IP Surveillance Solution Security Recommendations

Contents

Security Settings

Depending on the user needs, different security levels should be used. The user should follow the steps listed in the desired security level as well as following all steps from previous levels.

Security Level	Default	Standard	Moderate	Advanced
Description	Ease of use. Suggested for demo and testing use only.	Suggested settings for small installation sites.	Suggested settings for sites that have a system administrator.	Suggested settings for large network infrastructures with a dedicated IT team.
Camera Steps	N/A	- Factory Default the device - Check and upgrade device firmware - Change root account and password - Set up time and date	- Set up Address Filtering - Set up HTTPS - Disable Discovery Services	- Set up IEEE 802.1X - Set up SNMP monitoring
VMS Steps	N/A	- Setup Windows firewall (Windows Based Server) - Factory Default VMS device (Linux Based Server) - Change default account and password for VMS server	- Install and setup Anti-Virus software (Windows Based Server)	- Create a non-admin user account for VMS user
Network Steps	N/A	- Change default account and password for router and switch	- Install and setup hardware firewall	- Setup a VPN for outside connections

Default Security Level

For ease of use, devices are shipped with a default account and password. The default security level should only be used for demo and testing purposes.

Standard Security Level

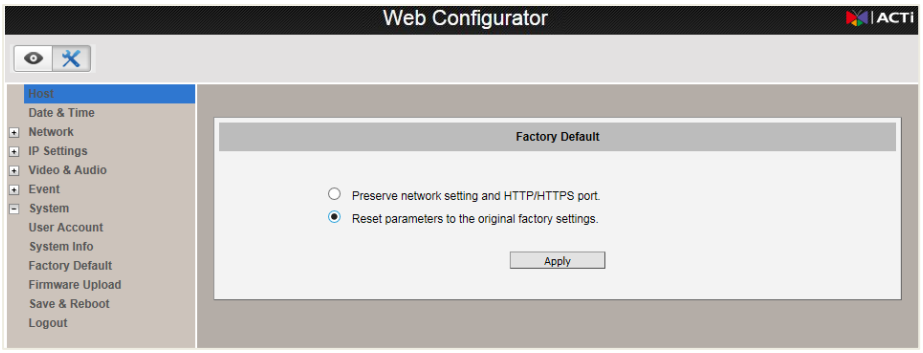
Camera Steps:

Factory Default

To make sure there are no unknown firmware modifications in the device, factory default the device to restore all firmware settings.

To factory default the device:

Click on the option icon  => System=>Factory Default=> Reset parameters to the original factory settings=> Apply

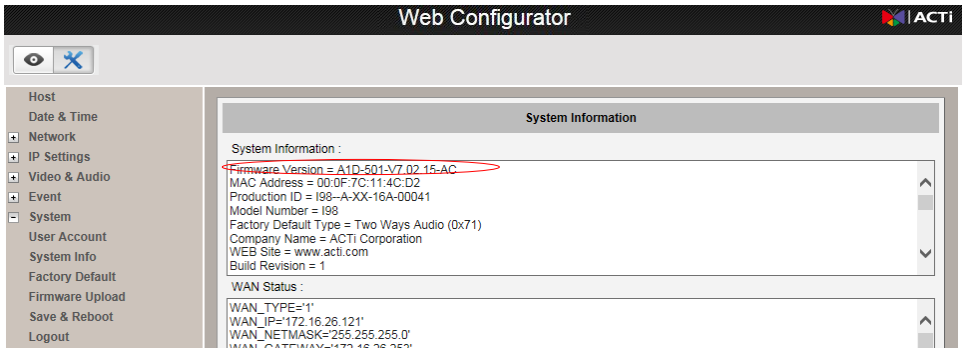


Check and upgrade the firmware

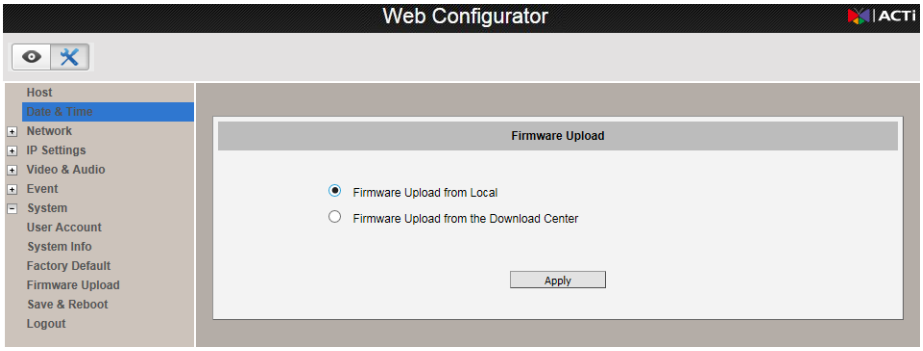
New device firmware usually contains new features and bug fixes. It is recommended to check for firmware updates on a regular basis.

1. Go to ACTi website to download the latest firmware.

2. Click on the option icon  => System=>System Info to see the device firmware version



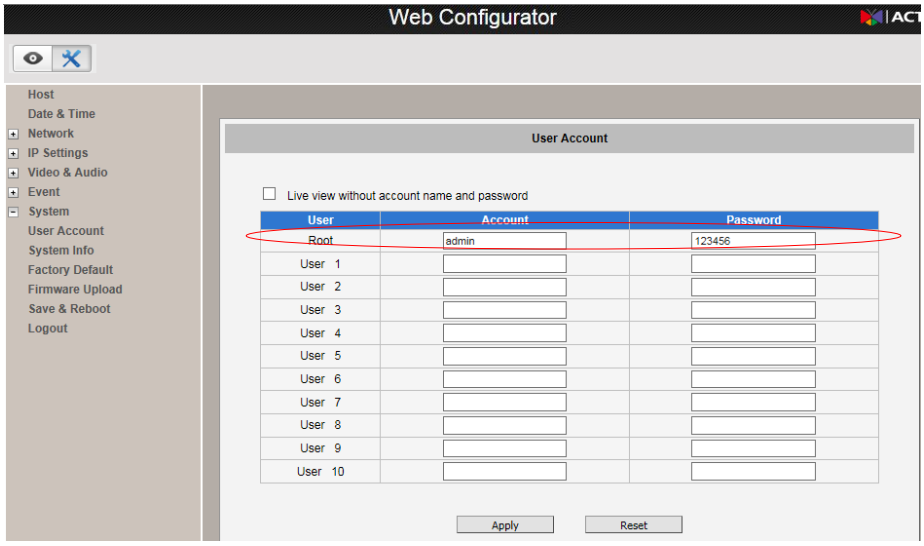
3. To upgrade the device, click on Firmware Upload=>Select Firmware Upload from Local=>Apply=> Browse for the newest device firmware that was downloaded=>Apply.



Change the Root Account and Password

The root account and password should be changed once setup and testing are completed in order to reduce the risk of unauthorized firmware changes. It is recommended to use different accounts and passwords for each device to mitigate the effect of one compromised device.

To change the root account: Click on the option icon => System=>User Account=> Enter the desired user account and password in the root user row.



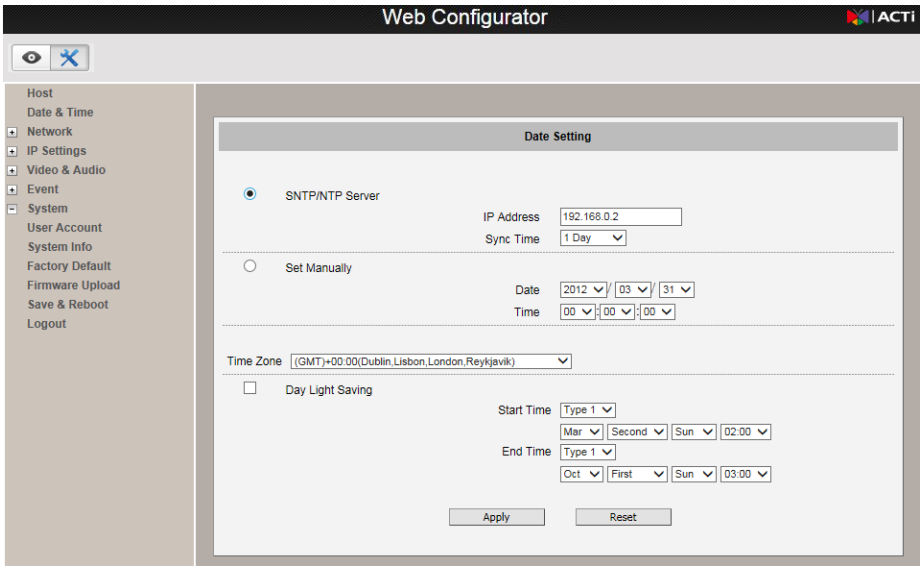
Set up time and date

Each video frame contains a time stamp. The accuracy of the time stamp is very important for incident investigators. Therefore the clock of the camera has to be adjusted to most accurate time possible.

There are two ways to adjust the date and time – automatically by getting date and time regularly from any of the NTP servers worldwide, or manually by selecting proper time zone, date and time. The automatic way can be used only if the camera has an access to NTP servers. If you are using an isolated Local Area Network without Internet access, you can only use Manual date and time

adjustment mode. For more details, please refer to the device firmware user manual.

To set up the time: Click on the option icon => Date & Time=> SNTP/NTP Server or Set Manually=> Choose Time Zone=>Enable/Disable Day Light Saving=> Apply.



VMS Steps:

Setup Windows Firewall (Windows Based Server)

To turn on Windows Firewall: Type Windows Firewall in the Start Menu=>Open Windows Firewall=>Click Use recommended settings.

Factory Default VMS device (Linux Based Server)

To make sure there are no unknown modifications in the device, factory default the device to restore all settings.

Change default account and password for VMS server

It is recommended to change the default account and password for the VMS server to prevent unauthorized access.

Network Steps:

Change default account and password for router and switch

To prevent network settings being modified by unknown personnel, it is recommended to change the default account and password of the router and switch.

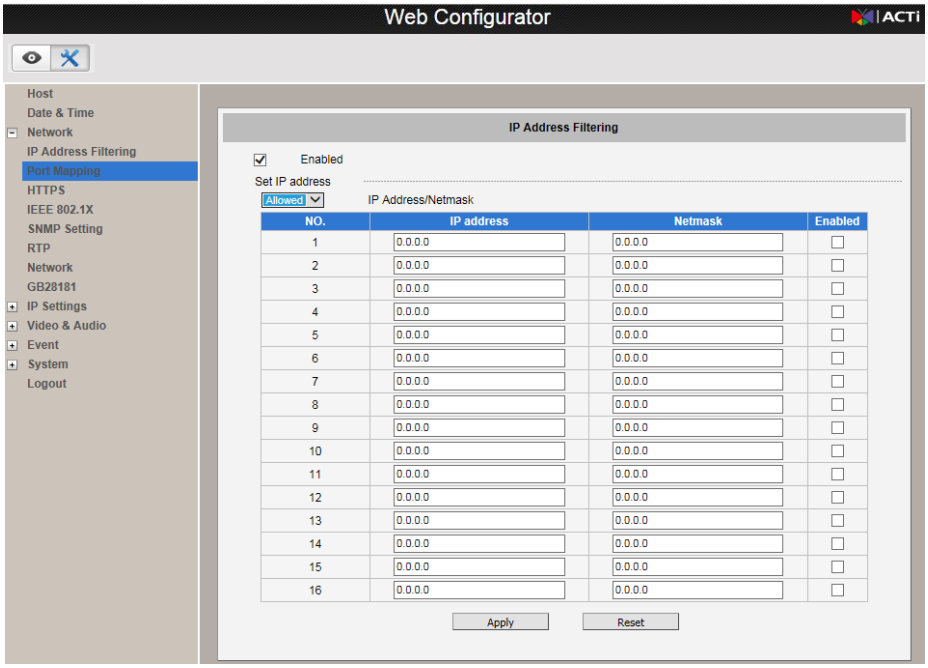
Moderate Security Level

Camera Steps:

IP Address Filtering

It is recommended to limit access to the device by setting up IP address filtering to prevent unauthorized modifications and access to live video stream. For more details, please refer to the device firmware user manual.

To set up IP Address Filtering: Click on the option icon => Network=>IP Address Filtering=> Enabled=>Select Allowed for Set IP address=>Enter the IP address for authorized clients=>Apply.



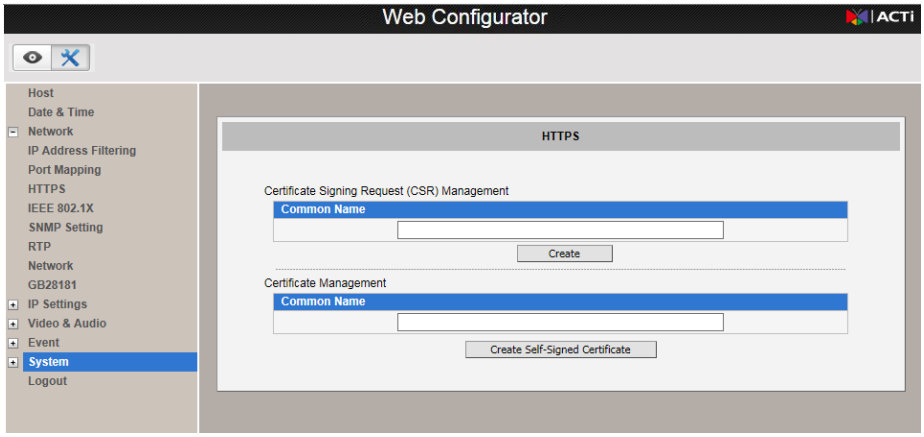
HTTPS

HTTPS protocol allows creating a secure channel over an insecure network in order to protect the data sent between the camera and its counterpart. Two things are required to have a secure communication – encrypted data, and verified counterpart of the communication. To make sure that the messages are being sent and received from true counterpart, the certificate is needed. There are two methods to create certificates – Certificate Signing Request (CSR) and Self-Signed Certificate.

Certificate Signing Request (CSR): User uses a signed certificate issued by trusted Certification Authority (CA).

Self-Signed Certificate: User wants to use the certificate created and issued by user himself.

To enable HTTPS: Click on the option icon => Network=>HTTPS=> Press Create or Create Self-Signed Certificate button and configure settings in the pop-up screen to install the certificate=> New setting will take effect after Save & Reboot.



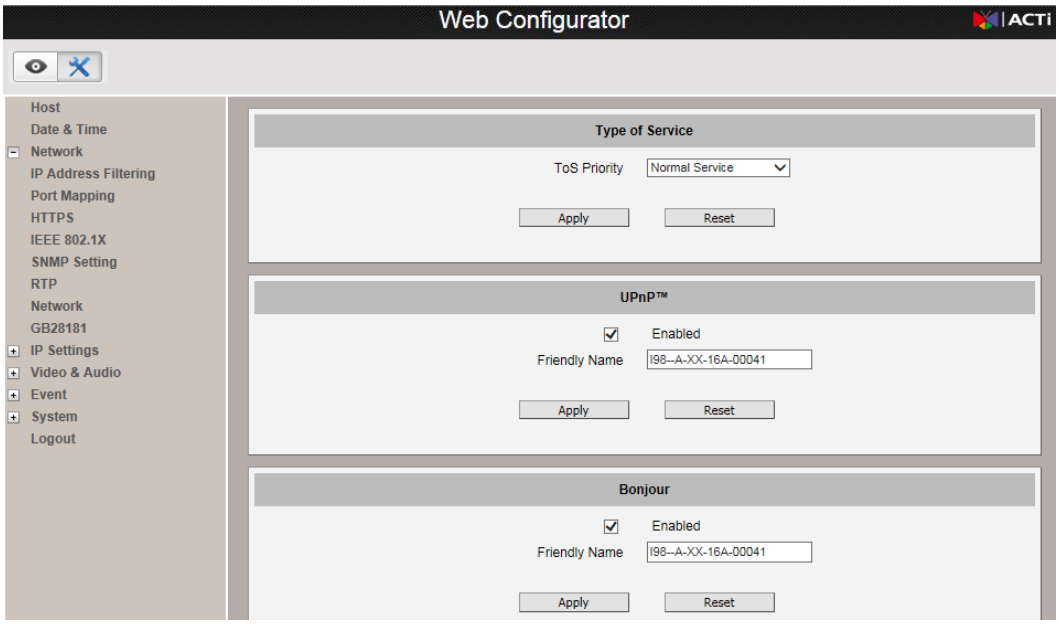
Disable Unused Services

To allow easy setup, devices have discovery protocols enabled by default. After setup and installation is completed, the discovery protocols should be disabled to prevent the devices from being seen on the network.

UPnP™ provides the option to enable or disable the Universal Plug and Play capability of the camera. Having the UPnP™ enabled allows the other network devices to seamlessly discover it on the network for convenient identification and access. Bonjour provides the option to enable or disable the ability of the camera to be discovered by the other network devices using Bonjour protocol, developed by Apple Inc.

To Disable UPnP™: Click on the option icon =>Network=>Network=>Uncheck UPnP™=>Apply.

To Disable Bonjour: Click on the option icon => Network=>Network=>Uncheck Bonjour=>Apply.



VMS Steps:

Install and Setup Anti-Virus Software (Windows Based Server)

It is recommended to install anti-virus software to prevent the NVR system from being compromised.

Network Steps:

Install and Setup a Hardware Firewall:

A hardware firewall is recommended in addition to a software firewall for more complicated networks. Devices that do not have a software firewall can be protected through the use of a hardware firewall.

Advanced Security Level

Camera Steps:

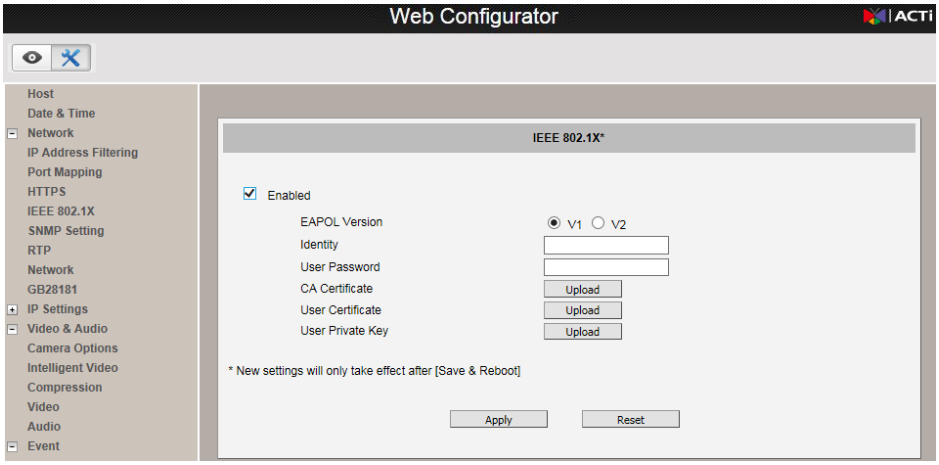
IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server.

The supplicant is a client device (such as an IP camera) that wishes to attach to the LAN/WLAN. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized.

To Enable IEEE 802.1x: Click on the option icon => Network=> IEEE 802.1X=> Enabled=>Enter the information required=> Apply=> Save & Reboot.



SNMP monitoring

SNMP provides an easy way to manage network devices. The main features are:

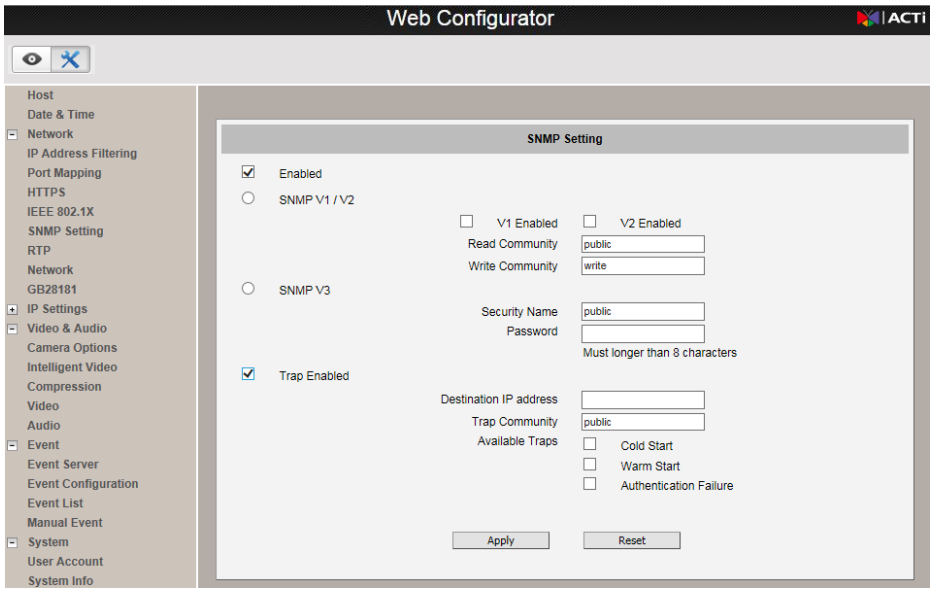
1. Monitoring device uptime
2. System detail description. (Ex: model name, model description and firmware version.)
3. Collect interface information. (Ex: MAC address, interface speed, local port.)
4. Measuring network interface throughput.

Once SNMP function is enabled, install and run the SNMP management software on the computer server.

To Enable SNMP: Click on the option icon => Network=>SNMP Setting=>Enabled=>Enter settings=>Apply.

SNMP traps enable notifications from devices. Devices may send message to the management server whenever significant events occur such as cold start, warm start and authentication failure. The manager will get the information immediately and take action if necessary.

To Enable SNMP Trap: Click on the option icon  => Network=>SNMP Setting=>Trap Enabled=>Enter settings=>Apply.



VMS Steps:

Create a non-admin user account for VMS user

To limit access to VMS system settings, set up a non-admin user account for users to use.

Network Steps:

Setup a VPN for outside connections

To allow a secure method for outside connections into the network, a VPN should be setup.