Honeywell

Pro-Watch Intelligent Command

5.0

800-24386V5 | May 2020

Installation Guide

Disclaimer

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

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

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

Copyright © 2020 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

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

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

Copyright © 2020 Honeywell. All rights reserved.

Pro-Watch® is a registered trademark of Honeywell Integrated Security. 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.

XPSMTP - Copyright © SQLDev.Net 1991-2006 (<http://SQLDev.Net>)
All rights reserved.

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.

Neither the name of SQLDev.Net nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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.

Modified redistributions of source code, binaries and/or documentation must carry the above copyright as required by clauses (1) and (2) and may retain the name "SQLDev.Net" in source code, documentation and metadata.

The name "SQLDev.Net" is a trademark of SQLDev.Net B.V. the Netherlands.

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 Integrated Security representative or visit us on the web at http://www.honeywellintegrated.com/ for information about ordering.

Feedback

Honeywell Integrated Security appreciates your comments about this manual. Please visit us on the web at http://www.honeywellintegrated.com/ to post your comments.

TABLE OF CONTENTS

1.1 Introduction **1**
1.1.1 Purpose of this Document 1
1.1.2 Warning: Personal Data 1
1.1.3 Compliance 2
1.1.4 Audience 2
1.2 Operating Systems Supported by Pro-Watch Intelligent Command **2**
1.3 Important Notes Before You Begin **2**
1.3.1 No Upgrade Support 3
1.3.2 Badge Photos 4
1.3.3 Warning: Personal Data 4
1.4 Pro-Watch Intelligent Command Installation Prerequisites **4**
1.5 Pro-Watch Intelligent Command Prerequisites Download Link **7**
1.5.1 Dot Net FrameWork 4.7.1 7
1.5.2 Dot Net FrameWork 4.8 7
1.5.3 Dot Net Core Hosting Bundle 2.2.5 7
1.5.4 Dot Net Core Hosting Bundle 3.1.1 7
1.5.5 VC++ 2010 (x86) redistributable 7
1.5.6 VC++ 2010 (x64) redistributable 7
1.5.7 VC++ 2013 redistributable 7
1.5.8 VC++ 2015-2019 redistributable 7
1.5.9 SQL Native Client 11 7
1.5.10 Re-Write Software (rewrite_amd64_en-US.msi) 7
1.6 Installing Pro-Watch Intelligent Command (IC) 5.0 ..... **8**
1.6.1 All in One Box/Machine (All tiers installation model) 9
1.6.2 Application Tier Installation 11
1.6.3 Core Tier Installation 14
1.6.4 Web Tier Installation 16
1.7 Domain User Credentials **19**
1.8 Pro-Watch DB Credential **20**
1.9 Click Install to Proceed with Installation **21**
1.10 Importing and Exporting SSL Certificate **22**
1.10.1 In Web Tier Machine 22
1.10.2 In Core Service Installed Machine 23

Appendix Troubleshooting the Web Client Installation

A.1 Different Scenarios **24**
A.2 Dynamic IP Restriction Configuration **25**
A.2.1 Introduction 25
A.2.2 Installation of IP and Domain Restrictions 26
A.2.3 Configuring Dynamic IP Restrictions for Web Application 26
A.2.4 Pro-Watch Three Tier Deployment 27

Honeywell

Pro-Watch Web Installation

1

1.1 Introduction

1.1.1 Purpose of this Document

The Pro-Watch Intelligent Command Guide provides the procedures and information necessary to install Pro-Watch Intelligent Command application on below recommended Microsoft Windows operating systems:

- Microsoft Windows operating systems
- Windows Server 2012/2012 R2
- Windows Server 2016
- MS Server 2019
- Windows 10 Professional Build 1607

1.1.2 Warning: Personal Data

Please be aware that this product can store personal data.

Personal data is protected by the General Data Protection Regulation (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to comply with regarding the use and distribution of this data.

Further details can be found on the GDPR website of the EU:

https://ec.europa.eu/commission/priorities/justice-

1.1.3 Compliance

To obtain applicable EU compliance Declaration of Conformities for this product, please refer to our website:

http://www.security.honeywell.com/hsce/international/index.html.

For any additional information regarding the compliance of this product to any EU-specific requirements, please contact:

Honeywell Security & Communications

Honeywell Security - Quality Assurance Dept., Newhouse Industrial Estate

Motherwell

Lanarkshire ML1 5SB

Scotland

United Kingdom

Tel: +44(0) 1698 738200

Email: UK64Sales@Honeywell.com

1.1.4 Audience

This guide is written for the Pro-Watch system administrator who installs the Pro-Watch Intelligent Command software on local machines.

1.2 Operating Systems Supported by Pro-Watch Intelligent Command

- Windows 10 build 1607 and higher
- Windows Server 2012/2012 R2
- Windows Server 2016
- MS Server 2019

1.3 Important Notes Before You Begin

a. Upgrading to Pro-Watch 5.0 requires a minimum SQL version of SQL 2012.

b. Pro-Watch 5.0 requires a new license when upgraded from a previous version.

c. If you are using SQL Server 2012 , then set compatibility level of Pro-Watch Database to >= 100. Please use below steps to SQL script to set Compatibility level:

i) Open Sql Server Management studio

ii) Click New Query

iii) Select Pro-Watch Database. By default it will be "PWNT"

iv) Execute below SQL script:

```
ALTER DATABASE PWNT SET COMPATIBILITY_LEVEL = 110;
```

d. Please set Power-Shell execution policy in windows before installing PWIC.Please refer below steps

   i) Open Powershell as administrator

   ii) Run below command:

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine

e. The Pro-Watch API is not backwards compatible with Pro-Watch. API version 5.0.0.174 released with Pro-Watch 5.0 will not work with prior versions of Pro-Watch.

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.

f. In 3 tier deployment, **it is highly recommended** to configure administrative share for **Application TIER machine to store & access MAPS from Web TIER machine.**

   Please find below the instructions to configure administrative share for specific user

   i. In Application Tier Machine , Right-click the OS drive (Example: C drive) and select Properties.

   ii. In the Properties box, select the Security tab and verify that the Administrator's group has full privileges.

   iii. To set up OS drive sharing with a specific account, select Sharing and click Advanced Sharing.

   iv. Share this folder, provide a share name, and set user permissions.

1.3.1 No Upgrade Support

Upgrade Scenario for Web: There is no upgrade support for Web installations.

(1) User must un-install all the web components including the following:

- **Authentication Authorization Service**
- **Thinktecture Identity Service**
- **Pro-Watch WEBUI**
- **Pro-Watch Web Services**
- **Pro-Watch Event Service**

(2) After Un-Installation, User must ensure that Web related residual files are deleted from installed folder ,If not please delete the folders manually.

Example:

If user installed in C:\Program Files (x86)\ then delete below folders:

C:\Program Files (x86)\Honeywell\UnifiedSecurityPlatform

C:\Program Files (x86)\Honeywell\ThinktectureIdentityService

C:\Program Files (x86)\Honeywell\AuthenticationAuthorizationService

(3) Reboot the system.

(4) Then you must re-install 5.0 Web components, which will install Thinktecture and Auth & Auth freshly along with Web components.

1.3.2 Badge Photos

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

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

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

1.3.3 Warning: Personal Data

Please be aware that this product can store personal data.
Personal data is protected by the **General Data Protection Regulation** (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to obey regarding the use and distribution of this data.

Further details can be found on the **GDPR website of the EU** (https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).

1.4 Pro-Watch Intelligent Command Installation Prerequisites

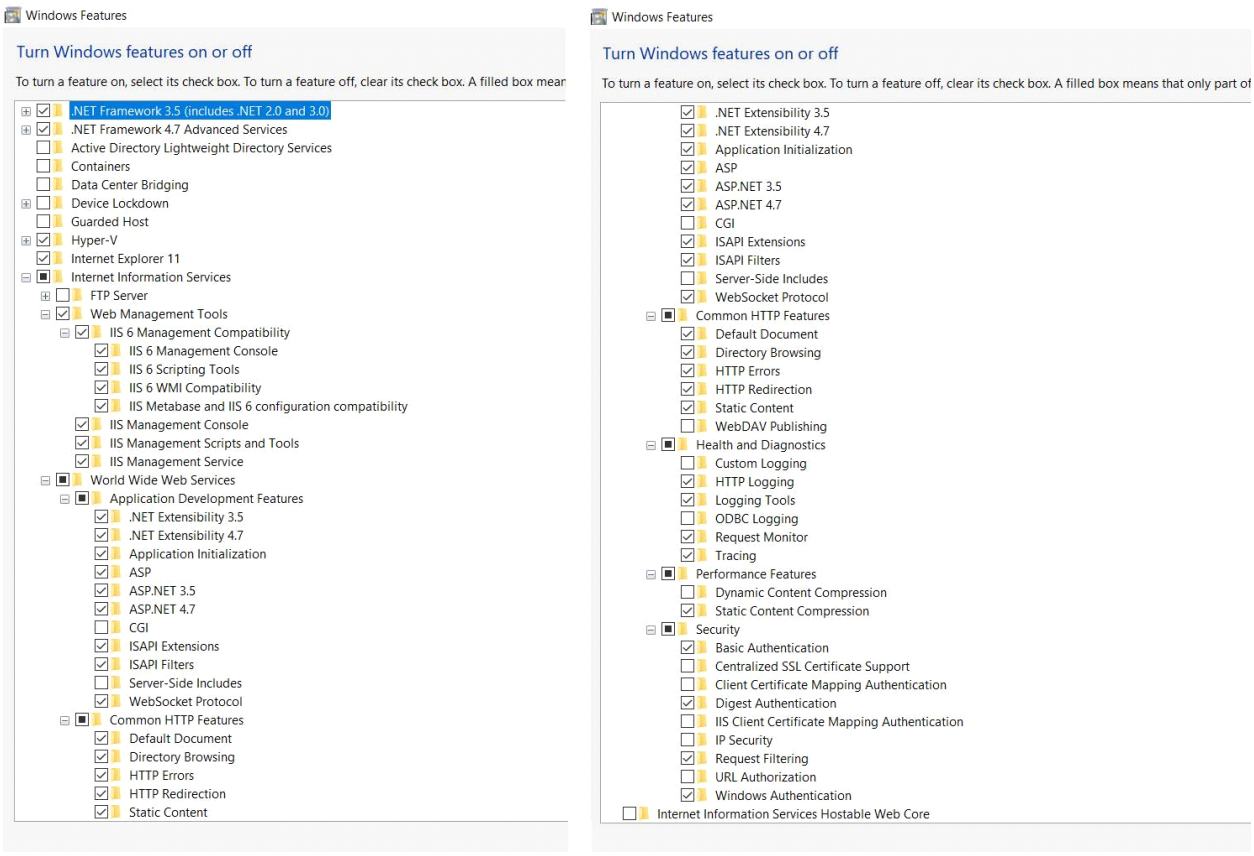
The following prerequisites should be available in any target machine for the installer to continue and install successfully.
Installer will exit if any of the prerequisites is not available.

1. Turn ON the following Windows IIS features:
   - IIS Metabase
   - IIS Web Socket
   - IIS Application Initialization
   - IIS 6 WMI Compatibility
   - IIS Windows Authentication
   - IIS Basic Authentication

- IIS 6 Scripting Tools
- IIS 6 Management Console
- IIS Management Console
- IIS Management Scripts and Tools
- IIS Management Service
- IIS ASP.Net
- IIS Http Errors
- IIS Static Content
- IIS .NET Framework
- IIS Digest Authentication
- IIS Tracing
- IIS Request Monitor
- IIS Logging Tools
- IIS HTTP Logging
- IIS Directory Browsing
- IIS HTTP Redirection
- IIS Static compression

Note: Disable WebDAV settings in IIS.

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



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

4. Make sure Pro-Watch NVR, Pro-Watch VMS and Pro-Watch Core are installed.

1.5 Pro-Watch Intelligent Command Prerequisites Download Link

1.5.1 Dot Net FrameWork 4.7.1

https://www.microsoft.com/en-us/download/details.aspx?id=56116

Minimum Version: 4.7.02558

1.5.2 Dot Net FrameWork 4.8

https://support.microsoft.com/en-in/help/4503548/microsoft-net-framework-4-8-offline-installer-for-windows

Minimum Version: 4.8.3928

1.5.3 Dot Net Core Hosting Bundle 2.2.5

https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-aspnetcore-2.2.5-windows-hosting-bundle-installer

Minimum Version: 2.2.5.0

1.5.4 Dot Net Core Hosting Bundle 3.1.1

https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-aspnetcore-3.1.1-windows-hosting-bundle-installer

Minimum Version: 3.1.1.19615

1.5.5 VC++ 2010 (x86) redistributable

https://www.microsoft.com/en-in/download/details.aspx?id=5555

Minimum Version: 10.0.40219

1.5.6 VC++ 2010 (x64) redistributable

https://www.microsoft.com/en-in/download/details.aspx?id=14632

Minimum Version: 10.0.40219

1.5.7 VC++ 2013 redistributable

https://www.microsoft.com/en-in/download/details.aspx?id=40784

It is recommended to install both X86 & x64 versions of VC++ 2013 redistributable.

Minimum Version: 12.0.30501.0

1.5.8 VC++ 2015-2019 redistributable

https://support.microsoft.com/en-in/help/2977003/the-latest-supported-visual-c-downloads

It is highly recommended to install both x86 & x64 versions of VC++ 2015-2019 redistributable.

Minimum Version: 14.24.28127.4

1.5.9 SQL Native Client 11

https://www.microsoft.com/en-us/download/details.aspx?id=50402

Minimum Version: 11.4.7001.0

1.5.10 Re-Write Software (rewrite_amd64_en-US.msi)

https://www.microsoft.com/en-us/download/details.aspx?id=47337

Minimum Version: 7.2.1993

1.6 Installing Pro-Watch Intelligent Command (IC) 5.0

Complete the following steps to setup Pro-Watch Intelligent Command 5.0.

1. Run "**Pro-Watch Intelligent Command.exe**" as Administrator.
2. Accept the **Licensing Agreement** to proceed further with the installation:

3. Pro-Watch Intelligent Command installer will support all in one-box and Multi-Tier architecture deployment model.

   For Multi-Tier deployment, Installation should run in sequence order as below

   i. Application Tier

   ii. Core Services

   iii. Web Tier

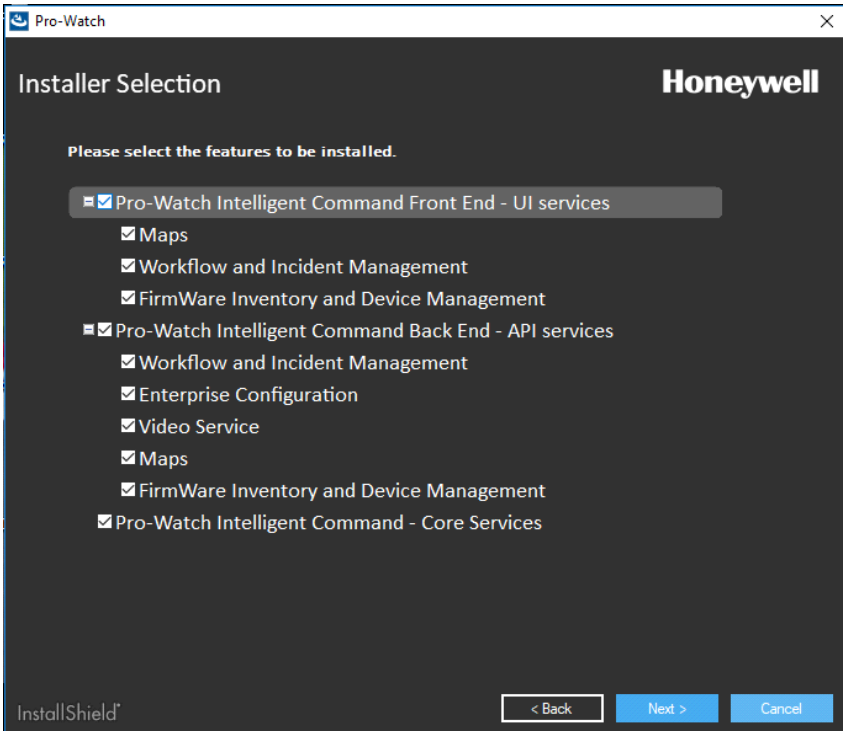
Choose below Tiers for your environment.

i. Pro-Watch Intelligent Command Front End - UI services,

ii. Pro-Watch Intelligent Command Back End - API services &

iii. Pro-Watch Intelligent Command - Core services

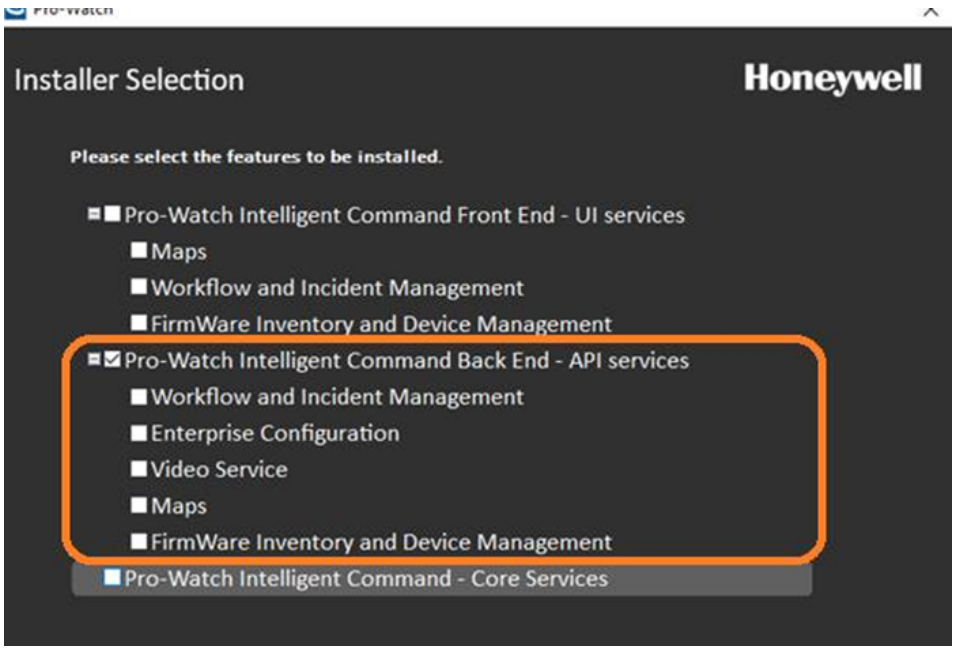
1.6.1 All in One Box/Machine (All tiers installation model)



Select all the tiers.

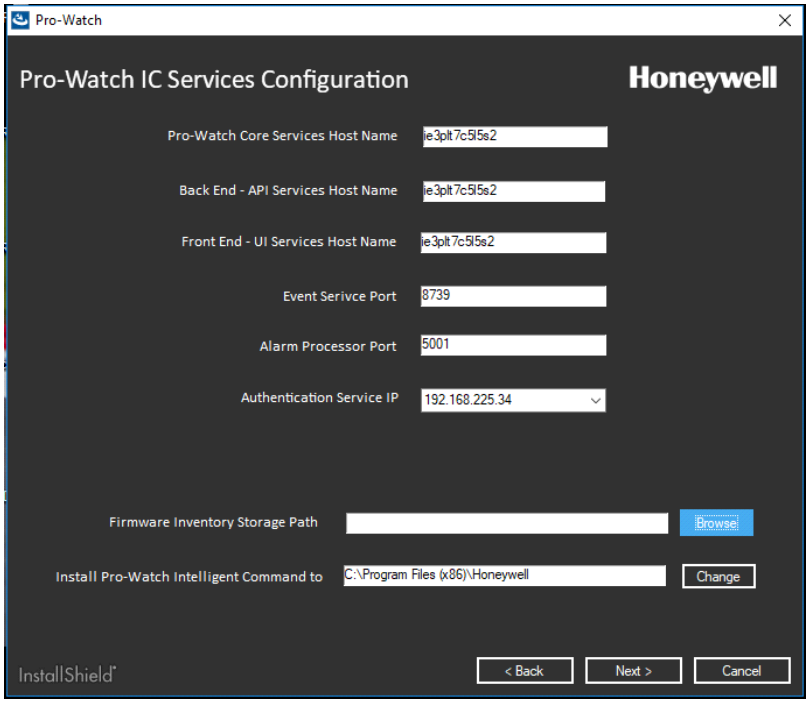
Note: The installer must individually unselect those licensed features that will not be used. For example, here is an example below where the head

element “Pro-Watch Intelligent Command Back End - API Service” is selected but none of its sub-head elements:



1.6.1.1 Service Configuration for All in One box/Machine

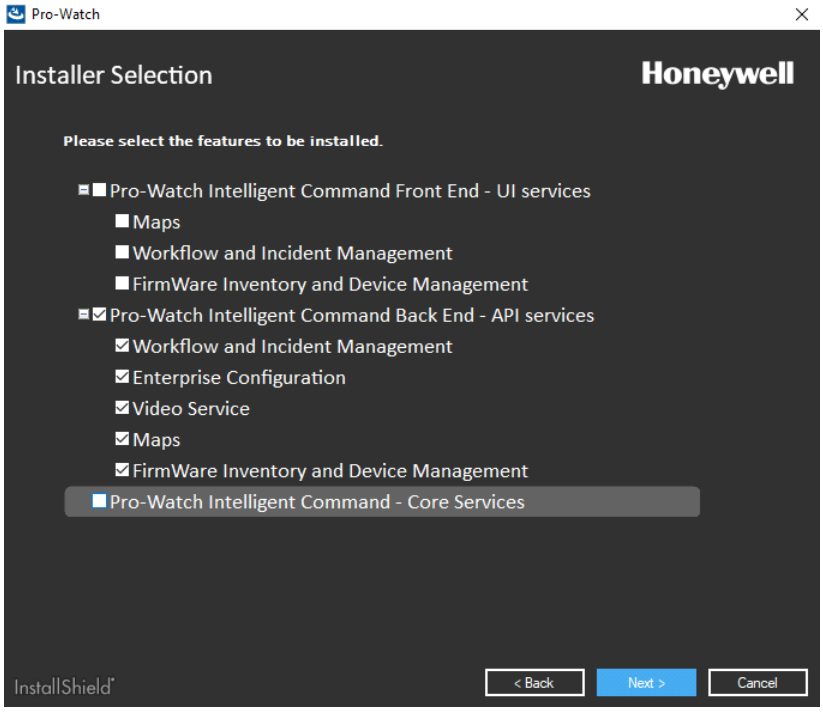
Based on All Tiers selection, service address settings automatically populate the default host name and default port values for servers. Choose firmware folder path and that should have Read/Write permission.



Note: Firmware path must exist and the service user must have the file with read/write access to that path.

Please continue installation from Step 4.

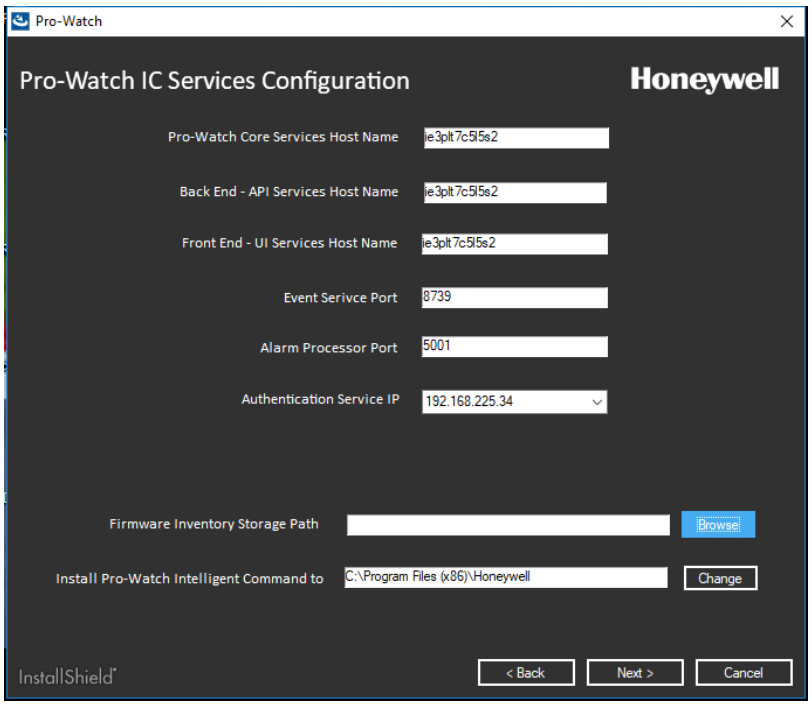
1.6.2 Application Tier Installation



Note: The User must have the shared folder for installing the Maps, so that they can configure the Maps generator utility from App tier to Web tier.

1.6.2.1 Service Configuration for Application tier

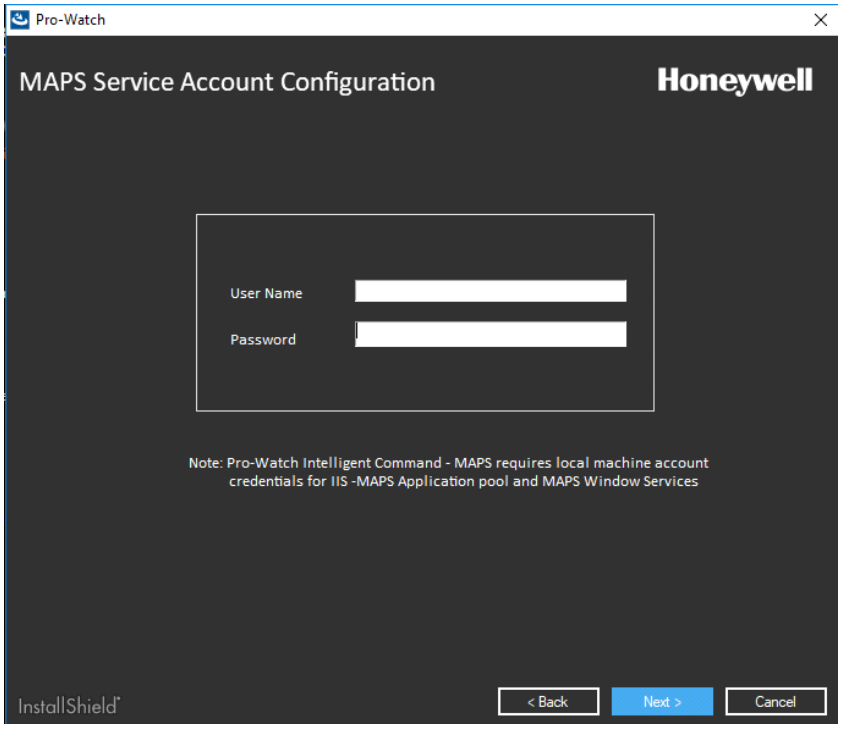
Based on Application Tier selection, service address settings automatically populate the default host name and default port values for servers. Choose firmware folder path and make sure that it has Read/Write Permission.



Note: Firmware path must exist and the service user must have the file read/write access to that path. If user provides local system path for Firmware files storage during installation, then it is highly recommended to provide local system path outside the web root folder for better security.

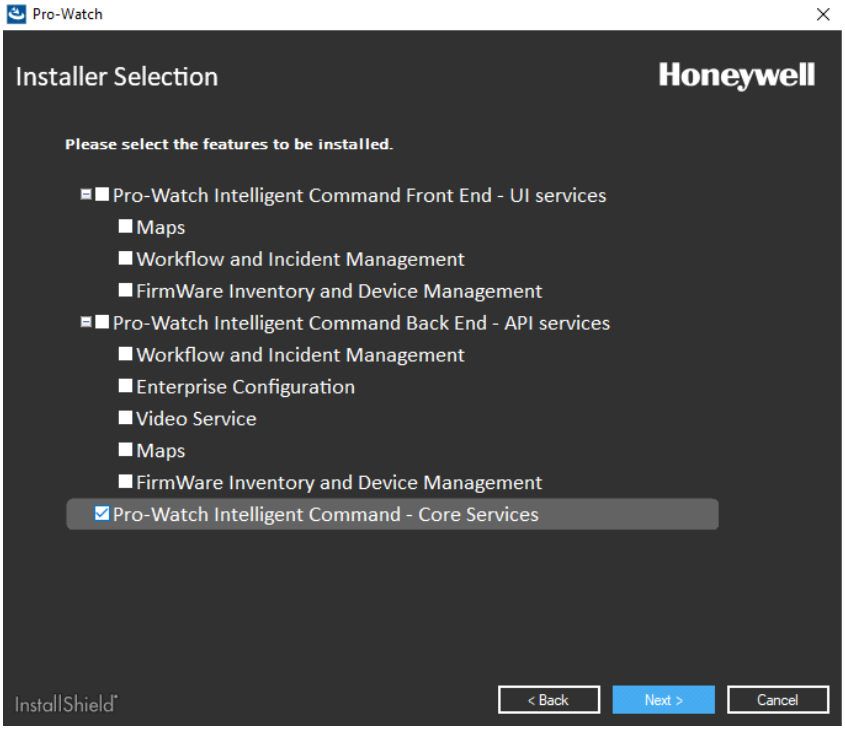
1.6.2.2 Maps Service Configuration for Application Tier

Map service requires local machine account credentials for IIS maps application pool and maps windows service.



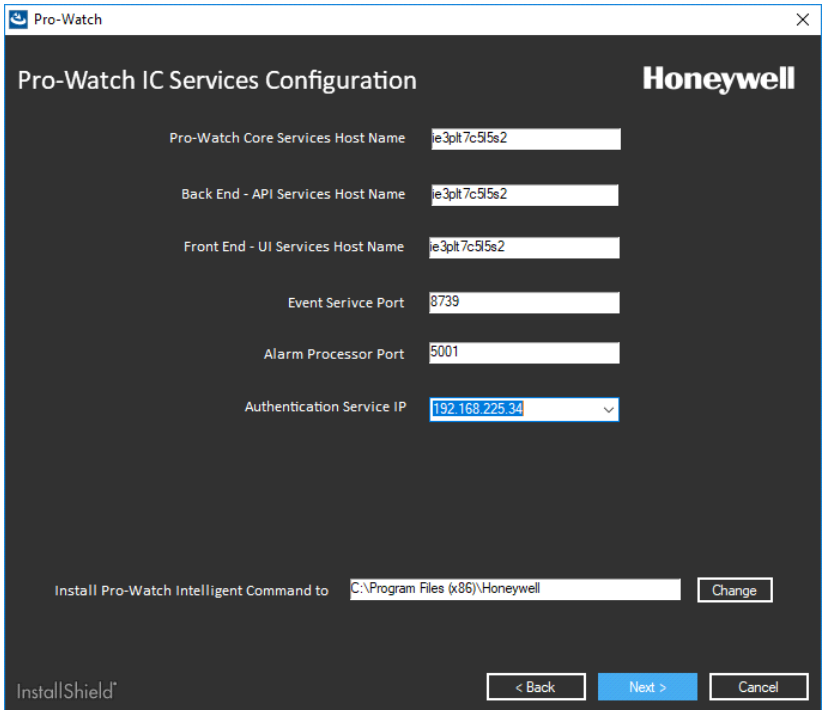
Please continue installation from Step 1.6.

1.6.3 Core Tier Installation



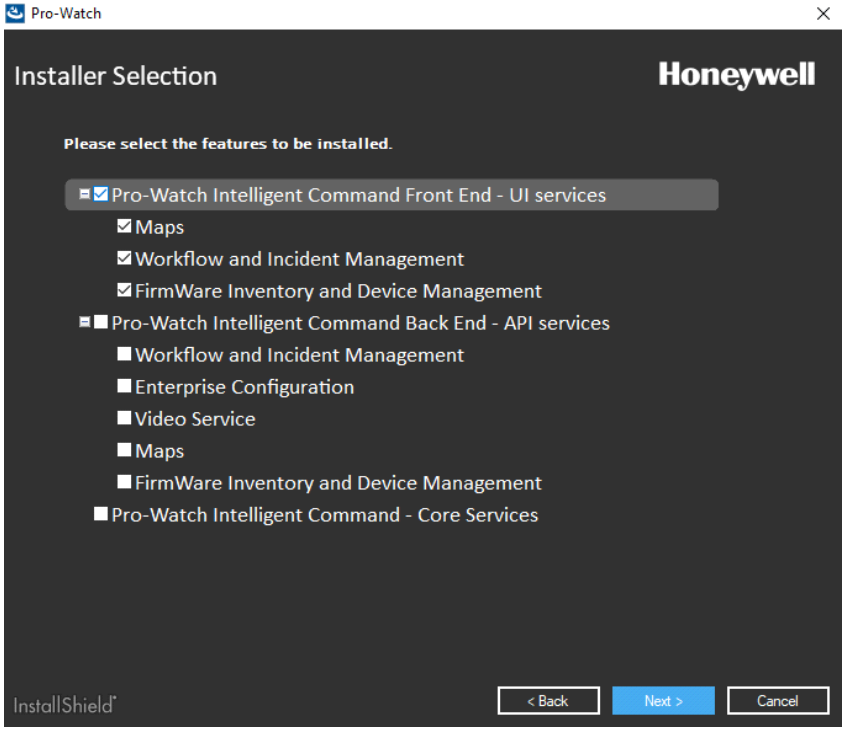
1.6.3.1 Service Configuration for Core Tier

Based on Core Tier selection, service address settings automatically populate the default host name and default port values for servers.



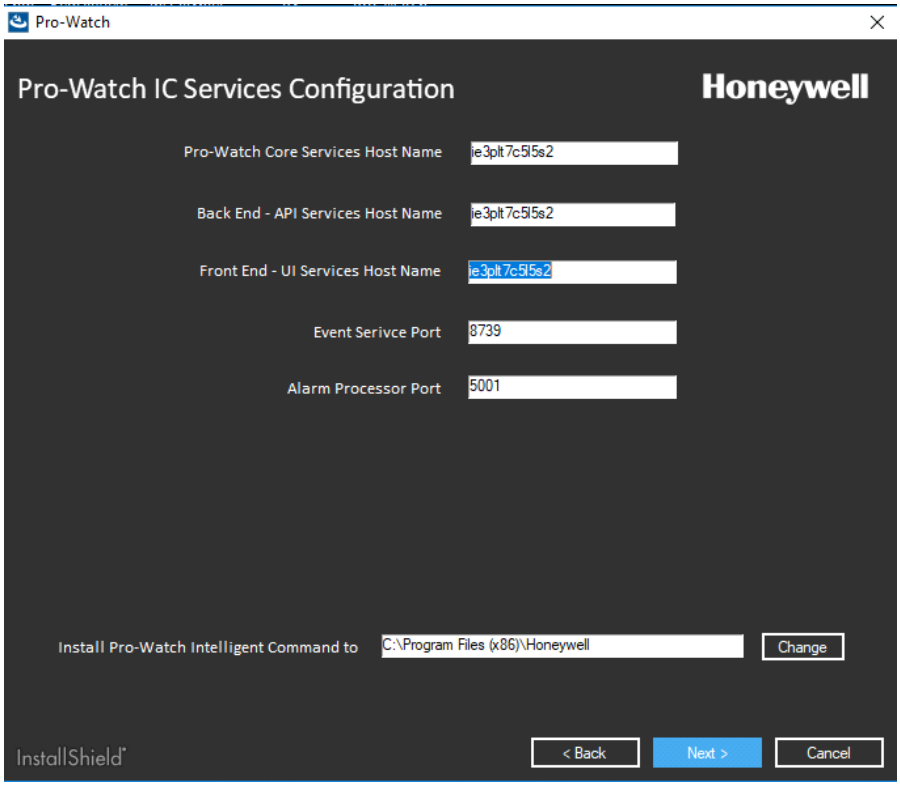
Please continue installation from Step 1.6.

1.6.4 Web Tier Installation



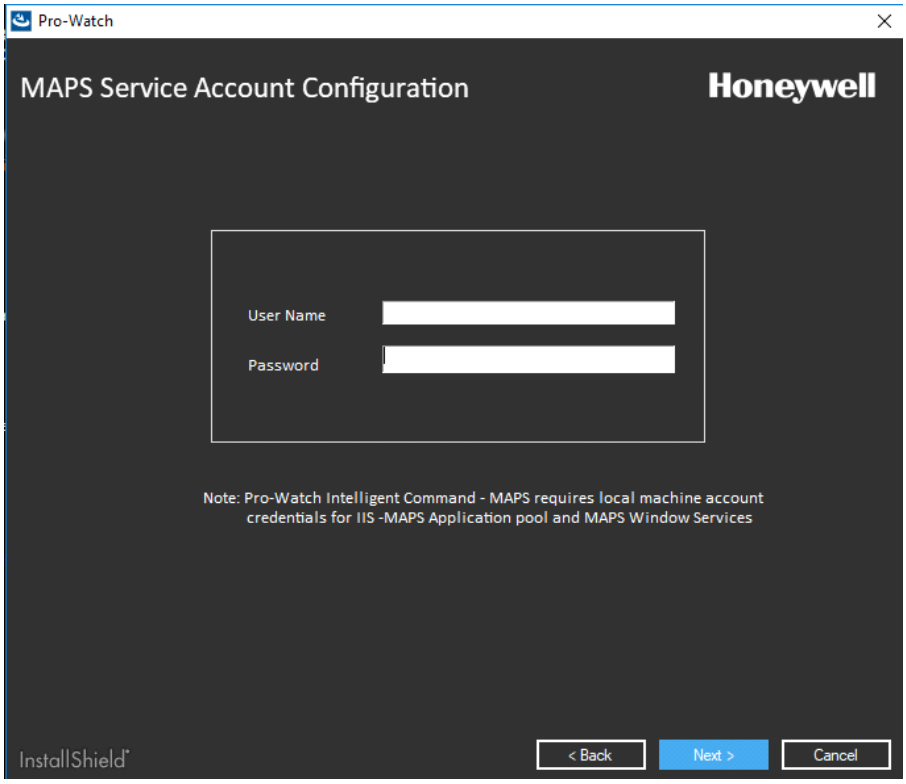
1.6.4.1 Service Configuration for Web Tier

Based on Web Tier selection, service address settings automatically populate the default host name and default port values for servers.



1.6.4.2 Maps Service Configuration for Web Tier

Map service requires local machine account credentials for IIS maps application pool and maps windows service.



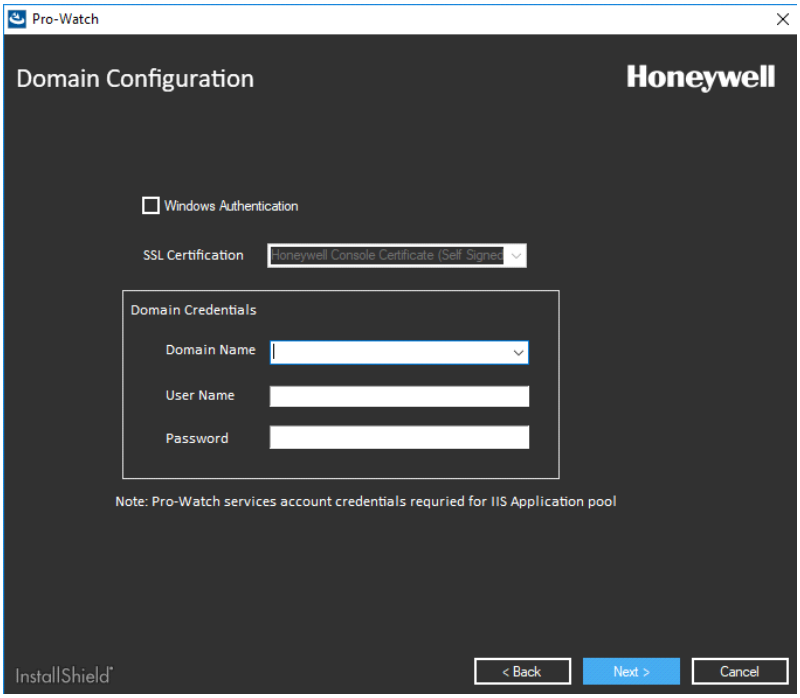
1.7 Domain User Credentials

SSL Certification is read only and it will generate Self signed certificate.

Installer will get the User Credentials for IIS Settings

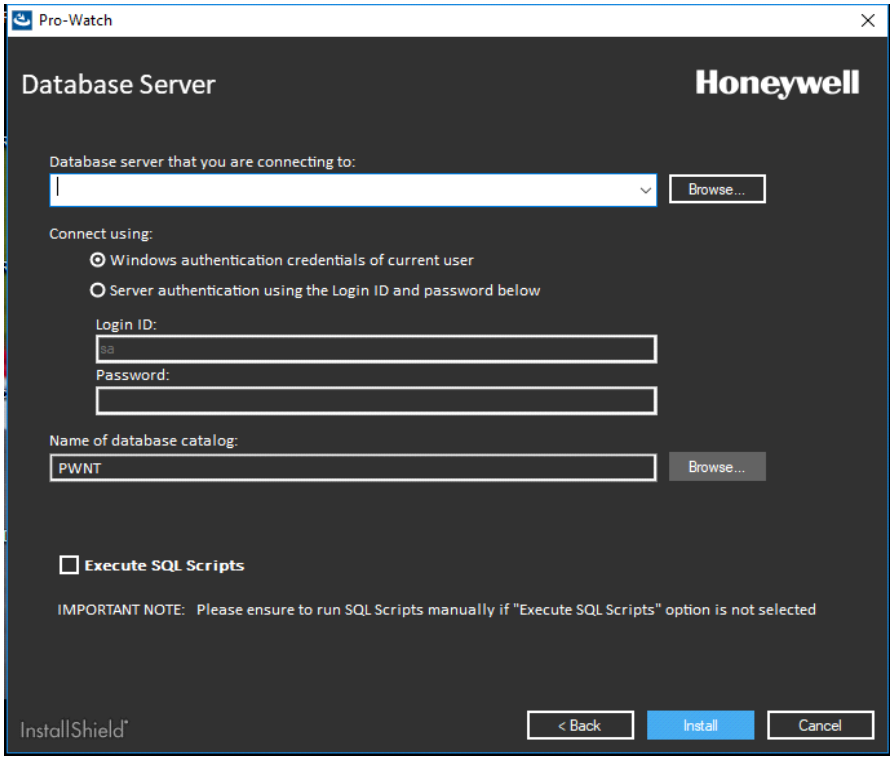
i. The account must be a part of the admin group in installing machine.

ii. The account must be a part of Pro-Watch.



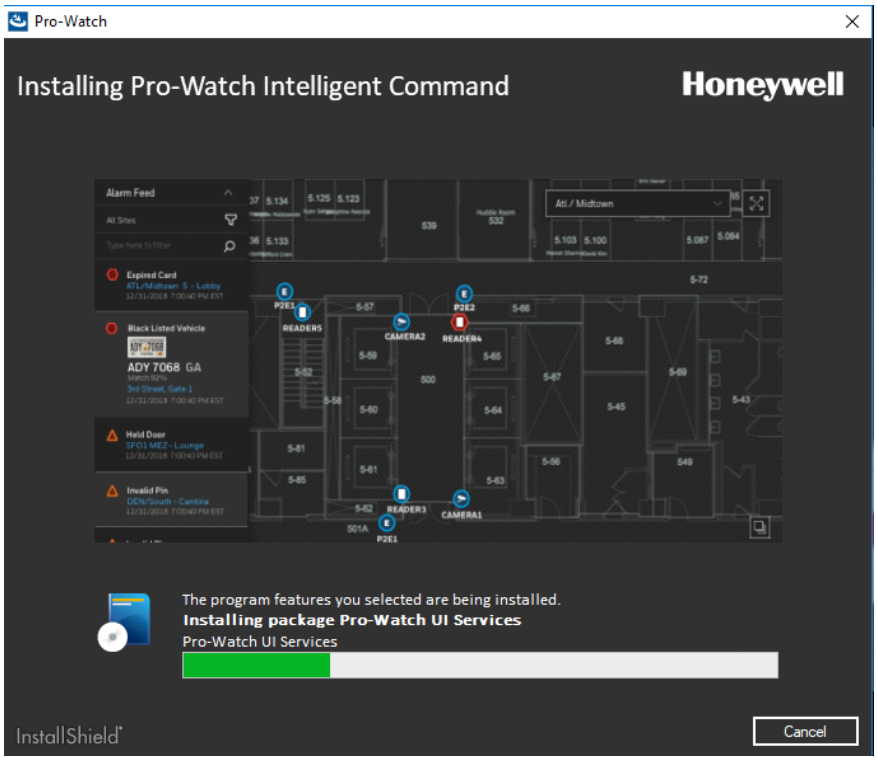
1.8 Pro-Watch DB Credential

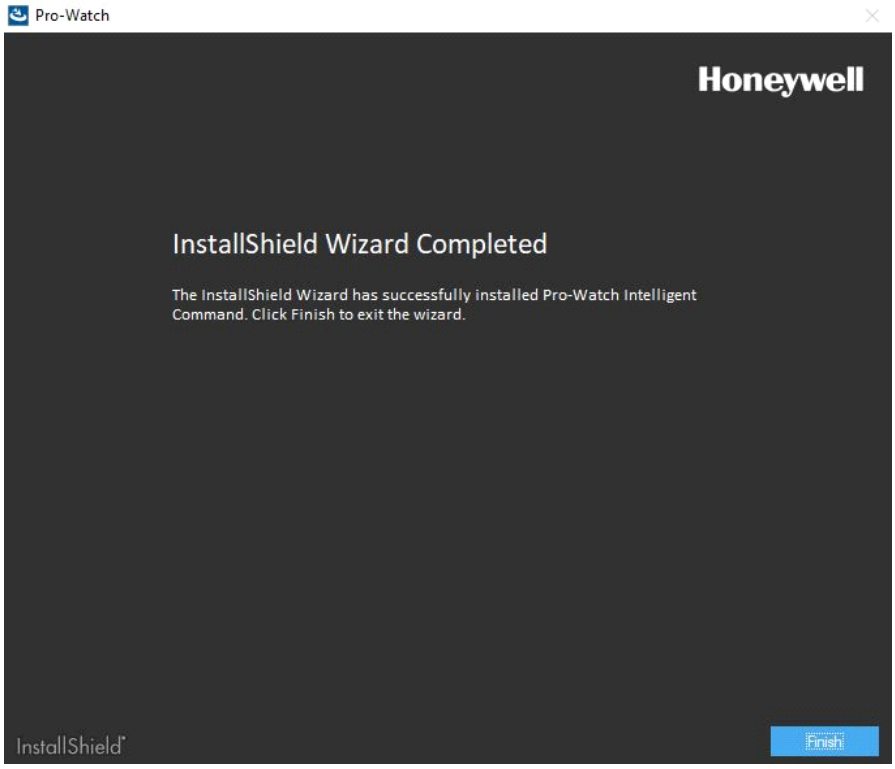
Installer will not proceed, if DB details and credential are invalid. If "Execute SQL Scripts" check box is checked then Installer will execute all SQL Scripts (.sql) files.



1.9 Click Install to Proceed with Installation

In windows servers (Windows 2016 & Windows 2019) it will take approximately 30 minutes to complete the installation.





Note: It is mandatory to RESTART Windows OS after installation\un-installation of Pro-Watch Intelligent Command.

1.10 Importing and Exporting SSL Certificate

Alarm processor module requires Web Tier Live alarm certificate and thumbprint to sync the connection between services.

This section describes how to use Import.ps1 and Export.ps1 script files.

These Powershell scripts will work only for "Honeywell security console" certificate.

Install App-tier, Core Service & Web Tier in separate machines.

Please follow the below steps in two different types of machines.

1.10.1 In Web Tier Machine

1. Run Export.ps1 powershell script with Admin rights in below path:

   C:\Program Files (x86)\Honeywell\UnifiedSecurityPlatform\Web\LiveAlarm\Util\Export.ps1

   NOTE: It will export existing "Honeywell security console" certificate and generate thumbprint.

   a. Honeywell_Certificate.pfx

b. Thumbprint.txt

2. Copy Honeywell_Certificate.pfx and Thumbprint.txt files to Core Service machine.

1.10.2 In Core Service Installed Machine

1. Paste the copied files (Honeywell_Certificate.pfx,Thumbprint.txt) to below path:

   C:\Program Files (x86)\Honeywell\UnifiedSecurityPlatform\AlarmProcessing\Util

2. Run Import.ps1 powershell script with Admin rights. (This script will import SSL Certificate, Bind IIS with new certificate & update the thumbprint in appsettings.json file.)

Appendix A: Troubleshooting the Web Client Installation

There is a log that is created for the web client located in the [Install Path]\Honeywell\UnifiedSecurityPlatform\Web\WEBUI\App_Data directory] called Site.txt. This log will capture any errors with the web client.

A.1 Different Scenarios

Scenario 1: Login is not successful with an authentication failed message.
Possible Resolution:

Step 1: IIS Reset

Try login again. If unsuccessful, then:

Step 2: If Pro-Watch WebAPI installed as windows service, then restart the "PWWebAPI" service

Try login again. If unsuccessful, then:

Step 3:

If token-based authentication is used, this may be because the service was unable to successfully get a token for the login.

The Site.txt log will contain an entry for token fetch, but without any results. Verify that configuration files for all services are setup correctly according to this document.

Scenario 2: User receives message that license limit is 0 (zero) users on logon.

Possible Resolution:

Step 1: IIS Reset

Try login again. If unsuccessful, then:

Step 2: If Pro-Watch WebAPI installed as windows service, then restart the "PWWebAPI" service

Try login again. If unsuccessful, then:

Step 3: The ThinktectureURL in the Web API configuration file is not pointing to the correct server name.

Scenario 3: Web Client accepts user credentials, but then redirects user back to the login page.

Possible Resolution: The Authentication in IIS for the services are

incorrect. Anonymous and Forms should be enabled for ThinktectureIdentityService, AuthenticationAuthorizationService, and PWWebAPI (if the API is hosted as a Windows Service).

The Authentication for ISPWebUI should be:

• Anonymous and Forms for standard or token-based authentication

• Windows for Windows authentication.

Possible Resolution: The server is missing a required hotfix. See Micosoft KB3052480 for resolution.

Scenario 4: If you need to avoid SSL certificate warnings in browse, follow the steps below:

Step 1: If you have a trusted certificate from a third party, select the certificate name during installation.

Step 2: If you do not have a trusted certificate from a third party, manually create a new "Self-Signed" Certificate with fully qualified name and select the certificate during installation (or) bind the certificate in IIS:

i. Run > inetmgr >Default Web Site

ii. Right click and select Edit Bindings.

iii. Then, select the created "Self-Signed" Certificate with fully qualified name.

Scenario 5: Unable to logout/Internal Server error.

Possible Solutions:

a. Clear browser cookies.

b. Logout & Login.

Scenario 6: On Service account password change.

Solution:

a. Reset all App pool credentials.

b. Reset Physical Path credentials.

A.2 Dynamic IP Restriction Configuration

A.2.1 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.

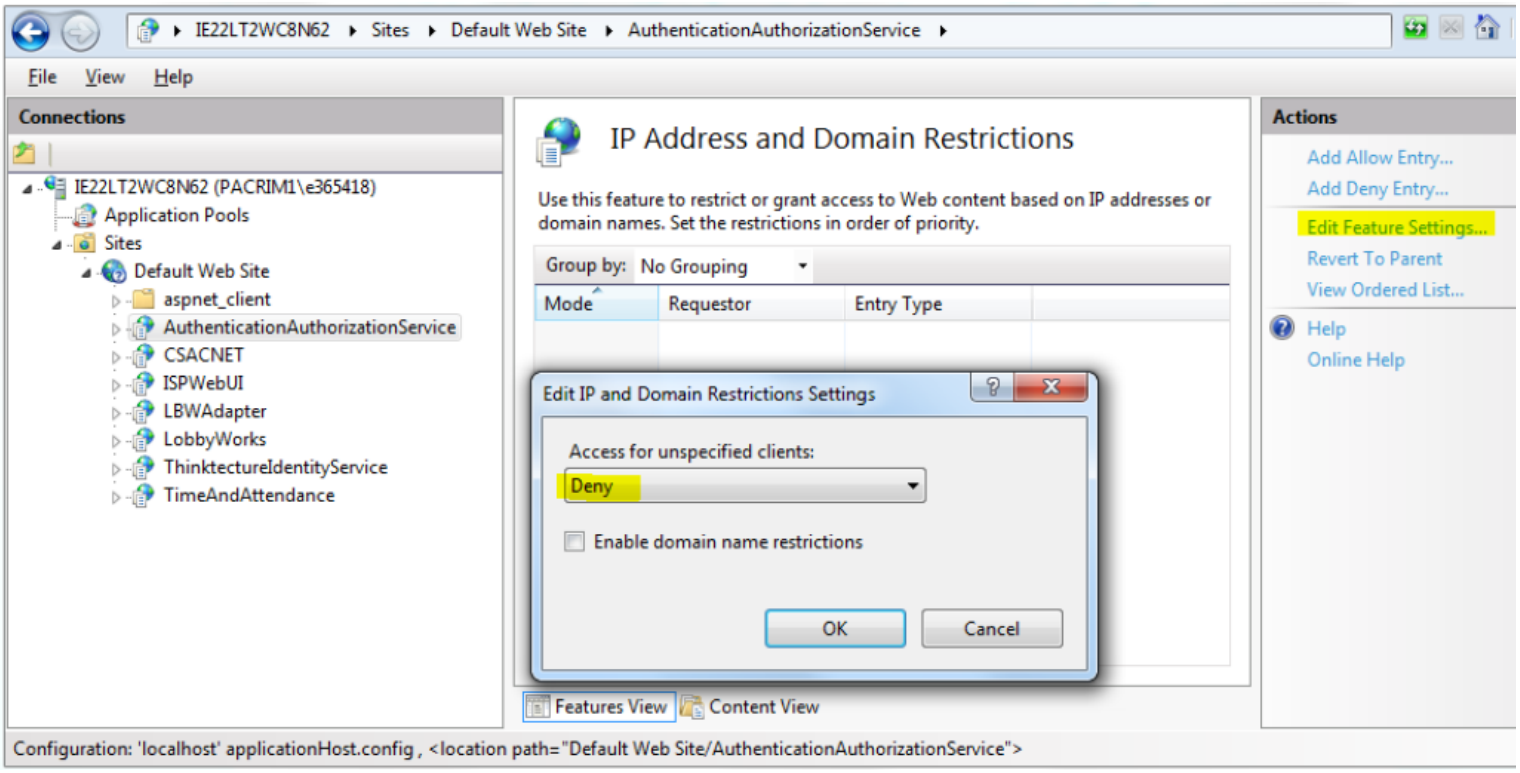
A.2.2 Installation of IP and Domain Restrictions

Refer to the web site https://www.iis.net/configreference/system.webserver/security/ipsecurity for the installation of IP and domain Restrictions

A.2.3 Configuring Dynamic IP Restrictions for Web Application

Steps:

1. Open IIS Manager.
2. In the left-hand side tree view select web application (for example AuthenticationAuthorizationService) to configure IP address filter.
3. In the Features View click "Dynamic IP Restrictions" or "IP and Domain Restrictions".
4. Edit Feature Settings > Deny for "Access for unspecified clients":



A.2.4 Pro-Watch Three Tier Deployment

IMPORTANT NOTE: If DTU is hosted in Windows Service, no setting is required.

For ThinktectureIdentityService, perform the following Steps:

1. Select Web Application.
2. Click "IP Address and Domain Restrictions".
3. Click "Edit Feature Settings" in the Actions pane.
4. Select "Deny" for "Access for unspecified clients" and click OK.
5. Click "Add Allow Entry..." in the 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), perform the following steps:

1. Select Web Application.
2. Click "IP Address and Domain Restrictions".
3. Click "Edit Feature Settings" in the Actions pane.
4. Choose "Deny" for "Access for unspecified clients" and click OK.
5. Click "Add Allow Entry..." in the 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 of WebUI installed for "Specific IP address".

Copyright © Honeywell Inc. All Rights Reserved

Honeywell Integrated Security
135 W. Forest Hill Avenue
Oak Creek, WI 53154
United States
800-323-4576
414-766-1798 Fax
www.honeywellintegrated.com

Specifications subject to change without notice.

© 2020 Honeywell, Inc.
Document 800-24386V5

Honeywell