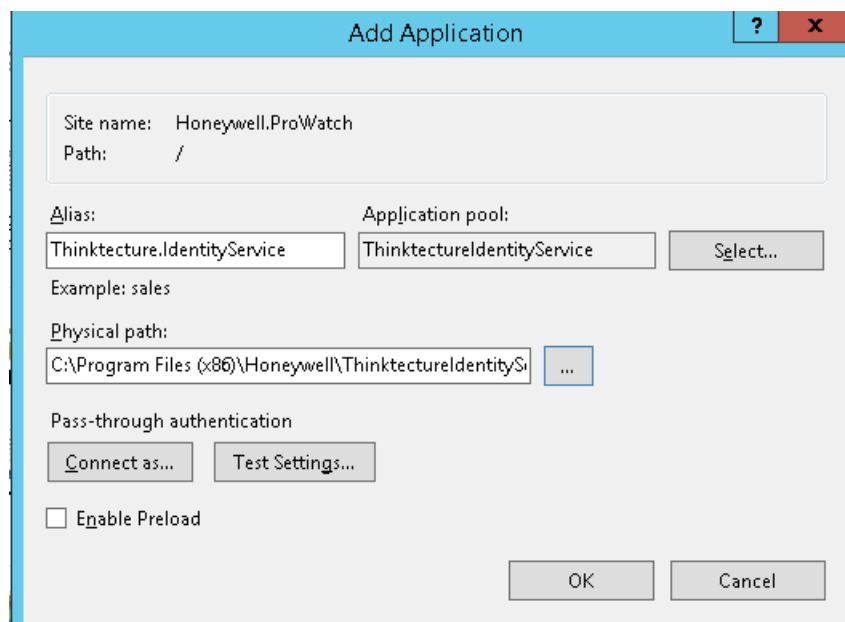
Use different port numbers (means ports not used by Default Web site bindings) for each binding if Default Web Site is running. Otherwise stop the default web site and use the ports used by it.

1.10.1 THINKTECTURE Identity Service

1. Add an application in the newly created web site.



2. Provide the Application alias name (**Thinktecture.IdentityService**) and physical path (**C:\Program Files (x86)\Honeywell\ThinktectureIdentityService**). Make sure the application pool is the same as of that of this site in the Default Web Site.



3. Click 'OK' to get it done.

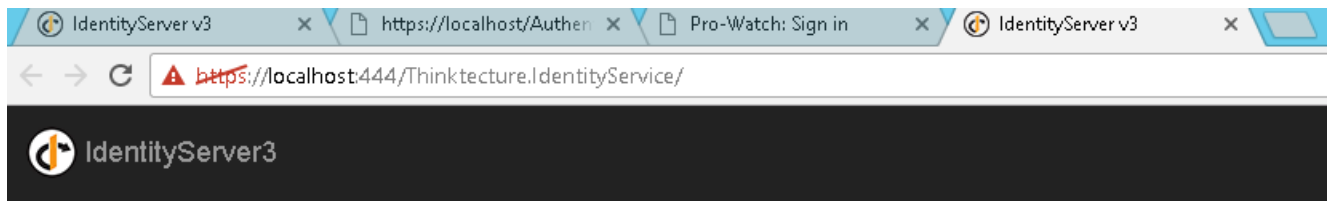
Overview

Moving Pro-Watch Components to Non-Default Website

4. In the ThinkTecture web.config file, change the "idsrv" app setting as per the new web site binding port number.

```
</assemblyBinding>
</runtime>
<entityFramework>
  <defaultConnectionFactory type="System.Data.Entity.Infrastructure.SqlConnectionFactory, EntityFramework">
  <providers>
    <provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer">
    </providers>
  </entityFramework>
<appSettings>
  <!--Absolute path or certificate Name it's in root folder of idServer-->
  <add key="CertificateName" value="Certificate/idsrv3test.pfx"/>
  <add key="CertificatePassword" value="idsrv3test"/>
  <add key="cacheDuration" value="20"/>
  <add key="cacheService" value="https://CacheService.api-UCP-Platform.Org/CachingService/api/cache"/>
  <!--make cacheEnabled true if cache service up otherwise false-->
  <add key="cacheEnabled" value="true"/>
  <!--Use machine name instead localhost otherwise token validation may fail-->
  <add key="idsrv" value="https://WIN-0CV6A1JR8NN:444/ThinktectureIdentityService/" />
  <!--GetSelfPrivileges validate for this scope in the token-->
  <add key="userPrivescopes" value="prowatch"/>
  <!-- AccessTokenLifetime set to 10 hours-->
  <add key="AccessTokenLifetime" value="3600"/>
  <add key="AbsoluteRefreshTokenLifetime" value="86400"/>
  <add key="SlidingRefreshTokenLifetime" value="43200"/>
  <!--Pro-Watch Database connection information-->
  <add key="PwDatabaseServer" value="WIN-0CV6A1JR8NN\SQLEXPRESS2K16"/>
  <add key="PwDatabase" value="PWNT"/>
  <add key="PwConnectionString" value="..." />
</appSettings>
```

5. (Optional): Browse the newly created application to see this result.



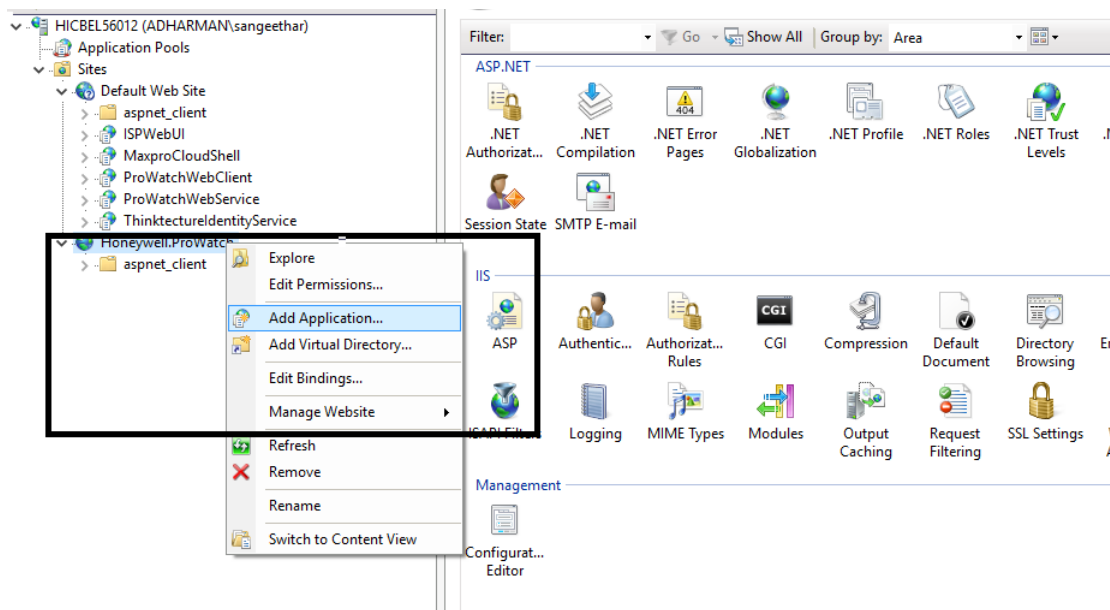
IdentityServer publishes a [discovery document](#) where you can find metadata and links to all the endpoints, key material, etc.

IdentityServer allows users to view and revoke [application permissions](#) previously granted to client applications.

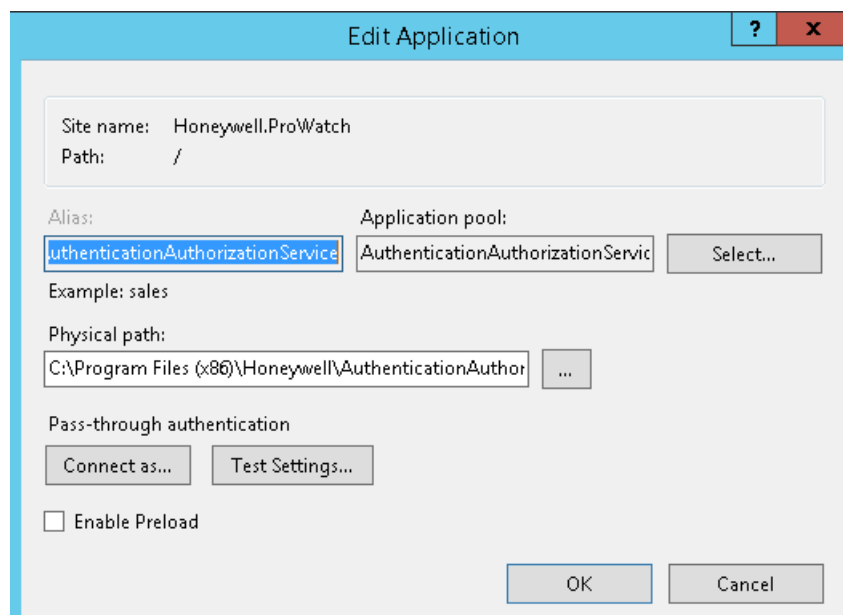
Here are links to the [documentation](#), and [ready to use samples](#).

1.10.2 AUTHENTICATION Identity Service

1. Add an application in the newly created web site.



2. Provide the Application alias name (**AuthenticationAuthorizationService**) and physical path (**C:\Program Files (x86)\Honeywell\AuthenticationAuthorizationService**). Make sure the application pool is the same as of that of this site in the Default Web Site.



3. Click 'OK' to get it done.
4. Update the Web.config values of this site

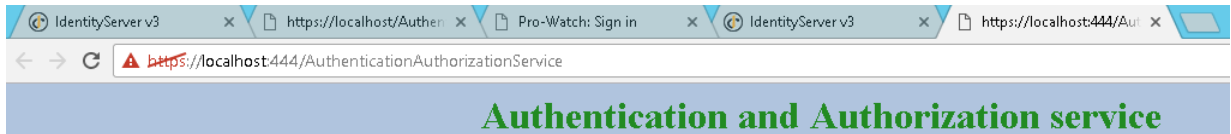
Overview

Moving Pro-Watch Components to Non-Default Website

The 'ThinkTectureProvider' endpoint value needs to be updated to point to the newly created IdentityServer endpoint.
(https://localhost:444/ThinktectureIdentityService in this case)

```
<iSPInfrastructure>
  <providers>
    <add name="ThinkTectureProvider" appName="AzAndAnServer" endpoint="https://localhost:444/ThinktectureIdentityService" faultRetry="5" />
  </providers>
</iSPInfrastructure>
```

5. (Optional): Browse the newly created application to see this result.

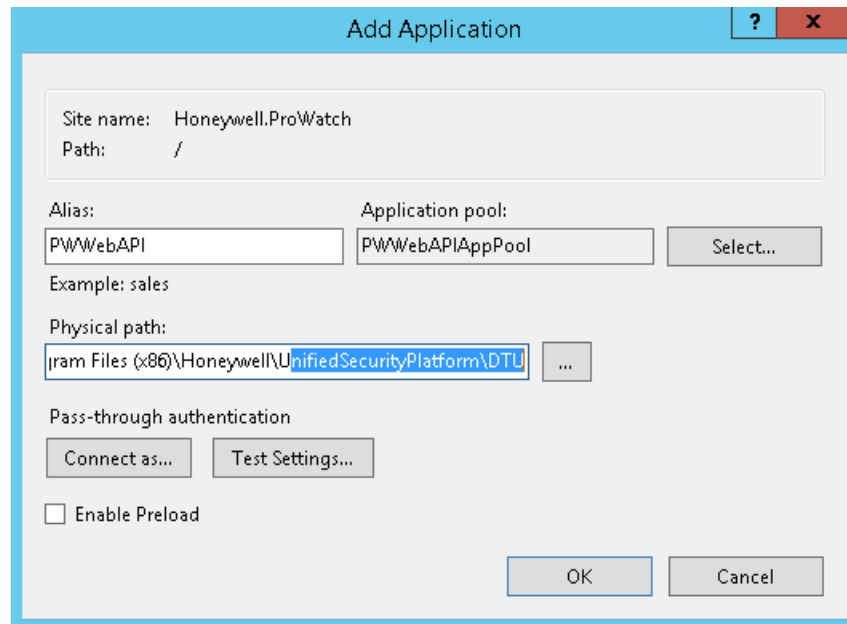


1.10.3 PW Web API



Important Note: If DTU is hosted in Windows Service, skip to the 4th step.

1. Add an application in the newly created web site.
2. Step 2: Provide the Application alias name (**PWWebAPI**) and physical path (**C:\Program Files (x86)\Honeywell\UnifiedSecurityPlatform\DTU**). Make sure the application pool is the same as of that of this site in the Default Web Site.



3. Click '**OK**' to get it done.
4. Update the Web.config (DTU is IIS hosted) / PW-DTU-WinService.exe.config (DTU is Windows Service hosted) values of this site.
 - a. The app setting 'BaseAnAURL' to be set to the URL of the Auth and Auth site that is just created

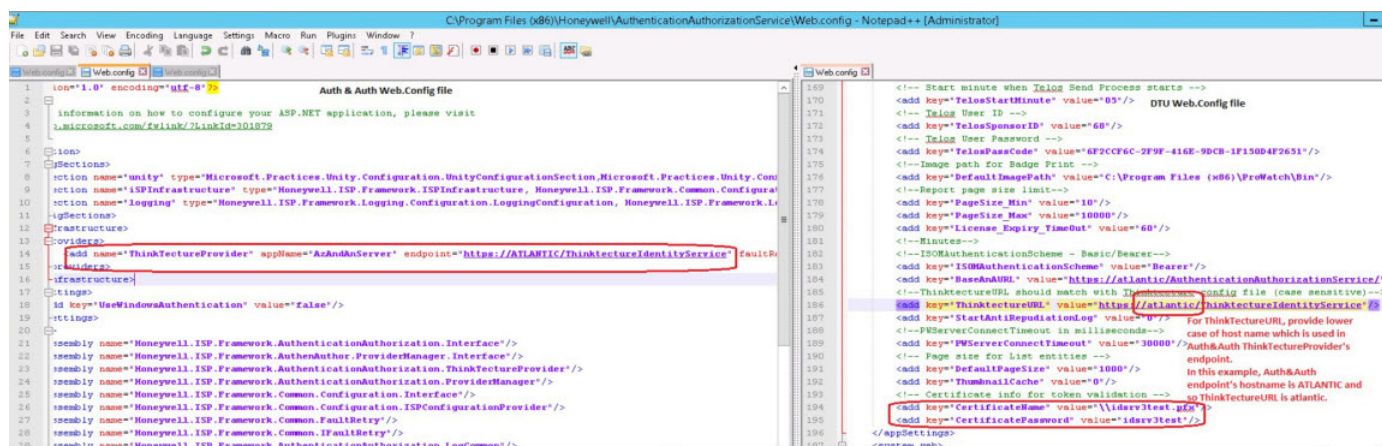
(<https://localhost:444/AuthenticationAuthorizationService> in this case):

```

58 <add key="BadgePhotoCustomField" value="BADGE_DISPPHOTO"/>
59 <!--Report page size limit-->
60 <add key="PageSize_Min" value="10"/>
61 <add key="PageSize_Max" value="10000"/>
62 <add key="License_Expiry_TimeOut" value="60"/>
63 <!--Minutes-->
64 <!--ISOMAuthenticationScheme - Basic/Bearer-->
65 <add key="ISOMAuthenticationScheme" value="Bearer"/>
66 <add key="BaseAnAURL" value="https://win-0cv6alir8nn:444/AuthenticationAuthorizationService/" />
67 <!--ThinkTectureURL should match with ThinkTecture Config file (case sensitive)-->

```

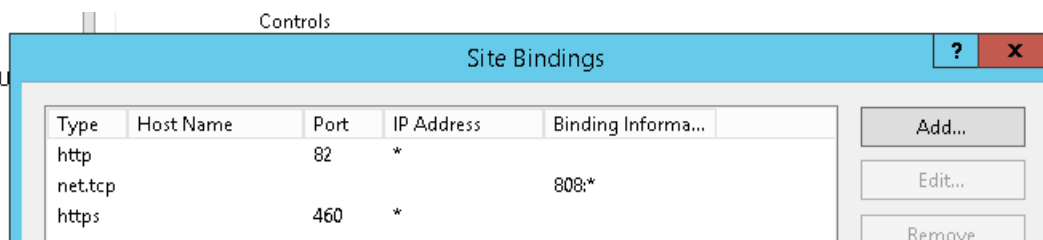
b. The app setting 'ThinkTectureURL' to be set to the value of



c. If DTU is hosted in Windows Service, Restart the "Pro-Watch Web API" service.

1.10.4 4.ISP Web UI

1. Add an application in the newly created web site, or a new web site could be created and an application could be added to this new site (so that services and UI are on different layers).



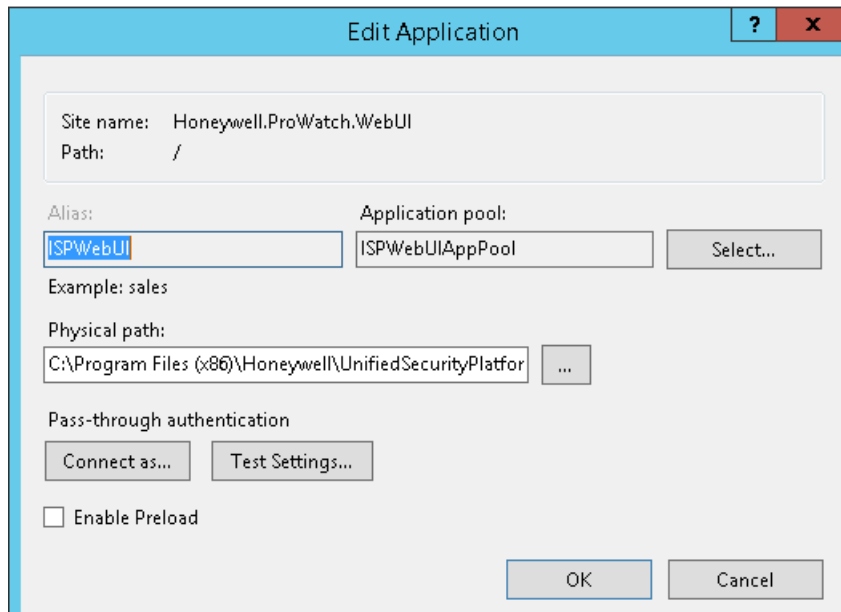
Important Note: Make sure your port is not used by any other application.

2. Step 2: Create a new application in this site and provide the Application alias name (ISPWebUI) and physical path (C:\Program Files

Overview

Moving Pro-Watch Components to Non-Default Website

(x86)\Honeywell\UnifiedSecurityPlatform\Web\WEBUI). Make sure the application pool is the same as of that of this site in the Default Web Site.



3. Click '**OK**' to get it done.
4. Update the Web.config values of this site.

In the configuration section, the 'isom ipAddress' needs to be updated to point to the Web API site created. In this case, it is,

- a. If DTU is hosted in IIS, then set

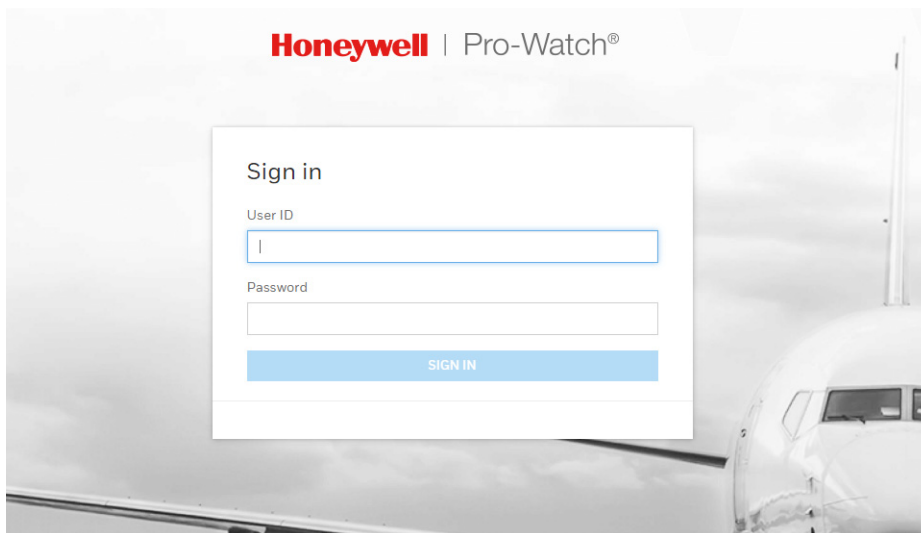
```
<isom ipAddress="localhost:444/PWWebAPI" protocol="https"
authenticationType="Basic"/>
```

If DTU is hosted in Windows Service

```
<isom ipAddress="localhost:8733" protocol="http"
authenticationType="Basic" />
```

- b. '**ISPAuthEndPoint**' appSetting value needs to be set to the AuthNAAuth service endpoint.
(**https://localhost:444/AuthenticationAuthorizationService/api/AuthenticationAuthorization/** in this case)

5. (Optional): Browse the newly created application to see this result.



The original sites created in Default Web Site could be removed since they are no more required.



Important Notes:

- 1. Make sure your port is not used by any other application.**
- 2. Localhost may be replaced by machine name.**

1.11 Dynamic IP Restriction Configuration



Note: Execute the steps described in this section only after you log in successfully to the application. These are steps essential for windows and token based authentication.

1.11.1 Introduction

The Dynamic IP Restrictions (DIPR) module for IIS 7.0 and above provides protection against denial of service and brute force attacks on web servers and web sites. To provide this protection, the module temporarily blocks IP addresses of HTTP clients that make an unusually high number of concurrent requests.

1.11.2 Installation of IP and Domain Restrictions

Refer the web site

<https://www.iis.net/configreference/system.webserver/security/ipsecurity> for the installation of IP and domain Restrictions.

1.11.3 Pro-Watch Single-Tier and Two-Tier Deployment

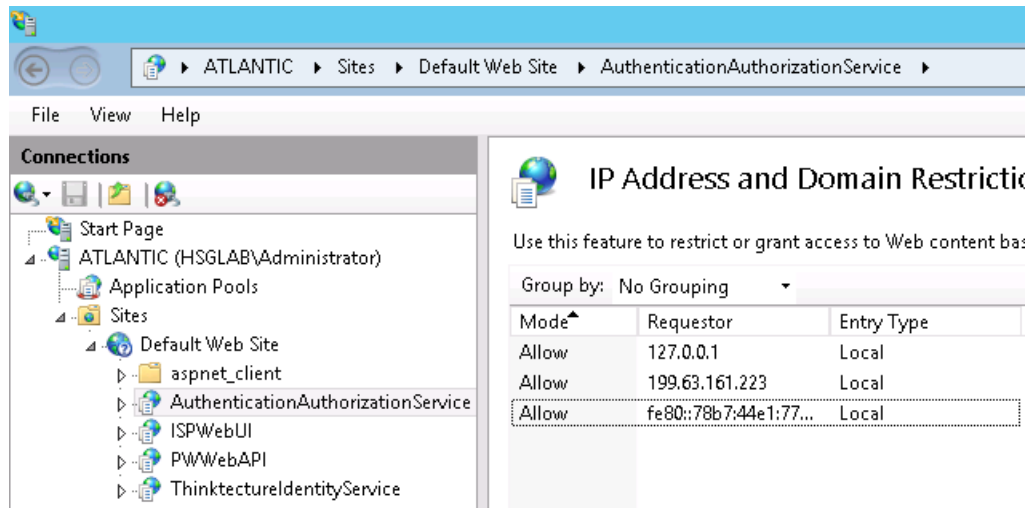
For each of the below web applications

- ThinktectureIdentityService,
- AuthenticationAuthorizationService
- PWWebAPI (It will be available in IIS if DTU is IIS hosted. *If DTU is hosted in Windows Service, there is no setting required for DTU.*)

do the following:

1. Select Web Application
2. Click "**IP Address and Domain Restrictions**".
3. Click "**Edit Feature Settings**" in Actions pane.
4. Choose "**Deny**" for "Access for unspecified clients" and Click **OK**.
5. Click "**Add Allow Entry**" in actions pane.

6. Provide the local machine IPv4 address, IPv6 address and 127.0.0.1 for **"Specific IP address"**:



1.11.4 Pro-Watch Three Tier Deployment

For ThinktectureIdentityService, perform the following steps:

1. Select Web Application
2. Click **"IP Address and Domain Restrictions"**
3. Click **"Edit Feature Settings"** in Actions pane.
4. Select **"Deny"** for "Access for unspecified clients" and Click **OK**.
5. Click **"Add Allow Entry..."** in actions pane.
6. Provide the local machine IPv4 address, IPv6 address and 127.0.0.1 for **"Specific IP address"**.

For AuthenticationAuthorizationService, PWWebAPI (If DTU installed in IIS):

1. Select Web Application
2. Click **"IP Address and Domain Restrictions"**.
3. Click **"Edit Feature Settings"** in Actions pane.
4. Choose **"Deny"** for "Access for unspecified clients" and Click **OK**.
5. Click **"Add Allow Entry..."** in actions pane.
6. Provide the local machine IPv4 address, IPv6 address and 127.0.0.1 for **"Specific IP address"**.
7. Provide the **machine IP** (ipv4 and IPv6 address) of the WebUI installed for **"Specific IP address"**.

Pro-Watch Web Client



2

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 X768 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>) 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.

2.4 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 39.
- **Using Security tab** - Refer to section [IE11 Security Settings](#) on page 42.

2.7.1 IE11 Advanced Settings

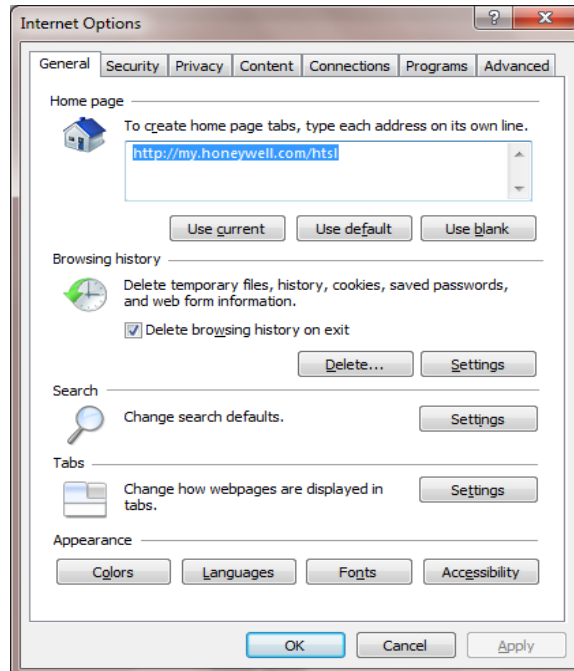
To enable the security settings for IE11 using Advanced tab:

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:

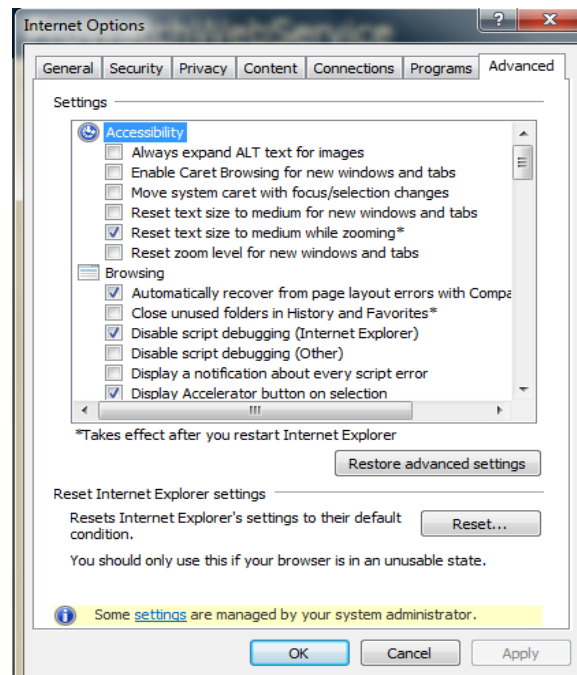


Figure 1 *Internet Options Dialog Box*



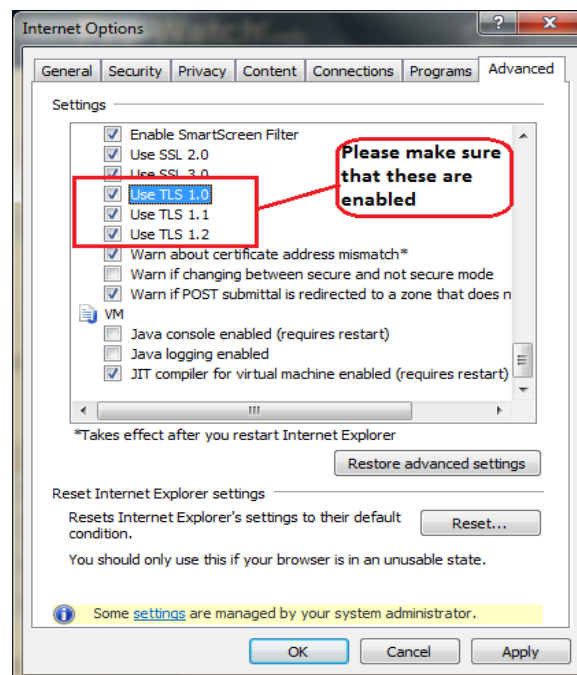
3. Click the **Advanced** tab.

Figure 2 Internet Options - 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

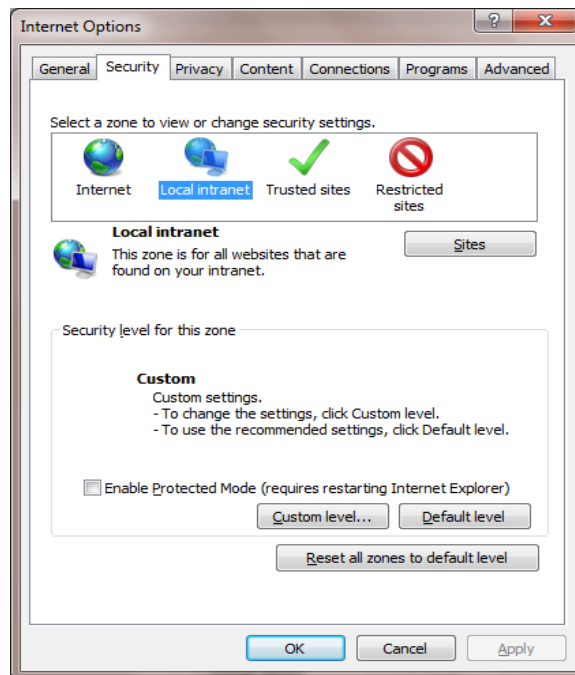
To enable the security settings for IE11 using Security tab:

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](#)):



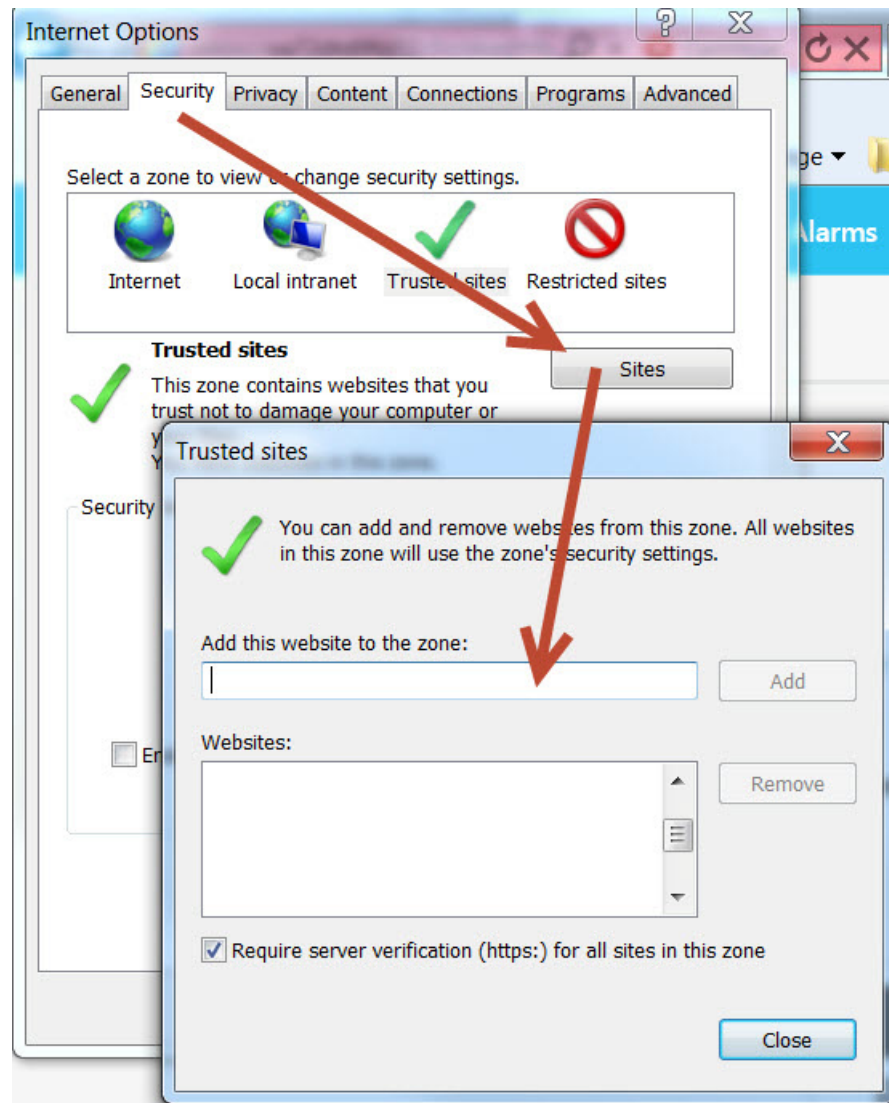
3. Click and select the **Security** tab.

Figure 4 Internet Options - Security Tab



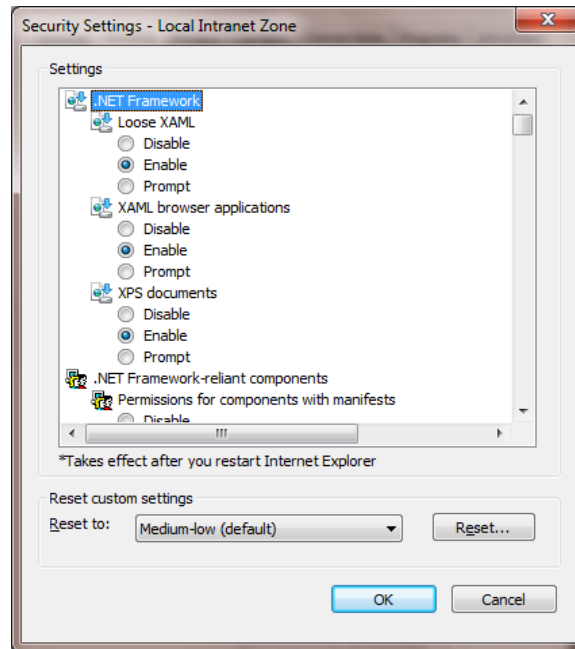
4. In the **Select a zone to view or change security settings**, select the **Trusted Sites** option.

5. Click the **Sites** command button to display the **Trusted Sites** dialog box:



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.

Figure 5 Security Settings - Local Internet Zone Dialog box



9. In **Settings**, scroll down and then select the following options.

Table 1 IE11 Security Settings

IE11 Security Category	IE11 Security Component	Value
.NET Framework	Loose XAML	Disable
.NET Framework	XML browser applications	Enable
.NET Framework	XPS documents	Enable
.NET Framework	Permissions for components with manifests	Enable
.NET Framework-reliant components	Run components not signed with Authenticode	Enable
.NET Framework-reliant components	Run components signed with Authenticode	Enable
ActiveX controls and plug-ins	Allow ActiveX filtering	Enable
ActiveX controls and plug-ins	Allow previously unused ActiveX controls to run without prompt	Disable
ActiveX controls and plug-ins	Allow scriptlets	Disable
ActiveX controls and plug-ins	Automatic prompting for ActiveX controls	Disable

Table 1 IE11 Security Settings

ActiveX controls and plug-ins	Binary and script behaviors	Enable
ActiveX controls and plug-ins	Display video and animation on a webpage that does not use external media player	Disable
ActiveX controls and plug-ins	Download signed ActiveX controls	Prompt
ActiveX controls and plug-ins	Download unsigned ActiveX controls	Disable
ActiveX controls and plug-ins	Initialize and script ActiveX controls not marked as safe for scripting	Disable
ActiveX controls and plug-ins	Only allow approved domains use ActiveX without prompt	Disable
ActiveX controls and plug-ins	Run ActiveX controls and plug-ins	Enable
ActiveX controls and plug-ins	Run antimalware software on ActiveX controls	Enable
ActiveX controls and plug-ins	Script ActiveX controls marked safe for scripting (takes effect after your restart Internet Explorer)	Enable
Downloads	File download	Enable
Downloads	Font download	Enable
Downloads	Enable .NET Framework setup	Enable
Miscellaneous	Access data sources across domains	Disable
Miscellaneous	Allow META REFRESH	Enable
Miscellaneous	Allow scripting of Microsoft web browser control	Disable
Miscellaneous	Allow scrip-initiated windows without size or position constraints	Disable
Miscellaneous	Allow webpages to use restricted protocols for active content	Prompt
Miscellaneous	Allow websites to open windows without address or status bars	Disable
Miscellaneous	Display mixed content	Prompt
Miscellaneous	Don't prompt for client certificate selection when only one certificate exists	Disable

Table 1 IE11 Security Settings

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

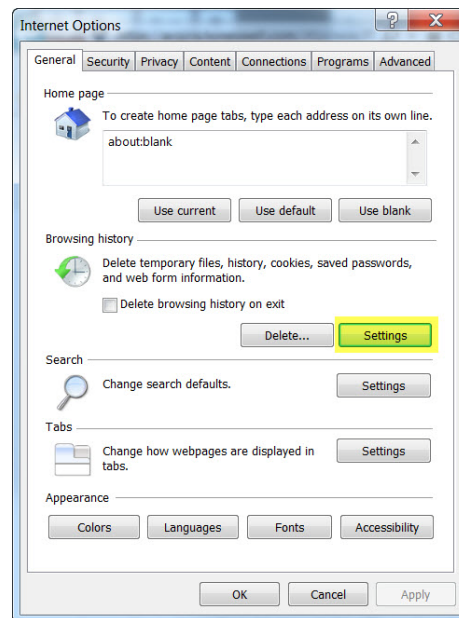
10. After making all the correct selections as described in the above table, click **OK**.

- 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.

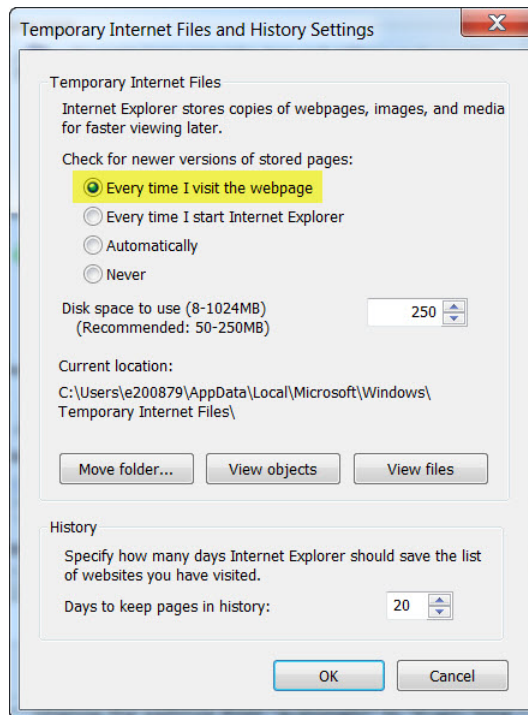
2.8 Temporary Internet Files Setting for IE11

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:



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.

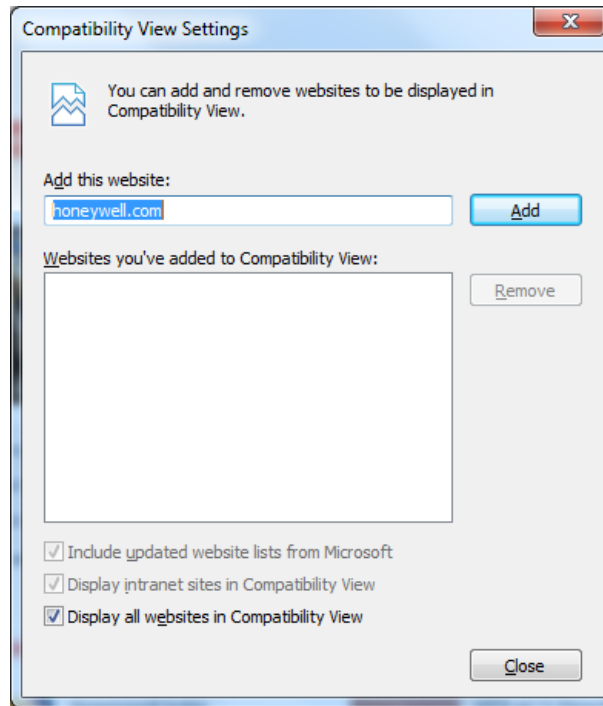
2.9 Configuring the Browser Mode

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 4.3.5 Web Client.

To configure the browser mode for the Pro-Watch 4.3.5 Web Client:

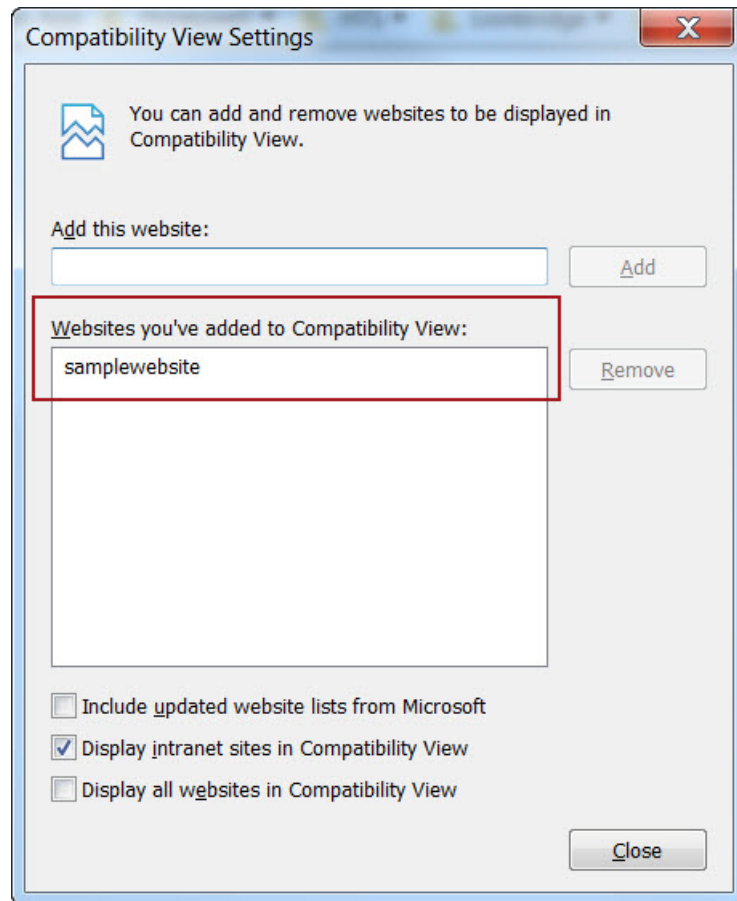
1. Launch **Internet Explorer 11**.
2. Click **Tools** from Internet Explorer browser menu to display the **Tools** Menu.
Or
Press **Alt+T** if the browser menu is not displayed in Internet Explorer.
3. Select **Compatibility View Settings** from the **Tools** menu to display the **Compatibility View Settings** window as shown in [Figure 6](#).

Figure 6 *Compatibility View Settings window*



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:



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

5. Click **Close** to close to dialog box.

2.10 Web Client User Account Prerequisites

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

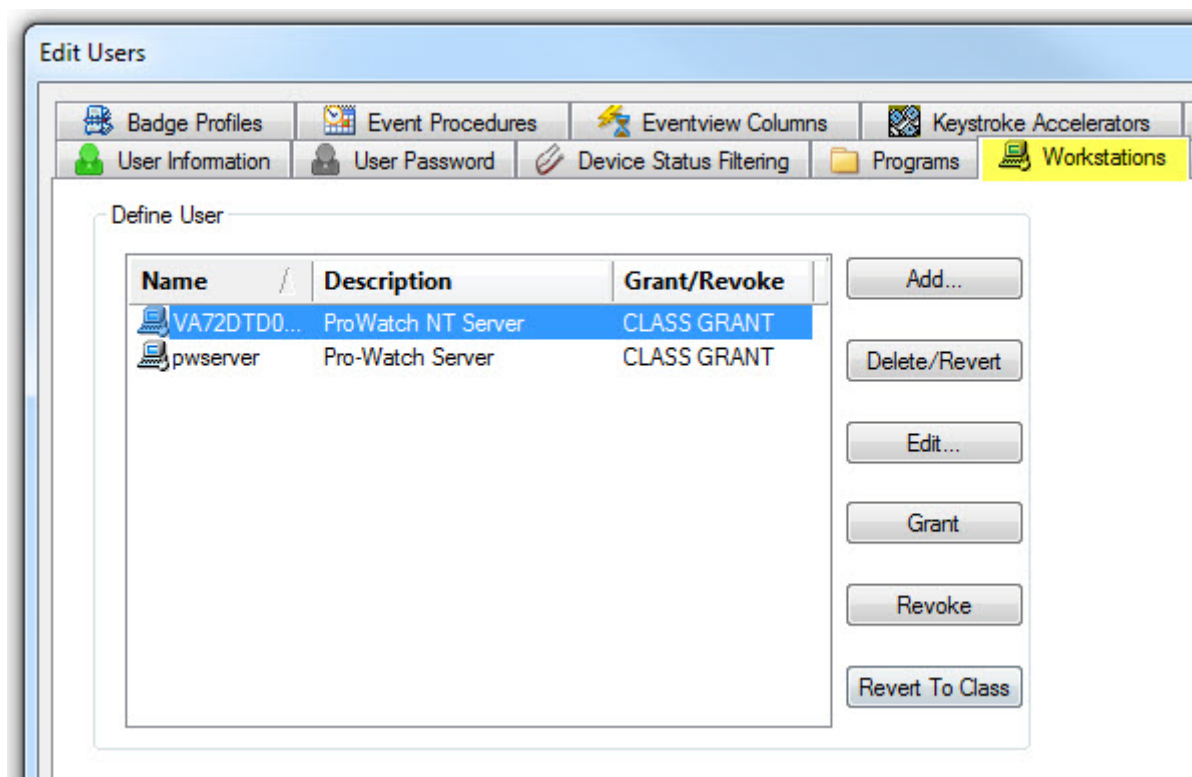
2.10.1 Create a Valid Pro-Watch User Account

Refer to the *Pro-Watch Software Suite 4.3.5 User Guide*, 7-901071V13, 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:



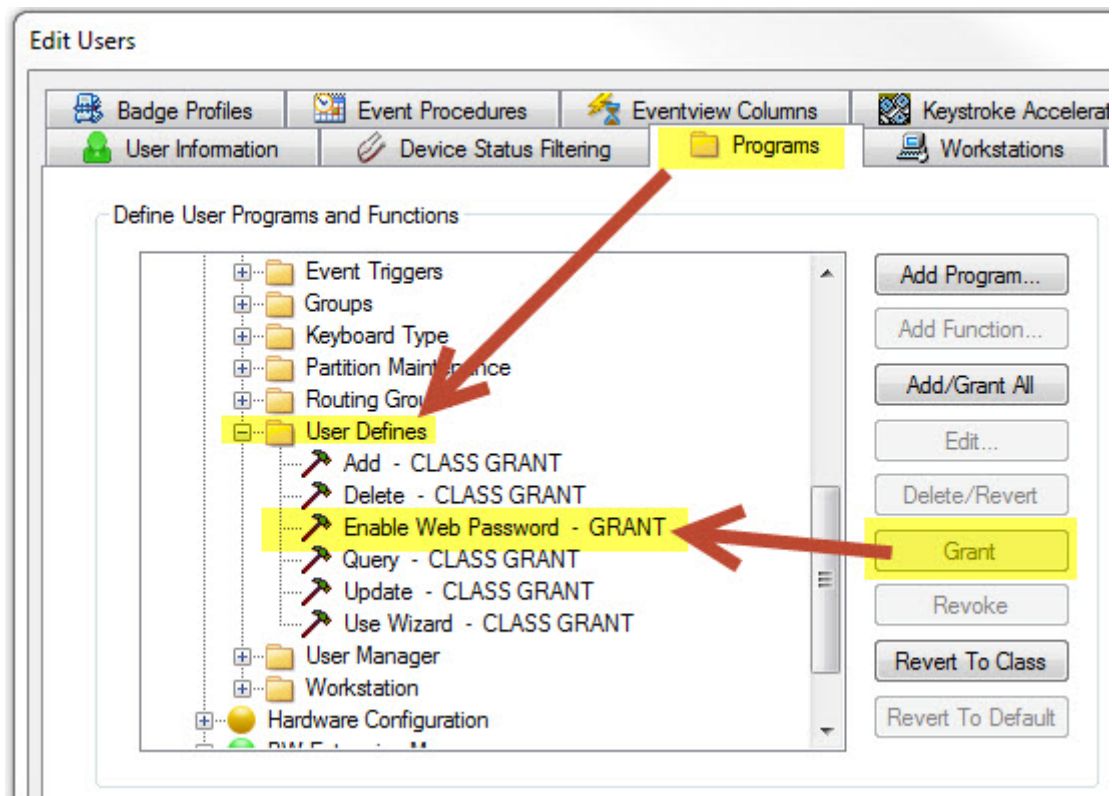
3. If your workstation is not displayed in the **Define User** list, click the **Add** button, browse and find your workstation and add it to the list.
4. If the workstation is not in grant status, select the workstation and click the **Grant** button.
5. When done, click the **OK** button at the bottom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

For more information refer to the *Pro-Watch Software Suite 4.3.5 User Guide*, 7-901071V13, 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.

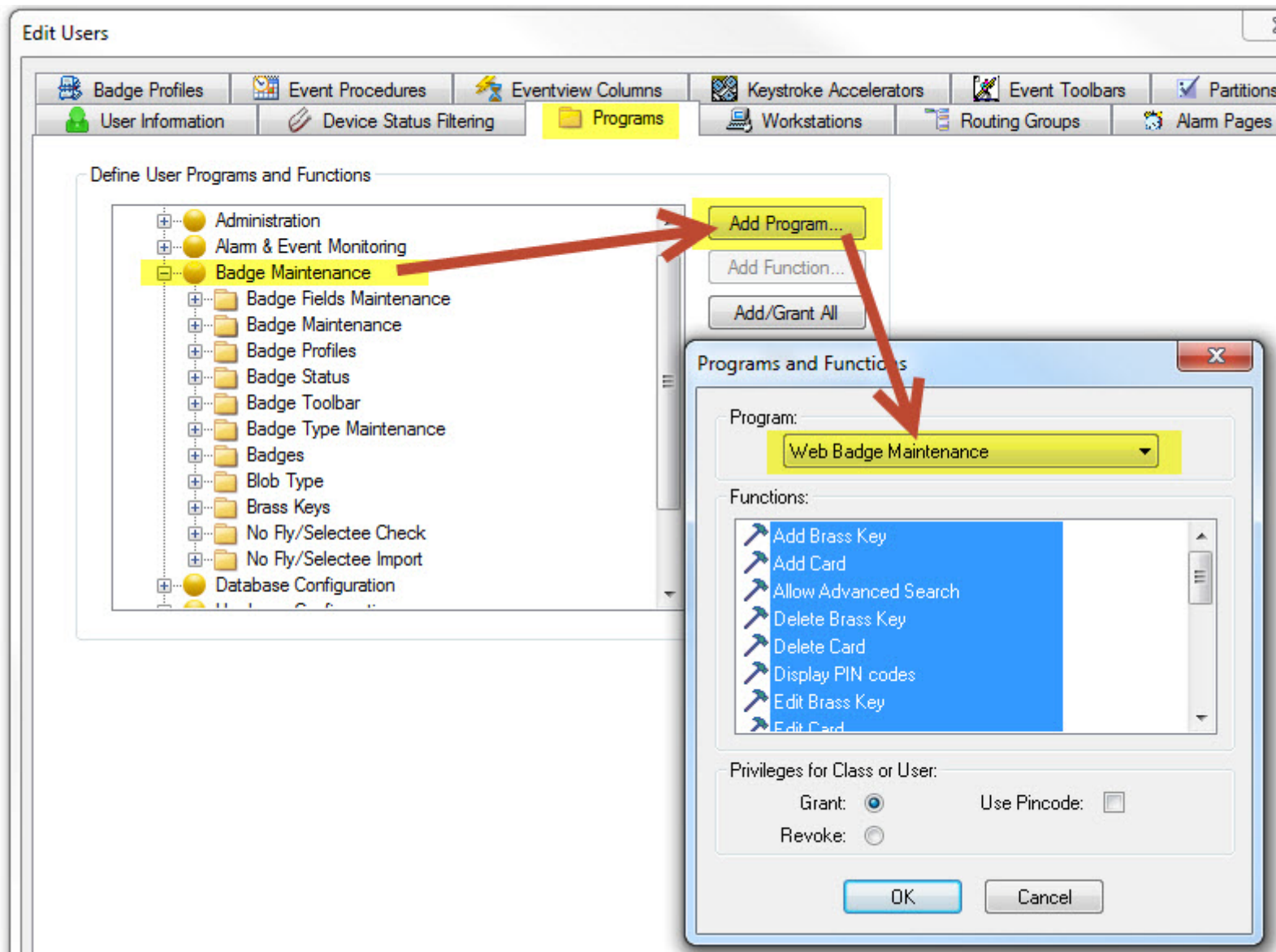
2.10.3.1 Setting the Web Password

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

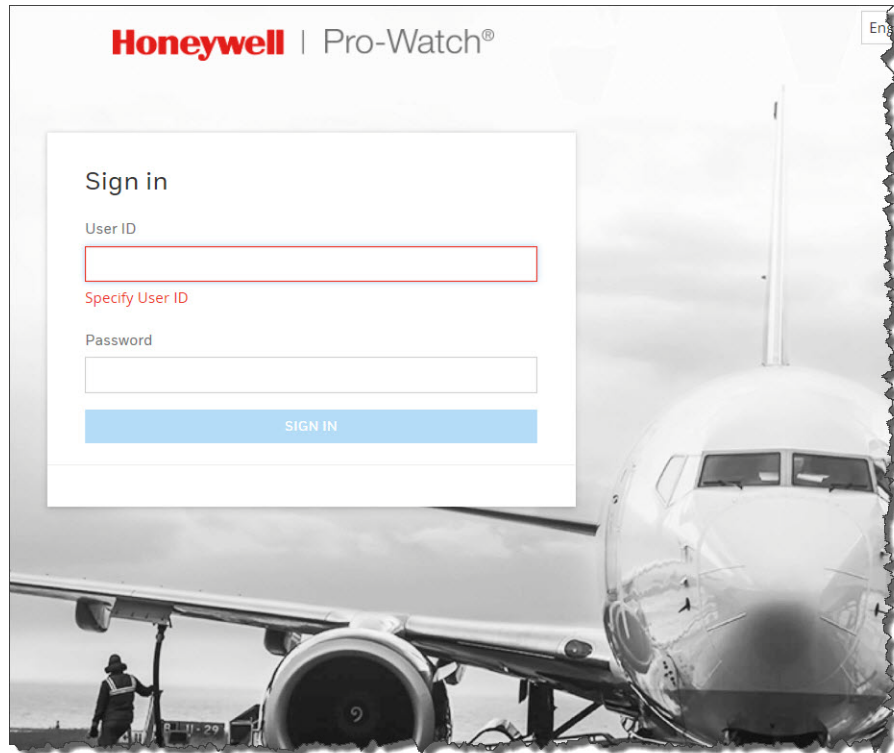
To access the Pro-Watch Web Client:

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



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 4.3.5 User Guide, 7-901071V13* about setting Web Client passwords for Pro-Watch users. Also see [Enable Your Web Password](#) in this section.

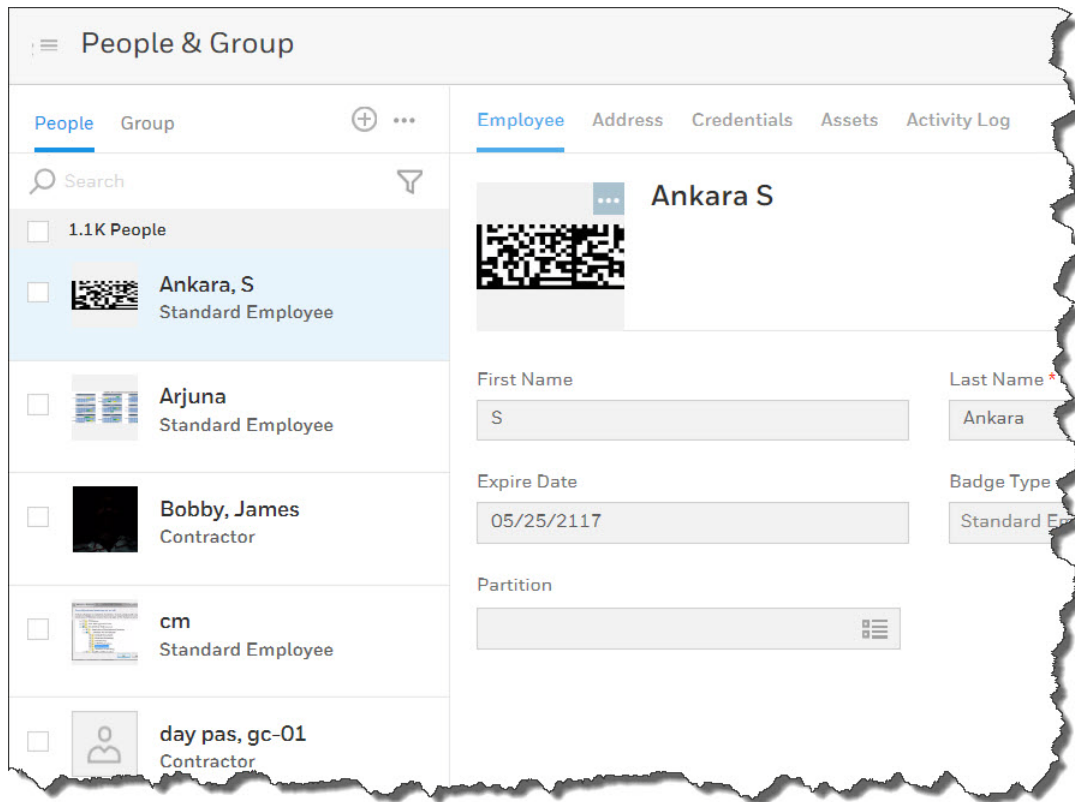
3. Click the **Login** button to display the Pro-Watch Web Client interface page.

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.

Figure 8 Pro-Watch Web Client Home Page



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" />
```

</httpErrors>

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 55. The following sections describe the features of the Pro-Watch Web Client Home page.

2.12.1 Home Navigation Links



Table 2 Home Navigation Links


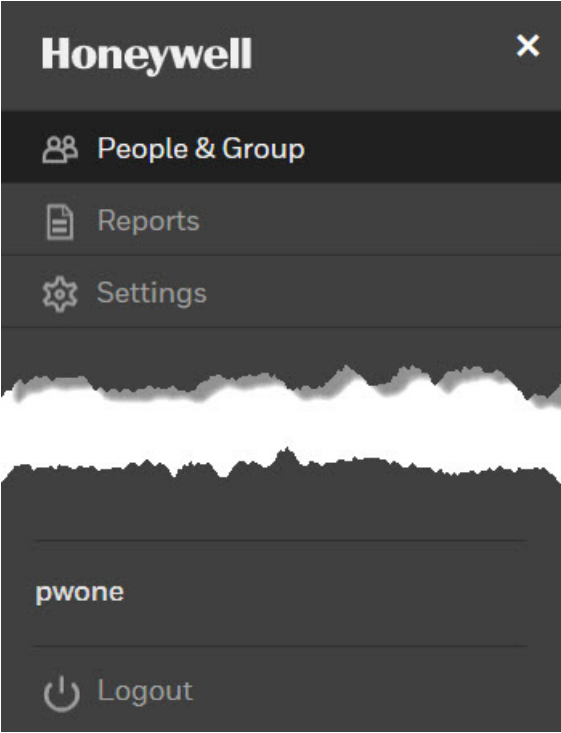
Link	Description
	<p>Click to display the Honeywell Menu to display the following options:</p>  <p>Click People & Group to display the Badging module. Click Report to display the Report module. Click Settings to display the Settings module. Click Logout to log out of the web client. NOTE: You can display this menu by clicking the “People & Group” title as well.</p>

Table 2 Home Navigation Links

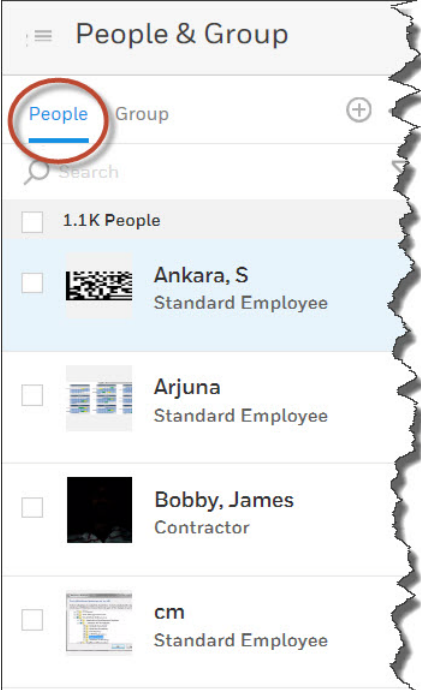
Link	Description
People	<div>Click People to display the list of badge-holders:</div> <div></div> <div>Click a badge-holder name to display the respective badging record information on the right pane.</div>

Table 2 Home Navigation Links

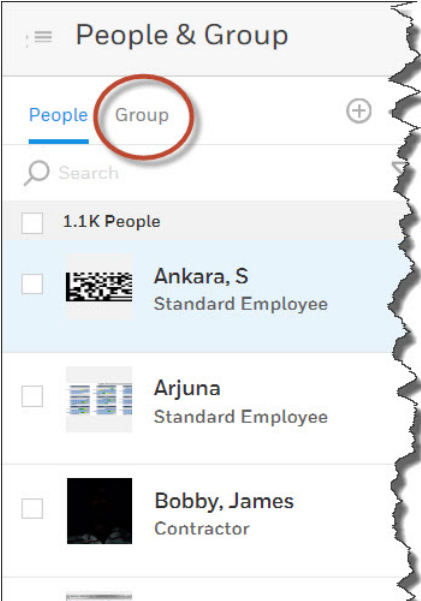

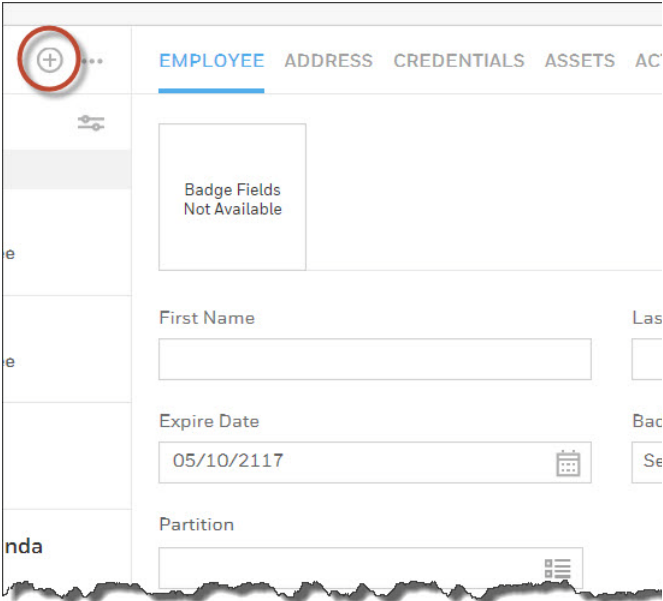

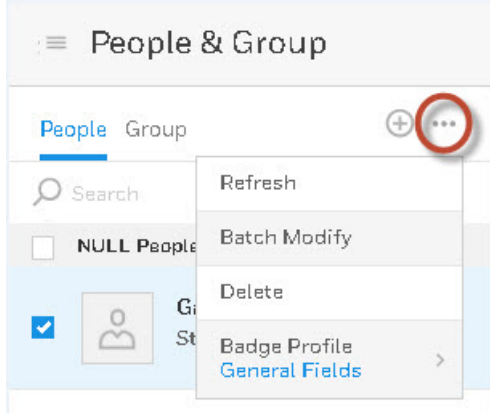

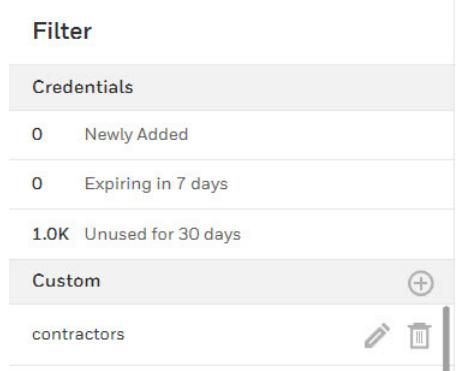

Link	Description
Group	<p>Click Group to display the list of groups available to assign to individual badge-holders:</p>  <p>Click a group name to display the respective group information on the right pane.</p>
	<p>Click the ADD link to add a new badge record (displayed in the right pane):</p> 

Table 2 Home Navigation Links

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

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 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=31bf3856ad364836" />
  </providers>
</sessionState>
<customErrors mode="Off" />
</system.web>
<!-- custom webServices -->
```

Refer to *Pro-Watch® Software Suite 4.3.5 Installation Guide, 7-901073V11* for more information on how to set the time out for a session.

2.13 Modules

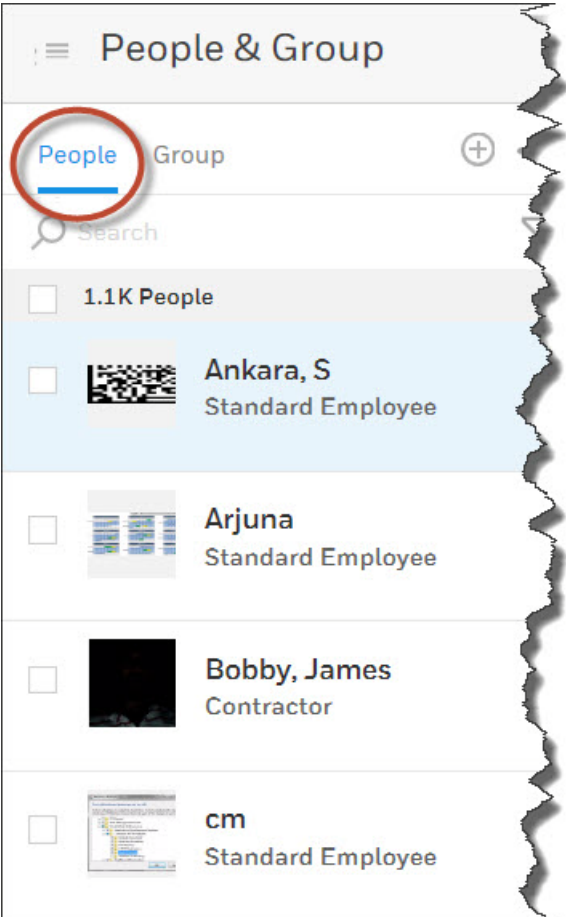
The Pro-Watch Web Client allows the user to access the following modules:

- **Badging:** Refer to the [Badging](#) section.
- **Report:** Refer to the [Reporting](#) section.
- **Settings.** Refer to the [Settings](#) section.

2.14 Badging

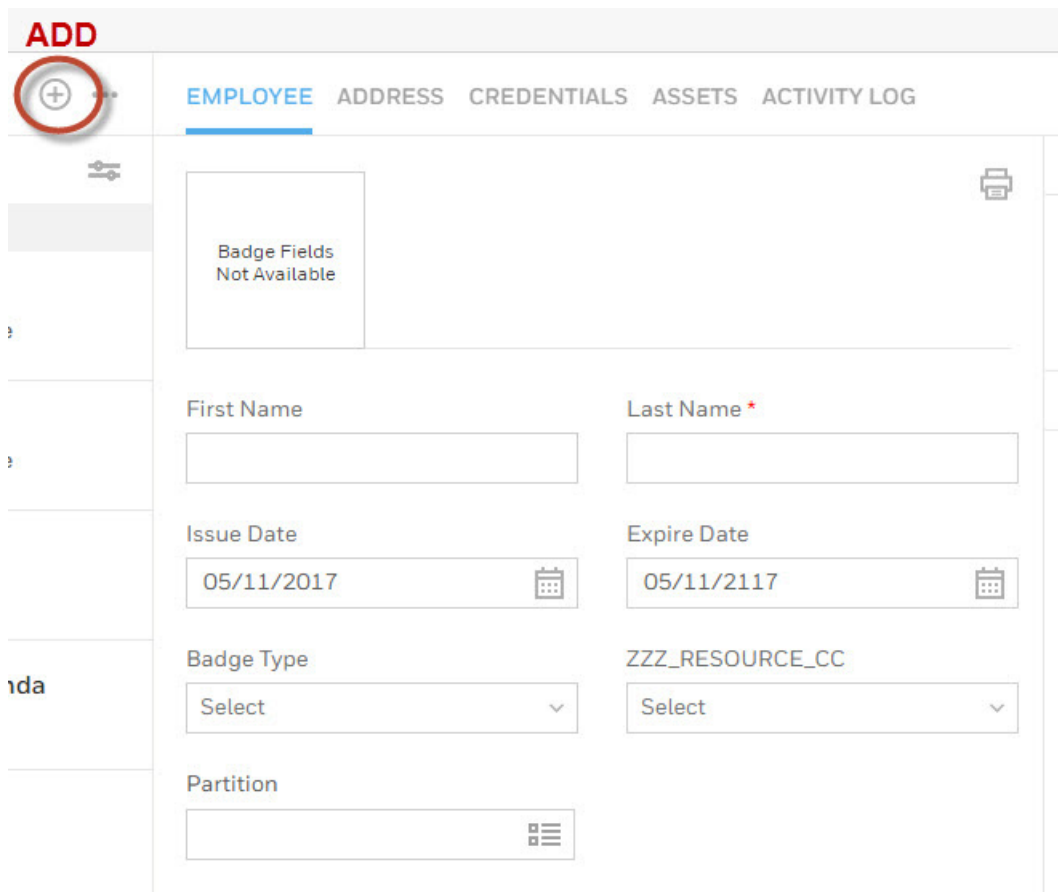
Click the **Honeywell Menu** (3 horizontal bars) on the Home page and select **People & Group** link to display the Badge-Records Badging screen:

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.



ADD

EMPLOYEE ADDRESS CREDENTIALS ASSETS ACTIVITY LOG

Badge Fields Not Available

First Name Last Name *

Issue Date Expire Date

05/11/2017 05/11/2117

Badge Type ZZZ_RESOURCE_CC

Select Select

Partition

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 card are credentials but all credentials are not cards.

Employee Address **Credentials** Assets Activity Log

345345
Expires on 05/30/2018

345435
Expires on 05/09/2019

ADD NEW CREDENTIAL

Credential Details Permissions

Credential Number

345345

Status

Active

Type

Standard Employee

PIN

1272

View More

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

Credential Number*

Card Number required

Credential Status*

Active

Type*

Select

PIN

Type or generate

PIN Verify

Permissions

Access Group*

Additional Rights

CANCEL

Add

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:

Employee Address **Credentials** Assets Activity Log

345345 Expires on 05/30/2018

345435 Expires on 05/09/2019

ADD NEW CREDENTIAL

Credential Details **Permissions**

1Group

All Access

1 Additional Rights

Copy (10) of Demo Clearance Code 2 Doors

SCHEDULED

2 Additional Doors

Entrance 2 System All Times

GRANTED

Reader1

REVOKED

1. To view a summary of **Additional Rights**, click the **filter icon** on the upper-right:

Credential Details **Permissions**

1Group

All Access

1 Additional Rights

1 All ✓

0 Temporary

0 Timed

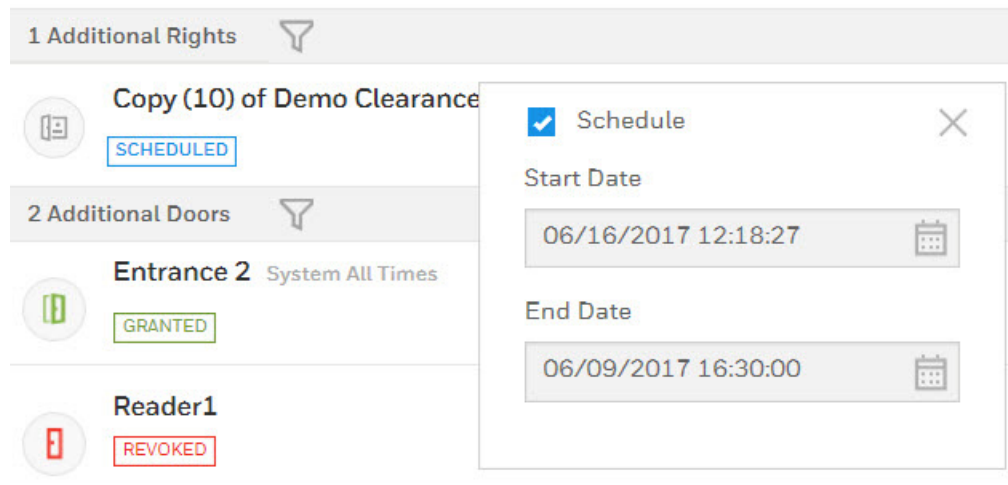
0 Certification

Clearance Code 2 Doors

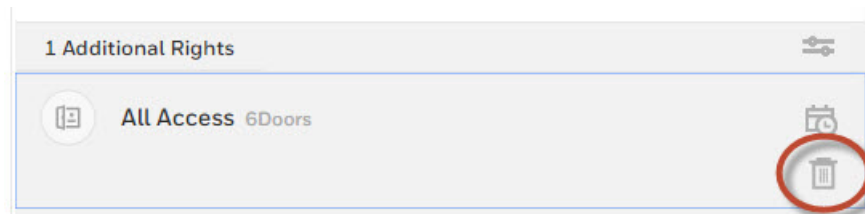
Reader1

REVOKED

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:

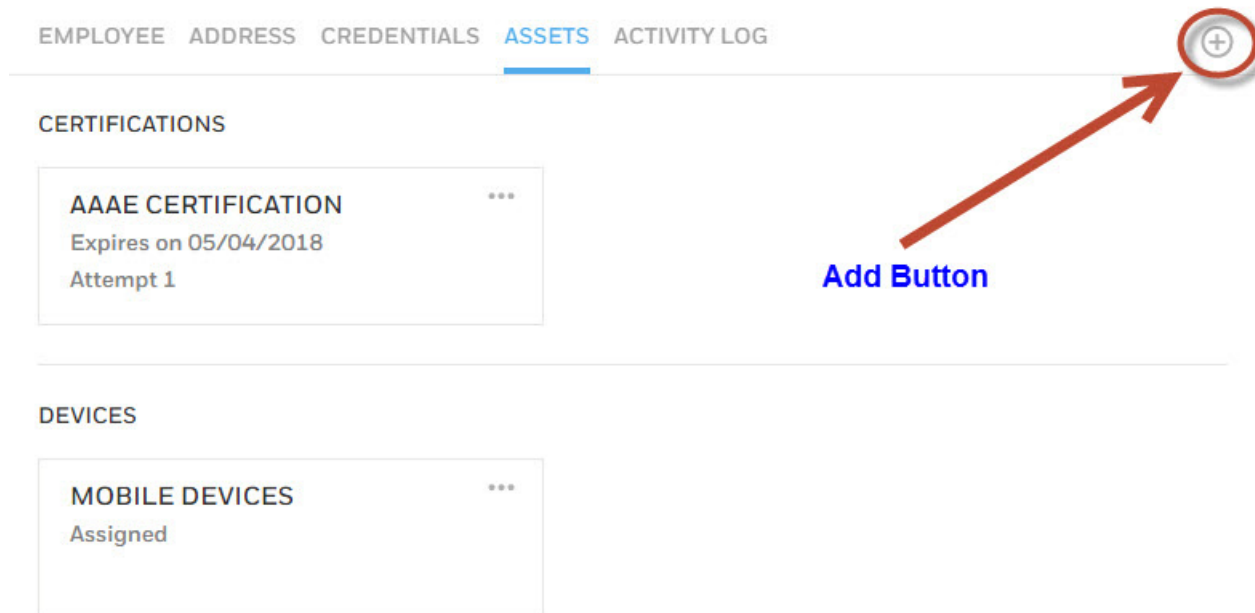


3. To **delete** an additional right, click the **Delete** icon (which deletes without any further warning):



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

Certification Select	Issue Date
Expiry Date	Attempt Select
Score	Supervisor
Note <div></div>	
<input type="checkbox"/> 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

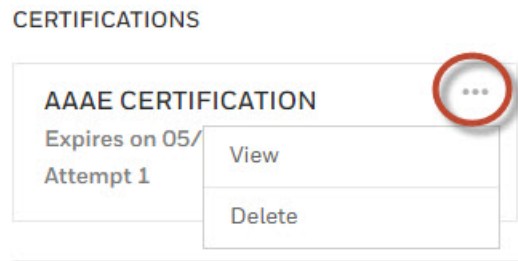
Device	Assets No
<input type="text" value="Select"/>	<input type="text"/>
Status	Issue Date
<input type="text" value="Select"/>	<input type="text" value="05/22/2017"/>
Due Date	Date Returned
<input type="text"/>	<input type="text"/>
Note	
<input type="text"/>	

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.

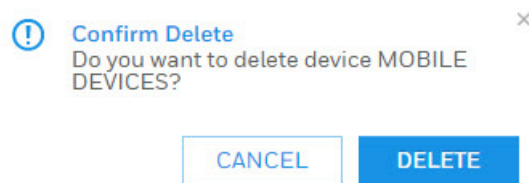
- Click the **Actions** link to display the drop-down menu:



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

To Delete a Certification or Device

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



- 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:

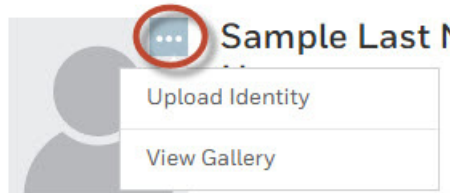


Edit all the fields you like; then click **Save**.

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:

Upload Identity

No Image Uploaded

Image Type:

Display Photo

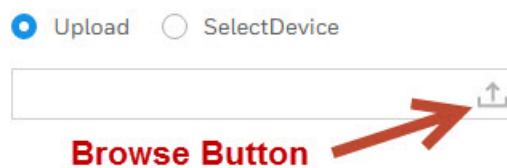
☒ Upload ☐ SelectDevice

CANCEL

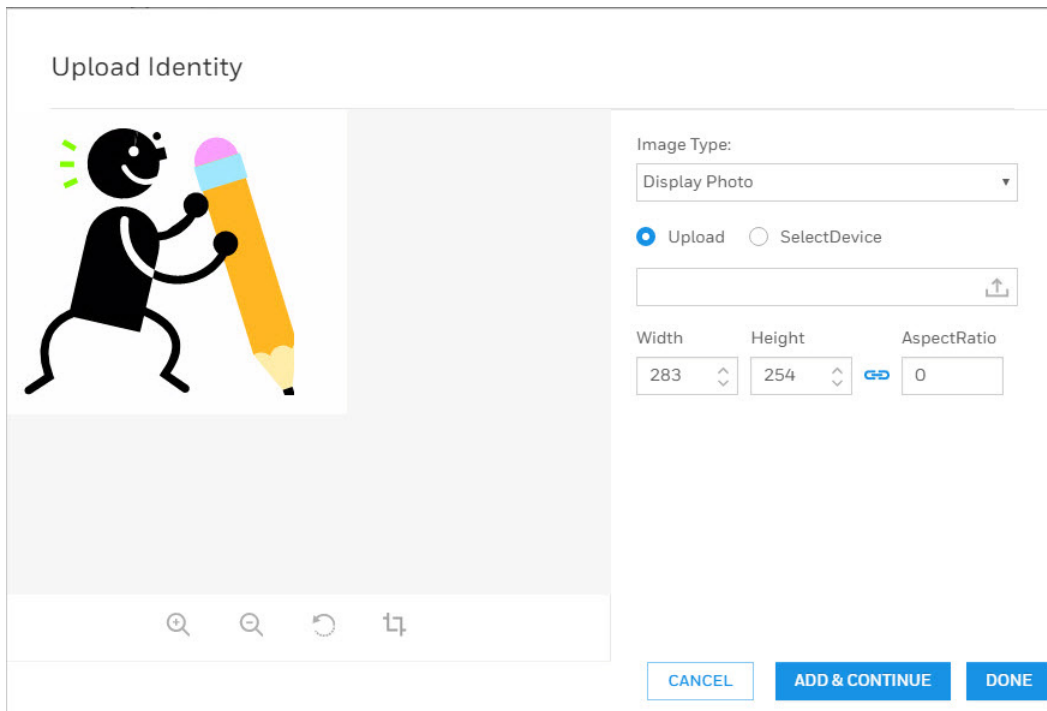
ADD & CONTINUE

DONE

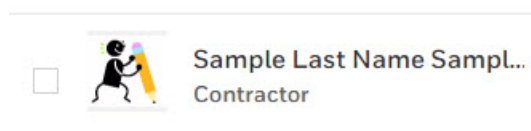
5. Select an **Image Type** from the drop-down menu.
6. Select **Upload** option-button. Then click the **Browse Button** to find the image you want to load:



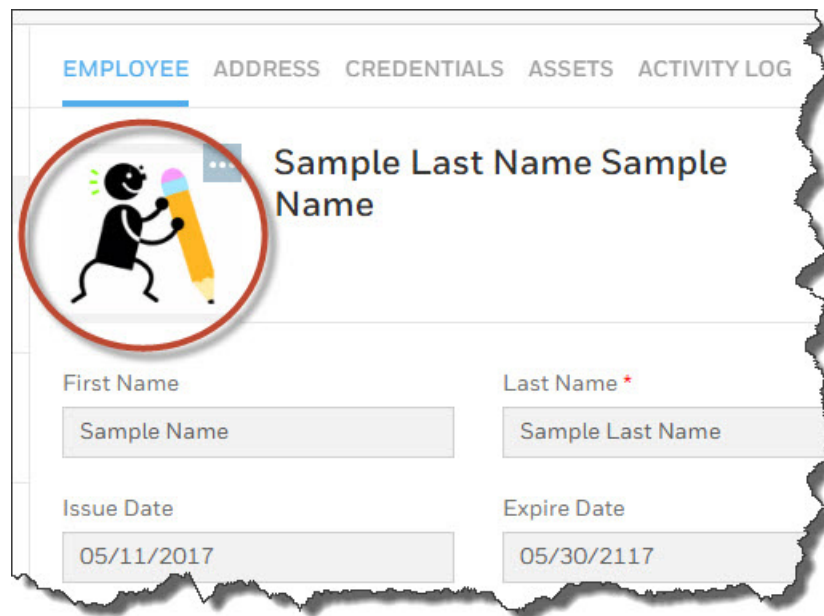
7. Browse and select an image. Click **Open** to upload the image to the **Upload Identity** page:



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 display in the badge record list:



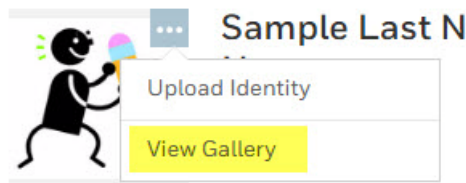
10. Select and double-click the badge record to have the new image display in the full badge record as well:



The screenshot shows the 'EMPLOYEE' tab in the Pro-Watch Web Client. A badge record for 'Sample Last Name Sample Name' is highlighted with a red circle. The badge record includes fields for First Name, Last Name, Issue Date, and Expire Date.

EMPLOYEE	ADDRESS	CREDENTIALS	ASSETS	ACTIVITY LOG
Sample Last Name Sample Name				
First Name		Last Name *		
Sample Name		Sample Last Name		
Issue Date		Expire Date		
05/11/2017		05/30/2117		

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



The screenshot shows a drop-down menu with two options: 'Upload Identity' and 'View Gallery'. The 'View Gallery' option is highlighted in yellow.

Sample Last N
Upload Identity
View Gallery

12. To capture an image from a device, select **Select Device** option-button in the **Upload Identity** screen:

Upload Identity

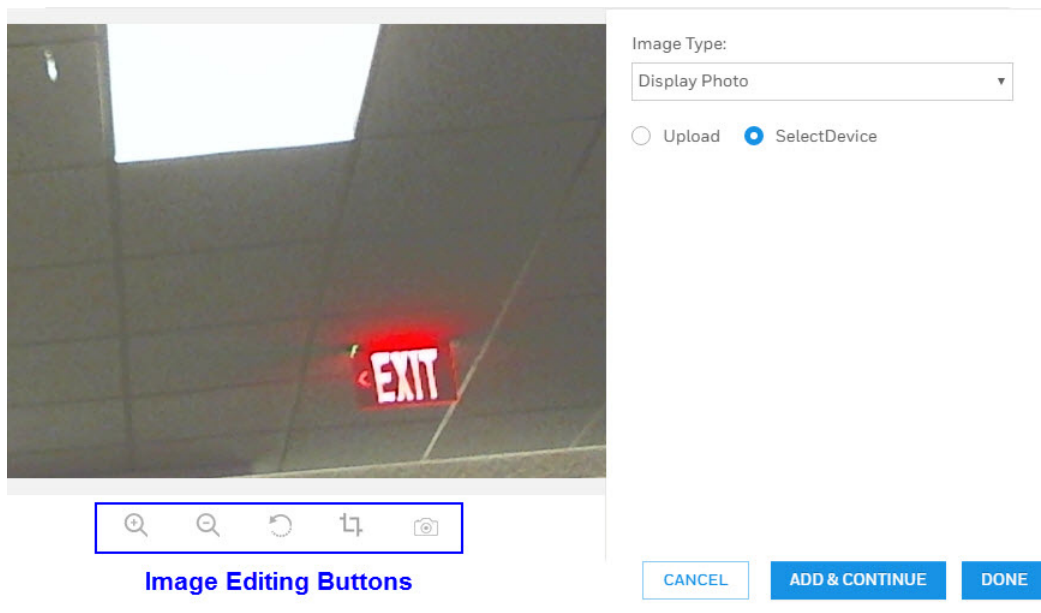


Image Type:
Display Photo

☐ Upload ☒ SelectDevice

Image Editing Buttons

CANCEL ADD & CONTINUE DONE

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 display 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**.

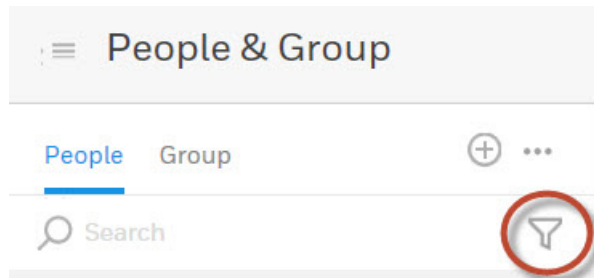
2.14.5 Searching for a Badge

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**.

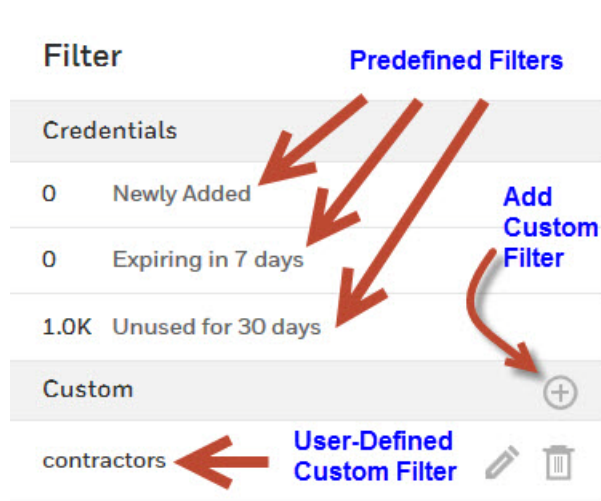
The system will either return the badge you are searching for, or, if there are more than one badges that satisfy the search criteria, it will return multiple results. You can select the one you like.

2.14.6 Advanced Search Filters

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

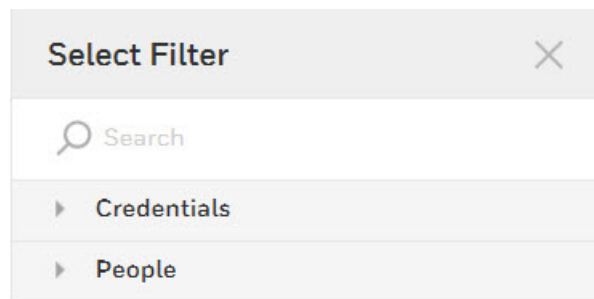


Clicking the filter icon will display a list of **predefined** (but configurable) and **user-defined custom** filters:



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:


▼ Credentials
<input type="checkbox"/> Card Number
<input type="checkbox"/> Card Status
<input type="checkbox"/> Company
<input type="checkbox"/> Card Type

▼ People
<input type="checkbox"/> First Name
<input type="checkbox"/> Last Name
<input type="checkbox"/> Issue Date
<input type="checkbox"/> Expire Date

The variables you've selected will be displayed on the Filter profile:

☰

People & Group


Filter 

First Name


Last Name


Card Number


Company

All Access 

Card Type

Contractor 

Select Filter 

 Search

▼ Credentials

☒ Card Number

☐ Card Status

☒ Company

☒ Card Type

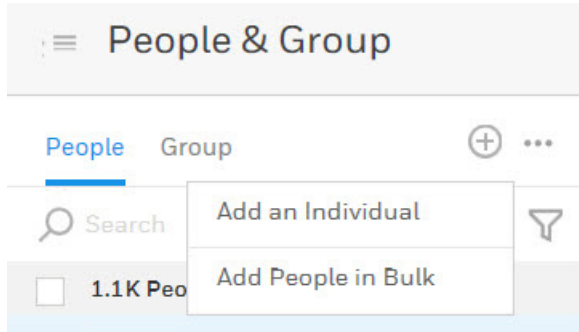
► People

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:



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

Add People: Bulk

Number of People *	Card Number *
<input type="text"/>	<input type="text" value="Enter the starting card number"/>
Employee Type *	Partition
<input type="text" value="Select"/>	<input type="text"/>
Access Group *	<input checked="" type="checkbox"/> Download Cards
<input type="text"/>	
Validity <input type="checkbox"/>	

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

OK

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

Credential Number*

Card Number required

Credential Status*

Active

Type*

Select

PIN

Type or generate

PIN Verify

Permissions

Access Group*

Additional Rights

CANCEL

ADD

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 83 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

CANCEL ADD

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

Employee Address **Credentials** Assets Activity Log

345345 Expires on 05/30/2018

345435 Expires on 05/09/2019

ADD NEW CREDENTIAL

Credential Details Permissions

Credential Number Status

345345 Select

PIN


1272


View More

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:

[View Less](#)

Validity ☒

Activate 05/18/2018 15:59:59 

Deactivate 05/30/2018 15:59:59 

Last Access

Last Reader

User Level 0

Disable Card (Days) 0

☐ Use Counts


No Of Attempts 0

Parade Text

Card Notes

☐ ADA ☐ Trace Card ☐ PIN Exempt ☐ VIP ☐ Guard

Create Date 05/17/2017 09:34:06

Return Date Select 

Card Number Extension

Last Print Date

Print Count 0

10. Enter the appropriate values into all the card fields displayed in the above screens. See Table 2-1 on page 83 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. The “extended shunt time” needed is set up on the PW-5000 door configuration.
Card Number Extension	Enter an extended card number, if any.
Credential Number	Card number entered by the user.
Credential Status	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.
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.

Credential Field	Description
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.

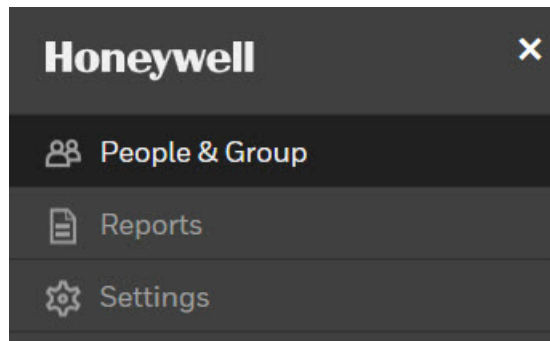
12. Click the **Save Card** button to save the new card. Click **Cancel** not to save the new card.

2.14.10 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.

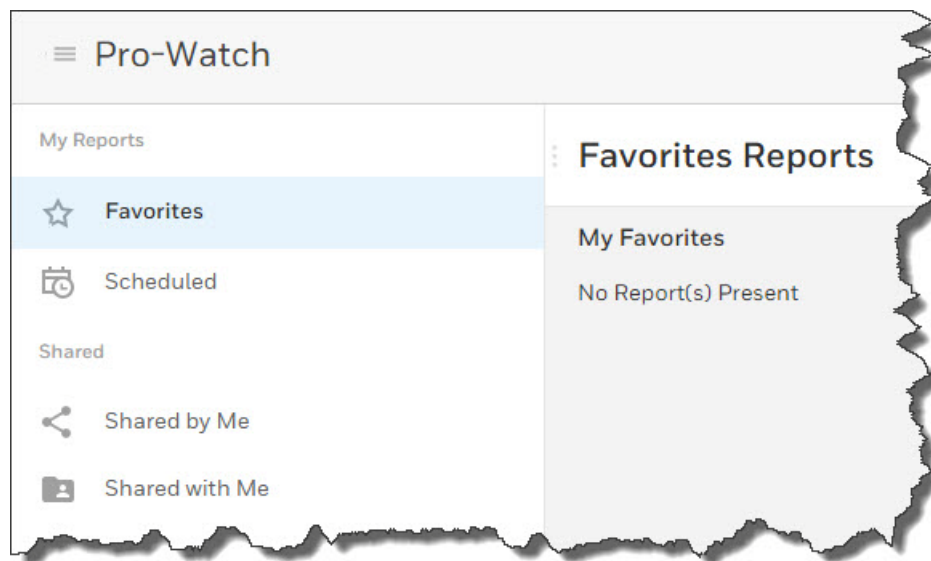
2.15 Reporting

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

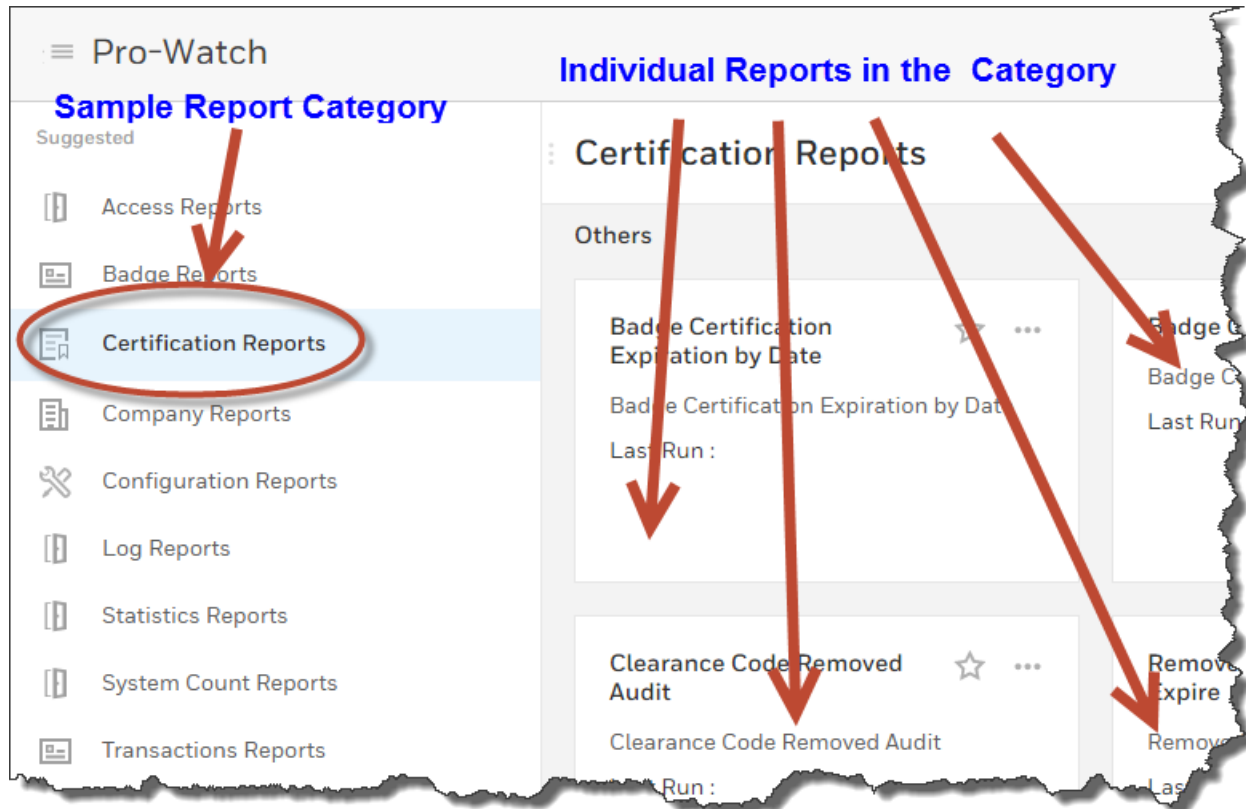
If you have more than 20,000 rows per report, the report export behavior may change depending on your system setup.

2.15.3 Add, Edit or Delete a Report

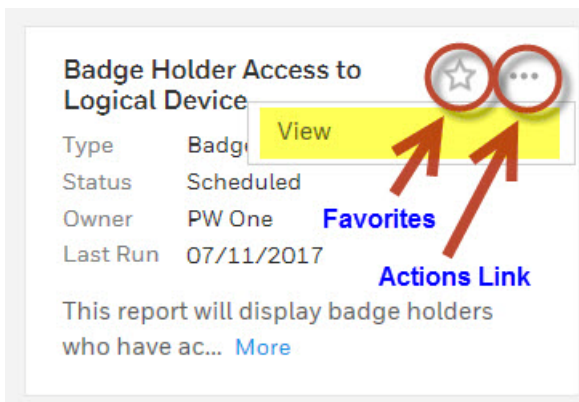
You cannot create a new report, edit or delete an existing report from inside the thin web client. However, you can view the sample reports created in Pro-Watch thick client.

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**:



Badge Holder Access to Logical Device

Type : Badge Owner : Rinas A Last Run : 05/17/2017 08:55 AM

Runtime Filters - Enter Values

1	Last Name	Begins With	%
2	First Name	Begins With	%
3	Card Number	Begins With	%
4	Company	Begins With	%
5	Logical Device	Begins With	%
6	ClearanceCode	Begins With	%

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

Export Type	Row and Column Sizing
PDF	None

☒ 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

Pro-Watch

Search

People & Group

Reports

General

Card Activity Log (Days)

30

Define Card Usage Filters

Fields

Show Data for

☒ Newly Added
In the last 5 days

5 Days

☒ Expiring
In 5 Days

Today This Weekend 5 Days

☒ Unused
In the last 5 days

5 Days

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

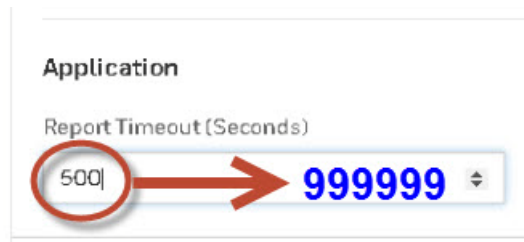
2.16.2.1 Reports General Settings

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

The screenshot shows the Pro-Watch Web Client interface. The top navigation bar includes a search bar and a pencil icon circled in red. The left sidebar has 'People & Group' and 'Reports' (selected). The main content area has tabs for 'General' and 'Email'. Under 'Branding', there are two boxes: 'ADD WATERMARK' and 'ADD LOGO'. Under 'Output Settings', there are sections for 'Print' (with checkboxes for Report Header, Report Footer, and Report Filter) and 'Display' (with radio buttons for Portrait and Landscape, and checkboxes for Row Number and Alternate Row Color). At the bottom right are 'CANCEL' and 'SAVE' buttons.

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.

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



Application

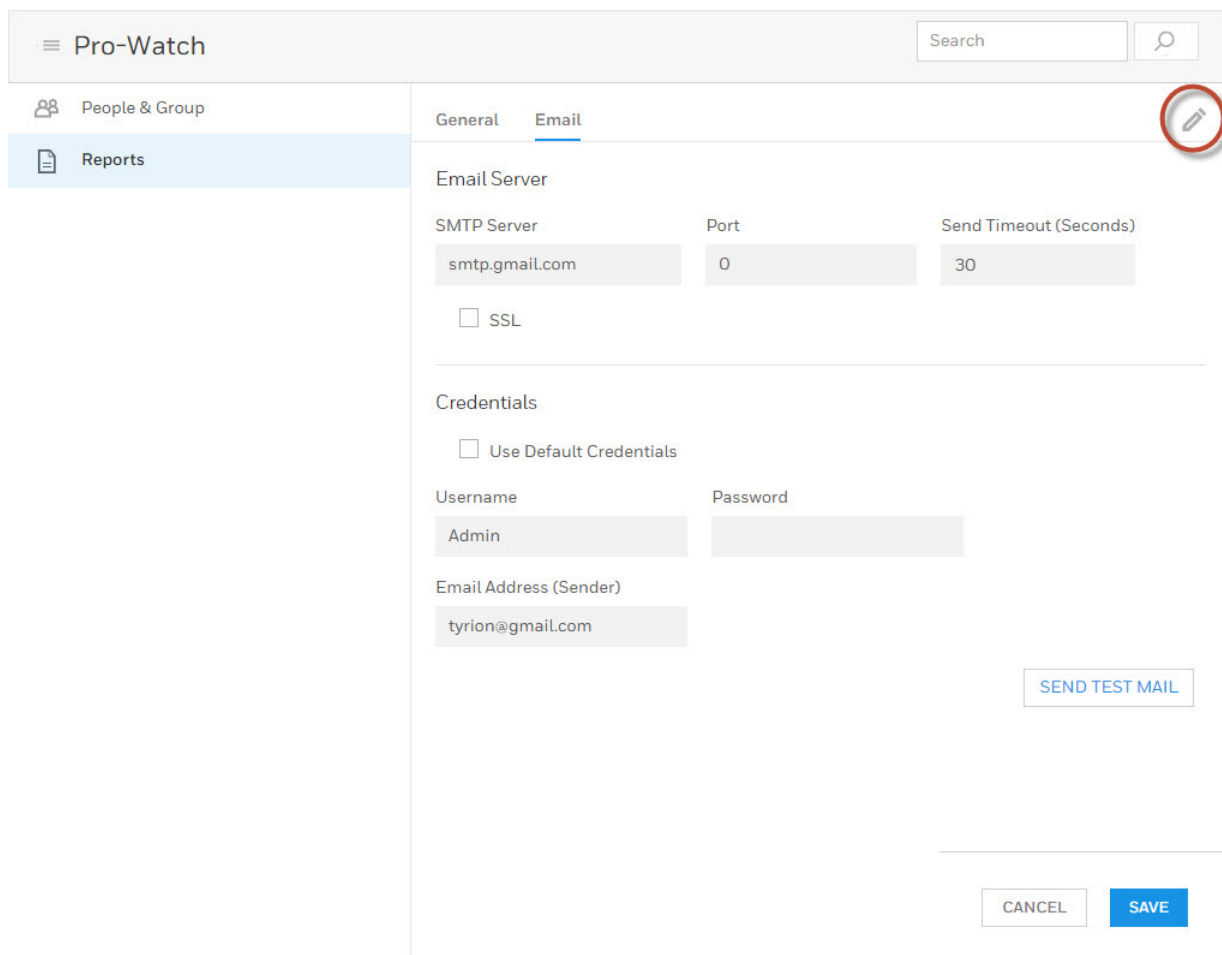
Report Timeout (Seconds)

500 → 999999

- Click **Save**.

2.16.2.2 Reports Email Settings

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



Pro-Watch

Search

People & Group

Reports

General Email

Email Server

SMTP Server smtp.gmail.com Port 0 Send Timeout (Seconds) 30

☐ SSL

Credentials

☐ Use Default Credentials

Username Admin Password

Email Address (Sender) tyrion@gmail.com

SEND TEST MAIL

CANCEL SAVE

- Click the **pencil icon** on the upper-right to launch the edit mode.
- Enter the appropriate values for **SMTP Server, Port, Send Timeout (Seconds)** fields.
- 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** link to send yourself a test email.
8. Click **Save**.

(This page is left blank intentionally for double-sided printing.)



Troubleshooting

A

In this appendix ...


[Introduction](#)

[Steps to Follow](#)

A.1 Introduction

This chapter describes what to do if you get the below “**Your connection is not private**” warning message and you are not able to proceed.

It is always recommended to use a purchased certificate but if you want to continue with a self-signed certificate, follow the procedure explained to overcome the below issue.



Your connection is not private

Attackers might be trying to steal your information from **ie3piw8jkr542** (for example, passwords, messages, or credit cards). NET::ERR_CERT_INVALID

☐ [Automatically report](#) details of possible security incidents to Google. [Privacy policy](#)

HIDE ADVANCED

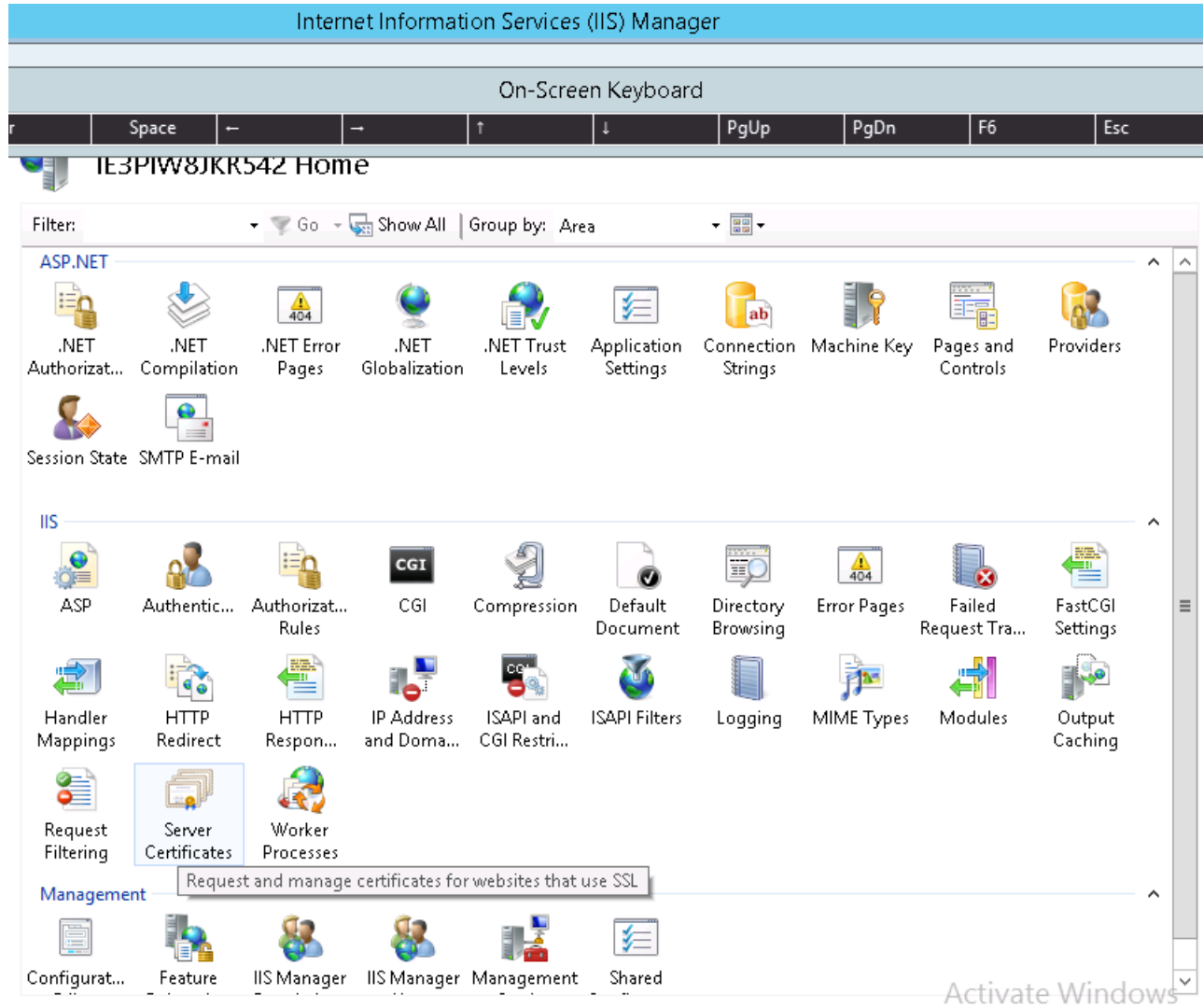
Reload

ie3piw8jkr542 normally uses encryption to protect your information. When Google Chrome tried to connect to ie3piw8jkr542 this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be ie3piw8jkr542, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

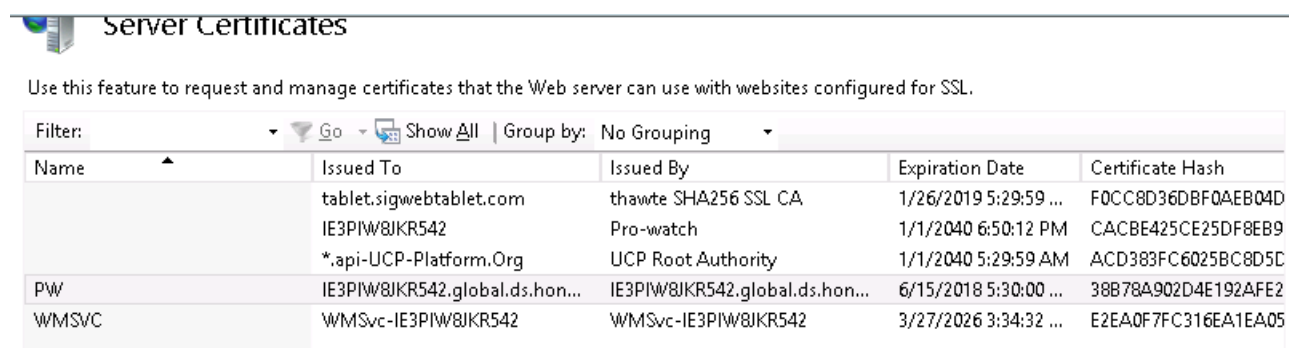
You cannot visit ie3piw8jkr542 right now because the website sent scrambled credentials that Google Chrome cannot process. Network errors and attacks are usually temporary, so this page will probably work later. [Learn more](#).

A.2 Steps to Follow

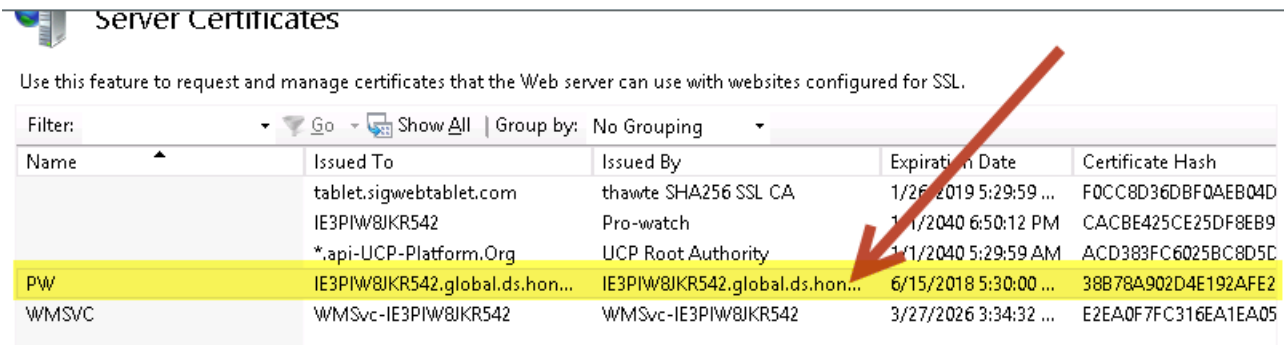
1. Go to IIS:



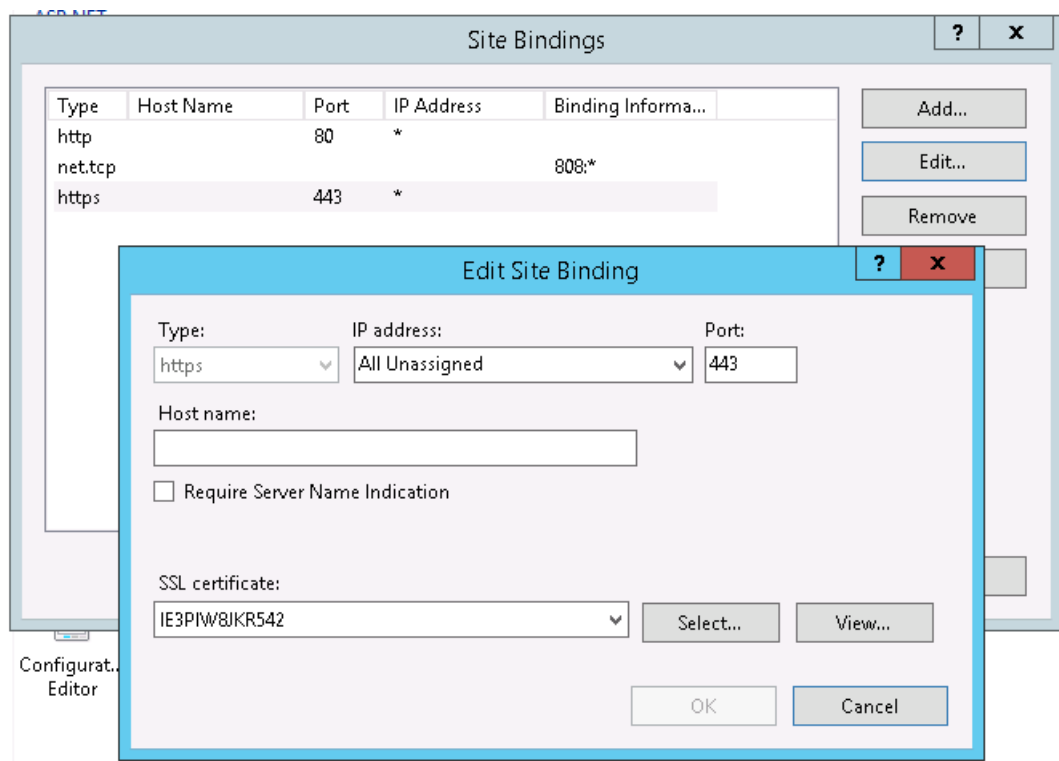
2. Click **Server Certificates** to display the **Server Certificates** screen:



3. Display the **Site Bindings** screen by clicking on the default site:



4. Click the **Edit** button to display the **Edit Site Bindings** screen:



5. Enter **"PW"** into the **SSL Certificate** field. Or click **Select** and select the PW certificate.

6. Click **OK**.

Index



A

- audience** 3
- authentication**
 - token-based 19
 - Windows 11

B

- badging** 60
- browser**
 - configure 45
 - mode 46
 - support 36

C

- configuring the browser** 45

D

- dynamic IP restrictions** 33

F

- features** 60

H

- home page** 54

I

- IE9 security settings** 42
- installing** 7

L

- login** 52

M

- modules** 60
- moving PW components** 19, 25

P

- permissions**
 - workstations 10
- prerequisites** 36
- Pro-Watch**
 - moving components 19, 25
 - Web Client Login 52

R

- reports** 83
 - settings 88
- restrictions**
 - dynamic IP 33

S

screen

resolution 36

size 36

settings 87

advanced 37

badging 87

reports 88

security 37

security for IE8 37

temp Internet files 45

supported web browsers 36

T

troubleshooting 91

U

user

workstation permissions 10

W

web client

installing 7

workstations 10

(This page is left blank intentionally for double-sided printing.)

Honeywell Security and Fire

EMAAR Business Park Building 2,
Level 2, Office 201 Sheikh Zayed Road,
P.O. Box: 232362, Dubai, U.A.E.
Telephone: +971 4 4505800
www.honeywell.com

Honeywell