Honeywell

Honeywell 35 Series

IP Cameras

HC35W43R3	HC35W43R2	HC35WB3R3	HC35WB3R2
HC35WE3R3	HC35WE3R2	HC35W45R3	HC35W45R2
HC35WB5R3	HC35WB5R2	HC35WE5R3	HC35WE5R2
HC35W25R3	HC35W48R3	HC35W48R2	HC35WB8R3
HC35WB8R2	HC35WE8R3	HC35WE8R2	HC35WZ2R25
HC35WZ5R30	HC35WZ5R30W	HC35WB8R2	HC35WB5R5
HC35WE5R2G	HC35W25R3-M	HC35W42R2	HC35WB2R2
HC35W45R2M	HC35W25R3-H	HC35WP5B	HC35CE5R3
HC35CB5R3	HC35WF6R1	HC35WFCR1	HC35WMBAR1
HC35TB5R1JT07	HC35TB5R4JT10	HC35TE5R3JT21	HC35TE5R4JT35

Network Security Guide

Recommended

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

Copy Right

Revision

Issue	Date	Revisions
A	02/2022	New document.
B	11/2024	Add new 35 series SKUs. Add RTSP over UDP Multicast. Update TLS 1.2 & TLS 1.3. Update Lockout Function.

Table of Contents

Figures

1 Scope

This document describes network security features of Honeywell's 35 Series IP cameras and provides guidelines for improving the security of your video surveillance system.

2 Application Scenarios

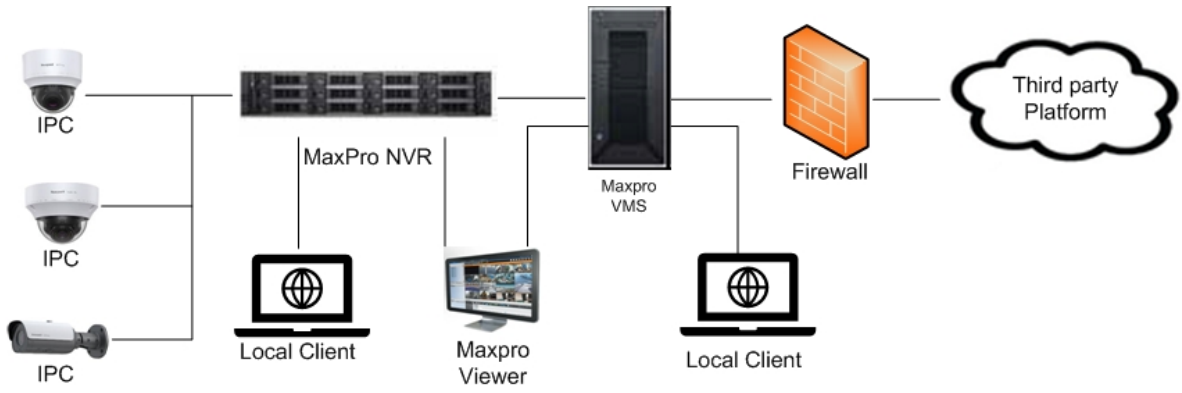
Surveillance systems are commonly set up on a standalone network, consisting of cameras, NVRs/DVRs, and a headend.

To minimize security risks introduced during deployment, please make sure the camera is deployed in a trusted network. If the network connection to the Internet, regardless of its directness or indirectness, there should have a firewall, network-based IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) in place, and configure firewall to block all ports that are enabled in the camera except for HTTPS (443 or user-defined) or there are explicit special access requests that get approval from your CIO or similar position.

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

In an intranet environment, Honeywell recommends enabling the camera's IP/MAC filter by going to **Setup > System Setup > Access List** to configure **Allowed IP Address** (The menu path for some special models may be different, so please refer to the user guides.) to prevent denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Figure 2-1 Internet Connection with Firewall (Recommended)



Note: *This guide only introduces how to secure the data and communication of 35 Series IP cameras. Honeywell strongly recommends that you should follow our recommended scenes to deploy camera in a secure environment due to reasons below.*

- RTSP/RTP is today the most popular live stream transmission protocol, which is widely used in almost all IP cameras, however, it has some security risks which can cause the sensitive data disclosure. RTSP over multicast is the same. RTSP over HTTPS is supported and recommended on our device.
- 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 35 Series IP cameras, you can modify it to V1 / V2 if it needs to be compatible with existing SNMP agent, which has some known security risks that can cause the sensitive data disclosure.
- ONVIF is a standard for how IP products within video surveillance and other physical security areas can communicate with each other, however, it has some security risks which can cause the sensitive data disclosure. Default we disable ONVIF, if you want to use it, ONVIF over HTTPS is recommended on our device. You can modify it to ONVIF over HTTP if you need camera to compatible with exist VMS/NVR, which has some known security risks that can cause the sensitive data disclosure.
- SMTP is an Internet standard network protocol for email transmission, with which the TLS is used by default for 35 Series IP cameras. You can set the device as non-TLS mode to make the device compatible with the existing SMTP server, however, which has some known security risks that can cause the sensitive data disclosure.
- IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. Honeywell 35 Series IP camera also support to connect to IEEE802.1X authentication network. Although the IEEE802.1X server is out of scope, Honeywell recommends you should deploy IEEE802.1X Server in secure environment if you enable the IEEE 802.1x client.

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

Note:
- *It is recommended that you should do physical protection regularly for IP camera.*
- *It is strongly recommended that you should follow local law to legitimately use the IP camera. 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.*

Please contact our technical support on how to deploy and configure firewall or configure Honeywell NVR.

3 Software Updates

Upgrade

Ensure that your camera firmware is up-to-date and that you are running the latest version of Unified Tool (refer to User manual).

Downgrade

Downgrade may pose security risk to IP camera as old firmware may not necessary security updates or security controls.

4 Removable Storage

Always scan SD cards and USB flash drives for viruses before using them with your camera.

5 Password Management

When you log in to your camera for the first time, you will be required to initial the default 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 (taken from the following set: -_!@%^.~?#$=+*:,&).

Honeywell recommends that you change your password every 90 days.

Note: *The strong password rule can't be enforced on ONVIF server due to the camera needs to be complied with the ONVIF standard and pass the ONVIF tool's test. It is recommended that you should follow the above Honeywell password rules on ONVIF client when setting/changing your password.*

6 Port Management

Honeywell has implemented strict port management on 35 Series IP cameras, disabling unused or unsecured network services such as Telnet, SSH, and FTP.

The following ports are enabled by default, you can manually disable them according to your practical application

- **80** (HTTP)
- **3702** (ONVIF)
- **554** (RTSP)
- **4096** (Unified tool discovery)
- **443** (HTTPS)
- **5353** (Bonjour)

7 Account Management

The admin user can assign different levels of access to different user accounts. “Viewer” user may only be allowed to monitor and change their own password, while “Administrator” user may also be allowed to access various setup functions.

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

8 Lockout Function

By default, user accounts are locked after five consecutive failed login attempts. The default lockout time is **5 minutes**.

Note: *For HC35W25R3-H / HC35WP5B / HA35P2L28 / HA35P5L37 / HA35P5F12 / HC35CE5R3 / HC35CB5R3 / HC35CE5R3K / HC35WF6R1 / HC35WFCR1 / HC35WMBAR1, the account is still locked if the camera is restarted.*

9 Session Timeout Mechanism

System will logout after **30 minutes** without operation on web interface, then you need to log in again. System will close the session after **60s** when web be closed abnormally.

10 HTTPS Secure Communication

Honeywell has enabled HTTPS by default on 35 Series IP cameras. For example, if you enter "http://171.2.1.32" in your web browser, the address will redirect to https://171.2.1.32.

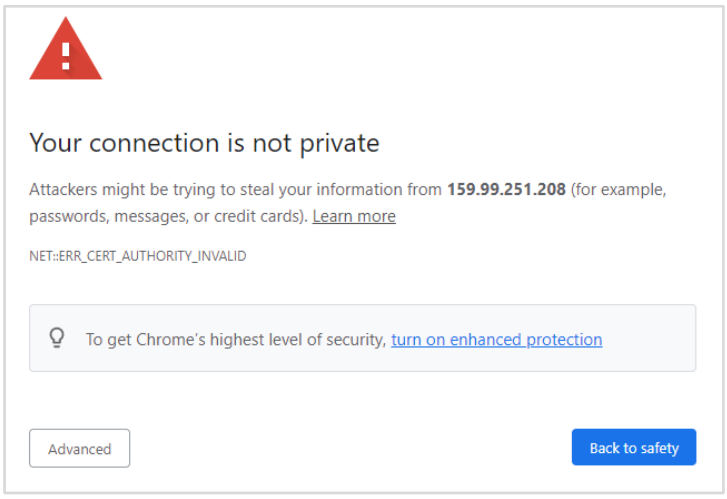
Installing a Security Certificate

When you log in to your camera for the first time, you will be prompted to download and install a signed security certificate.

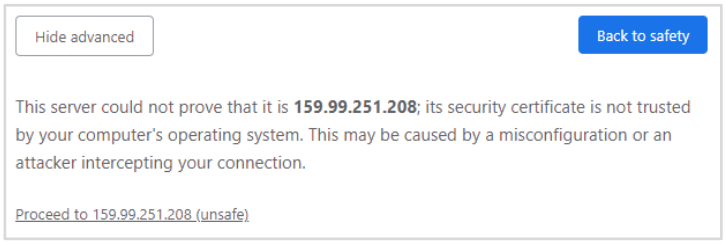
To download and install a signed security certificate, follow these steps:

1. Enter the IP address of the camera into your browser's address bar. You will see the following warning message:

Figure 10-1 Security Certificate Problem (Google Chrome)

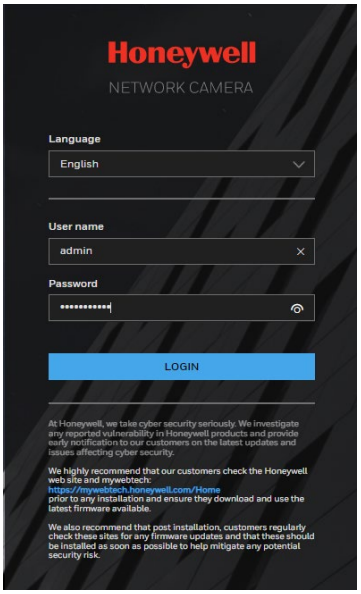


2. Click **Advanced**.



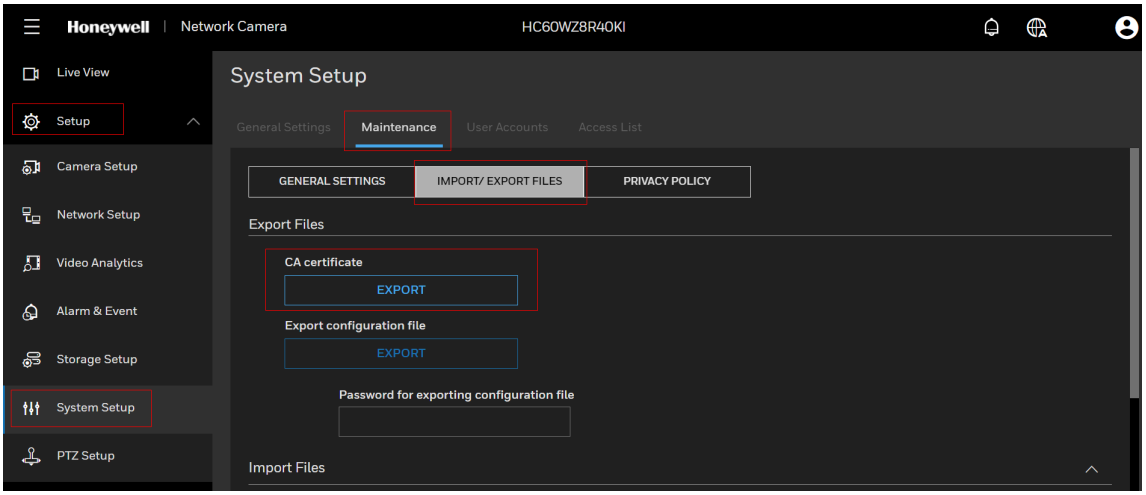
3. Click **Proceed to 159.99.251.208 (unsafe)**.
4. If you haven't initialized your camera, in the initial page, Set the default admin username and password, and then click **SAVE**.
5. If you have initialized your camera, in the login page, input your username and password, then **LOGIN**.

Figure 10-2 Login Interface

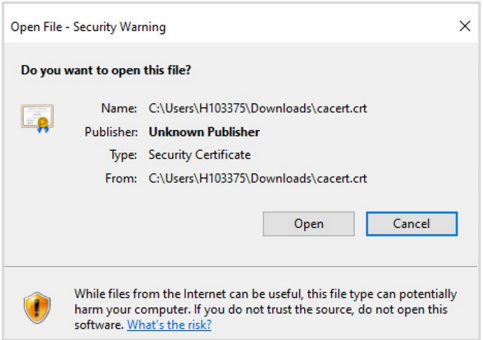


6. Go to **Setup** > **System Setup** > **Maintenance** > **IMPORT/ EXPORT FILES** page, and then find **CA certificate** row, click **EXPORT**, and save the root certificate **ca.crt**.

Figure 10-3 Certificate Tab

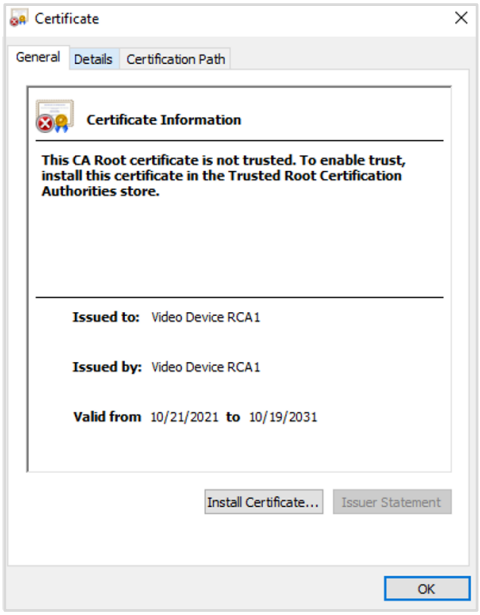


7. Double-click the ca.crt file, then click **Open** to open the certificate.



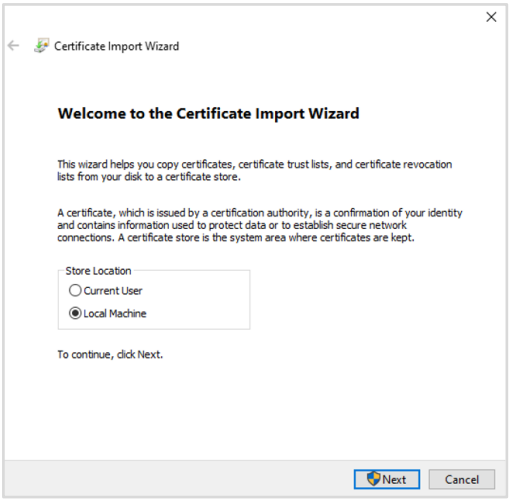
8. In the **Certificate** window, on the **General** tab, click **Install Certificate**.

Figure 10-4 Install Certificate



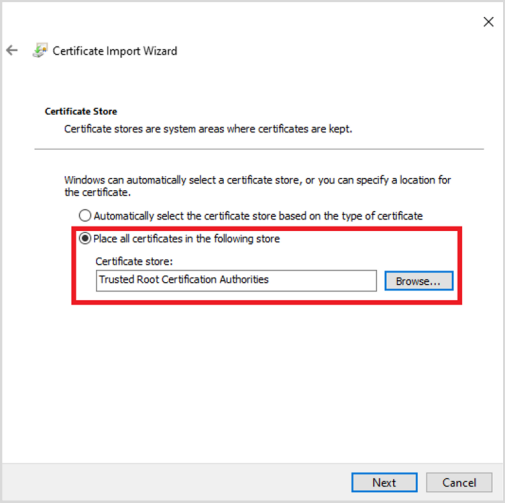
9. The **Certificate Import Wizard** opens. Click **Next** to continue.

Figure 10-5 Certificate Import Wizard 1



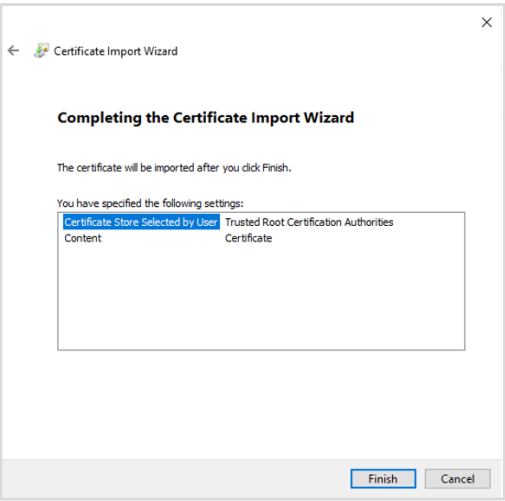
10. Select **Place all certificates in the following store**, select **Trusted Root Certificate Authorities** as the certificate store, and then click **Next**.

Figure 10-6 Certificate Import Wizard 2



11. Click **Finish** to import the certificate.

Figure 10-7 Certificate Import Wizard 3



You should now be able to reopen the web browser without receiving a warning about the website security.

Note:
- *Your Honeywell Camera/NVR requires a secure connection (HTTPS) to connect to the network to ensure your privacy. If you change the IP address, you will need to reboot the device for the warning messages to disappear.*
- *Do not configure a security exception as it will leave you vulnerable to phishing sites.*

Customized Certificate Info

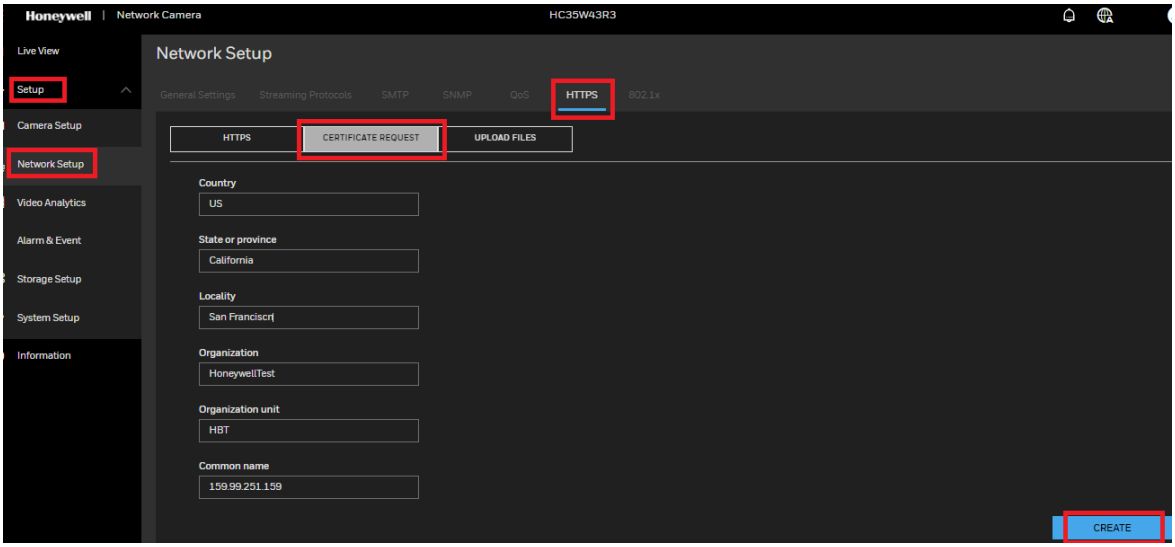
The self-signed certificate, which is not secure enough, is used as default for 35 Series IP Cameras. To

increase the security of HTTPS communication, it is recommended that you should customize the certificate information and import the Well-known certificate.

User can fill in certificate information he wants, and the certificate request file is provided to the certificate issuing authority for signing, then import to camera.

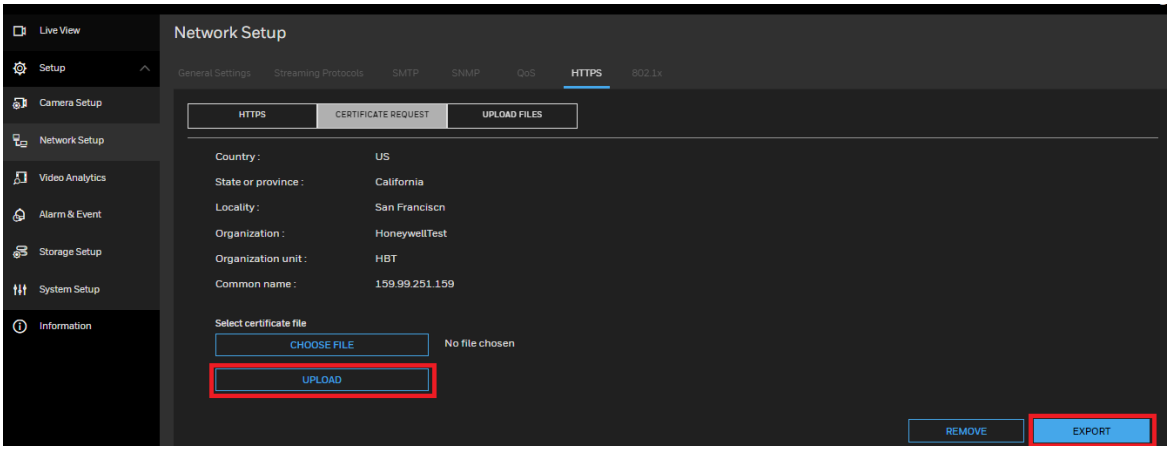
1. Go to **Setup** > **Network Setup** > **HTTPS** > **CERTIFICATE REQUEST** page.
2. Enter the required information, then click **CREATE** button.

Figure 10-8 Create Certificate Request



3. Click **EXPORT** to export your customized certificate request file.

Figure 10-9 Upload the Certificate



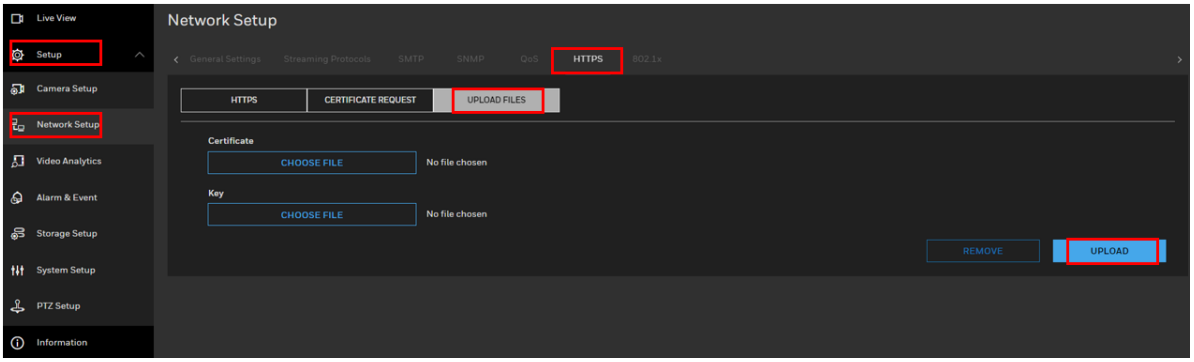
4. Use this request file to generate the Well-Known certificate from the Well-Known CA.
5. Click the **CHOOSE FILE** and **UPLOAD** button in Figure 10-9 to upload the Well-Known certificate file.
6. Then the Well-known certificate will be used instead of the original self-signed certificate.

The following interface for importing the Well-known certificate and key file directly is also provided on 35 Series IP Cameras.

1. Navigate to **Setup → Network Setup → HTTPS → UPLOAD FILES** page.

2. Select the Well-known certificate and key file that got from the Well-Known CA, then Click **UPLOAD** to import them to camera.

Figure 10-10 Upload Files



Then the Well-known certificate will be used instead of the original self-signed certificate.

Note: *If the certificate requirement file is exported from a device, only the certificate file needs to be imported; but if the certificate requirement file is exported from user self-signed or Well-known CA, both the certificate file and the key file need to be imported.*

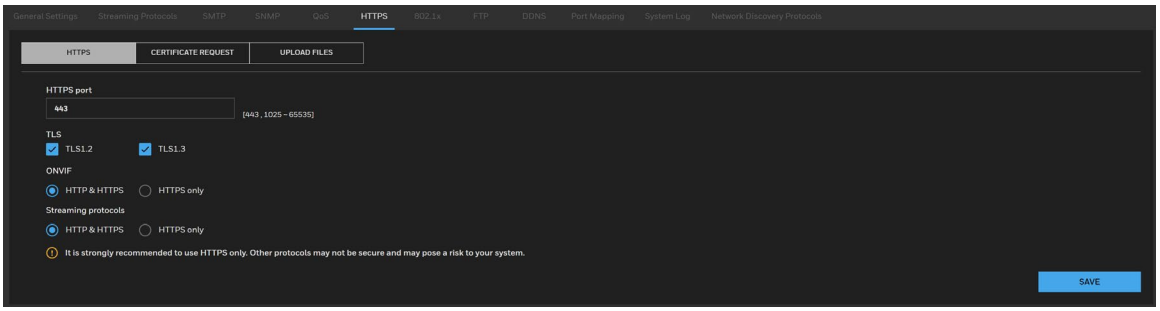
11 TLS 1.2 & TLS 1.3

All Honeywell 35 Series IP cameras use “TLS 1.2 only” to enhance “data transportation security”.

Note: *HC35W25R3-H / HC35WP5B / HA35P2L28 / HA35P5L37 / HA35P5F12 / HC35CE5R3 / HC35CB5R3 / HC35CE5R3K / HC35WF6R1 / HC35WFCR1 / HC35WMBAR1 cameras support “TLS 1.2 & TLS 1.3” to enhance “data transportation security”.*

For TLS 1.2 and TLS 1.3 setting, go to **Setup > Network Setup > HTTPS > HTTPS**. In the **TLS** (Transport Layer Security) section, the options for TLS 1.2 and TLS 1.3 are checked by default. Users can set the TLS according to their own security requirement.

Figure 11-1 TLS Setting



12 Backup and Recovery

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

13 Decommissioning / Disposal Management

Honeywell recommends that you should do factory default to clear the configuration / private data and reset it to factory default setting before the camera is decommissioned or resold (Please refer to the "Restoring the Camera" chapter in the user guide).

If there is a SD card in the camera, please remove and format it as well.

14 RTSP over UDP Multicast

35 Series IP cameras support RTSP over UDP multicast. It doesn't offer inherent security features. This is because:

- **UDP is connectionless**: There's no verification of who is receiving the data.
- **Multicast sends to a group**: Anyone on the network segment configured for the multicast group can potentially receive the stream.

  Here are some approaches to improve security for RTSP over UDP multicast:

- **Network Segmentation**: Isolate the multicast stream on a dedicated network segment with access controls. This limits who can be on the network and potentially eavesdrop.
- **VLANs**: Create a Virtual LAN (VLAN) specifically for the multicast stream. This further restricts access within the physical network.
- **IPsec tunnels**: Encrypt the entire data stream using IPsec tunnels. This encrypts both RTSP control messages and the media data itself. Requires configuration on both sender and receiver.
- **Secure Real-time Transport Protocol (SRTP)**: This is a security protocol specifically designed for RTP (the media transport protocol used with RTSP). SRTP encrypts and authenticates the media content. Requires compatible players and servers.

  Additional Considerations:

- **Strong passwords**: Use strong passwords for accessing the RTSP server and any management interfaces for the cameras or encoders.
- **ACLs (Access Control Lists)**: Implement Access Control Lists (ACLs) on network devices to restrict access to the multicast group based on IP addresses or MAC addresses.

Remember: Security is layered approach. Combining multiple techniques provides the best protection.

15 Vulnerability Reporting

Honeywell encourage 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 800-26989 Rev B –11/2024