| | | | | | |
|---|---|---|---|---|---|
| **Title:** | Hikvision Factory Hardening Practices | **Version:** | v1.0 | **Date:** | 080116 |
| **Product:** | Cameras/NVRs/DVRs/VMS | | | **Page:** | 1 of 7 |
| **Action Required:** | None, Information Only | | | | |

## Summary

This document provides a brief overview of factory hardening, securing data in transit, and additional steps for hardening Hikvision products. Hikvision products have telnet disabled by default and the super-user with admin right has been removed. There is no default password on Hikvision devices. Specific packets associated with the plug-and-play function are encrypted. We provide for the ability to change default ports to make IP appliances less "visible" on the network and, therefore, less prone to attack.

With HTTPS enabled, all command and control data will have SSL and TLS encryption and is securely transmitted via TCP/IP using cryptographic keys based on SSL and TLS to prevent eavesdropping or tampering.

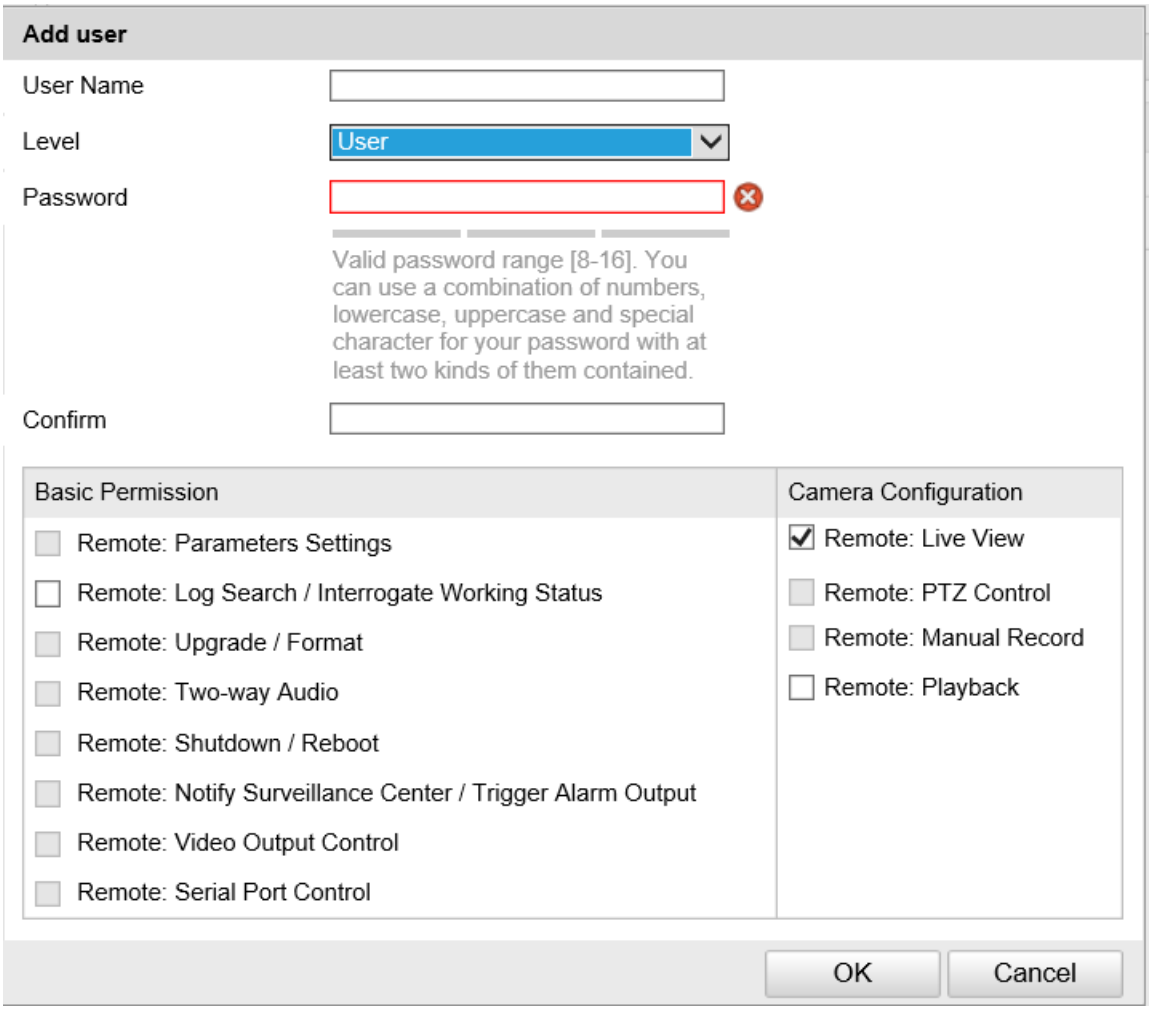
## Activating Hikvision Products

Prior to first use, Hikvision Cameras, NVRs, and DVRs require activation by setting a strong password. Hikvision's Secure Activation requires a minimum of eight characters of three or more different characters: numerals, uppercase letters, lowercase letters, and special characters. There is no default password; activation requires that a complex password be set to activate and use Hikvision devices in order to increase product security.

## User Accounts

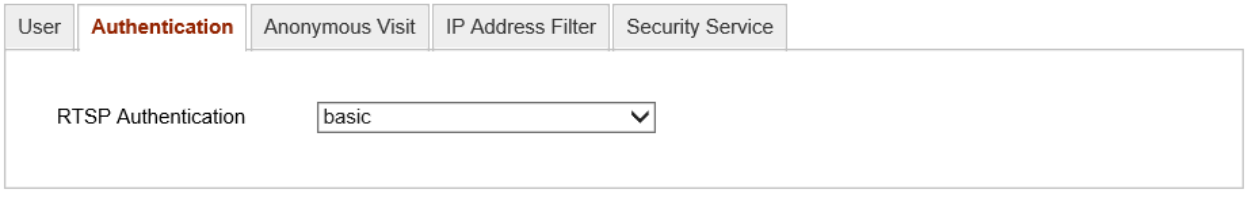
There are three type of User Accounts; Admin, Operator, and User to provide for granular user permissions. The *admin* user has all permissions by default and can create, modify, or delete other accounts. User accounts can be created by setting the user level such as Operator or User.


908 Canada Court, City of Industry, CA 91748 • Phone: +1 909-895-0400 • Fax: +1 909-595-0788
E-Mail: techsupport.usa@hikvision.com • www.hikvision.com




## The Live View Stream Can Be Secured with Real Time Streaming Protocol (RTSP)

Authentication is required to secure the live view stream with Real Time Streaming Protocol (RTSP). Options are basic or disabled.



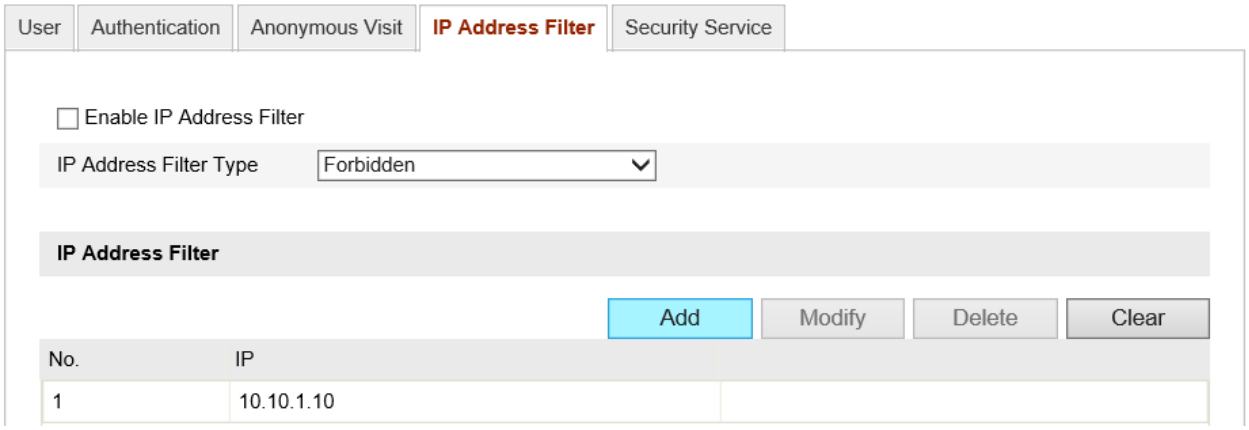


908 Canada Court, City of Industry, CA 91748 • Phone: +1 909-895-0400 • Fax: +1 909-595-0788
E-Mail: techsupport.usa@hikvision.com • www.hikvision.com

Enabling or disabling **Anonymous Visit** permission can be accomplished by setting **Enable** or **Disable** from a drop-down list.


## The IP Address Filter Can Be Configured for Access Control

The IP Address Filter can be set as shown below:



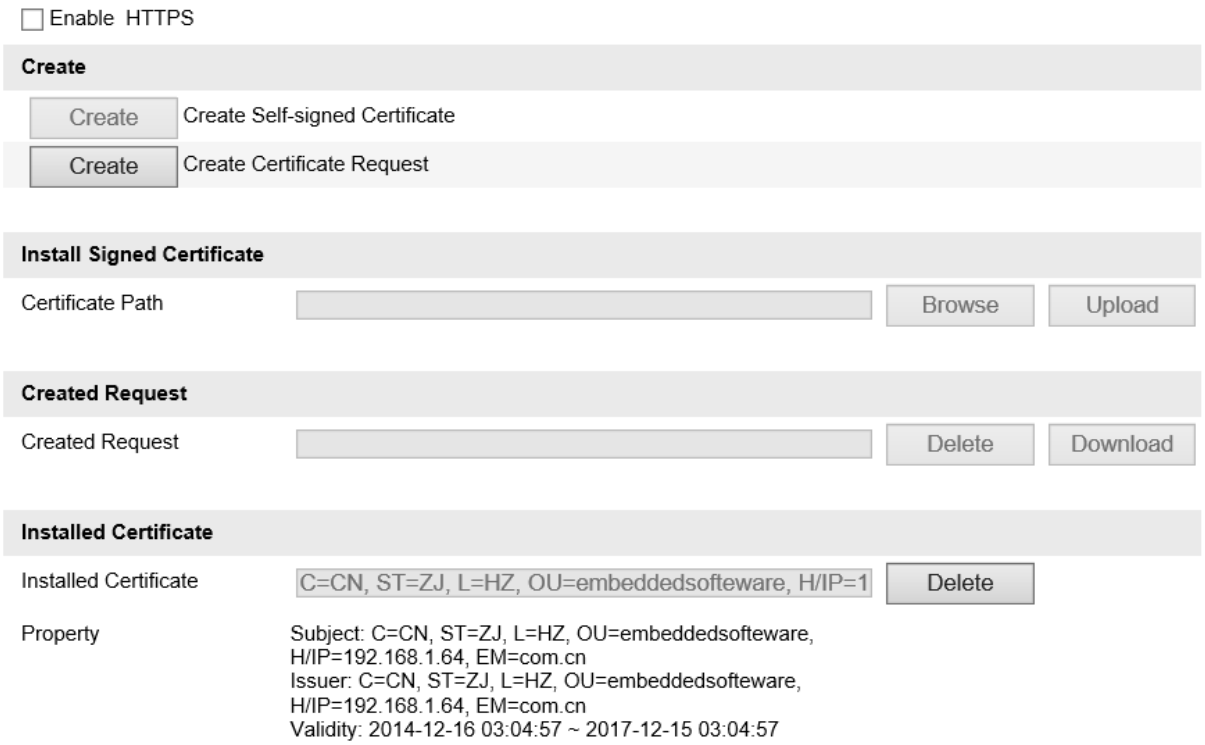

## The Camera's Security Service Enables Remote Login and Improved Data Communication Security

The Security Service can be configured with the following features:


- The **Enable SSH** checkbox enables/disables the data communication security.

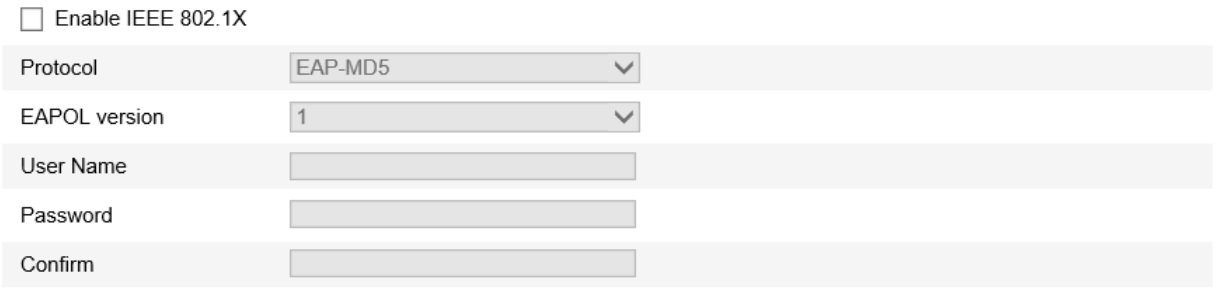

908 Canada Court, City of Industry, CA 91748 • Phone: +1 909-895-0400 • Fax: +1 909-595-0788
E-Mail: techsupport.usa@hikvision.com • www.hikvision.com

- The **Enable Illegal Login Lock** checkbox locks the device if an incorrect user name or password is input five times sequentially.
- The Web site and the associated Web server can be secured with HTTPS for the device one is communicating with, which protects against man-in-the-middle attacks.
- The following steps enable HTTPS and set the https port number:




## User Authentication Required When Connecting To Hikvision Devices with IEEE 802.1X Standard

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to a network protected by the IEEE 802.1X standard. 802.1X settings can be configured as per the following example:




## Hikvision Cybersecurity Initiatives

Hikvision has embarked on numerous Cybersecurity initiatives, including the following:

- Hikvision has eliminated the use of default passwords.
- The company's products provide the flexibility to change default ports to make IP appliances less "visible" on the network and, therefore, less prone to attack.
- Hikvision software limits where network traffic can originate.
- The company's product team tests hardware and software to ensure any known issues are resolved prior to the release of new firmware.
- An internal security team has been established to review and make recommendations regarding possible security risks and future enhancements.
- Telnet is disabled by default.
- Super-user account admin rights have been removed.
- Hikvision conducts Cybersecurity seminars and Webinars on security best practices to assist integrators and end users.
- Notification procedures are distributed when issues are suspected.
- White papers and presentations are published to educate and inform the user base of security best practices.
- Hikvision products' implement secure activation procedures that require a minimum of eight characters of three or more different password characters: numbers, upper case letters, lower case letters, and special characters.


908 Canada Court, City of Industry, CA 91748 • Phone: +1 909-895-0400 • Fax: +1 909-595-0788
E-Mail: techsupport.usa@hikvision.com • www.hikvision.com

- Hikvision's Network and Information Security Lab audits hardening processes for compliance.
- Specific packets associated with the plug-and-play function are encrypted.

## Third-Party Testing

Hikvision has contracted the renowned security data and analytics company, Rapid7, to perform penetration tests and vulnerability assessments of its products.

- Testing includes cameras, embedded recorders, VMS, and software tools.
- All findings required access to the network. The Web interface was resilient against an array of attacks, including the OWASP Project Top 10.
- Network protocols were resistant to tampering.

## Third-Party Certification

- As part of a continuous improvement program, Hikvision achieved Capability Maturity Model Integration (CMMI)[1] Certification Level 5 in 2016.
- CMMI Certification Level 5 indicates a focus on continually improving process performance through both incremental and innovative technological improvements.
- In keeping with the CMMI standards, Hikvision's software development department has set up mandatory regulations regarding the acquisition of all open source material and downloads of development tools from authorized sources.

[1] CMMI certification entails control and optimization of development processes, including a standardized development environment, project planning, development tools, and working rules.

**Capability Maturity Model Integration** (**CMMI**) is a process improvement training and appraisal program and service administered and marketed by Carnegie Mellon University (CMU) and required by many DoD and U.S. Government contracts, especially in software development. CMU claims CMMI can be used to guide process improvement across a project, division, or an entire organization.


908 Canada Court, City of Industry, CA 91748 • Phone: +1 909-895-0400 • Fax: +1 909-595-0788
E-Mail: techsupport.usa@hikvision.com • www.hikvision.com

| | | | | | |
|---|---|---|---|---|---|
| **Title:** | Hikvision Factory Hardening Practices | **Version:** | v1.0 | **Date:** | 080116 |
| **Product:** | Cameras/NVRs/DVRs/VMS | | | **Page:** | 7 of 7 |
| **Action Required:** | None, Information Only | | | | |

## Hikvision Security Center Website

Hikvision's online Security Center provides users with the knowledge to better protect their systems. The Security Center includes, among other information, the following items:

- Updated security notices
- Cybersecurity best practices documentation
- Instructions on how to change passwords on Hikvision IP cameras and recorders
- Instructions on how to upgrade firmware on Hikvision IP cameras and recorders
- Contact information in the event of a security concern or potential vulnerability reporting


908 Canada Court, City of Industry, CA 91748 • Phone: +1 909-895-0400 • Fax: +1 909-595-0788
E-Mail: techsupport.usa@hikvision.com • www.hikvision.com