



Pro-Watch[®] Software Suite

Security Manual

Copyright © 2018 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.

1. Pro-Watch Security Manual	2
1.1 Notice	2
1.2 Introduction	2
1.2.1 Intended Audience	2
1.2.2 Related Documents	2
1.2.3 Assumptions and Prerequisites	2
1.3 Developing a Security Program	3
1.3.1 Forming a Security Team	3
1.3.2 Identifying Assets	3
1.3.3 Identifying and Evaluating Threats	4
1.3.4 Identifying and Evaluating Vulnerabilities	4
1.3.5 Identifying and Evaluating Privacy Issues	4
1.3.6 Creating a Mitigation Plan	4
1.3.7 Implementing Change Management	4
1.3.8 Planning Ongoing Maintenance	5
1.3.9 Security Response Team	5
1.4 Microsoft Security Updates and Service Packs	6
1.5 Securing access to the Windows operating system	8
1.5.1 Windows user accounts and passwords	8
1.5.1.1 Password policies and settings	8
1.5.1.2 User account policies and settings	10
1.5.2 Permissions	10
1.5.2.1 Installation	10
1.5.2.2 Operations	10
1.5.3 Hardening References	11
1.6 Pro-Watch Security Features	11
1.6.1 Secure Deployment Architecture	11
1.6.2 Authentication Mechanism	12
1.6.3 Passwords	12
1.6.4 Accounts Management and Permission	13
1.6.5 User Accounts and Groups created by Pro-Watch	16
1.6.6 Encryption Mechanism	16
1.6.7 TLS & Certification Management	18
1.6.8 Third-party Applications	18
1.7 Physical Ports, Protocols, and Services	19
1.7.1 Pro-Watch Application Server	19
1.7.2 Pro-Watch Database Server	20
1.7.3 Pro-Watch API (Ports & Protocols)	20
1.7.4 Pro-Watch Client	20
1.7.5 Pro-Watch Web Client	21
1.7.6 RPC/DCOM	21
1.8 System Monitoring	21
1.8.1 Security Audit Logs	21
1.8.2 Other Parameters to Monitor	22
1.8.3 Setting Up Event Response Team	23
1.8.4 Sysmon Configuration	23

Pro-Watch Security Manual

Notice

Notice

This document contains Honeywell proprietary information.

Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2017 – Honeywell International

Introduction

Intended Audience

This guide has been created exclusively for the Information Technology (IT) personnel who are employed by Honeywell customers that use the Pro-Watch Access Control System. Pro-Watch manages various commercial building security and integrated functions. Pro-Watch software utilizes commercial off the shelf computing and network hardware using standard Microsoft Networking and Operating Systems.

Related Documents

Pro-Watch 4.3 Software Suite User Guide

Pro-Watch 4.3 Installation Guide

Pro-Watch 4.3 Enterprise Guide

Pro-Watch 4.3 Release Notes

Pro-Watch 4.3 A&E Specs Document

Pro-Watch 4.3 Web Interface User Guide

Pro-Watch 4.3 Compatibility Matrix

Pro-Watch 4.3 Data Sheet

For More Information

Please consult any of the above documents, all listed at this page:

<http://www.honeywellintegrated.com/products/integrated-security/sms/index.html>

Assumptions and Prerequisites

This guide is primarily intended for IT personnel who are responsible for planning the configuration and maintenance of the network infrastructure that the Pro-Watch system exists within.

It therefore assumes a high degree of technical knowledge and familiarity with:

- Microsoft Windows operating systems
- Networking systems and concepts
- Security issues and concepts

Attention

As you develop a security program for your Security system you should be aware that detailed information, if not protected, can fall into the hands of organizations that could cause harm to your control system or process operations.

Important terminology

The following Microsoft terms are important when understanding security concepts and configuration. [Definitions](#) can be found on the related Microsoft web sites. For example, see: <https://msdn.microsoft.com/en-us/goglobal/bb964658.aspx#g> and [https://msdn.microsoft.com/en-us/library/windows/desktop/ms721607\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms721607(v=vs.85).aspx)

- **Access Control List (ACL)** is a list of permissions assigned to an object. It defines the users or system procedures that are granted access to the object in question.
- **Access Mask**
- **Access Token** provides the login credentials for a session, including the identity of the user, the user's group (if any) and the privileges granted to the user.
- **Global Group**
- **Group**
- **Group Memberships**
- **Group Policy**
- **Group Policy Object (GPO)**
- **Local Group**
- **Organizational Units (OU)**
- **Permission**
- **Privilege**
- **Universal Group**
- **User Account**
- **User Account Control**
- **User Rights**

Developing a Security Program

A **Security Program** is a risk-analysis driven, life-cycle approach to securing a **Security System Network**. This chapter describes the key components of a Security Program.

An additional part of a Security Program is formulating and documenting a comprehensive **Disaster Recovery Plan**.

Forming a Security Team

To form a team you should:

- Define **executive sponsors**. It will be easier to ensure the success of security procedures if you have the backing of senior management.
- Establish a **cross-functional security core team** consisting of representatives from:
 - Security management (those responsible for defining and monitoring Security operations and maintaining the security and other subsystems)
 - Business applications (those responsible for applications interfaced to the Security system such as Human Resources, Logical Security etc.)
 - Business operation (those heavily dependent on the security system that ensures compliance, productivity or protection while doing their core operation)
 - IT system administration
 - IT network administration
 - IT security

Executive sponsorship and a formal team structure is a recommendation for the security program. The actual steps to implement that program are more critical and indispensable for the success of the program.

Identifying Assets

What is an "Asset"?

In this context the term "asset" implies anything of value to the company. The term covers equipment, intellectual property such as historical data and algorithms, and infrastructure such as network bandwidth and computing power.

Types of Assets

In identifying assets that are at risk you need to consider:

- People, for example, your employees and the broader community to which they and your enterprise belong.
- Equipment and assets, for example controller:
 - Network equipment (routers, switches, firewalls) and ancillary items used to build the system
 - Network configuration information (such as routing tables and ACL's)
 - Intangible assets such as bandwidth and speed
 - Computer equipment
 - Information on computing equipment (databases) and other intellectual property

Identifying and Evaluating Threats

You need to consider the potential within your system for unauthorized access to resources or information through the use of a network, and the unauthorized manipulation and alteration of information on a network.

Potential threats to be considered include:

- People, for example, malicious users outside the company, malicious users within the company, and uninformed employees.
- Inanimate threats, for example, natural disasters (such as floods, earthquakes, fire) or malicious code such as a virus or denial of service.

Identifying and Evaluating Vulnerabilities

Potential vulnerabilities that should be addressed in your security strategy include:

- The absence of security policies and procedures
- The absence of a disaster recovery plan
- Inadequate physical security
- Gateways from the Internet to the corporation
- Gateways between the business LAN and Security System Network
- The improper management of modems
- The improper management of firewalls
- Out-of-date virus software
- Out-of-date security patches or inadequate security configuration
- Inadequate or infrequent backups

You might also want to use Failure Mode Analysis to assess the robustness of your network architecture.

Identifying and Evaluating Privacy Issues

You must consider the potential for unauthorized access to personal data stored within your system.

Any information which may be considered sensitive by an individual such as home address, tax number, religion etc. should be protected and all access methods reviewed to ensure that correct authorization is applied. The Cardholder System is a prime example of a database holding personal information.

You also must be aware of the type of data you are sending outside the organization.

Example 1

If you are sending data to a support center, you must ensure that you are not breaching any privacy legislation or policy.

Example 2

If you are sending diagnostic packages offsite for support, you may need to remove personal data. Check with your manager before sending the package.

Creating a Mitigation Plan

As a part of your defense plan, you need to write **policies and procedures** to protect your assets from threats. The policies and procedures should cover your networks, your Windows nodes, and any other operating systems.

You should also perform risk assessments on your security system equipment. A full inventory of your assets will help you to identify threats and vulnerabilities.

You would then be in a better position to decide whether you can ignore, mitigate, or transfer the risk.

Implementing Change Management

Formal **change management** is vital to ensure that any modifications to the Security Network do not cause disruption to the system and the integrity of the system is maintained.

After a change is implemented, it is important that the system meets the same requirements as the components that were included in the original asset evaluation, as well as the associated risk assessment and mitigation plans.

Change management must incorporate a **change management system** where all requests for changes to the system can be logged. A **change control board** can then assess the change requests and perform a risk assessment of any change request before approving the change.

A plan for implementing the change request should aim to document the **risks** identified and a **strategy** for mitigating these risks. It should also document any **testing** required prior to implementing the change and the **results** of the testing. Part of the risk minimization/mitigation should include a **roll-back strategy** that can be invoked if there are problems implementing the change request.

The best practices outlined in the **Information Technology Infrastructure Library** (ITIL <http://www.itsm.info/ITIL.htm>) are useful to implement change management if change management processes do not exist in an organization.

Planning Ongoing Maintenance

Constant vigilance of your security position should involve:

- Regular monitoring of your system.
- Regular audits of your network security configuration.
- Regular security team meetings to stay up-to-date with the latest threats and the latest technologies for dealing with security issues.
- Ongoing risk assessments as new devices are placed on the network (see “Implementing Change Management”).
- The creation of an Incident Response Team (see “Security Response Team”).

Additional security resources

You should also be proactive about security by reviewing additional security resources like:

- Microsoft: <http://www.microsoft.com/technet/security>
- The National Institute of Standards and Technology document *System Protection Profile - Industrial Control System*: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=822602
- SANS Internet Storm Centre: <http://isc.sans.org>
- CERT: <http://www.cert.org>
- AusCERT: <http://www.auscert.org.au>

Refer to Information Security Standards:

- European Network and Information Security Exchange: <http://www.enisa.europa.eu/>
- British Standards Institution – Information Security: <http://www.bsi-global.com>
- ISO: <http://www.iso.org>
 - For information management system: <https://www.iso.org/isoiec-27001-information-security.html>

Refer to Information Technology - Security Techniques:

- ISO 15408 Evaluation Criteria for IT Security parts 1 -3 https://www.niap-ccevs.org/Documents_and_Guidance/cc_docs.cfm
- ISO/IEC 27002 provides best practice recommendations on information security management
- The Instrumentation, Systems, and Automation Society: <http://www.isa.org/isa99/> for Industrial Automation and Control Systems Security

Security Response Team

The responsibilities of a **Security Response Team (SRT)** might include:

- Monitoring the Microsoft and Honeywell software updates.
- Monitoring the antivirus software updates.
- Risk assessment of each security update, antivirus update, and any other update as it is made available.
- Determining the amount of verification required for any update and how the verification is to be performed. In extreme cases it may be helpful to have an offline system available so that full functionality testing is possible. This would be particularly useful where it is normal practice to install hot fixes as soon as they are announced, rather than waiting for Honeywell qualification.
- Determining when the update is to be installed. There may be times when the SRT determines that an update is so important that you cannot wait for Honeywell's verification cycle; in such a situation you may have to verify and install it early on all of your systems.
- Ensuring the deployment of qualified security updates on the Pro-Watch servers and clients.
- Checking that Microsoft Baseline Security Analyzer is run periodically to ensure that security updates have not been missed.
- Reviewing network infrastructure patches and configuration changes that will help to secure the network against the latest methods of attack.
- Monitoring account usage

- Enforcing and auditing security policy
- Detecting intrusion and maintaining domains

Microsoft Security Updates and Service Packs

An important part of the overall security strategy is to set up a system for ensuring that the operating system software is kept up to date.

At the same time, remember that frequent updates to critical Security System can be error prone, and may, over time, destabilize your system. Therefore such updates should be undertaken judiciously and with care.

Microsoft Security Updates

Microsoft releases a range of security updates and other operating system and software updates.

Note that only Honeywell-qualified Microsoft updates are supported. You should therefore wait until Honeywell has validated Microsoft updates before installing them. It is also recommended that you implement a controlled system for the distribution of all updates.

Timely information on security updates can be obtained by subscribing to the Microsoft Security Bulletin Summary at:

<http://www.microsoft.com/technet/security/bulletin/notify.msp>

Attention

Before installing security updates on the Pro-Watch installed system, you should refer to the Honeywell web sites <https://www.honeywellintegrated.com/> and <http://www.honeywellintegrated.com/products/integrated-security/sms/>. These sites provide information on the status of qualified updates and Hot Fixes of Microsoft for Pro-Watch software.

Attention

Before installing any critical updates or making any system changes, **ALWAYS back up the system** or take snapshot. This will provide a safe and efficient recovery path if the update fails.

There may be situations where a quick response to a threat is required, or an update is required before Honeywell has qualified the update. Honeywell recommends trialing the update on a non-production system to ensure that the Pro-Watch server software continues to operate correctly before making changes to production systems. In these situations you must create a **backup** of the system and unload the Pro-Watch database and stop Pro-Watch services prior to installing any updates.

Microsoft Service Packs

A service pack is a tested, cumulative set of all security and other updates. Service packs may also contain additional fixes for problems that have been found internally since the release of the product, and a limited number of customer-requested design changes or features.

Honeywell-qualified Microsoft Security Updates

Definition

The phrase "Honeywell-qualified Microsoft[®] security updates" refers to those patches

- provided by Microsoft[®]
- tested against the current shipping version of Pro-Watch[®], with
- no adverse effects observed.

How to Get Them

To get the list of Honeywell-qualified Microsoft security updates:

1. Go to Honeywell Integrated Security website (<http://www.honeywellintegrated.com/index.html>), and then
2. Click the "Microsoft[®] Patches Tested with Pro-Watch" link at the bottom of the page.
3. Or go directly to http://www.honeywellintegrated.com/documents/7_201027_03_MSpatch.pdf for the PDF document listing the latest patches that have been delivered by Microsoft[®] and tested against Pro-Watch. (See the screenshot below for a sample.)
4. To download any of the updates, just click the BLUE LINK before the name of the update. For example:

Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<http://www.honeywellintegrated.com>

The purpose of this document is to identify the patches that have been delivered by Microsoft® with Pro-Watch. All the below listed patches have been tested against the current shipping version of Pro-Watch. No effects were observed. Microsoft Patches were evaluated up to and including CVE-2018-0800. Patches are applicable to a Pro-Watch system.

2018 – Microsoft® Patches Tested with Pro-Watch

CVE-2017-5715	Vulnerability in CPU Microcode Could Allow Information Disclosure
CVE-2017-5753	Vulnerability in CPU Microcode Could Allow Information Disclosure
CVE-2017-5754	Vulnerability in CPU Microcode Could Allow Information Disclosure
CVE-2018-0800	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0781	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0780	Scripting Engine Information Disclosure Vulnerability

Sample Screenshot

Here is a sample screenshot of the PDF document in question:

Honeywell Security Group
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
Phone: 1-502-297-5700
Phone: 1-800-323-4576
Fax: 1-502-666-7021

<http://www.honeywellintegrated.com>

The purpose of this document is to identify the patches that have been delivered by Microsoft® which have been tested against Pro-Watch. All the below listed patches have been tested against the current shipping version of Pro-Watch with no adverse effects being observed. Microsoft Patches were evaluated up to and including CVE-2018-0800. Patches not listed below are not applicable to a Pro-Watch system.

2018 – Microsoft® Patches Tested with Pro-Watch

CVE-2017-5715	Vulnerability in CPU Microcode Could Allow Information Disclosure
CVE-2017-5753	Vulnerability in CPU Microcode Could Allow Information Disclosure
CVE-2017-5754	Vulnerability in CPU Microcode Could Allow Information Disclosure
CVE-2018-0800	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0781	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0780	Scripting Engine Information Disclosure Vulnerability
CVE-2018-0778	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0777	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0776	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0775	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0774	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0773	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0772	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0770	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0769	Scripting Engine Memory Corruption Vulnerability
CVE-2018-0767	Scripting Engine Information Disclosure Vulnerability

Securing access to the Windows operating system

An essential component of any security strategy for a Security System Network is to secure access to the operating system and to ensure that:

- Only authorized users have access to the system
- User access to files, systems, and services is limited to those necessary for the performance of their duties

Windows user accounts and passwords

Access is gained to the Windows operating system by logging onto the system using a user account name and password. This is true for both local and remote terminal services access. Because user accounts may be well known or easily guessed within an organization, the password becomes the prime vehicle for authentication. User account and password policies are therefore important security measures.

Password policies and settings

The most popular technique for breaking into a system is to guess user names and passwords. Consequently, it is essential that passwords are difficult to guess and that they are changed often.

Password settings

You can apply system-wide control of passwords by means of Group Policy. Alternatively, you can apply individual control to each account.

The following settings are suggested.

Note

If any changes on the password to account which is used by the windows services, that service needs to be updated with the right password and restarted.

Parameter	Setting	Comment
Maximum password age	45 to 90 days	Forces the choice of a new password after this time. The setting for the Administrator account should be shorter. A maximum of 30 is recommended.
Minimum password age	1 to 5 days	Prevents too rapid a cycling of passwords.
Minimum password length	8 characters	Improves encryption and makes guessing harder.
Password uniqueness	8 to 13 old passwords	Prevents reuse of the same password too quickly.
Account lockout	10 attempts	Prevents continual password guessing by disabling account after the specified number of attempts. Consider disabling account lockout for operator (or other user) accounts where denial of service or loss of view would be detrimental to safety or the continued operation.
Lockout duration	30 minutes	Specifies the period of time during which a user will not be able to log on following an account lockout. (Note that the administrator can re-enable the account before the expiration of the specified lockout period.)
Lockout counter	29 minutes	The time before the account lockout is reset to zero. For example, with the account lockout set at 10, and the lockout counter set at 29 minutes, lockout will occur if there are 10 invalid logon attempts within 29 minutes. Note that the lockout counter must be less than the lockout duration.

Strong passwords

It is recommended that you enforce strong passwords, that is, passwords consisting of at least 8 characters including one numeric. If you enforce password complexity, a strong password must contain at least three of the follow four character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers (0 through 9)
- Special characters (such as, !, \$, #, &)

Weak passwords that are easy to guess provide an opportunity for unauthorized access. Minimum password complexity can be enforced by group policy or local password policy.

An alternative way of increasing password complexity is to recommend the use of a pass phrase, for example, "the cow jumped over the moon" rather than a password. The extra characters dramatically increase the difficulty for a hacker attempting to crack the password; it is also much easier to remember than a random collection of letters, numbers, and other characters.

For generating strong passwords, refer to the section in this manual for [generating strong password](#).

Account lockout

The lockout values shown in Table on page 125 are those suggested by Microsoft and are discussed in their white paper "Account Lockout Best Practices"

Information

Account Lockout Best Practices.doc is available from:

[https://technet.microsoft.com/en-us/library/hh994563\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh994563(v=ws.11).aspx)

Account lockout policy must be used with caution. Although it will slow down an attempted password guessing attack; it will not prevent a determined attacker, who will capture logon packets and use cryptographic tools to break the password offline. It may also lead to a Denial of

Service, where authorized users find themselves unable to log on. It is generally better to rely on strong passwords and system audit log monitoring to prevent and detect password cracking attempts.

User account policies and settings

As a general rule you should:

- Review user accounts on a regular basis.
- Disable or delete all unused accounts.
- Disable all guest accounts.

Permissions

Installation

Below are the installation time system permission requirements.

Application	Requirements	Comments
Clients, App Server, Comm Server	IIS	Required for Web Client
	You need Windows local admin rights to install the executables for all editions and config types (client, server, etc). Windows Local admins usually has sysadmin rights to SQL databases. If not, the installer login needs sysadmin in the sql server and database.	For simple installations (PWLT, PWPE), local admins takes care of everything. Note If the installer and service accounts are locked down and cannot be used interactively by techs, many big sites have a "firewall" account which is local admins.

Operations

Below are operation time permission requirements.

Application	Requirements	Comments
-------------	--------------	----------

<p>Application Server / Comm Server</p>	<p>Service account needs local admin. The three services we care about are PW Service (MICSERVER.exe), SQL Server service and SQL Agent service.</p> <p>Options:</p> <ol style="list-style-type: none"> 1. Run everything under the installation account like user PWCE 2. Make a separate service account example PW_Service and assigned ProWatch service, SQL service, and SQL Agent to it. 3. Make a separate service account for each of PW and SQL Server. <p>Requires:</p> <ul style="list-style-type: none"> • There is one pre-defined database role called PWNT_User which maps all tables,views,SPs,etc in the database PWNT with all rights. Other roles could be constructed but usually are not because it tends to be very complicated. Exceptions are customizations for individual customers. The only other db roles which usually apply are public and db_owner. • Public access to the master database. 	<div style="border: 1px solid black; padding: 5px;"> <p>Note PWEE requires service accounts to be domain-based to configure the Enterprise.</p> </div>
<p>Clients</p>	<p>User groups need PW_User role but can be ordinary users.</p> <p>User Groups need certain local security policies set: "load unload device drivers", "Act as part of the O/S", .. If not this last - Shadow login doesnt work.</p> <p>Requires:</p> <ul style="list-style-type: none"> • There is one pre-defined database role called PWNT_User which maps all tables,views,SPs,etc in the database PWNT with all rights. Other roles could be constructed but usually are not because it tends to be very complicated. Exceptions are customizations for individual customers. The only other db roles which usually apply are public and db_owner. • Public access to the master database. 	<p>At least one of the ProWatch users needs local admins to use certain functions like changing badge fields. If this is not permitted, the firecall account must be used or a sysadmin has to be involved to change badge fields.</p>

Hardening References

Hardening the Powershell

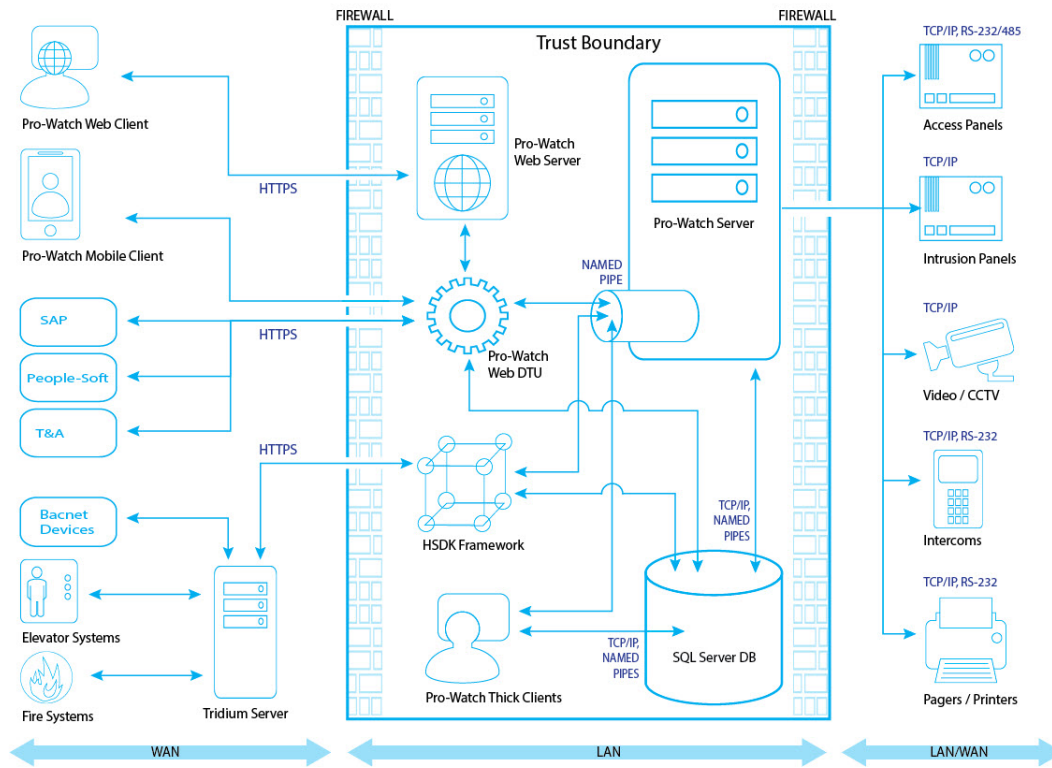
Powershell is an increasingly popular attack vector these days. Please refer to the link <https://www.asd.gov.au/publications/protect/securing-powershell.htm> , create a plan and harden the participating system.

Hardening the Active Directory

Refer <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory> for hardening active directory.

Pro-Watch Security Features

Secure Deployment Architecture



Authentication Mechanism

Pro-Watch supports different types of user authentication based on the configuration of the system

Type of Authentication	Description
Windows Integrated Authentication	Used by the thick client application automatically taking the authentication of the logged in windows user from the workstation through which the Pro-Watch is accessed.
Application Level Authentication	User is explicitly asked a username and password during Pro-Watch Client launch irrespective of the windows logged in user. These user name passwords are separately maintained specific to Pro-Watch access outside the windows user management.
Web Login Authentication	For every Pro-Watch user in the Pro-Watch configuration there is an optional web password that can be enabled to have the same user access the pro-watch web application or Pro-watch API.

Information

Web Application and Pro-Watch API can be configured to use either windows integrated authentication or web login authentication

It is recommended to use Windows integrated authentication and the best practices around the windows user and password management. Using integrated authentication enables you the following advantages:

- Use existing enterprise-wide security policies
- Use single signon
- Minimize the number of accounts required for operators
- Use Windows auditing to track user activities

Passwords

It is particularly important to handle passwords correctly. If an attacker acquires a user's password, they can gain access to the system and have

the same permissions as that user. In the worst case, an attacker might gain access to System Administrator's account and the entire system could be compromised.

Generate a Strong Password

Not all passwords are equally effective. Ensuring that users are choosing good, strong passwords is essential to securing Pro-Watch System. Users are required to choose passwords that are at least eight characters long. These characters cannot be ALL alphabetic or ALL numeric. When creating a password, the following guidelines can help generate stronger passwords:

- A random string of characters, including letters, numbers and uppercase, lowercase and special characters, (e.g., s13pj96!cD) is typically a strong password. However, these can be hard to remember.
- A long, nonsensical sentence (e.g. "I happily tarnished under 21 waterlogged potatoes, which meet up on Sundays") can be used as is. For systems that restrict password length, it can be contracted to include only the first character of each word (e.g., "lhtu21wp,wmuoS"). These are difficult for attackers to guess, but are typically easy (albeit silly) for users to remember.

Note: When picking a sentence as a passphrase, it is best to avoid well-known phrases and sentences, as these may be included in dictionary attacks (e.g., "Luke, I am your father").

- A string of random words (e.g., "coffee Strange@ Halberd 11 tortoise!") provides a much longer password that are single word or a random string of characters. However, password crackers are becoming more aware of this technique. Therefore, including a few random numbers and symbols can make your password harder to crack.

Remember, a good password is easy for a user to remember, but difficult for an attacker to guess.

Change Your Password Regularly

Change user passwords after a specified amount of time or on a predetermined date. This ensures that old passwords are not kept around indefinitely. If an attacker acquires a password, it is only useful to them until the password is changed.

Accounts Management and Permission

Pro-Watch has accounts, represented by users in Pro-Watch configuration. It is important that these accounts are properly managed. Failure to do so can make it easier for an attacker to penetrate the system, or make it more difficult to detect that an attack has occurred.

Use a Different Account for Each User

Each user account in the Pro-Watch system should represent a single user. Different people should never share the same account. For example, rather than a general "Supervisor" user that many Supervisors could use, each supervisor should have their own, separate account.

There are many reasons for each user to have their own individual account:

- If each user has their own account, audit logs will be more informative. It will be easy to determine exactly which user did what. This can help detect if an account has been compromised. In the below example of a *Pro-Watch Audit Log Report* displaying three different users making changes in table values, it is easy to determine who has made which change and when (*click the image to enlarge it*):

Table Description	Table Name	Key 1	Key 2	Operation	Before Value	After Value	Date/Time	User ID
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader2	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	0	6	4/24/2017 2:53:00 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader1	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	0	0	4/24/2017 4:01:01 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader1	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	0	0	4/24/2017 4:01:01 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader1	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	0	0	4/24/2017 4:01:01 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader1	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	6	0	4/24/2017 4:01:01 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader2	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	0	0	4/24/2017 4:01:01 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	EP_1501_Reader2	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	6	0	4/24/2017 4:01:01 AM	rinas
Logical Device Detail	LOGICAL_DEV_D	Door_11111111111111111111 11111111111111111111H	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	0	2	4/24/2017 12:00:00 P	rinas
Logical Device Detail	LOGICAL_DEV_D	Door_11111111111111111111 11111111111111111111H	0x0070D40949A88D5F11 D4A45600508BC86902	UPDATE	9	3	4/24/2017 12:00:01 P	rinas
Badge Cards	BADGE_C	RINAS PA	5558888	ADD			4/24/2017 1:02:44 PM	administrator
Badge Clearance Codes	BADGE_CC	RINAS PA	5558888	ADD			4/24/2017 1:02:44 PM	administrator
Badges	BADGE	RINAS PA	PA, RINAS	UPDATE	4/20/2117 3:59:48 PM	4/30/211 7:3:59:48 PM	4/24/2017 1:07:53 PM	administrator
Badges	BADGE	B_EMP_B_EMP	B_EMP_B_EMP	UPDATE	12/14/2116 3:38:10 PM	12/31/21 16 3:38:10 PM	4/24/2017 1:09:28 PM	administrator
Areas Table	AREA	Area 1		ADD			4/24/2017 1:09:44 PM	tkelly

- If an account is removed, it does not inconvenience many users. For example, if a user should no longer have access to Pro-Watch System, deleting or disabling their individual account is simpler. If it is a shared account, it makes the administrator difficult to manage the account used by multiple users. the only option would be to change the password and notify all users. Leaving the account as-is is not an option – the goal is to revoke the user's access.
- If each user has their own account, it is much easier to tailor permissions to precisely meet their needs. A shared account could result in users having more permissions than they should.
- A shared account means a shared password. It is an extremely bad security practice to share passwords. It makes it much more likely for the password to be leaked, and makes it more difficult to implement certain password best practices.

Each different user should have a unique individual account. Similarly, users should never use accounts intended and used for running system services.

Use Unique Service Type Accounts for Each Project

It is a common (bad) practice that some system integrators often use the exact same system/service credentials on every project they install. If one system is compromised, the attacker could potentially have credentials for access to many other projects installed by the same contractor.

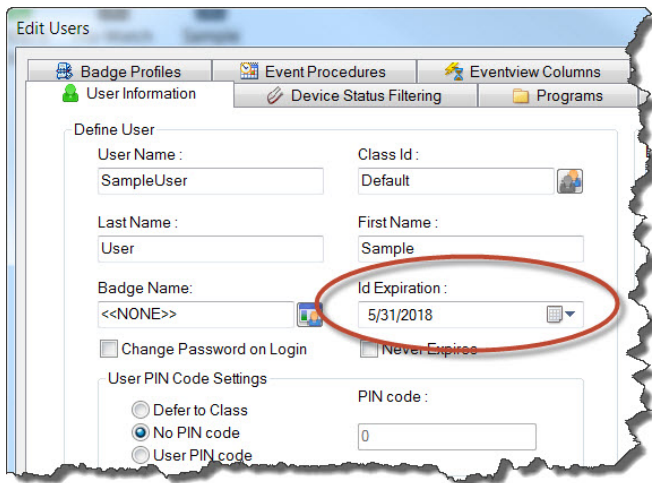
We highly recommend to use Unique Service type accounts for each project to mitigate and reduce any potential risks arise out of the above scenario.

Setup Accounts with Expiration Dates

It is a better practice to have the accounts expire on a specific date and have them renewed before account expiry if that user is expected to continue to use the Pro-Watch system. This ensures that no accounts are accidentally left enabled for a long duration.

In some cases, you may need to set up an account for a user who needs access only temporarily. For example, an auditor may need an account to inspect the system. In these situations, a new account should be created and set up to expire automatically when it is no longer needed.

Here is an example of a user account with a specific expiration date (*click the image to enlarge it*):



Change System/Service User Credentials

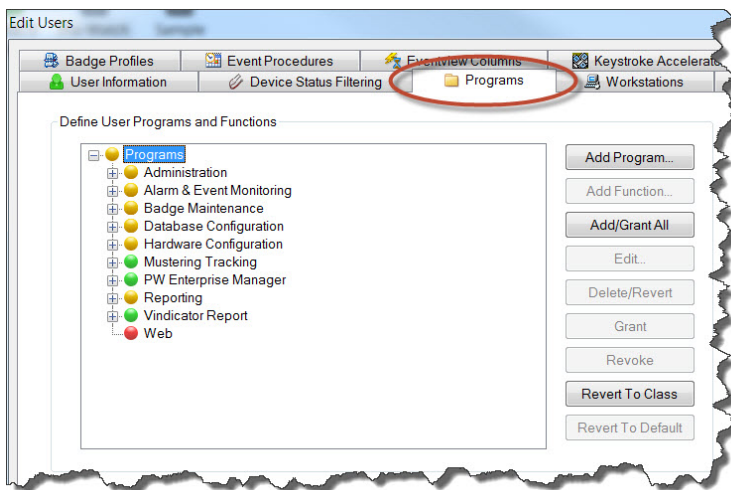
It may be necessary to periodically change the system/Service user credentials. For example, if an employee who is knowledgeable of the System/Service user credentials is terminated, you may want to change those credentials. Also, in most cases, it is better to configure such windows account with non-expiring passwords, so that those passwords expiring silently do not affect system operation.

Assign the Minimum Required Permissions

When creating a new user, think about what the user needs to do in Pro-Watch, and then assign the minimum permissions required to do that job. For example, a user who only needs to acknowledge alarms does not need access to the User management configuration or the Hardware configuration. Giving non-required permissions increases the chance of a security breach. The user might inadvertently (or purposefully) change settings that they should not change. Worse, if the account is hacked, more permissions give the attacker more power.

Use Program Functions in the User management of Pro-Watch db configuration to select appropriate and granular permissions for the user. Review the user permissions periodically.

You can grant or revoke specific programs and functions for a user through the Programs tab of Edit Users screen, as shown below (*click the image to enlarge it*):



By using the command buttons on this screen, you can add, delete, grant or revoke programs and functions.

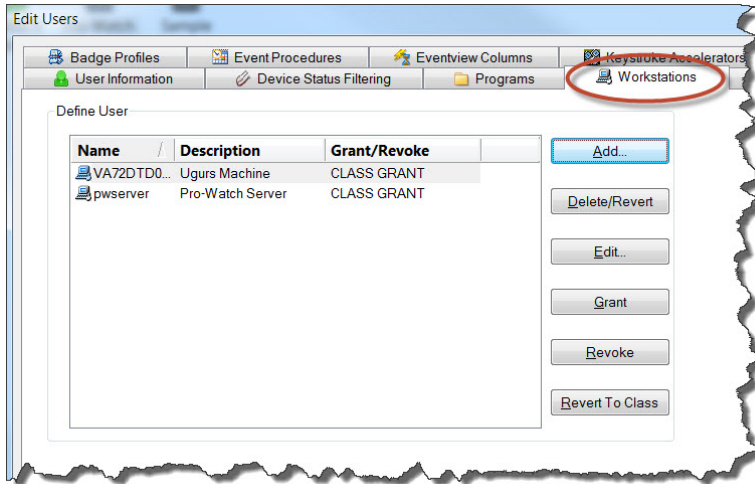
For more information, see the following in *Pro-Watch Software Suite User Guide*: "DBC-Users" chapter, "Programs Tab" section.

Assign Specific Workstations to User Accounts

Restrict users' access to workstation based on the necessity, so that the users are allowed to access the system only from those workstations to

perform their tasks. This also enables enhanced auditing to track and record which change is made by which user on which workstation/location.

You can assign specific workstations to a user through the Workstations tab of Edit Users screen, as shown below (*click the image to enlarge it*):



By using the command buttons on this screen, you can add, delete/revert, edit a workstation, and grant or revoke its assignment to the user.

For more information, see the following in *Pro-Watch Software Suite User Guide*: 1) (*For Non-System Users*) "DBC-Users" chapter, "Workstations Tab" section, 2) (*For System Users*) Hardware Configuration (HW Config) chapter, "Adding a System User" section.

User Accounts and Groups created by Pro-Watch

Authentication Type	Default User Account	Modifiable	Notes
Windows Integrated Authentication	No default user account created	NA	No user accounts are created by default during installation. The Administrator can create the windows account in advance required for the Pro-Watch administration and use the account during the installation
Application Login	PWAdmin	Yes	When enabled 'Application Login' authentication type (refer user guide for how to enable application login) a starting default user account will be created just in time with the name PWAdmin with default password for the initial login. This username or password can be modified or deleted by the user at anytime. <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p>Info This will not be created during installation time.</p> </div>
Web Login Authentication	No default user account created	NA	Web login is an add on to the other two login forms as above if required to be managed seperately for Pro-Watch based on the user needs and does not have any default username. By default web access is disabled.

Windows User Group: PWNT Windows User group gets created during installation under which all the Pro-Watch users will be assigned.

Encryption Mechanism

The below critically sensitive data and its encryption mechanism used in the Pro-Watch system.

User / Password

Component	User Type	Authentication Type	Encryption Type	Stored in	Password Policy	Username changeable	Pwd changeable	Comments
Prowatch Core	Service User	Windows NT	Windows hashing	Windows domain server as a hash	Windows	Yes	Yes	N/A
	pwdemo	Windows NT	Windows hashing	Windows domain server as a hash	Windows			N/A
	PWAdmin	Application login / Db	Hashed	SQL	Enforced in app	Yes	Yes	Not enabled by default
	PWNT	Windows NT Group				NA	NA	Group
Prowatch Web 4.3.5	PW Web logins		Hashed	SQL	Enforced in app	Yes	Yes	hashed and salted
Prowatch Web API	PW Web login		Hashed	SQL	Enforced in app	Yes	Yes	hashed and salted
Vendor Portal	Portal Login	Application login / Db	Hashed	SQL	Enforced in app	Yes	Yes	hashed and salted
Mobile App	PW Web logins		Hashed	SQL	Enforced in app	Yes	Yes	N/A
SQL Server	Windows login	Windows NT	Windows hashing	Windows domain server as a hash	Windows	Yes	Yes	uses the same as windows login

Admin Enrollment Pwd for Biometric is not a traditional password, but is more of a key used to get into Biometric.

Encryption in Communication

Important Note

By default the encryption is disabled. It is important to enable encryption while commissioning the system. Refer to the appropriate sections of Installation/User guides for instructions to enable encryption.

Category	Encryption Type	SSL / TLS version	Notes
Host (PW) to Controller			
PW6K	AES 256 bit	N/A	N/A
PW6K IP Client		TLS	N/A
Panel to Reader			
Weigand	No Encryption	N/A	N/A
OSDP	OSDP-SC based out of AES 128bit	N/A	N/A
PIV Card Reader	FIPS	N/A	N/A
Card to Reader			
HID Mobile Credential			See Manufacturer
Intelligent Controller (IC)			
Controller Web Server	https	TLS 1.1	N/A
Peripherals			
PW Client to Server	No native encryption	N/A	Typically deployed in trusted boundary. Recommended to use VPN for additional security.
PW Web Client	https	TLS	N/A
PW Mobile Client to server	https	TLS	N/A

Web API	https	TLS 1.2	N/A
Vendor Portal Web Access	https	TLS	N/A
Vendor Portal API	https	TLS	N/A

Additionally SQL Server can be setup to require secure connections, this will force the client connections to negotiate a secure channel communications method to reach the server. Here is the link to the basic process. [https://technet.microsoft.com/en-us/library/ms189067\(v=sql.105\).aspx](https://technet.microsoft.com/en-us/library/ms189067(v=sql.105).aspx) Any changes to a customer's production environment should be tested to ensure a working model prior to roll out.

TLS & Certification Management

Transport Layer Security (TLS) provides communication security over a network by encrypting the communication at a lower level than the actual data being communicated. This allows secure transmission of unencrypted sensitive data over an encrypted connection. TLS as a protocol replaces its predecessor, Secure Sockets Layer (SSL); however, because TLS originally evolved from the SSL standard, the terms "TLS" and "SSL" are often used interchangeably. Although many people still refer to TLS as "SSL", it is important to know that the latest version of SSL as a protocol (SSLv3) is not considered secure, and it is important to use the latest version of TLS available.

Using TLS protects data from anyone who might be eavesdropping and watching network traffic. It also provides proof of identity, so that an attacker cannot impersonate the server to acquire sensitive data. When possible, always use TLS.

Pro-Watch supports communication over TLS on various components/services. They are listed under Encryption section.

Setup Certificates

Pro-Watch uses HTTPS for many of its services, which requires a certificate. There are several options that can be used to address the need for a certificate:

- Purchase a certificate from an accredited certification authority.
- Use a certificate from the site's IT department, if there is a certificate authority infrastructure in place.

If you use a purchased certificate or a local certificate generated by the IT department, it must be installed according to the instructions provided. By using these types of certificates, you automatically establish a trust relationship.

Changing Panel Certificates

Default Panel certificates needs to be replaced with proper certificates. Use the panel website to configure valid certificate for each of the panel.

The screenshot shows the Honeywell Access Control Device Server Configuration Manager interface. On the left is a navigation menu with the following items: Home, Network, Host Comm, Device Info, Users, Auto-Save, Restore/Default, Apply Settings, Load Certificate (highlighted in green), and Log Out. The main content area is titled 'Load Certificate' and contains the following text and controls:

Please specify a certificate file(*.crt):
 No file chosen

Please specify the private key file(*.pem):
 No file chosen

Below this is the 'Certificate Information' section, which displays the following details:

Issued to: Mercury Security EP-series
 Issued by: Mercury Security Root CA
 Valid time: from 11/03/2010 to 09/07/2011

Third-party Applications

Honeywell does not recommend the installation and use of any unsupported Third-party Applications on any Pro-Watch computers. This includes

the Pro-Watch Application Servers, Pro-Watch Database Server and Pro-Watch Clients. 3rd party applications may affect the performance of these computers and perhaps even result in a loss of view of the building security. Only those applications listed in the compatibility matrix or those installed by Pro-watch installer, which have been tested and qualified should be installed on these computers.

Physical Ports, Protocols, and Services

Information

For Network Ports Used by Key Microsoft Server Products refer <https://msdn.microsoft.com/en-us/library/cc875824.aspx#EDAA>

Information

The list of standard ports (as assigned / maintained by IANA) is available here - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Pro-Watch Application Server

All of these ports can be both inbound and outbound.

Port	Protocol (TCP, UDP, HTTP, etc.)	Standard/Custom	Changeable (Y/N)	Use	Notes
139	TCP	Custom	No	Named Pipes	** If integrated with Pro-Watch VMS, also include VMS Client's MMShell.exe port requirements below
445	TCP	Custom	No	Badge Data Communicating with SQL Server via Named Pipes. Named Pipes uses SMB port (port# 445) 445 is a standard Microsoft port. For Network Ports Used by Key Microsoft Server Products https://msdn.microsoft.com/en-us/library/cc875824.aspx#EDAA	N/A
1433	TCP	Standard	Yes	Communications with SQL	Set per SQL instance
3001	TCP	Custom	No	Communications with PW3K/5K panels	N/A
3001	TCP	Custom	Yes	Communications with 6K panels	N/A
10001	TCP	Custom	Yes	Galaxy basic port; SEEP/CHIP Micro Cobox default ports	N/A
10002	TCP	Custom	Yes	Galaxy remote control port	N/A
10005	TCP	Custom	Yes	Galaxy alarm port	N/A
25	TCP	Standard	No	SMTP for emails on events or from PW Advanced/AP Badging and Compliance Reports	N/A
20007	TCP	Custom		VMS MMShell.exe Server Connection	Required for VMS integration

20009	TCP	Custom		VMS MMShell.exe Rendering Connection	Required for VMS integration
26026	TCP	Custom		VMS MMShell.exe Controller	Required for VMS integration
53	TCP	Standard		VMS MMShell.exe DNS Server	Required for VMS integration

Pro-Watch Database Server

Port	Protocol (TCP, UDP, HTTP, etc.)	Standard/Custom	Changeable (Y/N)	Use	Notes
1433	TCP	Standard	Yes	Communications with SQL	Set per SQL instance

Pro-Watch API (Ports & Protocols)

Component	Port	Protocol (TCP, UDP, HTTP, etc.)	Standard/Custom	Changeable (Y/N)	Use	Notes
Pro-Watch API (REST)	8734	HTTP, HTTPS	Custom	Yes	Configurable through .config file	Any of the mentioned protocols can be used.
Pro-Watch API (SOAP)	8732	HTTP, HTTPS	Custom	Yes	Configurable through .config file	Any of the mentioned protocols can be used.

Note

For security reasons, it is required to run the Pro-Watch API service and Pro-Watch Server on the same machine.

Note

For security reasons it is required to use HTTPS.

Pro-Watch Client

Port	Protocol (TCP, UDP, HTTP, etc.)	Standard/Custom	Changeable (Y/N)	Use	Notes
139	TCP	Custom	No	Named Pipes	N/A
445	TCP	Custom	No	Badge Data : Download card Uses Namedpipe. Communicating with SQL Server via Named Pipes. Named Pipes uses SMB port (port# 445) 445 is a standard Microsoft port. For Network Ports Used by Key Microsoft Server Products https://msdn.microsoft.com/en-us/library/cc875824.aspx#EDAA	N/A
1433	TCP	Standard	Yes	Communications with SQL	Set per SQL instance

10001	TCP	Custom	Yes	Galaxy basic port; SEEP/CHIP Micro Cobox default ports	N/A
10002	TCP	Custom	Yes	Galaxy remote control port	N/A
10005	TCP	Custom	Yes	Galaxy alarm port	N/A
25	TCP	Standard	No	SMTP for emails on events or from PW Advanced/AP Badging and Compliance Reports	N/A

Pro-Watch Web Client

Component	Port	Protocol (TCP, UDP, HTTP, etc.)	Standard/Custom	Changeable (Y/N)	Use	Notes
IIS Server	80	TCP	Standard	No	Web Client	For HTTP
IIS Server	443	TCP	Standard	No	Web Client	For HTTPS

RPC/DCOM

Several subsystems use RPC/DCOM (Remote Procedure Calls / Distributed Component Object Model) for communications in addition to DCOM utilities RPC for connections.

When an RPC connection is first made, the client connects to the End-Point Mapper on port 135 on the server computer. The client is then provided with the port number of the service it is connecting to. This port number is allocated dynamically by RPC, and binds one TCP port and one UDP port to each RPC connection at run time. The range of port numbers RPC can use is from 1024–65535. The port range that can be used for RPC connections can be controlled to a smaller known set. For information on changing the port range, see the Microsoft Knowledge Base Articles KB300083 and KB908472.

System Monitoring

Steps outlined in this document when followed will result in a more secure system.

However, there is always the possibility that an attacker will succeed in circumventing all the safeguards and break in. In this case it is important to discover the break in and prevent further damage as rapidly as possible. The earlier a system break in is detected and the more evidence is captured, less damage will likely occur and the greater will be the chances of identifying the intruder.

Security Audit Logs

It is recommended that you enable the auditing of your file system and registry access. If there is a suspicion that the system is being misused, then Windows auditing provides a useful tool to track who has done what and when. Once auditing is enabled, the audit logs should be reviewed frequently by an accountable person, who can take action if unexpected activity is identified.

Considerations

The default action is to halt the system if the security log becomes full. This is to prevent activity occurring without any traceability. However, it also provides an opportunity for a Denial of Service (DOS) attack.

To prevent this, either increase the log file size and review the log before it fills up, or set one of the overwrite options (for example, "Overwrite events as needed"), and check the log frequently enough to prevent loss of events.

To view the log settings, launch the **Event Viewer** tool, select **Log > Security** and then select **Log > Log Settings**. Then change either the **Maximum Log Size**, or the **Event Log Wrapping** options.

You should ensure that the audit log is regularly inspected and cleared, or else disable the security option "Audit: shut down system immediately if unable to log security audits".

Configuring the log settings to overwrite will ensure that the system never stops when the log is full but this can also be used to hide events of interest by falsely filling the log with other events. This highlights the need for regular monitoring.

To enable auditing:

Either:

- Set the appropriate Group policy,
or
- Log on as the Local Administrator and
 - Launch the **User Manager** tool.
 - Select **Policies > Audit** and enable options of interest.

The most useful options are likely to be:

- Logon and Logoff - success and failure
- Process Tracking - success and failure
- Object access - success and failure

This enables the auditing of file system and registry access. It is then necessary to select the objects of interest and the user (or groups) whose actions are to be audited. Since it is necessary to specify an identity to audit (and by definition, it is not known who the intruder is), you should specify the group "Everyone".

To configure the auditing of file access:

1. Go to **Windows Explorer** and select the directory or file of interest.
2. Select **Properties > Security > Advanced > Auditing**.
3. Then add a user, for example, "Everyone" and the access to be audited; for example, "Open failure".

To configure the auditing of registry keys:

1. Run **regedt32**.
2. Select the key for which you want to set up auditing.
3. Select **Permissions > Advanced > Auditing** and add users as explained in the previous section.

Other Parameters to Monitor

It is important to monitor various other system parameters, review them periodically, and keep an eye on whether there are any unusual and unexpected system events.

Some of these parameters' baselines are specifically based on the site. It is recommended to monitor the usage and establish a baseline and threshold values for these parameters.

There may be some spikes on some of the parameters and it is recommended to watch and avoid a scenario that originates it or if possible, spread those actions causing the spike to non-peak hours. For example, loading a heavy report or archiving can be done on a non-peak hour of the site. This will enable monitoring the system for its uptime and prevent or detect early on any Denial of Service.

Monitor the following general parameters periodically and if necessary, take corrective action(s):

- Hard disk
 - Used and Free memory space on OS drives and data drives.
 - IO Read/Write operation.
- Network Usage.
- Memory usage of critical processes and the total system memory usage.
- CPU utilization of the system. If the system is VM, it is important to watch the CPU utilization of the VM system as well as the machine hosting all the VMs.

Monitor the following Pro-Watch specific parameters periodically and if necessary, take corrective action(s):

- Expiring Cards upcoming and on a particular day. Watch for a large number of cards all expiring on the same day. As a remedy, spread them across a number of days.
- Panel offlines for a long period without 'installed' checkbox unchecked.
- Average event rates for a site and any deviations from it.

- Pro-Watch Logs
- Audit Log
- Operator Log
- Pro-Watch Event Log – general alarms, threshold notifications, etc
- Pro-Watch Partitions – who can see what data
- Pro-Watch Users – program and functions access

Monitor other system logs including:

- SQL Server Logs
- Windows Event Logs
- Firewall Logs

Monitor every node in your system for the above parameters but not necessarily limited to the system where the below components are installed:

- Pro-watch DB
- Pro-watch Application Server
- Pro-Watch Remote Server
- Pro-Watch Web Server
- Pro-Watch API
- Pro-Watch DTU
- Vendor Portal API
- Vendor Portal DB

Setting Up Event Response Team

An **Event Response Team** should be ready to handle any security breach as it occurs. Their role is to identify the attack, prevent further damage, recover from the damage and capture evidence which could be used in prosecutions. In many instances the IT department will already have such a team; they simply need to be made aware of any specific requirements of the security system.

Many Government and industry bodies and computer vendors have published good papers on this topic, which should be reviewed when building the team.

Useful references include:

<http://technet.microsoft.com/en-au/security/default.aspx>

<http://www.sans.org/security-resources.php>

<http://csrc.nist.gov>

Sysmon Configuration

Refer the below links for the sysmon configuration

- <https://decentsecurity.com/enterprise/#/sysmon-enterprise-configuration/>
- <https://github.com/SwiftOnSecurity/sysmon-config>


Honeywell

Honeywell Access Systems

135 W. Forest Hill Avenue

Oak Creek, WI 53154

United States

 800-323-4576

www.honeywellaccess.com

+1 800 323 4576, Option 2 (North America only)

<https://mywebtech.honeywell.com>

© 2018 Honeywell International Inc. All rights reserved. No part of this publication may be reproduced by any means without written permission from Honeywell. The information in this publication is believed to be accurate in all respects. However, Honeywell cannot assume responsibility for any consequences resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes. For patent information, see www.honeywell.com/patents.