Honeywell
THE POWER OF **CONNECTED**

equIP® Series Network Security Guide

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

Application Scenarios

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

To minimize security vulnerabilities, avoid connecting to the Internet if there is no special requirement to do so. If you do connect it to the Internet, ensure that you use a firewall or intrusion detection system (IDS).

In an intranet environment, Honeywell recommends enabling the camera's IP/MAC filter (**Setup > Network Setup > IP Filter**) to prevent denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Figure 1 Internet Connection with Firewall (Recommended)

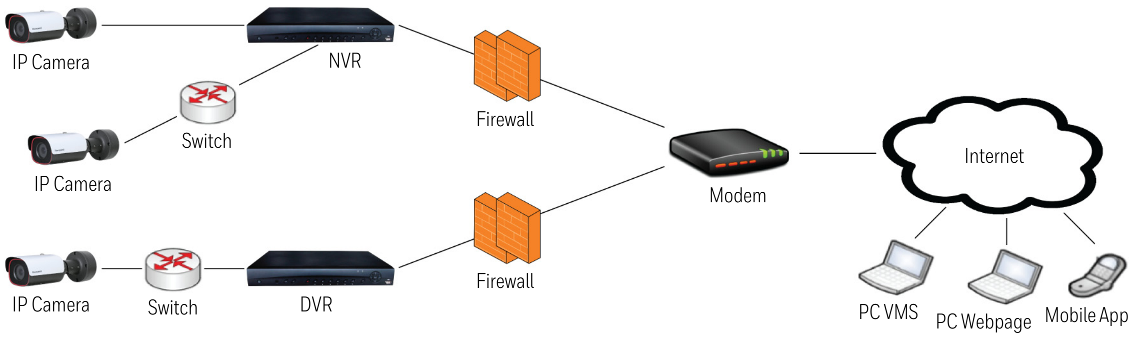


Figure 2 Intranet Connection with IP Filter Enabled (Recommended)

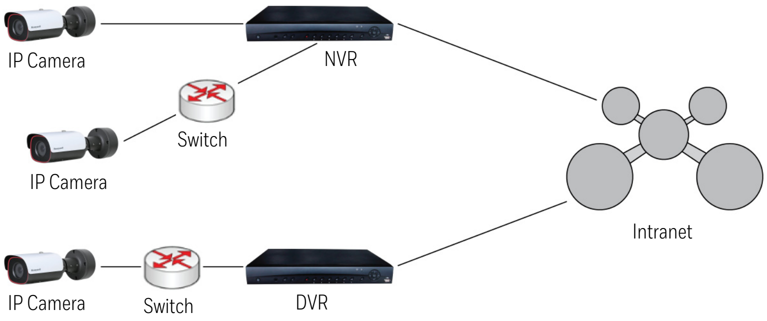
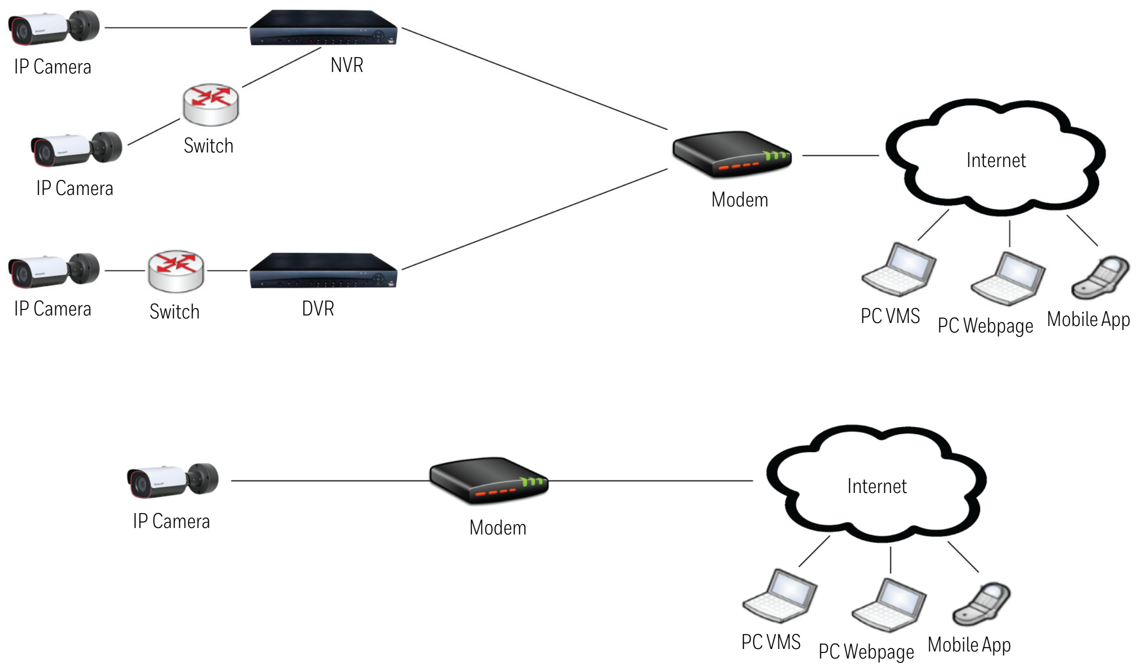


Figure 3 Internet Connection without Firewall (Not Recommended)



Software Updates

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

Removable Storage

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

Password Management

When you log in to your camera for the first time, you will be required to change 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.

Port Management

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

The following ports and services are permitted:

- **80** (HTTP)
- **443** (HTTPS)
- **554** (RTSP)
- **5000** (UPnP)
- **9080** (GLRPC)
- **37777** (Private Protocol)
- **49152** (Private Protocol)

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 also be allowed to access various setup functions.

Lockout Function

By default, user accounts are locked after five consecutive failed login attempts. The default lockout time is 15 minutes. The lock will also release if the camera is restarted.

HTTPS Secure Communication

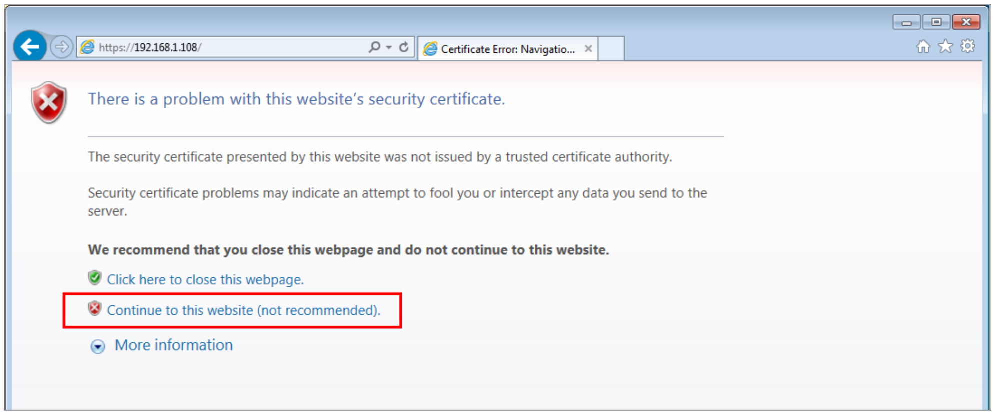
Honeywell has enabled HTTPS by default on equIP Series IP cameras. For example, if you enter "http://171.2.1.32" in your web browser, the address will redirect to "https://171.2.1.32."

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:



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

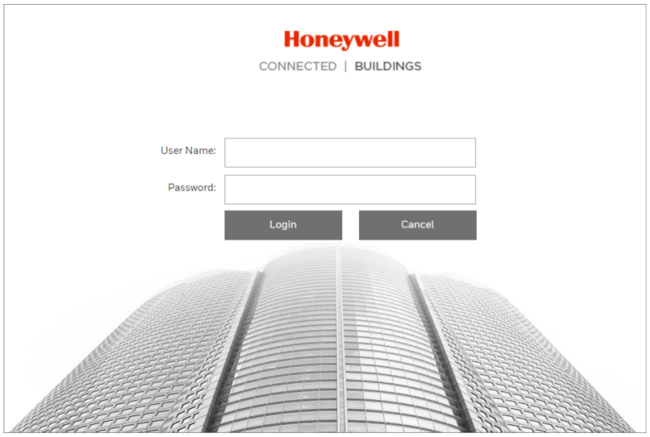
Click here to close this webpage.

Continue to this website (not recommended).

More information

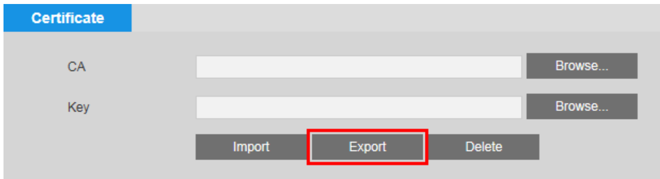
2. Click **Continue to this website**.

3. On the login page, enter the default admin user name (**admin**) and password (**1234**), and then click **Login**.



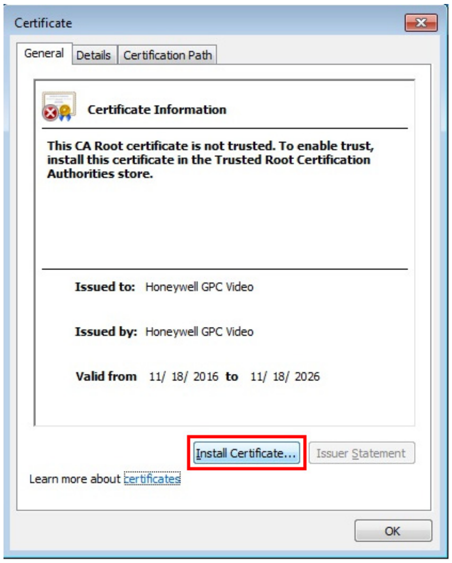
4. Create a new password. The web client interface opens in the browser.

5. Go to **Setup** > **Network Setup** > **Certificate**, and then click **Export**.



6. Double-click the **ca.crt** file.

7. In the **Certificate** window, click **Install Certificate**.



Certificate Information

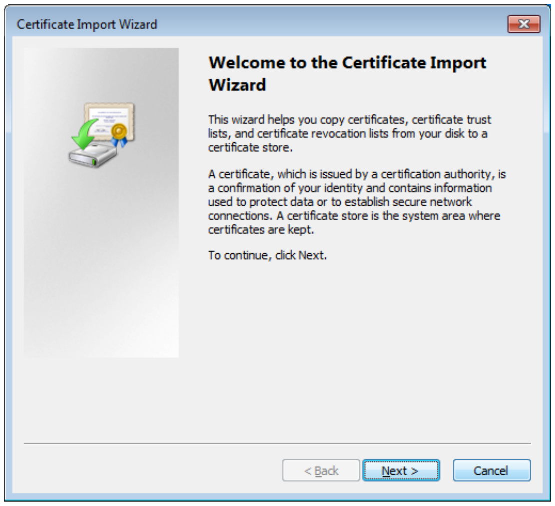
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Honeywell GPC Video

Issued by: Honeywell GPC Video

Valid from 11/ 18/ 2016 **to** 11/ 18/ 2026

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



Certificate Import Wizard

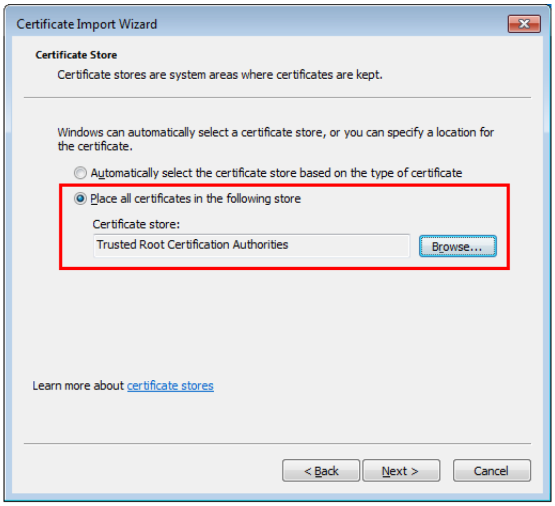
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

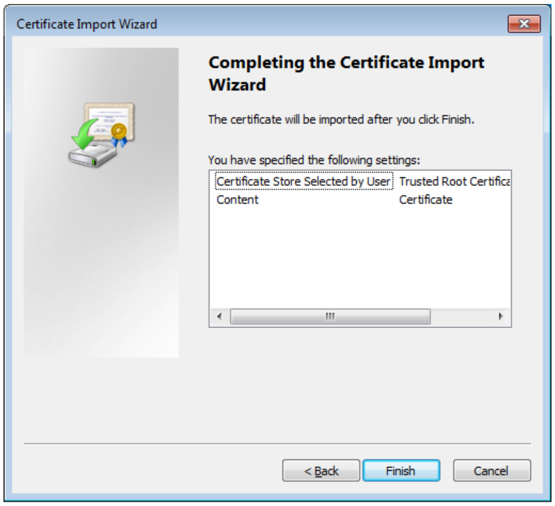
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

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



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

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

Note Your Honeywell 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.

Note Do not configure a security exception as it will leave you vulnerable to phishing sites.

TLS 1.2

All of Honeywell's equIP Series IP cameras use TLS 1.2 only. Outdated encryption algorithms, such as RC4, MD5, and SHA1, are not used.

Backup and Recovery

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

Vulnerability Reporting

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services. If you are a security researcher and believe you have found a security vulnerability, please send an email to us at security@honeywell.com with as much of the below information as possible. This information will help us to better understand the nature and scope of the possible issue.

- Type of issue (buffer overflow, SQL injection, cross-site scripting, etc.)
- Product and version that contains the bug
- Service packs, security updates, or other updates for the product you have installed
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue
- Proof-of-concept or exploit code
- Impact of the issue, including how an attacker could exploit the issue

To encrypt your message to our PGP key, please download it from here: https://www.honeywell.com/-/media/Honeywell_com/Files/Flash/Honeywell_CIRT.ASC?la=en.

You should receive a response within 24 hours. If for some reason you do not, please follow up with us to ensure that we received your original message.

For submission purposes, a security vulnerability is defined as a software defect or weakness that can be exploited in a cyber attack to reduce the operational or security assurances provided by the software.

Honeywell

www.honeywell.com/security
+1 800 323 4576 (North America only)
https://www.honeywellsystems.com/ss/techsupp/index.html

Document 800-23224 – Rev A – 04/2017