Honeywell

ADPRO® XO™

eFT-S

Network Security Guide

Recommended

Find the latest version of this and other Honeywell documents on our website: https://buildings.honeywell.com/security.

Copy Right

© 2024 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 https://buildings.honeywell.com/us/en/support/legal/patents.

Revision

Issue	Date	Revisions
A	02/2024	New document.

Table of Contents

Scope 1
Compatible SKUs and Binaries 1
Application Scenarios 1
Software Updates 3
- Firmware Encryption 3
- Upgrade 3
- Downgrade 3

Removable Storage 3
Password Management 3
- Change Default Password 3
- Increase password security. 4

Port Management 4
Account Management 5
XO Client Secure Communication 5
Lockout Function 6
Backup and Recovery 6
Decommissioning/Disposal Management 6
Secure Communications and Hardening 6
- Webserver Disabled by Default 7
- Secure Boot 7
- Secure Storage Key 7

Vulnerability Reporting 7

Figures

Figure 1 Internet Connection with Firewall (Recommended) 2
Figure 2 Change Default Password 4
Figure 3 Increase Password Security 4
Figure 4 Enable XO Client Secure Communication 6

Tables

Table 1 Compatible SKUs 1
Table 2 Binaries 1

Scope

This document describes network security features of Honeywell ADPRO XO NVR Network Video Recorder (NVR) and provides guidelines to improve security of your video surveillance system.

Compatible SKUs and Binaries

For compatible SKUs information, refer to the table below.

Table 1 Compatible SKUs

Part Number	Description
680020060	ADPRO eFT-S, 8 IP Cam. licenses, no HDD, 6 inputs, 2 outputs, no PoE, 2 HDD slots
682020060	ADPRO eFT-S, 8 IP Cam. licenses, no HDD, 6 inputs, 2 outputs, 8 PoE, 2 HDD slots
680021660	ADPRO eFT-S, 8 IP Cam. licenses, 6 TB HDD, 6 inputs, 2 outputs, no PoE, 2 HDD slots
682021360	ADPRO eFT-S, 8 IP Cam. licenses, 2 TB HDD, 6 inputs, 2 outputs, 8 PoE, 2 HDD slots

Table 2 Binaries

Binaries	Description
ADPRO XO Client	ADPROXOClient_05.04.xxx.exe (64-bit)
ADPRO eFT-S bin	HON_ADPROXO_eFTS_ARM64_5.4.xxxx.bin

Application Scenarios

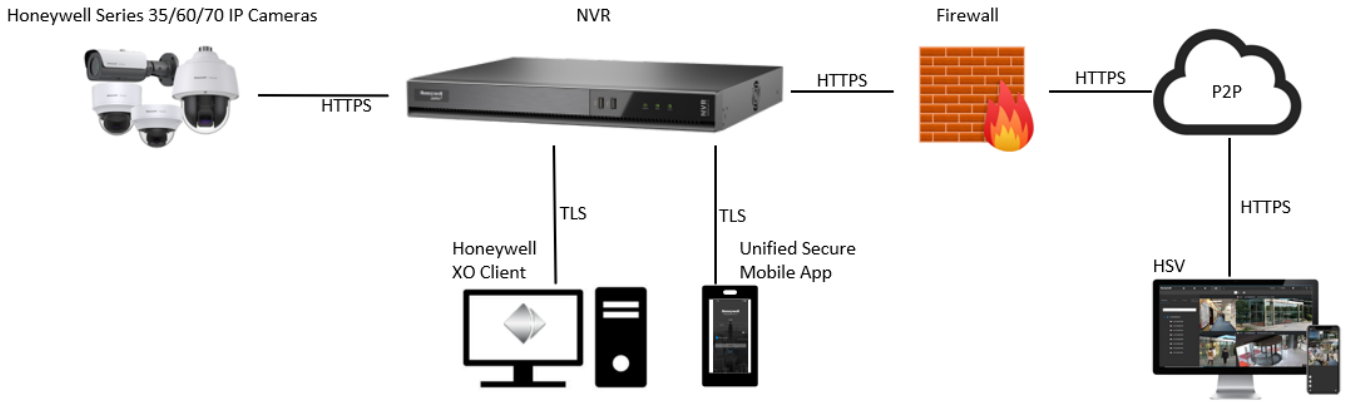
Surveillance systems are commonly set up on a standalone network consisting of cameras, NVRs/DVRs, and headend.

To minimize security risks introduced during deployment, please make sure the NVR is deployed in a trusted network. If the network is connected to the Internet, regardless of its directness or indirectness, there should be a firewall, network-based IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) in place.

In an intranet environment, Honeywell recommends user to use a dedicated router / switch to connect to the NVR and use whitelists of IP / MAC addresses to restrict access to this router / switch, which will effectively reduce the possibility of attacks (especially denial-of-service (DoS) and distributed denial-of-service (DDoS)) from the intranet.

It is recommended that you use NVR with Honeywell 35/60/70 series cameras and enable HTTPS for camera setting in NVR. The end-to-end stream encryption solution provides more secure stream transmission channel.

Figure 1 Internet Connection with Firewall (Recommended)



Note: *This guide only introduces how to secure the data and communication of Honeywell XO NVR. Total Honeywell solution is based on encrypted stream and commands (HTTPS). If there are other 3rd party cameras or platform connections, the encryption will be depended on the 3rd party.*

Honeywell recommends that you should follow our recommended scenes to deploy NVR in a secure environment due to:

- RTSP/RTP/RTCP over TCP/UDP are the most popular live stream transmission protocols today, which are widely used in almost all NVRs and IP Cameras. But they also have some security risks that can be exploited to cause the risk of sensitive data disclosure. RTSP over HTTPS is supported and strongly recommended on our device.
- SMTP is an Internet standard network protocol for email transmission, with which the TLS is used by default for Honeywell XO NVRs. You can set the device as non-TLS mode to make the device compatible with the existing SMTP server, however, it has some known security risks that can cause the sensitive data disclosure.
- SNMP is widely used in network management for network monitoring, default we are disable this function because not everyone need it. And if you want to use it, V3 is the recommended for XO NVR.

Since NTP / NAS / SMTP servers are out of scope, Honeywell recommends that you should deploy them in the same secure environment.

Note:

- *It is recommended that you should do physical protection regularly for NVR and its accessories.*
- *It is recommended that you should follow local law to legitimately use the NVR. When you need to collect some video recordings or snapshot data, especially some personal data, follow the data minimization principle and post up proper statement in the collected zone according to the local law.*

Contact our technical support on how to configure the firewall, NVR, HSV and HSV App.

Software Updates

Firmware Encryption

Honeywell provides Honeywell signed and encrypted firmware. The Honeywell signing can prevent tampered firmware being upgrade, and the encrypted firmware can prevent FW information disclosure.

Upgrade

Ensure that your NVR firmware is up to date and XO Client software updated.

Downgrade

Downgrade may cause security risk to NVR because old firmware may not have necessary security updates or security controls.

Removable Storage

Always scan HDD, USB and other storages for viruses before using them with your NVR

Password Management

When you log in your NVR for the first time, you will be required to initialize the admin password. The new password must be at least 8 characters in length, contain a mix of uppercase and lowercase characters, and include at least one number and at least one special character.

Honeywell recommends that you change all your passwords every 90 days for the NVR or its accessories.

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 at least 8 characters.

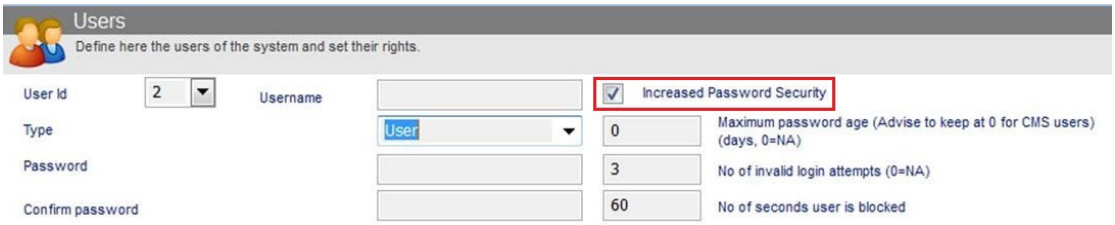
Figure 2 Change Default Password



Increase password security.

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.

Figure 3 Increase Password Security



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.*

Port Management

Honeywell has implemented strict port management on XO NVR, disabling unused or unsecured network services such as Telnet and FTP.

The following ports are required by the NVR normal functions:

- 554 (RTSP port for video stream)

- 443 (HTTPS port for video stream)
- 3000 and 3001 (Audio server port)
- 2000 and 2001 (Control port Communication)
- 33300 ~33400 (Camera event feedback - ports disabled by default)
- 3040 (NetFinder -port disable by default)
- 3041 (Network I/O - port disable by default)
- 5555 (iPIR Walk test - port disable by default)
- 10002 (Video interconnection - port disable by default)

Account Management

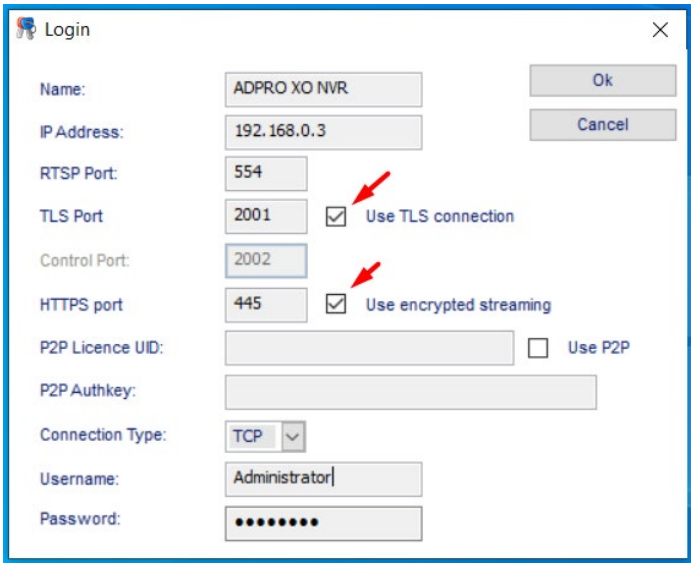
The admin user can assign different levels of access to different user accounts. For example, one user may only be allowed to monitor and play back video while another user may be allowed to use various setup functions.

It is recommended that you should apply different accounts to different users and entitle specific right to a designated account.

XO Client Secure Communication

Honeywell XO NVR supports logins using a secure remote client to set up, enable custom services and features, view streaming and more, the communication between the XO Client and XO NVR supports TLS v1.2 to control the device and supports streaming over HTTPS, ensure that the following checkbox are selected to protect the confidentiality and integrity of the data in transit.

Figure 4 Enable XO Client Secure Communication



Lockout Function

By default, user accounts are locked after 5 consecutively failed login attempts. The default lockout time is **30 minutes**. The lock will also be released if the device is restarted.

Backup and Recovery

Keep a backup of your NVR configuration settings, so that you can quickly recover your device if necessary.

Decommissioning/Disposal Management

Honeywell recommends that you should do factory default to clear the configuration or private data and reset it to factory default setting before the NVR is decommissioned or resold (refer to the sections about upgrade and maintenance in User Guide for more information).

If you need to install an HDD in the NVR, please format it before installation.

Secure Communications and Hardening

Ensure that the communication between Cameras, NVRs, VMS, NTP Server and any Gateway Module (such

as Video Guard device) should be within CCTV network with high security and use a firewall to restrict the communication.

Webserver Disabled by Default

The webserver is not supported by this eFT-S, the only way to manage and config the device is using the XO Client.

Secure Boot

ADPRO XO 5.4 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.

Secure Storage Key

ADPRO XO 5.4 supports a TPM Chip to protect private keys against unauthorized access and disclosure.

Vulnerability Reporting

Honeywell encourages coordinated disclosure of security vulnerabilities. Security researchers, industry groups, government organizations and vendors can report potential security vulnerabilities to Honeywell by choosing one of the two vulnerability types in the form below or by emailing us with below details mentioned.

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

Please encrypt using Honeywell's public PGP key and include the following:

- Product and version
- Description of the potential vulnerability
- Any special configuration 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.

Please encrypt using Honeywell's 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/

Building Automation – Security Americas (Head Office)
Honeywell Commercial Security
715 Peachtree St. NE
Atlanta, GA 30308
Tel: +1 800 323 4576

Building Automation – Security Mexico
Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,
CP 012010, CDMX, México.
Colombia: Edificio Punto 99, Carrera 11a.
98-50, Piso 7, Bogota, Colombia.
Tel: 01.800.083.59.25

Building Automation – Security Middle East/N. Africa
Emaar Business Park, Building No. 2, Sheikh Zayed Road
P.O. Box 232362
Dubai, United Arab Emirates
security_meta@honeywell.com
Tel: +971 4 450 5800

Building Automation – Security Europe/South Africa
Building 5 Carlton Park,
King Edward Avenue
Narborough, Leicester, LE19 0LF
United Kingdom
Tel: +44 (0) 1163 500714

Building Automation – Security Northern Europe
Stationsplein Z-W 961, 1117 CE Schiphol-Oost, Netherlands
Tel: +31 (0) 299 410 200

Building Automation – Security Deutschland
Johannes-Mauthe-Straße 14
D-72458 Albstadt
Germany
Tel: +49 (0) 7431 801-0

Building Automation – Security France
Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
Tel: +33 (0) 1 40 96 20 50

Building Automation – Security Italia SpA
Via Achille Grandi 22,
20097 San Donato Milanese (MI), Italy

Building Automation – Security España
Josefa Valcárcel, 24
28027 – Madrid, España
Tel.: +34 902 667 800

Building Automation – Security Asia Pacific
Building #1, 555 Huanke Road,
Zhang Jiang Hi-Tech Park Pudong New Area,
Shanghai, 201203, China
Tel: 400 840 2233

Building Automation – Security and Fire (ASEAN)
Honeywell International Sdn Bhd
Level 25, UOA Corp Tower, Lobby B
Avenue 10, The Vertical, Bangsar South City
59200, Kuala Lumpur, Malaysia
Email: buildings.asean@honeywell.com
Technical support (Small & Medium Business):

Vietnam: +84 4 4458 3369
Thailand: +66 2 0182439 Indonesia: +62 21 2188 9000
Malaysia: +60 3 7624 1530
Singapore: +65 3158 6830
Philippines: +63 2 231 3380

Honeywell Home and Building Technologies (India)
HBT India Buildings
Unitech Trade Centre, 5th Floor,
Sector – 43, Block C, Sushant Lok Phase – 1,
Gurgaon – 122002, Haryana, India
Email: HBT-IndiaBuildings@honeywell.com
Toll Free Number: 000 800 050 2167
Tel: +91 124 4975000

Building Automation – Security and Fire (Korea)
Honeywell Co., Ltd. (Korea)
5F SangAm IT Tower,
434, Worldcup Buk-ro, Mapo-gu,
Seoul 03922, Korea
Email: info.security@honeywell.com
Customer support: HSG-CS-KR@honeywell.com; +82 1522-8779
Tel: +82-2-799-6114

Building Automation – Security & Fire (Pacific)
Honeywell Ltd
9 Columbia Way
BAULKHAM HILLS NSW 2153
Email: hsf.comms.pacific@Honeywell.com
Technical support:
Australia: 1300 220 345
New Zealand: +64 9 623 5050

Honeywell

https://buildings.honeywell.com/security
+1 800 323 4576 (North America only)
Document 3014-0113-001 Rev A –02/2024