Honeywell

ADPRO® XO™

iFT Series, eFT Series, and iFT Gateway

Firmware version 5.3.x

Security Guide

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Honeywell. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Honeywell.

Trade Name Statement

ADPRO, Xchange, FastTrace, iFT, eFT, iFT-E, iFT Gateway, IntrusionTrace, LoiterTrace, XO, iTrace, iCommand, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Honeywell and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Honeywell. All proper health and safety precautions must be taken during the installation, commissioning, and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Honeywell is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through a Honeywell accredited training course can install, test and maintain the system.

Liability

You agree to install, configure, and use the products strictly in accordance with the User Manual and product documents available from Honeywell.

Honeywell is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits, or loss of data arising out of your use of the products.

Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation, or advice given by or on behalf of Honeywell or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Honeywell in relation to the products is limited to:

in the case of services, the cost of having the services supplied again; or

in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Honeywell harmless for any claim, cost, demand, or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

www.security.honeywell.com

TABLE OF CONTENTS

1 Security Guidelines 1

Purpose 1
Intended Audience 1
Solution Summary 1
Security Checklist 2
Packaging 2
Securing the ADPRO XO NVR 2
Software Updates 3
Removable Storage 3
Account Management 3
Backup and Recovery 3
Decommissioning/Disposal Management 4
Vulnerability Reporting 4
Physical Security 5
Security Updates 5
Authentication 5
Authentication Mechanism 5
Encryption 6
Data at Rest 6
Data in Transit 6
Privacy Considerations 7
Personally Identifiable Information 7
Disaster Recovery Planning 7

2 Security Best Practices 8

3 Security for ADPRO XO 10

Securely Receive and Configure the Product 10
XO Firmware 10
Security Seal 10
Securely Install and Maintain the Product 11
Change Default Password 11
Increase password security 12
NTP Server 12
Securely Use the Product 12

SSH and Telnet Disabled by Default 12
Webserver Disabled by Default 13
Support for SED 13
Secure Boot 13
Port Management 14
Secure Video Streaming 14
Using VPN Server from Windows Server 2019 in ADPRO XO 14

CHAPTER

1 SECURITY GUIDELINES

Purpose

This document describes the network security features of the ADPRO XO NVR. It guides you in securing the data and communication of the NVR and the connected IP cameras.

Intended Audience

The target audience for this document will include System Integrators, Facility Administrators, and end-users, where applicable. It provides guidance and directions that minimize the effects of threats and vulnerabilities in the system by guiding the end-users to support the security program.

Solution Summary

Set up surveillance systems on a standalone network consisting of cameras and the ADPRO XO NVR.

Minimize the security risks by deploying ADPRO NVR and the connected IP cameras in a trusted network. Secure a network with a direct or indirect connection to the internet, using a firewall, network-based IDS (Intrusion Detection System), or IPS (Intrusion Prevention System). The firewall configurations must block all enabled ports except for HTTPS (443 or user-defined) and allow only the special access requests with approval from the CIO or a similar position.

In an intranet environment, Honeywell recommends using a dedicated router/ switch to connect to the camera or the NVR and use whitelists of IP / MAC addresses to restrict access to this router/switch, which will effectively reduce the possibility of an attack on an IP camera or the NVR from the intranet.

Security Checklist

- Use the latest version of firmware and software.
- Secure the server machine against unauthorized physical access.
- The ethernet connecting to the PC must be a local private network secured by firewalls and intrusion detection systems.
- The NVR is running the latest version of the OS with all updates and service packs.
- Set up user accounts on NVR to limit access to files only for authorized users.
- Password change at the end of commissioning.
- Ensure doing SSL configuration.
- Avoid physical unauthorized access to the camera, router, and NVR.

Packaging

The SI team gets the individual products and related components of the ADPRO XO NVR in sealed, boxed packages. Follow the instructions provided in the Installation Manuals that are part of the package.

Securing the ADPRO XO NVR

The following are the recommendations for securing NVR.

- Set the NVR login password that is tough to guess and difficult to brute-force. Use a mix of upper and lowercase letters, numbers, and special characters.
- Configure firewall on NVR server. Create a list of trusted and banned IP/MAC addresses at the corresponding port addresses.
- Change the default ports on all CCTV devices on the network that you can access remotely via the internet. Devices use ports 80 and 443 for HTTP, HTTPS, and other default ports such as RTSP port 554 and 3100. It is a two-step process.

Use the XO Client to change the default port numbers, and make sure not to use the default port numbers for anything other than the usage defined in the following table. For details, see the Restrictions for Port Number Usage section in the XO Client Software User Manual.

Software Updates

Camera:

Ensure that your camera firmware is up-to-date and that you are running the latest version of Configuration Tool.

The downgrade may pose a security risk to IP cameras as old firmware may not necessarily have security updates or security controls.

Router:

Ensure that you are running the latest version of the firmware on the router. Refer to the manufacturer's user guide to update the router firmware.

NVR:

Ensure that you are running the latest firmware on the XO NVR and the latest version of the XO Client software. If running an outdated version, update with the patches or fixes for vulnerabilities and bugs.

Removable Storage

Always scan SD cards and hard disks for viruses before using them with your camera and NVR.

Account Management

The admin user can assign different levels of access to user accounts. For example, one user can monitor and playback video while another can access various setup functions.

Assign different accounts to each user and entitle a specific right to a designated account.

Backup and Recovery

Backup camera and NVR configuration settings so that, if necessary, you can quickly recover your device.

Decommissioning/Disposal Management

Honeywell recommends resetting to factory default to clear the configuration / private data and reset it to factory default setting before the camera or the NVR is decommissioned or resold (See Upgrade & Maintenance section in User Guide for more information).

If there is an SD card in the camera, please remove and format it as well. Similarly, format hard drives on the NVR.

Vulnerability Reporting

Honeywell encourages coordinated disclosure of security vulnerabilities.

Honeywell invites security researchers, industry groups, government organizations, and vendors to report potential security vulnerabilities. You can select one of the two vulnerability types in the form below or email us with the below details mentioned.

If the vulnerability affects a product, service, or solution, email us at PSIRT@Honeywell.com with the following instructions/details.

Use Honeywell's public PGP key for encryption and include the following:

- Product and version
- Description of the potential vulnerability
- The additional configurations required to reproduce the issue
- Step by step instructions to reproduce the issue
- Proof of concept or exploit code, if available
- Potential Impact

For all other security issues, email us at security@honeywell.com with the following instructions.

Encrypt using the Honeywell public PGP key and include the following:

- Website URL or location
- Type of vulnerability (XSS, Injection, etc.)
- Instructions to reproduce the vulnerability
- Proof of concept or exploit code, including how an attacker could exploit the vulnerability
- Potential impact

To encrypt your message to our PGP key, please download it from here: https://www.honeywell.com/en-us/product-security#items_1555827156/

Physical Security

Ensure physical access to devices is restricted.

Security Updates

As part of AMC, the system integrator / technical support team will ensure that security updates and service packs are released & updated periodically. The AMC provisions firmware updates Over The Air (OTA) via a secure HTTPS channel.

Authentication

Authentication Mechanism

The authentication scheme governs the camera server, router, and NVR. Access to all requires a valid Username and Password.

Users

The user accounts follow a strict Role-based Access Control mechanism. The following are valid account roles and privileges:

Super Admin: The Super Admin is typically a System Integrator or Honeywell personnel. The Super Admin has unrestricted access. Super Admin can create, read, update, and delete anything, which includes users, devices, organizations.

Admin: Typically, a Facility administrator belonging to the customer entity. **Admin** can read and does not have the ability to add new users, devices, buildings, floors.

User: Typically, Facility personnel belonging to the customer entity. User can only view videos, view and take snapshots, and have no permission to control anything.

Passwords

Password rotation

Do password rotation as part of an effective password management strategy. The password rotation at regular intervals ensures that compromised passwords are not usable for an indefinite time. However, password rotation does create additional work for the end-user, and if done too frequently, encourages insecure practices such as writing down passwords in easily discovered areas.

Password composition

- Passwords must be a minimum length of eight (8) characters.

- Passwords must contain lowercase letters, uppercase letters, numbers and special characters.
- Passwords must not contain any portion of your network username, full name, address, or other personally identifiable information.
- New passwords must differ from the previous password.
- Do not reuse passwords for seven iterations of changes.
- Do not share account passwords between individuals.

Session management

A new session starts with each successful user login. A session expires every two hours or in case of an extended period of inactivity, whichever occurs first.

Encryption

The following are the two states of digital data:

- Data at Rest
- Data in Transit

Data at Rest

All sensitive data stored in the IP Camera, router, and NVR are encrypted. This data includes:

- Current user password
- Previous user password
- Internal database password
- Security key for password reset
- Videos, snapshots Encryption uses AES 256.

Secure Data at Rest

ADPRO XO supports SED drives that enable always encrypting all the data on the disk.

Data in Transit

The data transfer between the following:

- NVR and IP Camera.
- Router and NVR if remote access is enabled

- Router and Web server (Client Workstation) if remote access is enabled
- Router and Web Client (Client Workstation)/ Web app if remote access is enabled
- Occasionally between IP Camera and Honeywell Server for Secure update

Privacy Considerations

Personally Identifiable Information

Honeywell makes available several free-text or picture capture fields within its products. The design of these fields is not supposed to encourage personal data (so users should refrain from adding personally identifiable information). Instead, they intended to enhance user experience (for example, facilitate the labeling of projects and their location).

Disaster Recovery Planning

When developing the disaster recovery plan, ensure that it includes ALL data required to restore system operation.

Consider the backup frequency. The backup frequency must be adequate to ensure including changes in a backup. Use a backup naming convention for ease of identification.

Backups could serve the following purposes:

- Save the configuration to restore the system after an unexpected eventuality such as fire destroying the system resulting in retrofitting.
- All data is saved locally in the event of a network outage.
- Precaution before a system update.

CHAPTER

2 SECURITY BEST PRACTICES

The following are the best practices/recommendations for an ADPRO XO implementation:

Vulnerability	Best Practice
Camera Passwords	**Ideal** – Unique long password for each camera. **Acceptable** – • **Public Network**: Different strong password for each camera • **VLAN or Physical Private Network**: Common strong password for all cameras.
Port Forwarding	It is recommended not to connect the unprotected server to the Internet. If the server is connected to the internet, then "Port Forward" as few ports as possible and utilize a modern and sophisticated firewall.
Firewalls	A security expert must setup and configure a modern and sophisticated firewall. Document all the configurations and regularly monitor the firewall configurations and make necessary changes.
Network Topology	**Ideal** – Place security camera system on physically separate network from the rest of network. **Acceptable** – If not possible to separate the systems physically, use a VLAN.
Upgrade XO software	The XO software consists of: • the server firmware = the software that runs on your ADPRO XO device. • the client software = the software that runs on your PC. It is preferable to use the latest server firmware and client software.
Device password	Since XO 04.05.005, it is mandatory to change the default password of the XO device on first login. Make sure to set a strong password. To prevent unauthorized access to a device from your PC, you can leave the password setting on your XO Client blank, forcing a user to always manually enter the password when connecting.
Video Surveillance System Passwords	Change your security camera system passwords on a schedule. Strong passwords must be enforced as a stringent company standard.
Secure connection	The technician user can White List the XO device IP for SSH, and the SSH connection over the control port can be used to debug errors on the XO device. Disable the technical grant when not needed.
Video Encryption	For a truly secure system, the video should be encrypted, both when it is stored on disk and when it is in transit. ADPRO XO supports the usage of SED (Self-Encrypting Drive). Enable encrypted streaming by selecting the **Use encrypted streaming** checkbox while logging into the XO Client.
Mobile Access	Ensure that you have an encrypted connection for the mobile application. Set high quality password; do password enforcement & account deletion when staff changes. ADPRO XO supports **iTrace iCommand** mobile app for remote monitoring, verification, and control (iOS and Android).

Vulnerability	Best Practice
Physical Access to Equipment and Storage	The room housing the NVR, and the cabinets, cables, switches, and video storage servers must be safe. The room housing the NVR must have secure access along with video security monitoring. This will not only protect your network, but prevents 'smash and dash' thefts on the facilities, where the recording DVR/NVR is stolen along with any other items.
Manage software vulnerabilities	Keep the software and the firmware up-to-date and secure. Check for and install regular updates. Be directly proactive in monitoring the known security vulnerabilities.

CHAPTER

3 SECURITY FOR ADPRO XO

Ensue the following to protect ADPRO XO from any security vulnerability.

Securely Receive and Configure the Product

The ADPRO XO device and the software (executable files and firmware files) can be received and configured securely. The security seal on your XO device helps you remain assured that it is not tampered with.

XO Firmware

The ADPRO XO firmware and their filenames are as follows:

Firmware	Filename
ADPRO XO Client	ADPROXOClient_05.03.000x.exe (64-bit)
ADPRO iFT/eFT bin	iFT_eFT_XO_05_03_000x_x64.bin (64-bit)
ADPRO iFT/eFT image	iFT_eFT_XO_05_03_000x_x64.img.zip (64-bit)
ADPRO iFT Gateway bin	ADPROXO_05.03.000x-arm-ft2_sunchiph3.bin (32-bit)
ADPRO iFT Gateway image	ADPROXO_05.03.000x-arm-ft2_sun- chiph3.img.zip (32-bit)

Security Seal

The iFT/iFTE, eFT and iFT Gateway devices have security seals which will show compromised security if they are broken.







Securely Install and Maintain the Product

XO Client forces changing the default password and Increased password Security is the default option while creating a new user.

Change Default Password

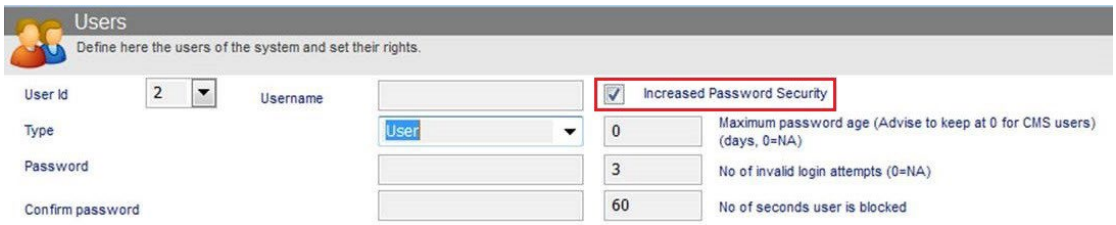
Change all the default user passwords on a XO system. (By default, this is User 0, User 1, User 15.) The new password must have an alphanumeric combination with at least 1 upper case letter, 1 lower case letter, and 1 digit and must be 8 to 15 characters in length.



Note: *Only XO Client forces changing the default password and the same is not applicable for other applications. Update password in the database of other applications when the XO password is changed. The password in the Xchange tool database must be the same as the XO password to be able to perform multiple firmware upgrade. Similarly, change passwords for all the applications with their own password database such as VCP (Video Central Platinum), VideoManager, iTrace, or any other 3rd party CMS.*

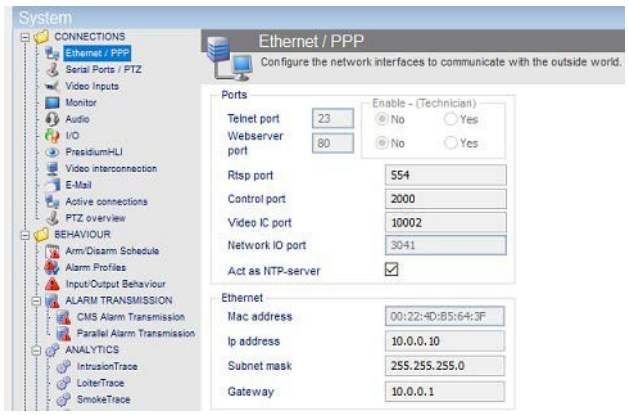
Increase password security

Using strong passwords lowers the chance of a security breach. Select the Increased password Security checkbox while creating a new user for the XO Client is now the default. You can set a value for the maximum password age, the number of invalid login attempts, and the number of seconds for which the user is blocked after the maximum number of invalid attempts.



NTP Server

Typically, a master XO device acts as a NTP server for other XO devices on the same site, but you can disable this if the XO device does not need to act as NTP server. (Deselect the **Act as NTP-server** checkbox on **System > Connections > Ethernet / PPP** page from XO Client.)



Securely Use the Product

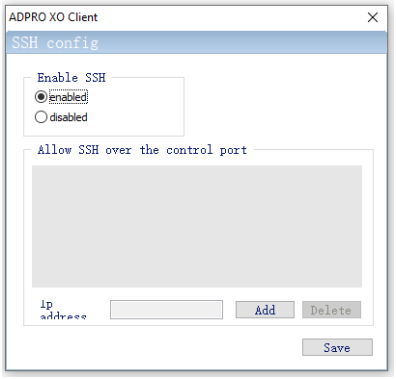
The accesses required for remotely investigating a field issue are disabled by default for secure use of the product.

SSH and Telnet Disabled by Default

Telnet and SSH are by default disabled on XO and can be enabled by a technician and a Whitelist for SSH can be filled in.

These accesses are activated only in rare scenarios such as remotely investigating a field issue. Ensure that these options are deactivated once again after the investigation. To enable/disable SSH, proceed as follows:

1. If required, enable the Technician user first.
2. Log on to the XO client as a technician user.
3. Choose System > Connections > Ethernet / PPP > SSH config.



4. Check enabled or disabled to enable SSH. You can also add Ip address and control port so that others are prohibited.
5. Click Save.
6. If required, disable the Technician grant again.

Webserver Disabled by Default

The Webserver is also disabled by default. It can only be reenabled by a technician on a system in which an admin user has enabled the technical grant.

Support for SED

For additional data safety, ADPRO XO 5.3 supports data storage in SED (Self-Encrypting Drive) which automatically and continuously encrypts the data on the drive without any user interaction.

Secure Boot

ADPRO XO 5.3 supports secure boot. Secure Boot detects tampering with boot loaders, key operating system files, and unauthorized option ROMs by validating their digital signatures. Detections are blocked from running before they can attack or infect the system. Secure Boot helps in ensuring the integrity of the firm- ware and the software.

Port Management

Honeywell has implemented strict port management on Honeywell XO Series NVR. The following ports are required by the NVR normal functions:

554 (RTSP port for video stream)

443 (HTTPS port for video stream)

3000 (Audio server port)

2000 (Control port)

33300 ~33400 (Camera event feedback port)

3040 (NetFinder port)

3041 (Network I/O port)

5555 (iPIR Walk test port)

10002 (Video interconnection port)

Secure Video Streaming

The XO 5.3 Client allows selecting the encrypted video streaming option. To enable encrypted video streaming, select the Use encrypted streaming checkbox while adding a device to the XO Client. The encryption is applied only on the input video stream and not on the input audio stream, and the XO device will need a restart when the encrypted streaming is applied.

Note: *The Honeywell Miracle cameras will not support audio-out functionality when encrypted streaming is used.*

Using VPN Server from Windows Server 2019 in ADPRO XO

You can set up VPN Server in Windows Server 2019 using its built-in Routing and Remote access features. The ADPRO XO 5.3 firmware supports using this VPN server. The security guidelines from Honeywell suggest configuring this key in Configure Pre-shared key, with a minimum of 30 characters, consisting of numbers, uppercase letters, and lowercase letters. Configure the key in the VPN Server and later configure it in the VPN configuration interface of the XO Client.

www.security.honeywell.com

ADPRO XO Security Guide
Rev.1.3
12/2022