VIVOTEK

Security Hardening Guide

Version 1.0

January 03, 2017

About this Document

The intended use of this guide is to harden devices and also provide collateral for deployment teams to deal with local network policy, configurations and specification.
All settings described in this document are made in the product's webpages. To access the webpages, see the User Manual of the specific product.

Liability/ Disclaimer

Please inform your local VIVOTEK office of any inaccuracies or omissions. VIVOTEK cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VIVOTEK shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights

VIVOTEK has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents or pending patent applications in the Taiwan, United Sates and other countries. This product contains licensed third-party software also. Please visit VIVOTEK website for more information.

Trademark Acknowledgments

The trademark "VIVOTEK" or any other trademarks, service marks, trade names, distinctive logos, pictures, or designs as designated by VIVOTEK and as used on or in connection with the Product are the sole properties of VIVOTEK ("VIVOTEK Trademarks and Trade Names").
VIVOTEK are registered trademarks or trademark applications in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

User hereby acknowledges and recognizes that any and all "VIVOTEK's Trademarks and Trade Names, patents, copyrights, know-how and other intellectual property rights" used or embodied in the Product are and shall remain the sole properties of VIVOTEK.
.

Support

Should you require any technical assistance, please contact your VIVOTEK reseller/distributor. VIVOTEK distributor contact information could be found on Where to Buy section at VIVOTEK website. To enhance customer satisfaction, your reseller/ distributor will reach us in a timely manner if the issue is not solved with first response.

We encourage you to take advantage of the many online resources VIVOTEK offers.

- VIVOTEK Downloads: With useful materials, such as brochure, firmware/software update.
- VIVOTEK Support: Including Top FAQ, Technical Videos, and Security Hardening Guide with efficient on-line assistance.
- VIVOTEK Customer Community: To obtain assistance from VIVOTEK technical support team, you can register and discuss problems in our on-line customer community and engage more with VIVOTEK's solutions, and service.

Learning Center

Visit VIVOTEK Learning Center for advanced feature articles and white papers and enjoy VIVOTEK Warrior Academy global training program.

Contact Information

VIVOTEK INC.
6F, No. 192, Lien-Cheng Rd., Chung-Ho Dist., New Taipei City, Taiwan. R.O.C. 23353
Tel: +886-2-8245-5282
Fax: +886-2-8245-5532
http://www.vivotek.com/

Table of Contents

Introduction

There is an information security team to review the product design inside VIVOTEK and VIVOTEK also has cooperated with many well-known information security companies for many years to make sure our products are secure.

However proper camera and network configurations are also key to security surveillance systems.

There are many suggestions for cyber defense in the document "The CIS Critical Security Controls for Effective Cyber Defense" (https://www.cisecurity.org/critical-controls/), we will instruct you all the related settings in the following chapter according to those suggestions.

Security related settings are divided into 3 levels : Basic, Advanced and Enterprise. You may determine the security level according to your environment and requirements.

Basic: We recommend you at least achieve the basic level. It is usually for closed network environments.

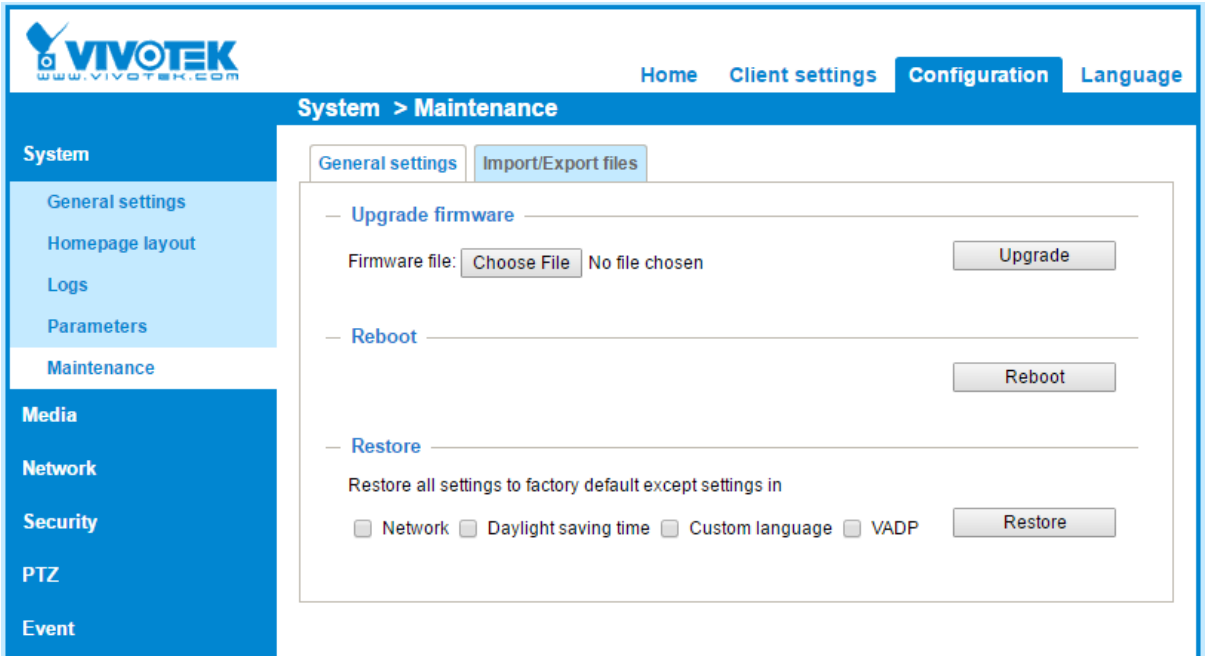
Advanced : Including the settings of Basic level and provides the settings for WAN accessible / Under insecurity network or risk environments.

Enterprise : Including the settings of Basic and Advanced levels and provides the settings for corporation with complex and sound network infrastructure and IT management.

Basic

Upgrade Firmware

CSC 2: Inventory of Authorized and Unauthorized Software
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 18: Application Software Security

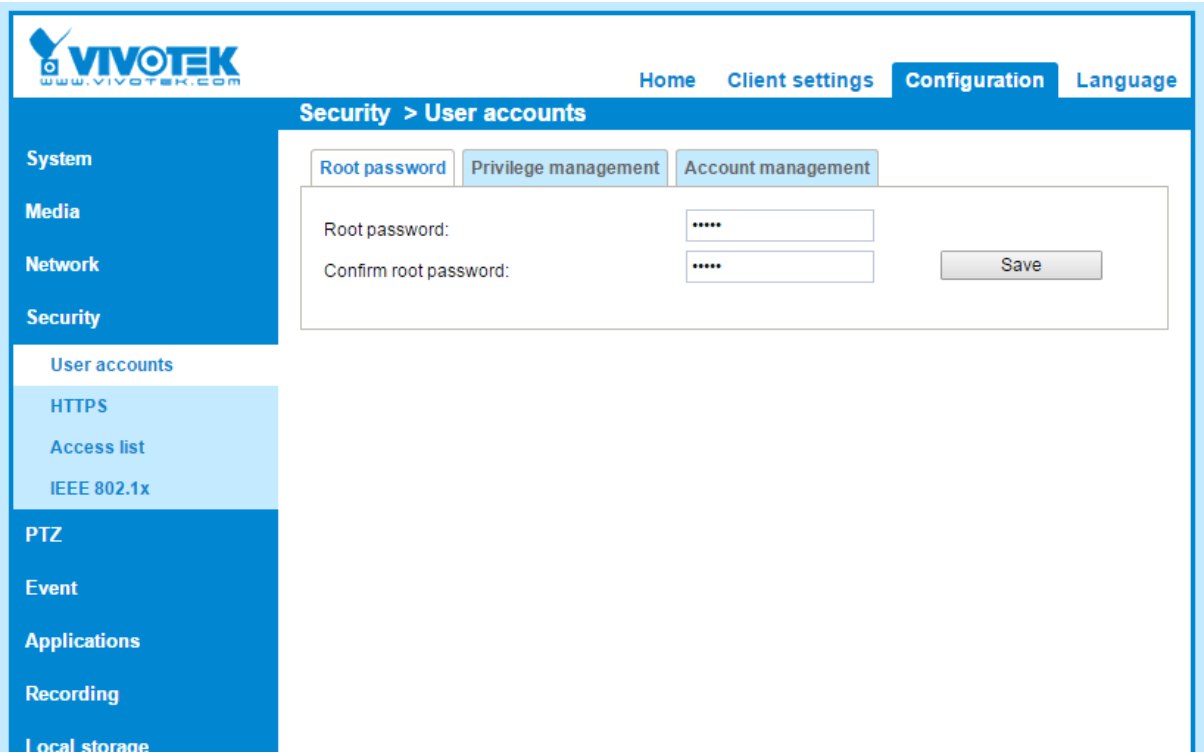


Always use the latest firmware. The latest firmware will fix all security issues and patch the security update from 3rd party libraries.

Not only public vulnerabilities, the latest firmware will also fix all the internal security issues uncovered by the VIVOTEK security team.

Set Root Password

CSC 5: Controlled Use of Administrative Privileges



The default password is blank and leaving the root password field empty means the camera will disable user authentication whether there are other existing accounts or not. Please assign a password as soon as possible once you enable the camera because it is VERY DANGEROUS and not recommended to leave it blank.

Assigning a password is very critical, and a good password just as important. A weak password is also dangerous, such as simple numbers:123456, 111111, and so are common words, such as admin, root, pass, qwerty... and so on.

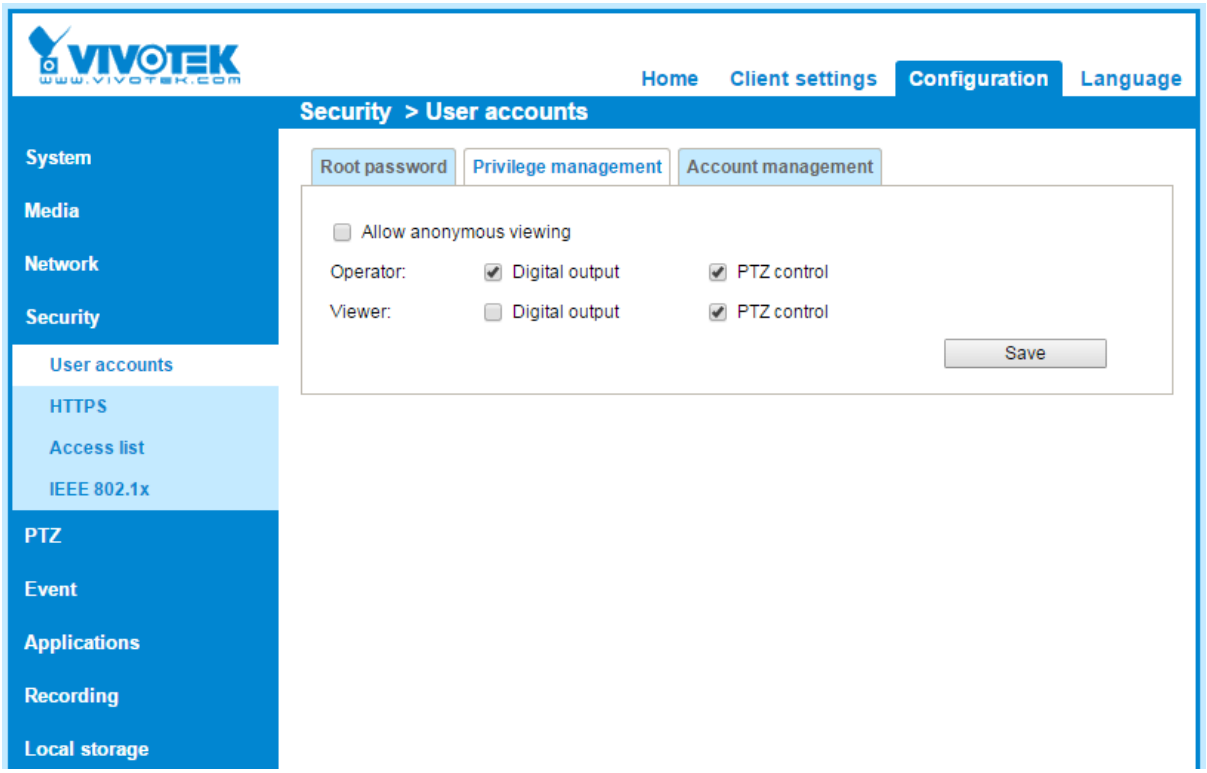
Passwords should contain:

- a minimum of 1 lower case letter [a-z] and
- a minimum of 1 upper case letter [A-Z] and
- a minimum of 1 numeric character [0-9] and
- a minimum of 1 special character: !$%-.@^_~

and the length must be at least 8 characters long.

Disable Anonymous viewing

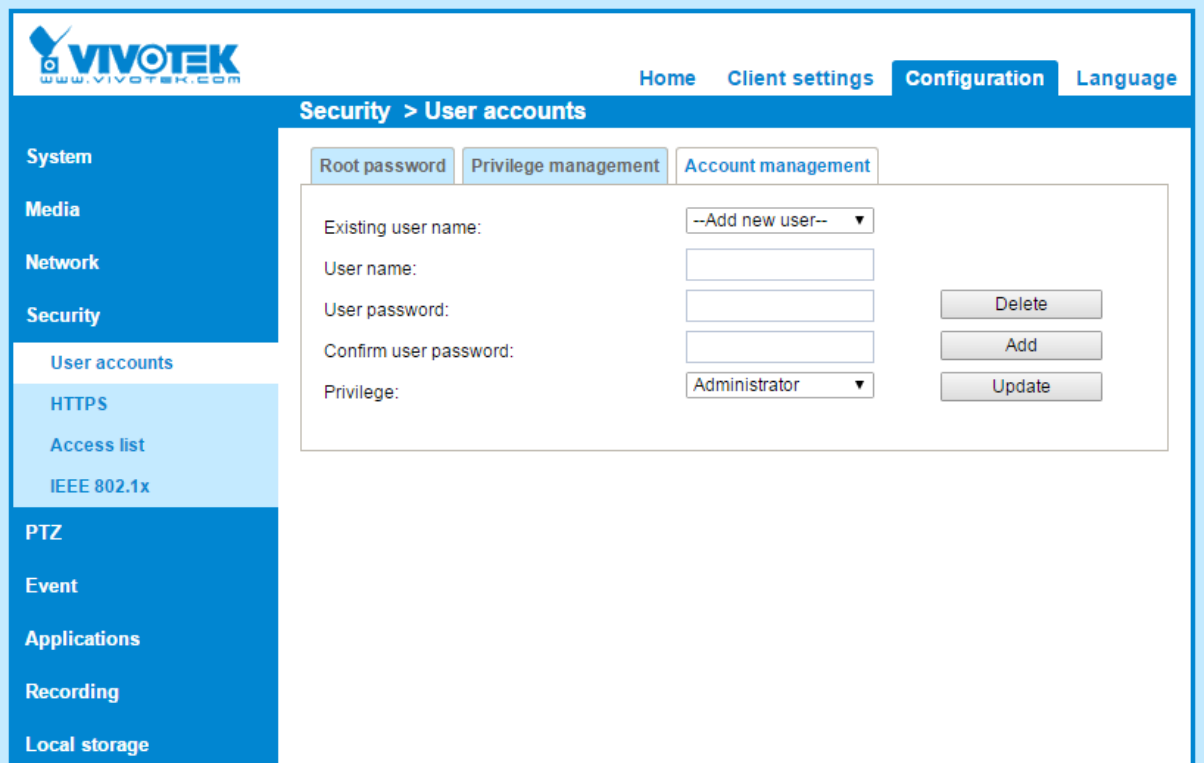
CSC 16: Account Monitoring and Control



Uncheck [Allow Anonymous viewing] if the camera is not public.
Once you enable Allow Anonymous viewing, the **RTSP streaming authentication will be ignored**.

Privilege management

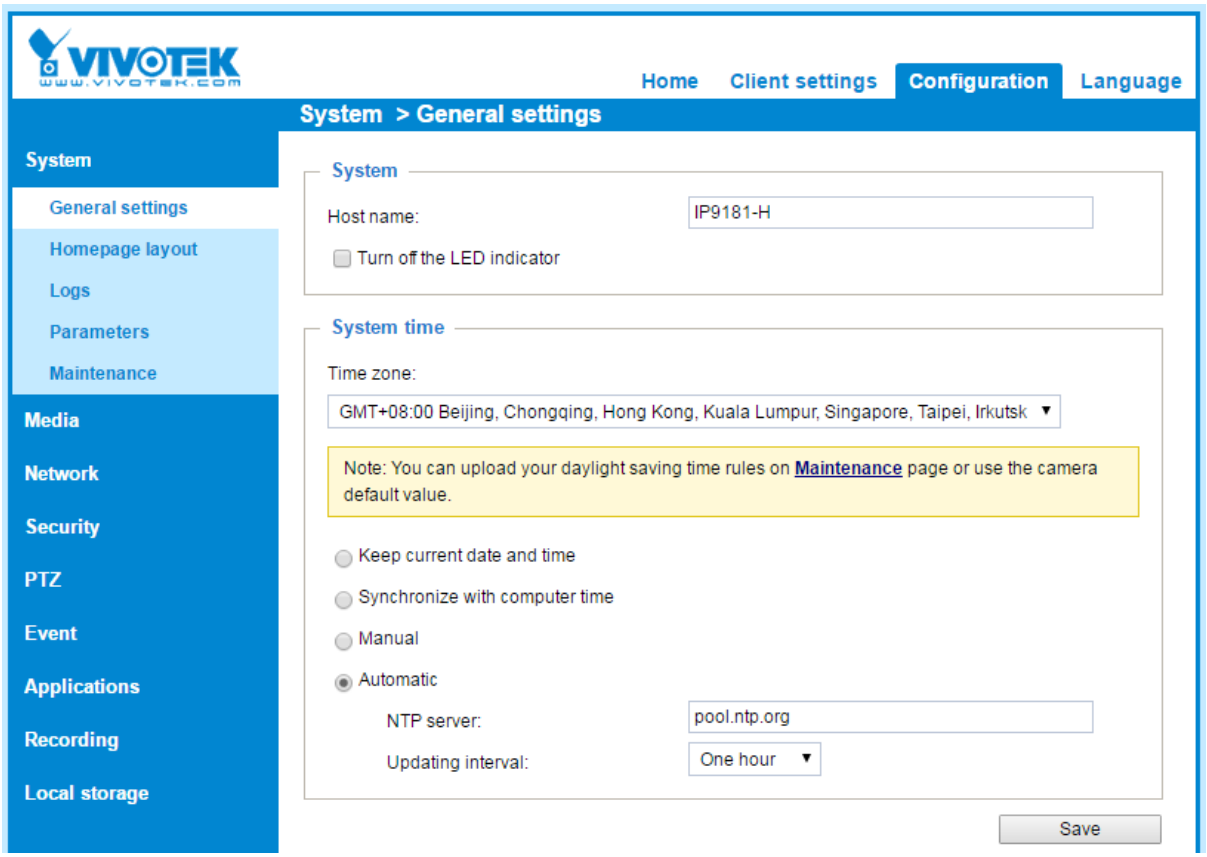
CSC 5: Controlled Use of Administrative Privileges
CSC 16: Account Monitoring and Control



There are 3 user groups inside VIVOTEK cameras: Administrator, Operator and Viewer. For users that only need viewing privilege, just assign a Viewer account for them.

Setup System Time

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs



Time Correction

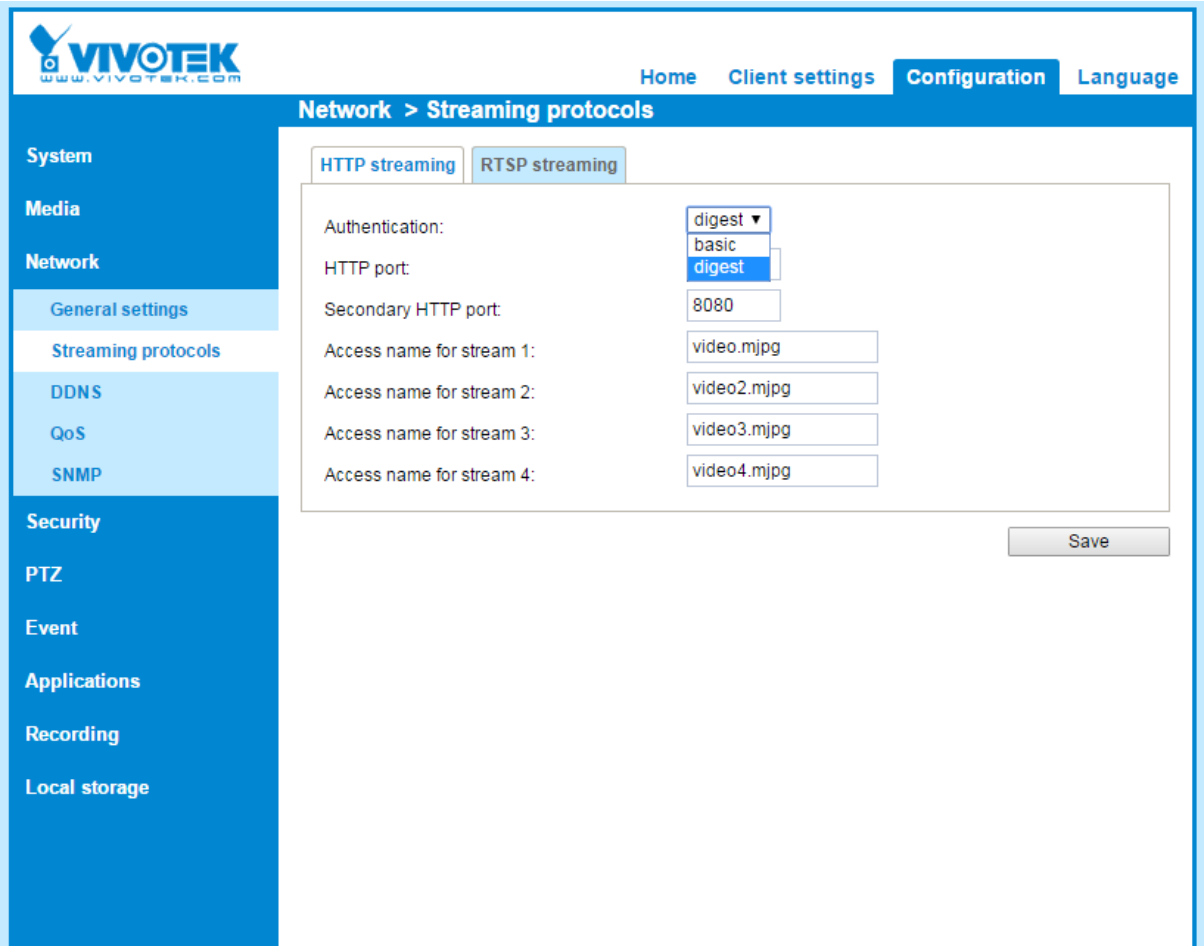
Correct dates and times are very important for incident response and data forensics. Therefore it is critical that in the system/application logs time-stamps have correct information.

NTP Server

It is recommended to synchronize the date/time with an NTP server. For public NTP server, please be careful of vulnerable servers.

Enable HTTP Digest Authentication

CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 16: Account Monitoring and Control



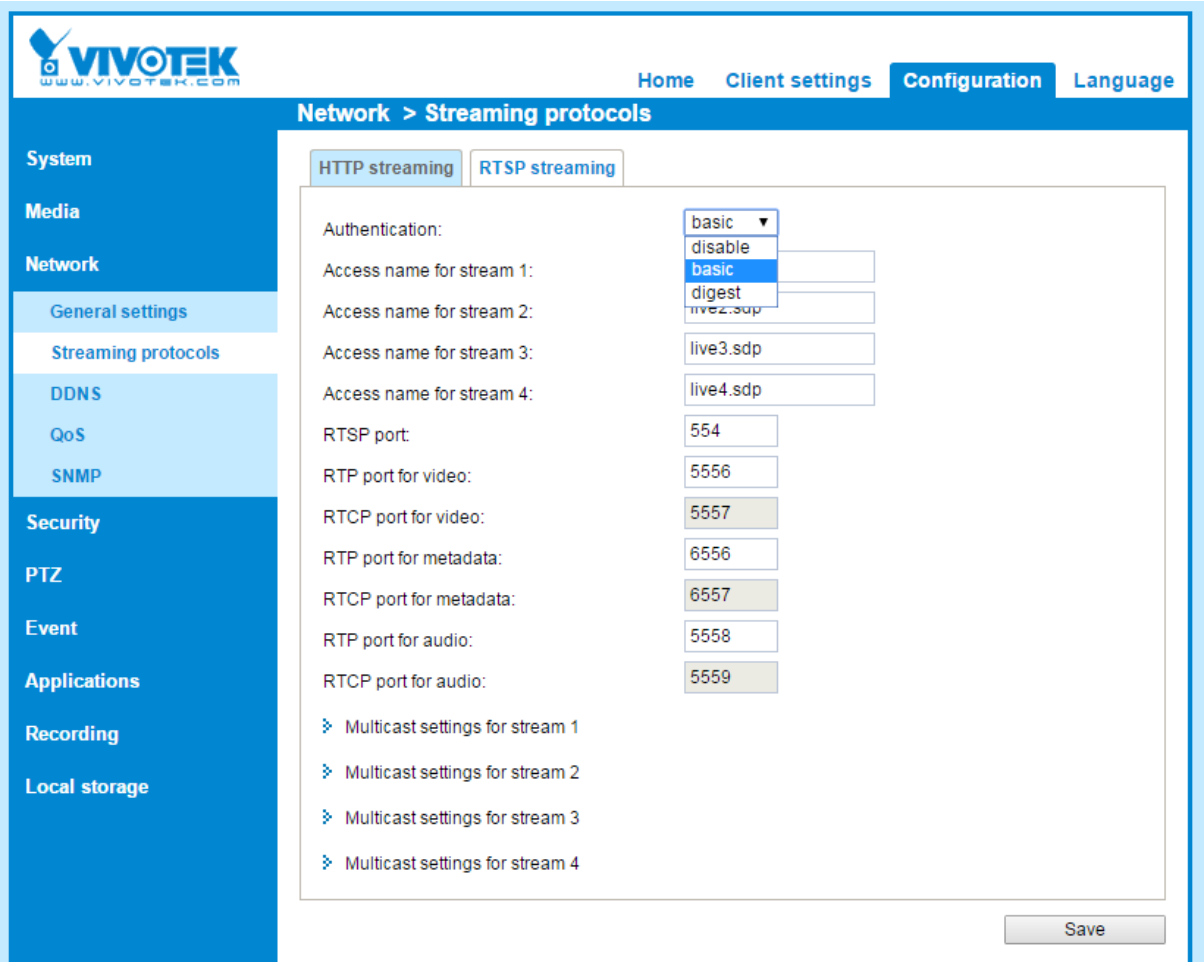
With Basic Authentication the user credentials are sent as cleartext and while HTTPS is not used, they are vulnerable to packet sniffing.

Use digest authentication if possible or enable HTTPS

VIVOTEK cameras support SSL and TLS, but we highly recommend using TLS 1.2 for better security. You may disable SSL and old TLS (1.0, 1.1) from your browser settings panel.

Enable RTSP Streaming Authentication

CSC 13: Data Protection
CSC 16: Account Monitoring and Control



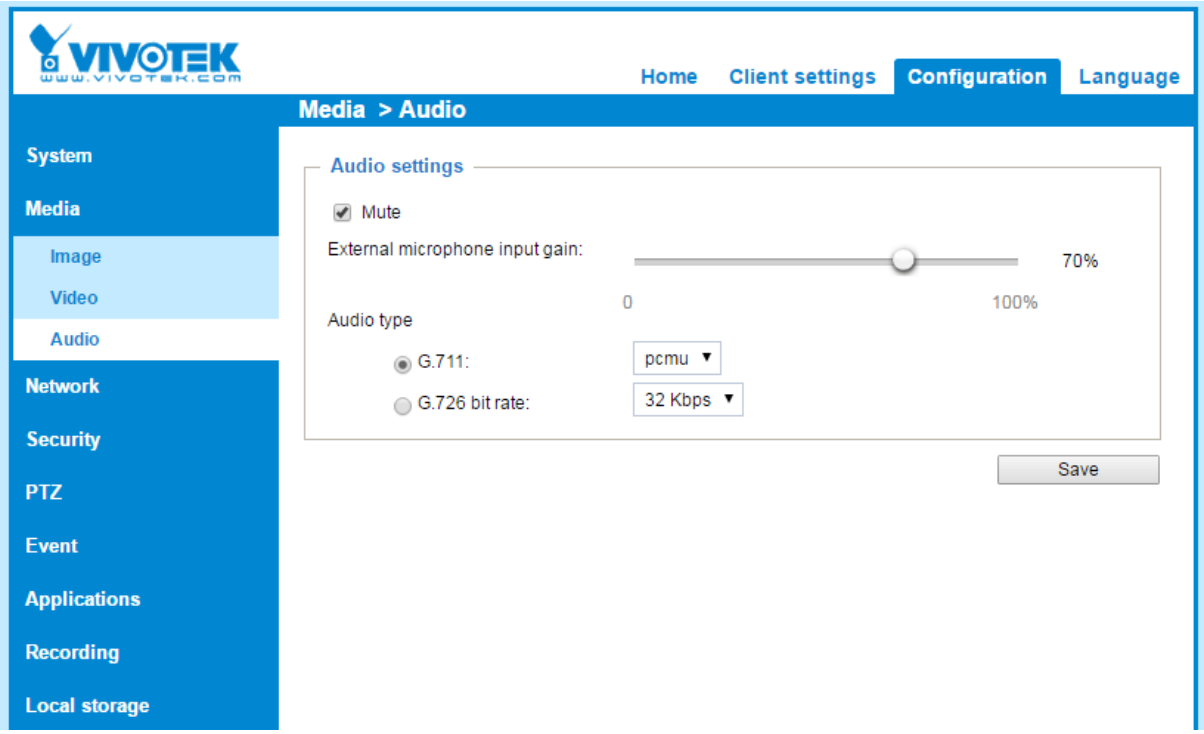
RTSP streaming authentication is a bit different from HTTP, it has a "disable" option in the authentication type. Unless your VMS/NVR doesn't support RTSP authentication, we suggest to use basic or digest strongly.

Disable Unused Services

CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 13: Data Protection

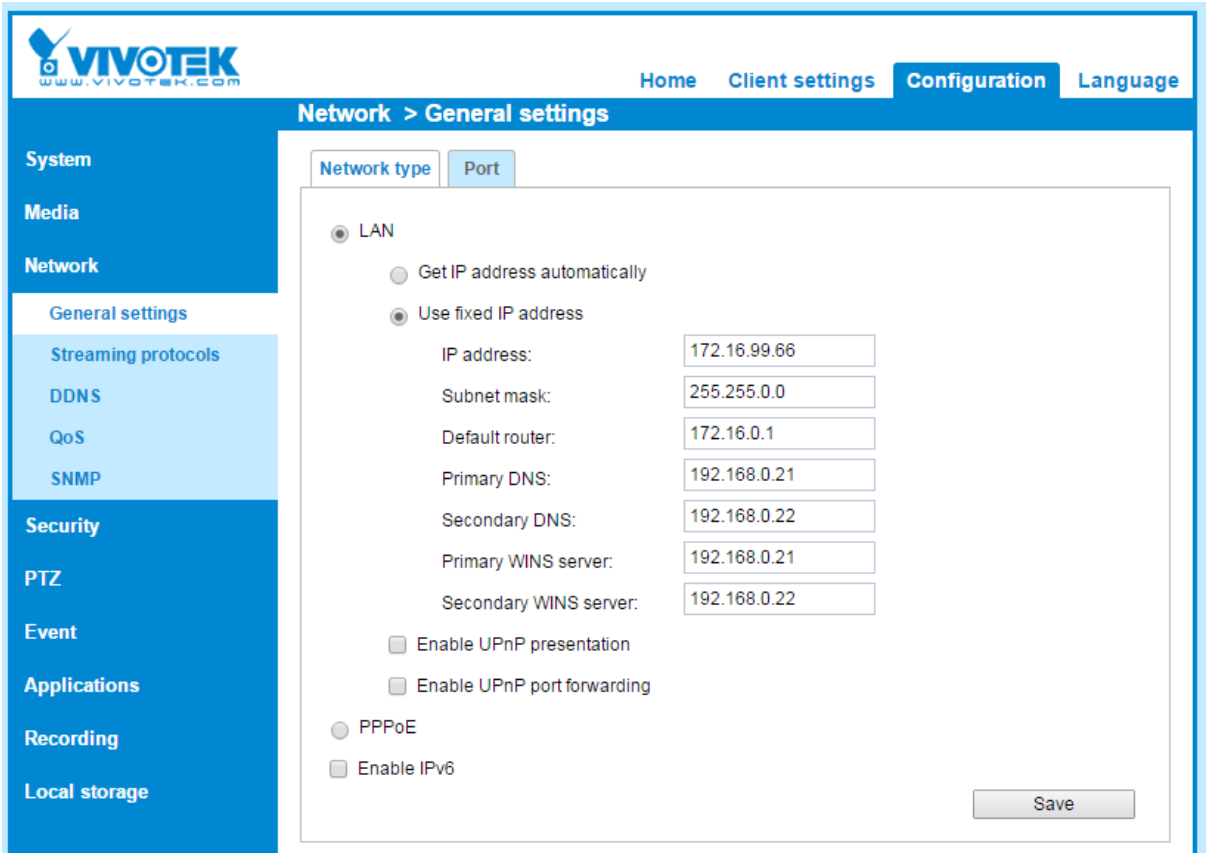
Disable Audio

If you don't need audio, check the [Mute] checkbox to protect the acoustic privacy.



Disable UPnP

If you don't use UPnP function, disable the UPnP presentation and UPnP port forwarding



Disable IPv6

Disable IPv6 if you do not need it.

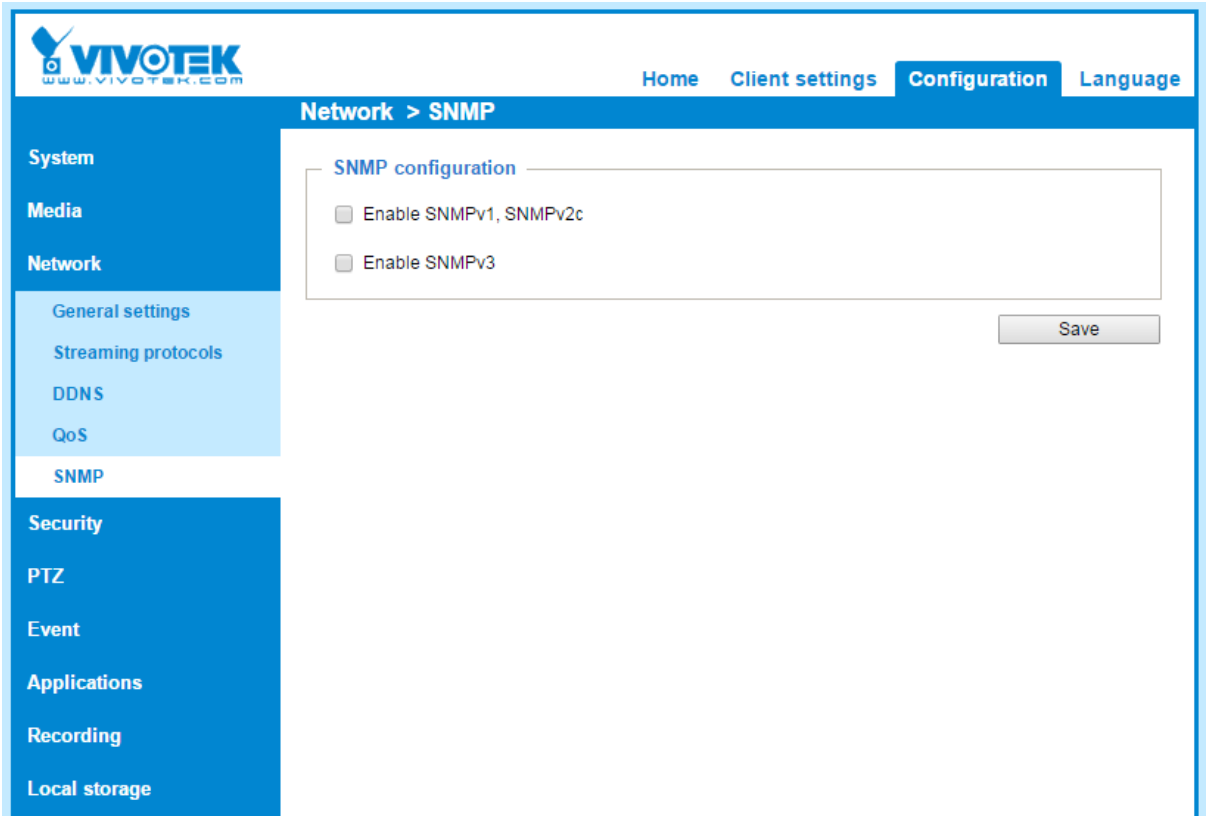
Disable Always Multicast

Uncheck always multicast, if you do not use it, to avoid flooding your audio/video data network. The camera can still mulitcast based on client's request.

Disable SNMP

Disable SNMP if you do not need this function.

SNMPv1 and SNMPv2 are not secure, if you really need SNMP, please adopt SNMPv3


VIVOTEK
Home
Client settings
Configuration
Language
Network > SNMP
System
Media
Network
General settings
Streaming protocols
DDNS
QoS
SNMP
Security
PTZ
Event
Applications
Recording
Local storage
SNMP configuration
Enable SNMPv1, SNMPv2c
Enable SNMPv3
Save

Advanced

Add user for VMS and other viewers

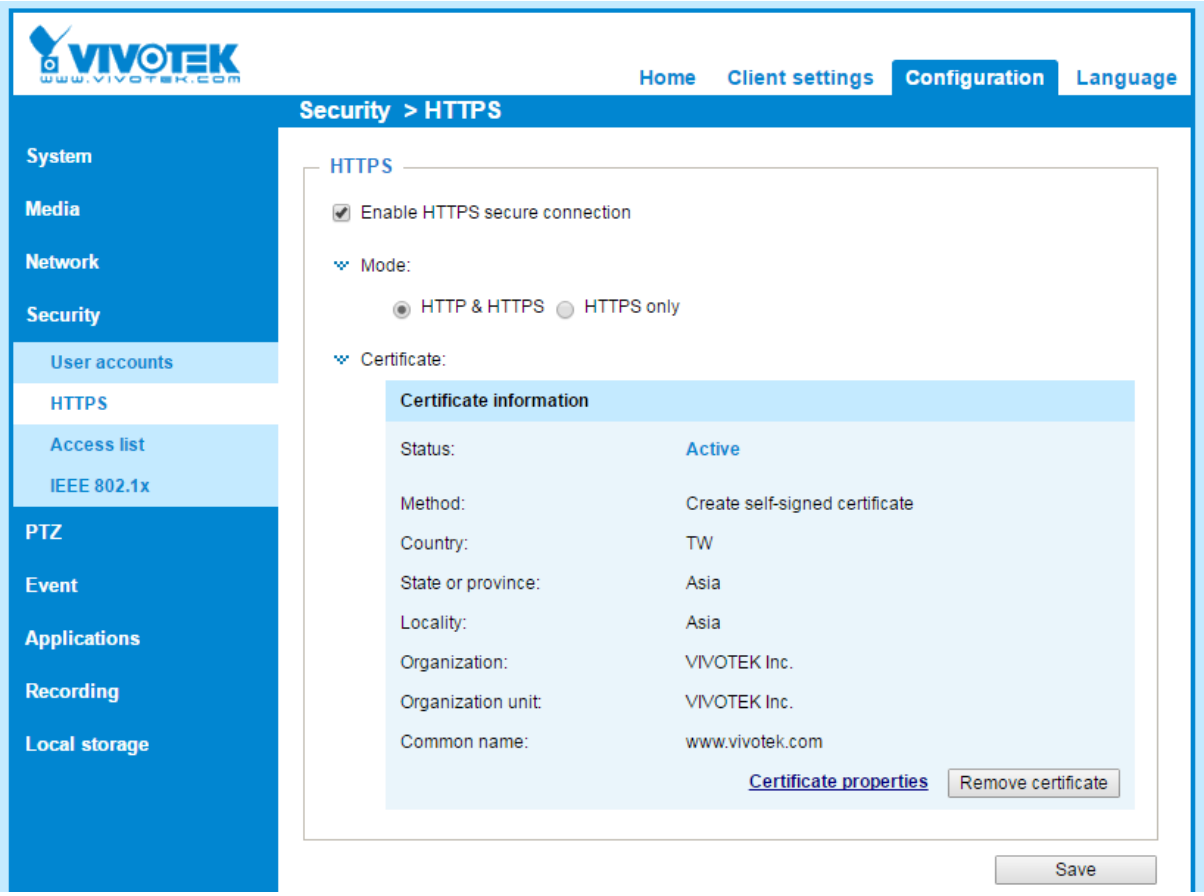
CSC 5: Controlled Use of Administrative Privileges

The root account has a higher privilege than the administrator (network services, such as FTP), please do not use the root account for VMS/NVR, as it can reduce the risk once the VMS/NVR is compromised by an attacker.

Enable HTTPS To Encrypt Traffic

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices,
CSC 13: Data Protection

HTTPS will encrypt all the traffic between client and device.

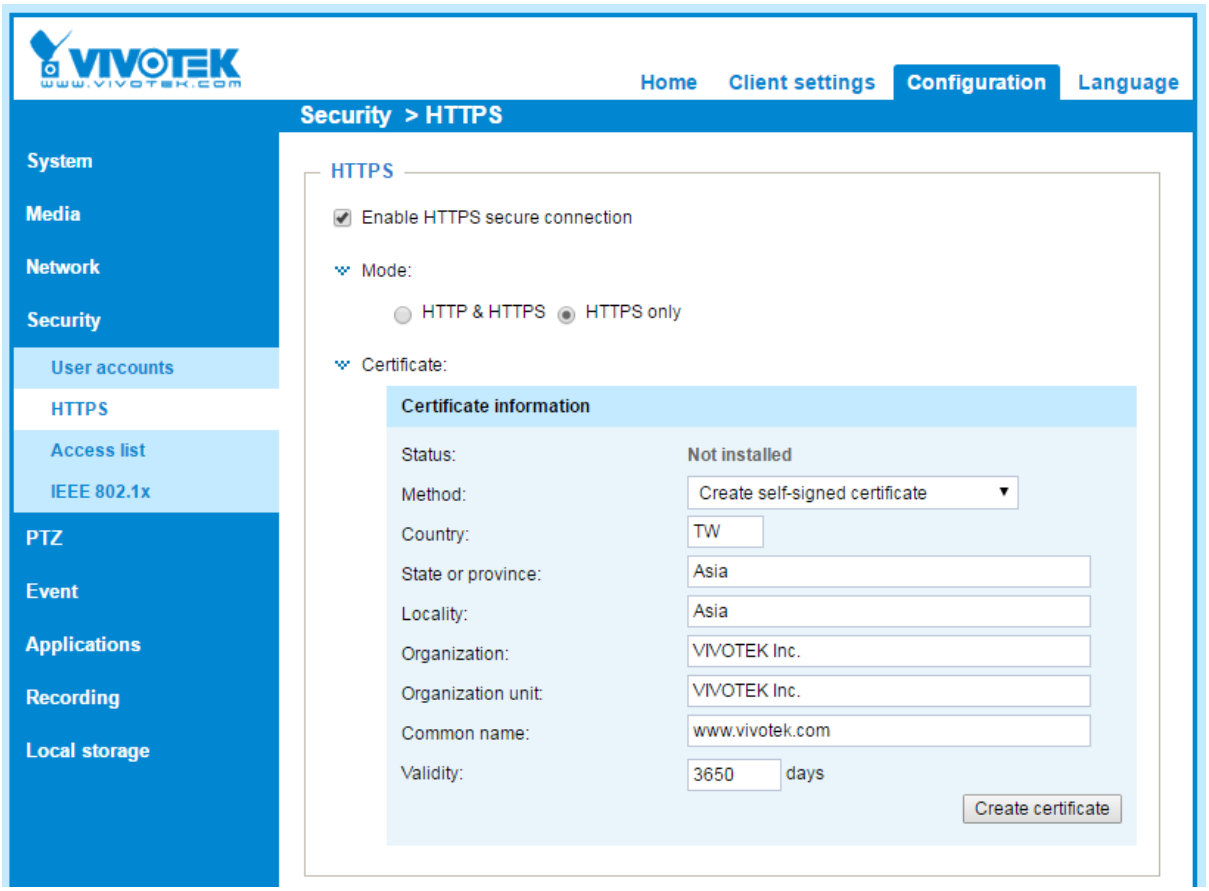


There are two types for the certificate

1. Self-signed certificate
    a. Self-signed is adequate for encryption purposes, but it has risk of MITM attack
2. CA-signed certificate
    a. You have to create certificate request, and send it to CA for signing. With CA-signed certificate, you can identify the camera confidently.

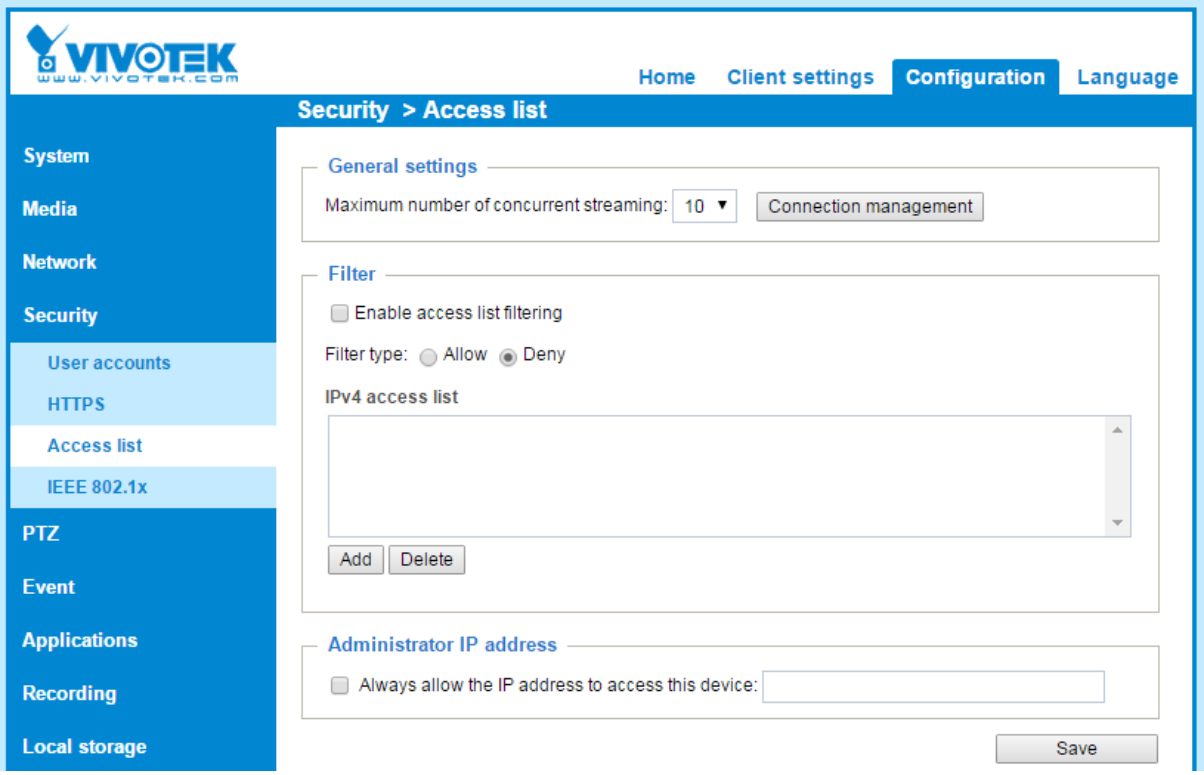
Video and audio streaming through RTSP/RTP won't be encrypted, and it is under the risk of sniffing. If you want to encrypt all Video/Audio data:

1. If you connect the camera using the cameras web interface, please choose HTTP in the protocol options of Client setting, and use https://IP-CAMERA to connect.
2. If you connect the camera by VMS/NVR, please make sure the protocol is RTSP over HTTPS



Reinforce Access List

CSC 12: Boundary Defense
CSC 14: Controlled Access Based on the Need to Know



Maximum number of concurrent streaming

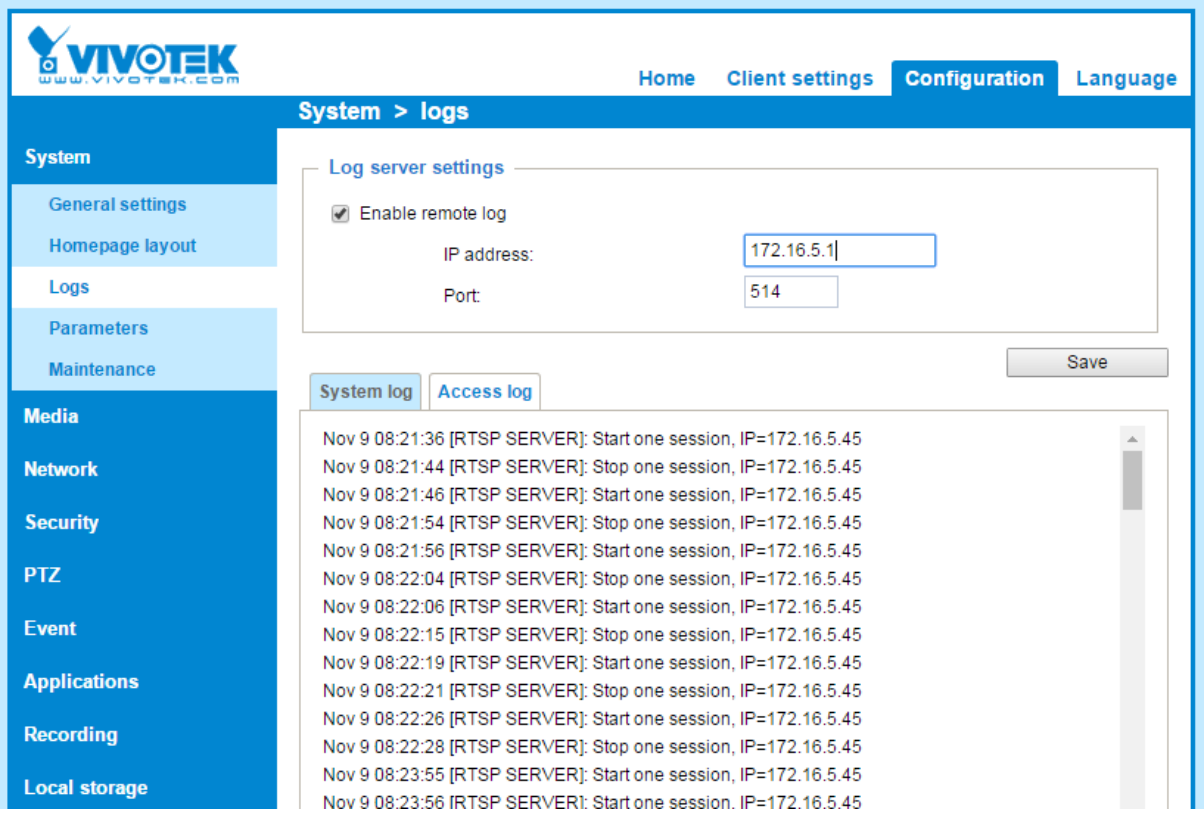
You may limit the maximum number of concurrent streaming if you know exactly how many clients will connect to this device.

Enable Access List Filtering

Enable access list filtering
If this device is only accessible by some certain clients (VMS/NVR/browser), you may set the allow list to strengthen security.

Enable Remote Logs

CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs



Remote log is an important function for enterprise-level surveillance systems. The local log could be erased once the device is compromised, but with remote log, the difficulty is increased.

Change the default port

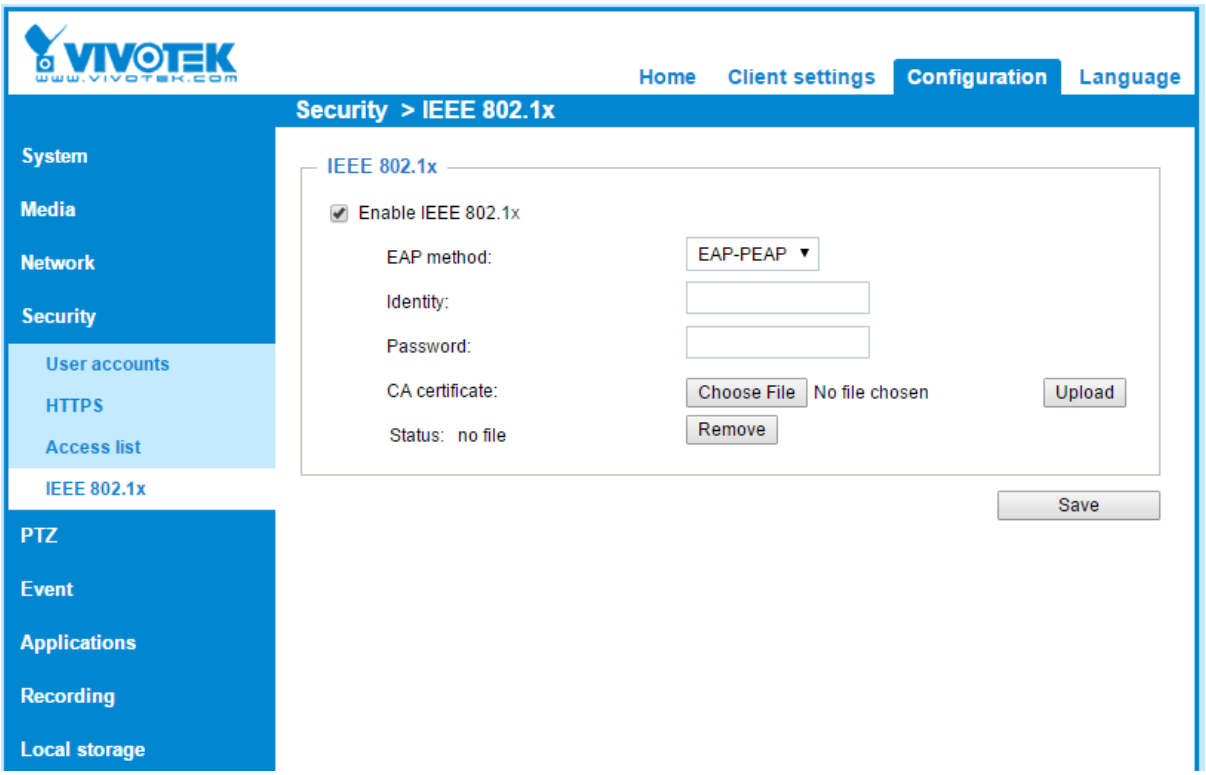
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers,

Changing the default HTTP/RTSP doesn't provide any serious defense against a targeted attack, but it will prevent some non-targeted and amateur script type attacks.

Enterprise

Deploy IEEE 802.1x Authentication Solution

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 15: Wireless Access Control



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. You can prevent unauthenticated devices from attaching to your network environment, and reduce the possibility of forging camera video.

EAP-TLS provides stronger security by requiring both server and client side certificate. Choose the one suited for your network infrastructure or contact the network administrator.

IPAM / VLAN / Subnet

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12: Boundary Defense
CSC 14: Controlled Access Based on the Need to Know

IP management is a basic work to reduce cyber threat. You should know the owner of each IP address and limit the available unused IP addresses.

You can use IPAM and proper subnet plan to archive it.

IPAM https://en.wikipedia.org/wiki/IP_address_management

VLAN is also a good tool for IP management. It allows you to isolate your surveillance system from the regular network environment.

Enable Log and Access Control on Switches

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

You can enhance the security levels via other network devices, such as switches, the switch can enhance the "access list" and "log" functions:

1. Limit access on switches
    a. Only a specific MAC address can access through a specific port
2. Enable Log
    a. You may enable the log on the switch to keep more information of network trace, and it may help on incident response.

Others

Physical damage

CSC 1: Inventory of Authorized and Unauthorized Devices

The most apparent threat to a network camera is physical damage, you may choose the proper camera model to reduce the risk of physical damage.

Subscribe to the VIVOTEK newsletter

CSC 4: Continuous Vulnerability Assessment and Remediation

VIVOTEK will publish security news on our website and newsletter when any security issue occurs.

Appendix A - The CIS Critical Security Controls for Effective Cyber Defense Version 6.1

https://www.cisecurity.org/critical-controls/

CSC 1: Inventory of Authorized and Unauthorized Devices
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CSC 2: Inventory of Authorized and Unauthorized Software
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices,
Laptops, Workstations, and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

CSC 5: Controlled Use of Administrative Privileges
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7: Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

CSC 8: Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 9: Limitation and Control of Network Ports, Protocols, and Services
Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12: Boundary Defense
Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CSC 13: Data Protection
The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification

CSC 15: Wireless Access Control
The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 16: Account Monitoring and Control
Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

CSC 18: Application Software Security
Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 19: Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack

and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

CSC 20: Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.