Useful Tips for Reducing the Risk of Unauthorized Access for Network Cameras

Important System administrators are advised to read.

This document explains the measures to safely use the network cameras.
The explanation is divided into "models released in and after 2022" and "models released before 2022", so please check the model in use from the following table.

Models released in and after 2022

▶ A-1 page

VB-H47

VB-M46

VB-S32VE

VB-S32D

VB-S820D

VB-S920F

Models released before 2022

▶ B-1 page

ME20F-SHN

VB-H

VB-H761LVE-H / VB-H761LVE / VB-H760VE / H751LE-H / VB-H751LE / VB-H730F Mk II / VB-H730F / VB-H710F / VB-H652LVE / VB-H651VE / VB-H651V / VB-H630VE / VB-H630D / VB-H610VE / VB-H610D / VB-H45 / VB-H43 / VB-H41

VB-M

VB-M741LE-H / VB-M741LE / VB-M740E / VB-M720F / VB-M700F / VB-M641VE / VB-M641V / VB-M640VE / VB-M640V / VB-M620VE / VB-M620D / VB-M600VE / VB-M600D / VB-M50B / VB-M44 / VB-M42 / VB-M40

VB-R

VB-R13VE / VB-R13 / VB-R12VE / VB-R11VE / VB-R11 / VB-R10VE

VB-S

VB-S910F / VB-S905F Mk II / VB-S905F / VB-S900F Mk II / VB-S900F / VB-S805D Mk II / VB-S805D / VB-S800D Mk II / VB-S800VE / VB-S800D / VB-S31D Mk II / VB-S31D / VB-S30D Mk II / VB-S30VE

ENGLISH

Models released in and after 2022

This chapter describes the following models. For network cameras other than the following models, refer to "Models released before 2022".

VB-H47

VB-M46

VB-S32VE

VB-S32D

VB-S820D

VB-S920F

Table of Contents

Introduction

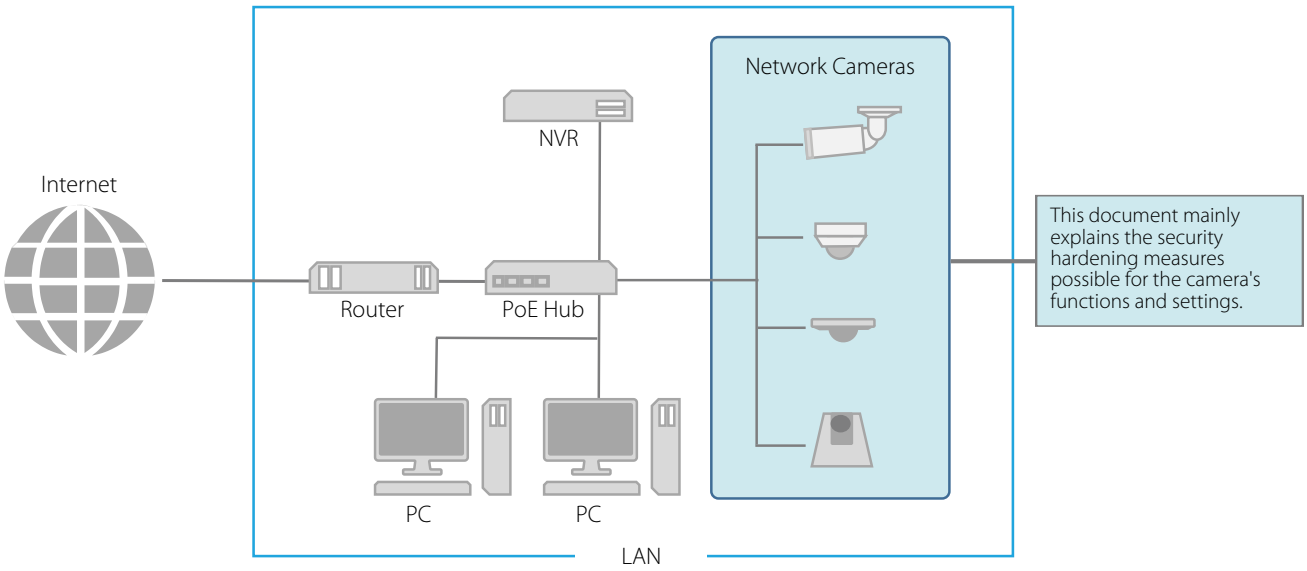
Devices that are connected to a network could be targeted for cyber attacks such as unauthorized accesses by non-intended unauthorized parties. Especially for network cameras, although they can be convenient since they have a variety of server functions, there is a risk of being attacked by hackers unless operated with security implementations. To completely eliminate all risks is impossible, however, by studying various risk angles and taking measures based on the security policies, it is possible to decrease the risk of cyber attacks.

This document explains the security hardening measures to the camera settings targeted for all customers with Canon Network Cameras (hereafter referred to as the cameras). Refer to this document and implement necessary measures according to the environment under the customer's responsibility, which will lead to safer camera operation.

About This Document

The security hardening measures explained in this document are mainly for the cameras, which are a part of an entire system as shown in the figure below. For the entire system's security hardening, measures must be taken according to the customer's network environment and/or purpose of the camera use.

Measures, not only from cyber attacks but against physical vandalism and mischief, are also important. Some of the examples of measures here are, embedding the cable that connects to the camera, isolating recording devices, restoring camera settings when disposing the camera, and remembering to remove the memory card, etc.



■ Warnings and Symbols

- In this document, there are screen shots of the camera's setting page explaining each measure, however, depending on the camera and firmware version used, the actual settings on the screen may differ. Each function's settings, as well as important points, are described in detail in the camera's "Operation Guide". Refer to the "Operation Guide" for the camera being used when setting up the camera.
- Any unauthorized reproduction of this document is prohibited.
- The contents of this document are subject to change without any prior notice.
- To the full extent permitted by laws and regulations, neither Canon Inc. nor any of its subsidiaries or affiliates shall be liable for any losses, direct, incidental or consequential damages, or liabilities that may be incurred as a result of network security incidents such as unauthorized accesses.

The following symbols used in this document indicate important and supplementary information.

Important Cautions and restrictions are written under this symbol. Make sure to read these carefully.

Note Supplementary descriptions and reference information are written under this symbol.

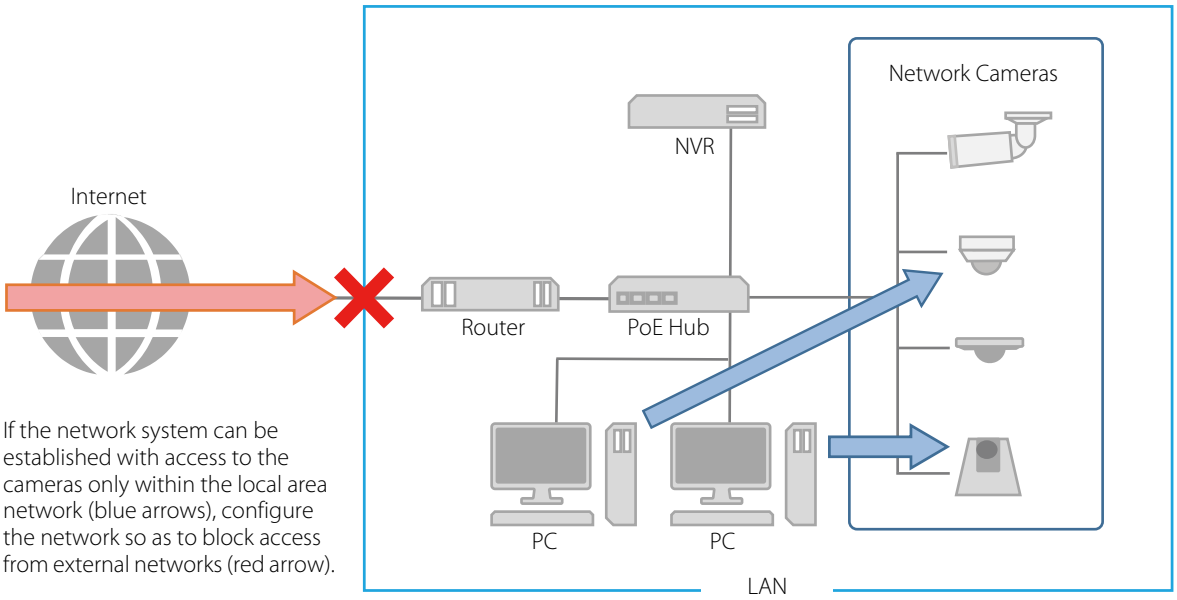
Operating in a Network Configuration Suitable to the Users' Needs

Before explaining what security hardening measures are possible with the camera's functions and settings, the network configuration suitable to the camera use is explained here. Check whether the camera access from outside is necessary.

■ Blocking Access from Outside

In order to reduce the security risk when checking the camera's video or changing the settings, it is effective to block access physically and/or virtually if it is unnecessary to be made accessible from an external network, such as the internet.

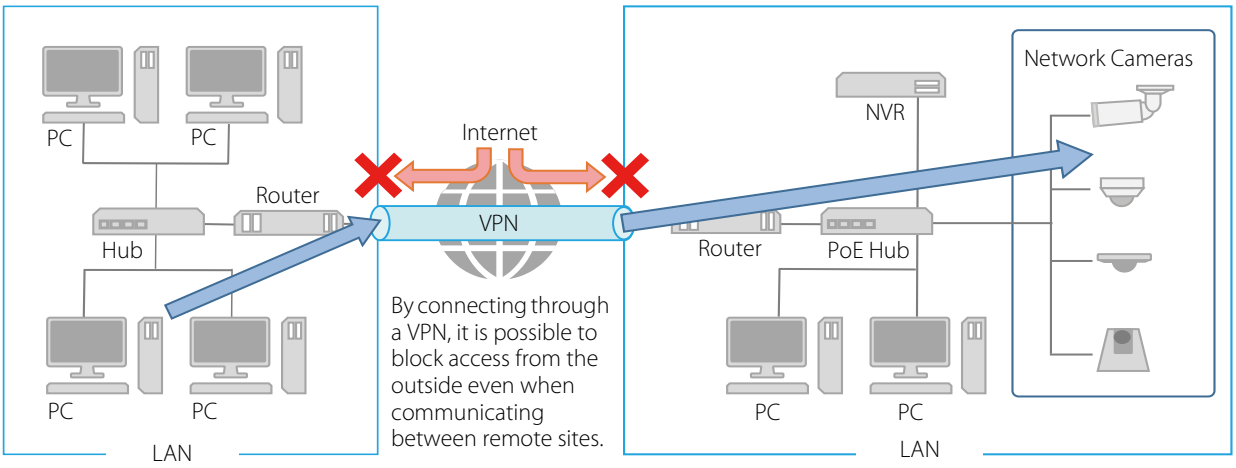
When access from a remote location is unnecessary and the devices accessing the camera can be limited, using only specific devices in the same local area network will enhance security. When it is necessary to access the camera from a remote location, it is important to use a method that can communicate safely, such as using a VPN that can block access from the outside.



If the network system can be established with access to the cameras only within the local area network (blue arrows), configure the network so as to block access from external networks (red arrow).

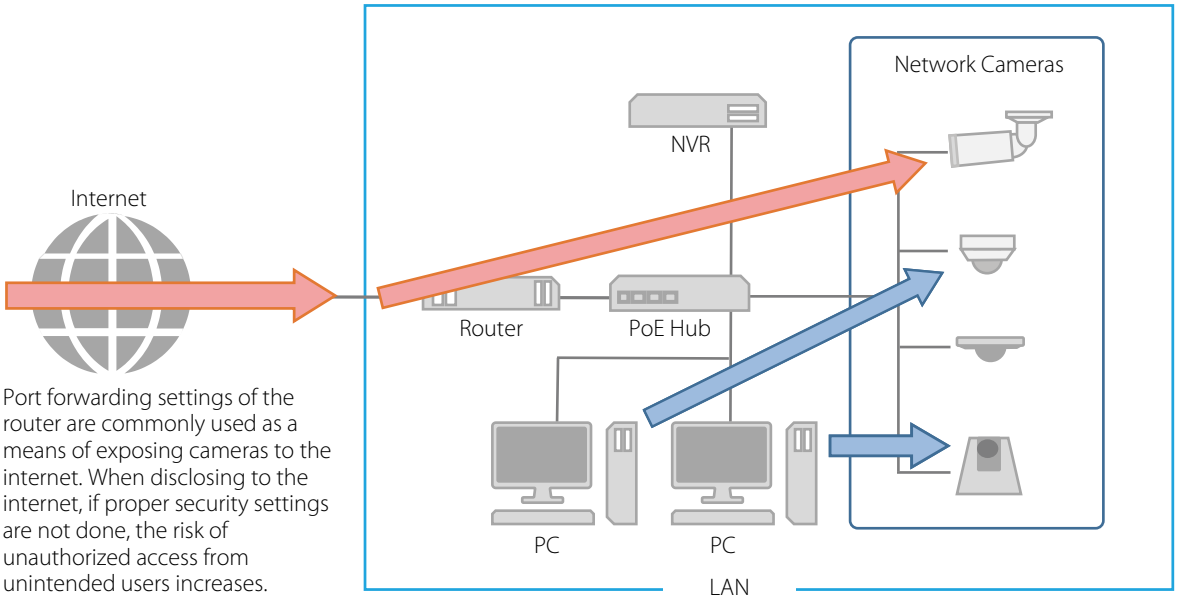
What is a VPN?

A VPN is an abbreviation of the word Virtual Private Network, which creates a virtual tunnel for a communication path that is capable of having a safe data exchange. By connecting LANs of different sites such as head office and branch offices via VPN, it is possible to block access from external networks.



■ Making Thorough Measures for Networks That can be Accessed Externally

In case of sharing videos with the general public, it is necessary to disclose the camera information to the internet so that the camera can be accessed from the outside by connecting to an external network such as the internet.



Port forwarding settings of the router are commonly used as a means of exposing cameras to the internet. When disclosing to the internet, if proper security settings are not done, the risk of unauthorized access from unintended users increases.

Networks that allow external access are highly convenient, but at the same time the risk of unauthorized access to devices on the network increases. Therefore, in such a network configuration as illustrated above, it is important not only to implement the countermeasures described in this document, but also to secure measures to the entire system such as authentication of each device and encryption of each communication on the network.

Chapter 1

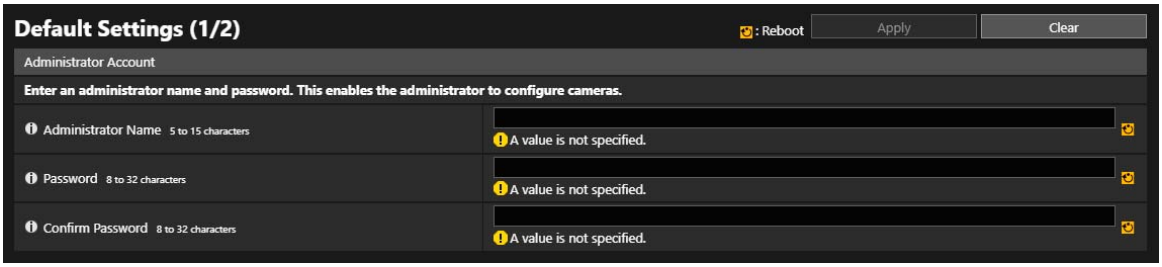
Basic Measures

Setting Administrator Name and Password

The administrator account has authority over all of the camera's settings and operations. If the administrator account is illegally used by an unauthorized party and tampering is done, there is a risk the camera will not be accessible. In order to prevent spoofing of the administrator account, the most fundamental measure for safe operation of the camera is to make the administrator name and password in an array of letters that are difficult to guess by unauthorized users. Strictly manage the administrator account and refrain from settings such as the same administrator account on multiple cameras.

The administrator account needs to be set when the camera is started for the first time. After setting, editing can be done in [Security] > [User Management] on the camera's setting page.

The administrator account is set in [Default Settings] when accessing the camera for the first time.



The administrator name and password can be changed in [Security] > [User Management] on the camera's setting page.

■ Setting a Strong Administrator Name and Password

In order to strengthen the administrator name and password, consider the following points:

- Combine at least 10 characters of alphanumeric characters or symbols and special characters permitted for the camera.
- Combine upper and lower case characters.
- Avoid commonly used words and string of characters that are easy to guess.

■ Other Passwords

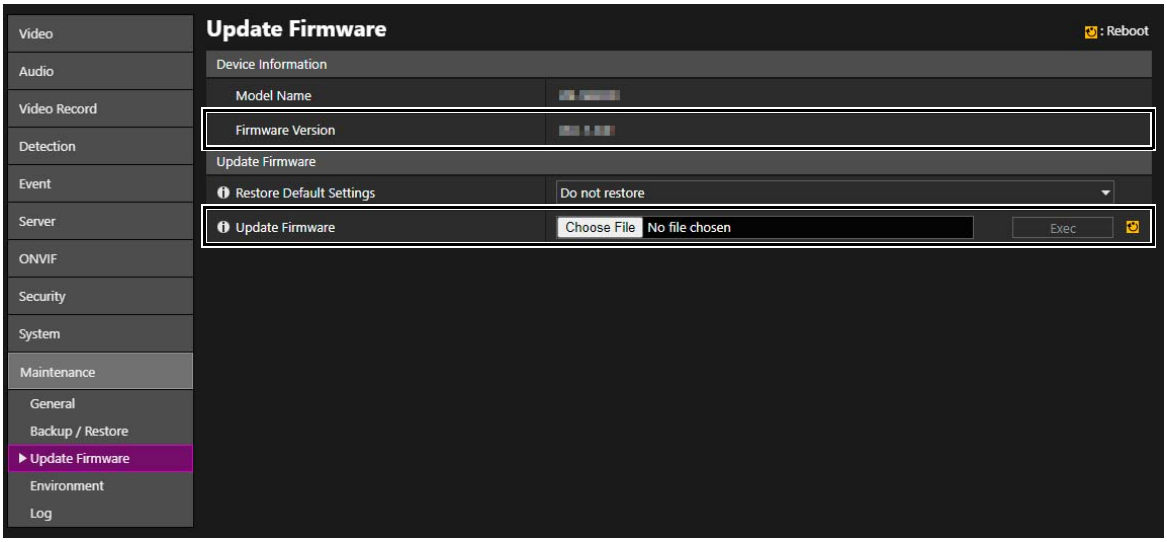
For the camera, in addition to the administrator account, the password for the authorized user (p. A-12), server authentication, and encryption are to be set. Set these passwords in an array of letters that are difficult to guess by unauthorized parties and manage them appropriately.

Using the Latest Firmware

The camera's firmware is updated as needed in order to improve performance of the functions and bug fixes. From the security point of view, it is important to always keep it updated because the measures against known vulnerabilities are applied to the latest firmware.

Check Canon's website regularly at the initial setting after purchasing the camera and during its operation, whether the latest firmware is provided.
The firmware version can be confirmed in [Maintenance] > [Device Information] > [Firmware Version] on the camera's setting page.

The firmware is updated in [Maintenance] > [Update Firmware] > [Update Firmware] on the camera's setting page.

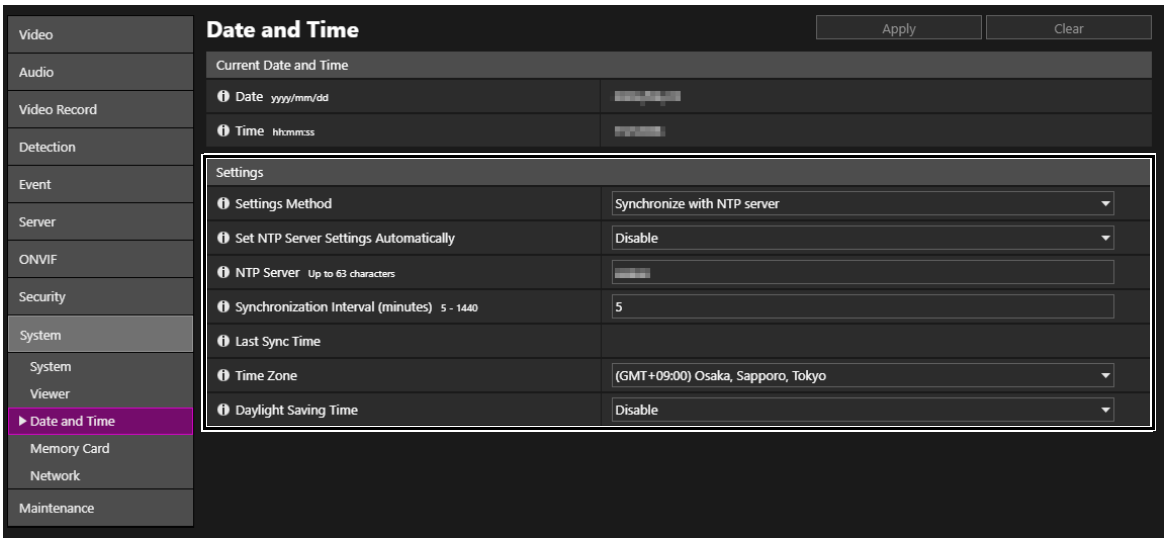


It is also possible to use the Camera Management Tool to update the firmware.
For details regarding the Camera Management Tool, refer to the "Camera Management Tool User Manual".

Setting Date and Time

Set the correct date and time for the camera. If there are indications that suspicious unauthorized access occurred, it may be possible to confirm the date and time of occurrence by checking the log.

Date and time is set in [System] > [Date and Time] > [Settings] on the camera's setting page.



Monitoring the Log

Camera connection status and operating conditions are recorded and saved as a log in the camera embedded memory and the memory card. Check the logs periodically to quickly find any signs of suspicious unauthorized access, such as repeated user authentication failures. For details on the log, refer to the camera's "Operation Guide".

■ Save Destination and Category of the Log

The log contents saved on the camera embedded memory and the memory card are different.

Logs saved on the camera embedded memory: Error log, Warning log, Information log

– All of the logs will be deleted, except for the date and time when the error log occurred and the error number, if the following operations are performed: rebooting, initialization, and restoring to the factory default settings. Also, all of the logs will be deleted if exceeding a certain size.

Logs saved on the memory card: Error log, Part of the Warning log, Information log

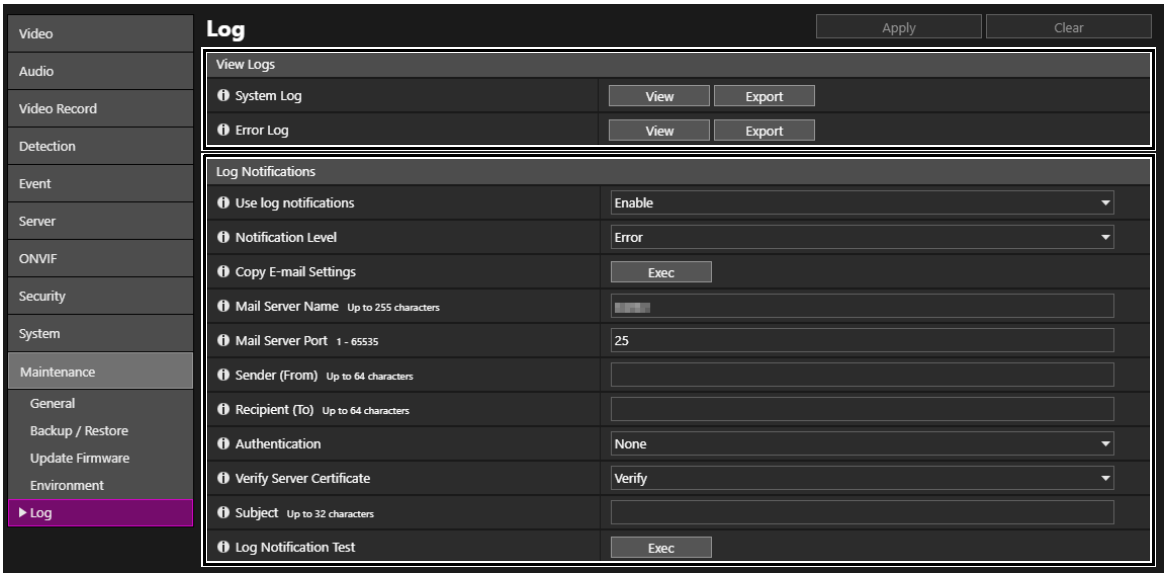
– The logs will not be deleted if any of the following operations are performed: rebooting, initialization, and restoring to the factory default settings.

■ Viewing, Notifying, and Downloading the Log

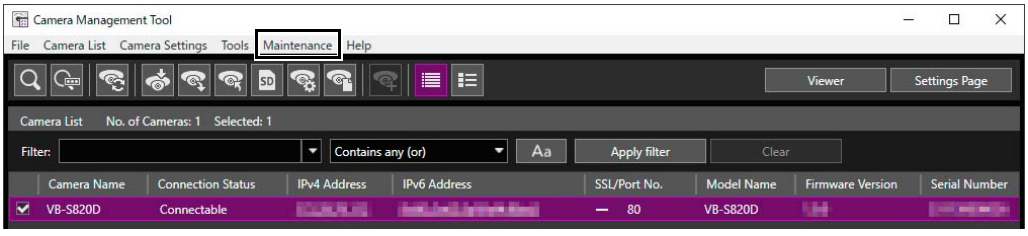
Log saved on the camera embedded memory can be confirmed in [View Logs] on the camera's setting page. It is also possible to notify the user of [Error] and [Errors and warnings] at the level the user set, if [Log Notifications] is enabled.

When using the Camera Management Tool, it is possible to download both the camera embedded memory log and memory card log as a file respectively.

Viewing and setting options of the log are set on the camera's setting page.
[Maintenance] > [Log] > [View Logs]
[Maintenance] > [Log] > [Log Notifications]



Download the log file in [Maintenance] > [Download Log] on the Camera Management Tool.



Example of the Camera Management Tool screen

■ Log Contents

Log level, code, fault level, category are as follows:

Log	Level	Code	Fault level	Category
Error log	Error	4xx Ex.) S410 Event service initialization error	Software-level failure (Task operations will stop)	[crit]
Error log	Error	3xx Ex.) S302 Error on saving settings	Operational error (Operations will continue)	[err]
Warning log	Warning	2xx Ex.) S220 PAN/TILT operation warning	Non-operational error	[warning]
Warning log	Warning	1xx Ex.) H144 Password specification error	Error external to the system	[notice]
Notification log	Information	0xx Ex.) S001 System started	Information on normal operation	[info]

Chapter 2

Measures Suitable to the Users' Environment

Managing Accounts Having Access to the Cameras [User Management]

"Administrator", "authorized user", and "guest user" are the three types of accounts that are able to access the camera.

The administrator account has authority over all of the camera's settings and operations. Administrator is the only account which is able to access the setting page. Therefore, in order to prevent leaks to unauthorized users, it is important to strictly manage information on the administrator account.

The "authorized user" and "guest user" are able to access the camera viewer. Understand what the "authorized user" and "guest user" are able to do, and set the minimum necessary authorization level and users.

■ "Authorized Users" Means Users Who Require Authentication

To allow only specific users, except the administrator, to access the camera viewer, set up an authorized user.

In the authorized user settings, register account information (user name and password) and grant camera viewer privileges (allow video distribution only, allow camera control, etc.). The same authority is given to all authorized users and it is possible to set the camera control similar to the administrator's camera control, therefore it is necessary to be careful to give authority to authorized users. Regularly review and manage the authorized users, and set the minimum necessary authorization level and users.

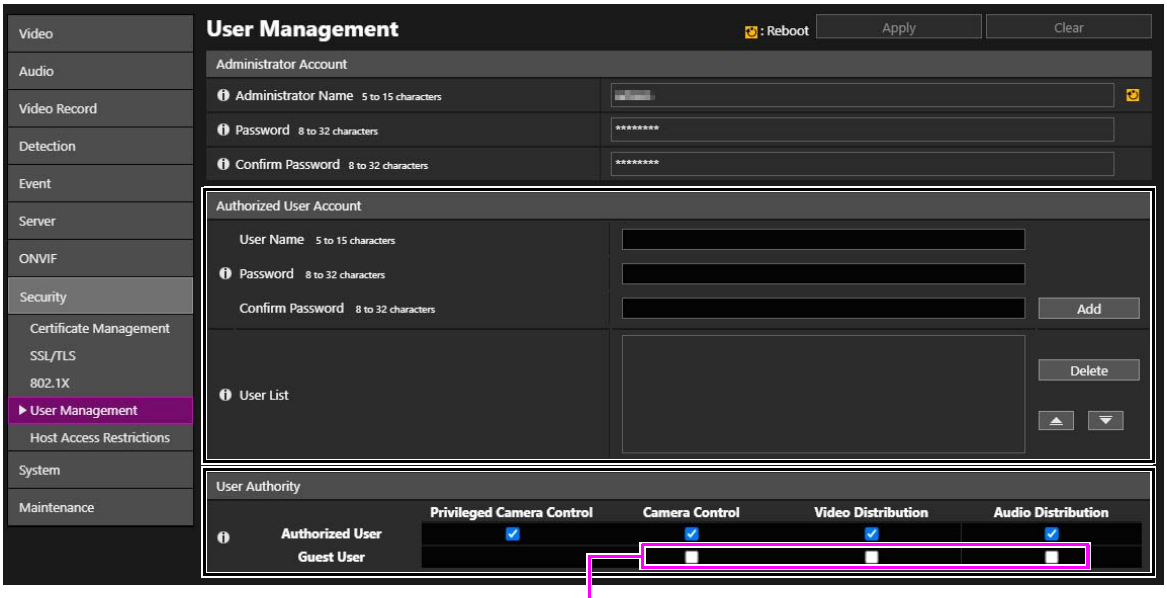
It is important to disable all the authorities of the guest users, which is described later, when wanting to restrict access to only authorized users. Unless these are disabled, access from the guest users will not be restricted.

■ "Guest Users"

Guest user means a guest account which does not need a user name and password. By enabling authorities for the guest users, anyone will be able to access the camera viewer without requiring user authentication. Also, this would allow camera control and video distribution commands without authentication. Therefore, authorities for guest users should be set only when the purpose of use of the camera is open to the general public, such as public release of the video, otherwise disable all authorities of the guest users.

When allowing access by guest users, grant only the minimum necessary privileges to them, since the same privileges are given to all guest users, just as to all the authorized users.

User management is set in [Security] > [User Management] > [Authorized User Account]/[User Authority] on the camera's setting page.

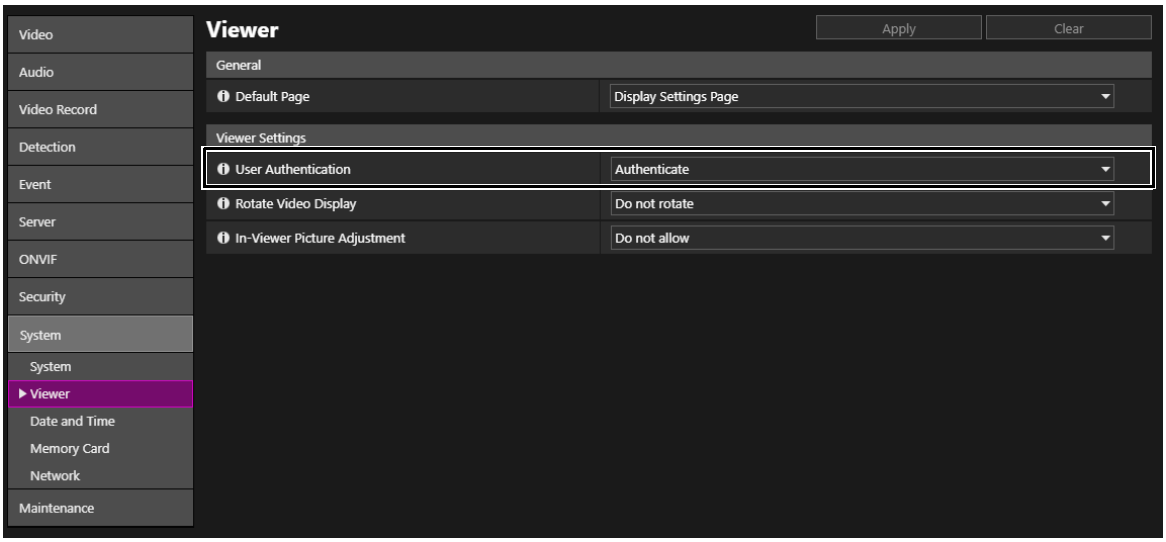


In order to cancel guest user authorities, clear all the check boxes.

■ Setting User Authentication for the Camera Viewer

It is possible to set the option of whether to authenticate users when accessing the camera viewer. However, the user authentication setting here is valid only in the camera viewer, and it is not applicable when accessing the camera by any other applications or viewers etc. Therefore, if the user authentication is to be applied to all kinds of access types, it is important to set the [User Authentication] to [Authenticate] and disable all privileges of the guest users as described above.

User authentication for the camera viewer is set in [System] > [Viewer] > [Viewer Settings] > [User Authentication] on the camera's Settings page.



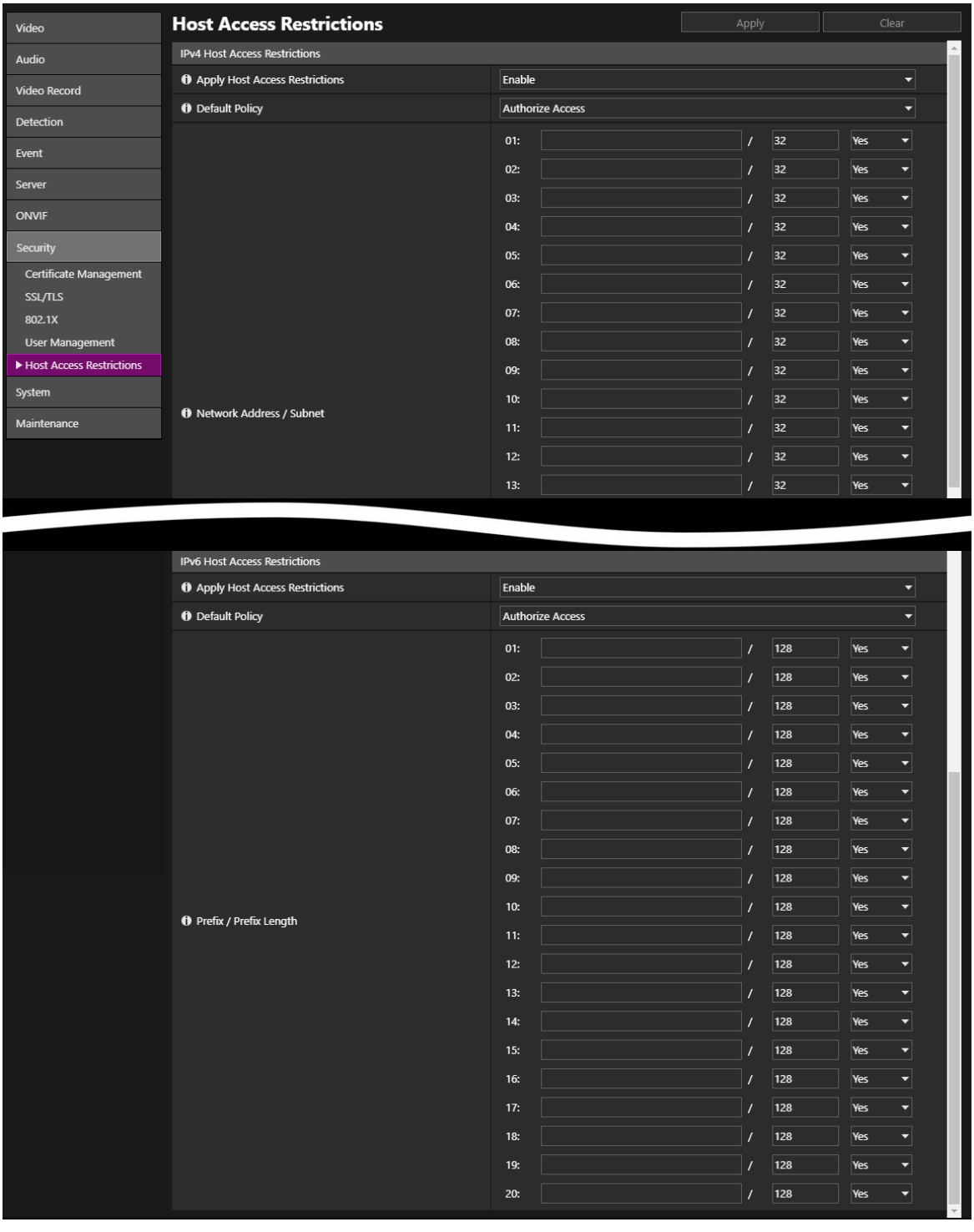
Restricting Hosts Having Access to the Cameras [Host Access Restrictions]

By specifying the hosts that can access the camera, the risk of unauthorized access can be reduced.

In order to restrict hosts to access the camera, allow communication with only specified hosts, and prohibit all other communication. Oppositely, there is also the method of prohibiting communication with specified hosts and allowing communication with all others.

Depending on the user's environment, the range of access restriction can be grouped on a network basis, or it can be set for each host. However, if mistakenly setting the administrator's IP address to prohibit communication, access from the administrator to the camera will be prohibited and there will be no other way than to restore to the factory default settings. Caution is needed when setting the access restrictions.

Host access restriction is set in [Security] > [Host Access Restrictions] > [IPv4 Host Access Restrictions]/[IPv6 Host Access Restrictions] on the camera's setting page.



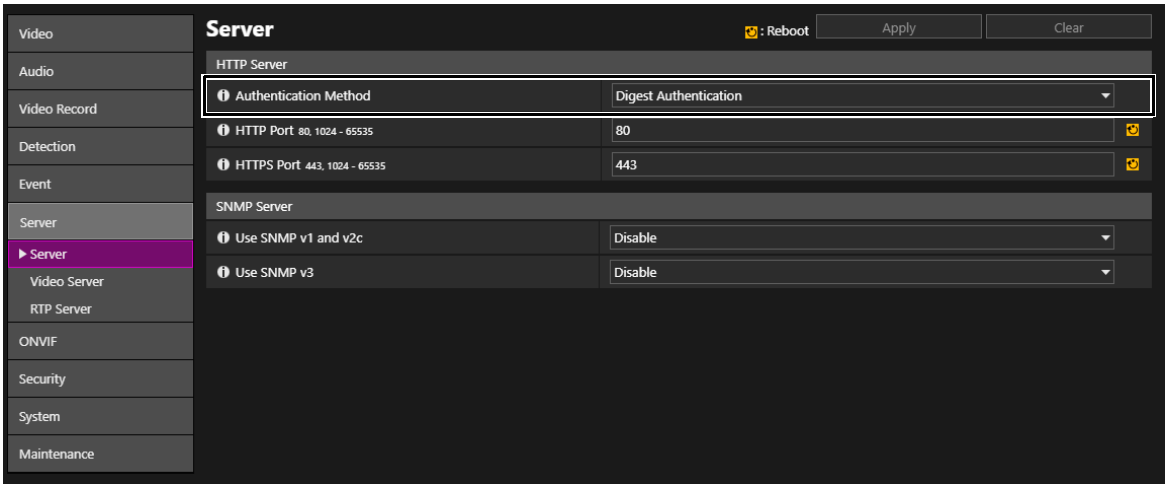
Setting to the Digest Authentication

When accessing the cameras via [HTTP Server] and [RTP Server], select [Digest Authentication] for the authentication method. When [Basic Authentication] is selected, the password can be easily leaked to unauthorized parties because the password will be sent on the network without being encrypted.

It is necessary to set the authentication method of the HTTP server and the RTP server respectively. Confirm that the application supports the digest authentication.

■ Digest Authentication (HTTP)

HTTP server authentication method is set in [Server] > [Server] > [HTTP Server] > [Authentication Method] on the camera's setting page.



■ Digest Authentication (RTSP)

RTP server's RTSP authentication method is set in [Server] > [RTP Server] > [RTP Server] > [RTSP Authentication Method] on the camera's setting page.

Changing the Port Number

It is important to limit unspecified access to prevent unauthorized access to the camera. The port number is an entrance to the communication between the camera and the external device, and a number is set for each communication protocol. A common number is used for the port number and network devices can be connected easily. Thus, there is a risk of it being used for intrusion by unauthorized parties.

In case there is a need to change the port number due to concern of security, make sure that the port numbers are not redundant with those of other communication protocols, and set it within the specified range. If the port number is changed, specify the port number in addition to the IP address in order to access the camera.

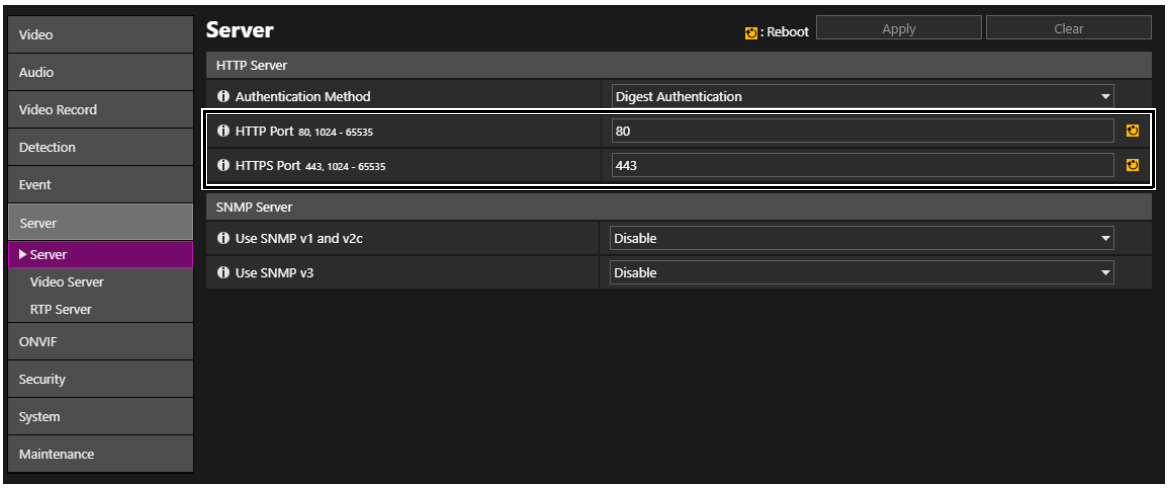
■ Example: Changing the Port Number

When connecting by the HTTPS, set "https://{Camera's IP address}:{Port Number}".

When the HTTPS port number is changed to 10443
https://192.168.100.1:10443

■ HTTP Port Numbers/HTTPS Port Numbers

HTTP/HTTPS port number is set in [Server] > [Server] > [HTTP Server] on the camera's setting page.



It is also possible to change the following port numbers:

■ RTSP Port Number

RTSP port number is set in [Server] > [RTP Server] > [RTP Server] on the camera's setting page.

■ Multicast Port Number

Multicast port number is set in [Server] > [RTP Server] on the camera's setting page.
[Audio Settings 1/2] > [Multicast Port]
[RTP Stream 1/2/3/4/5] > [Multicast Port]

Encrypting Communication [SSL/TLS]

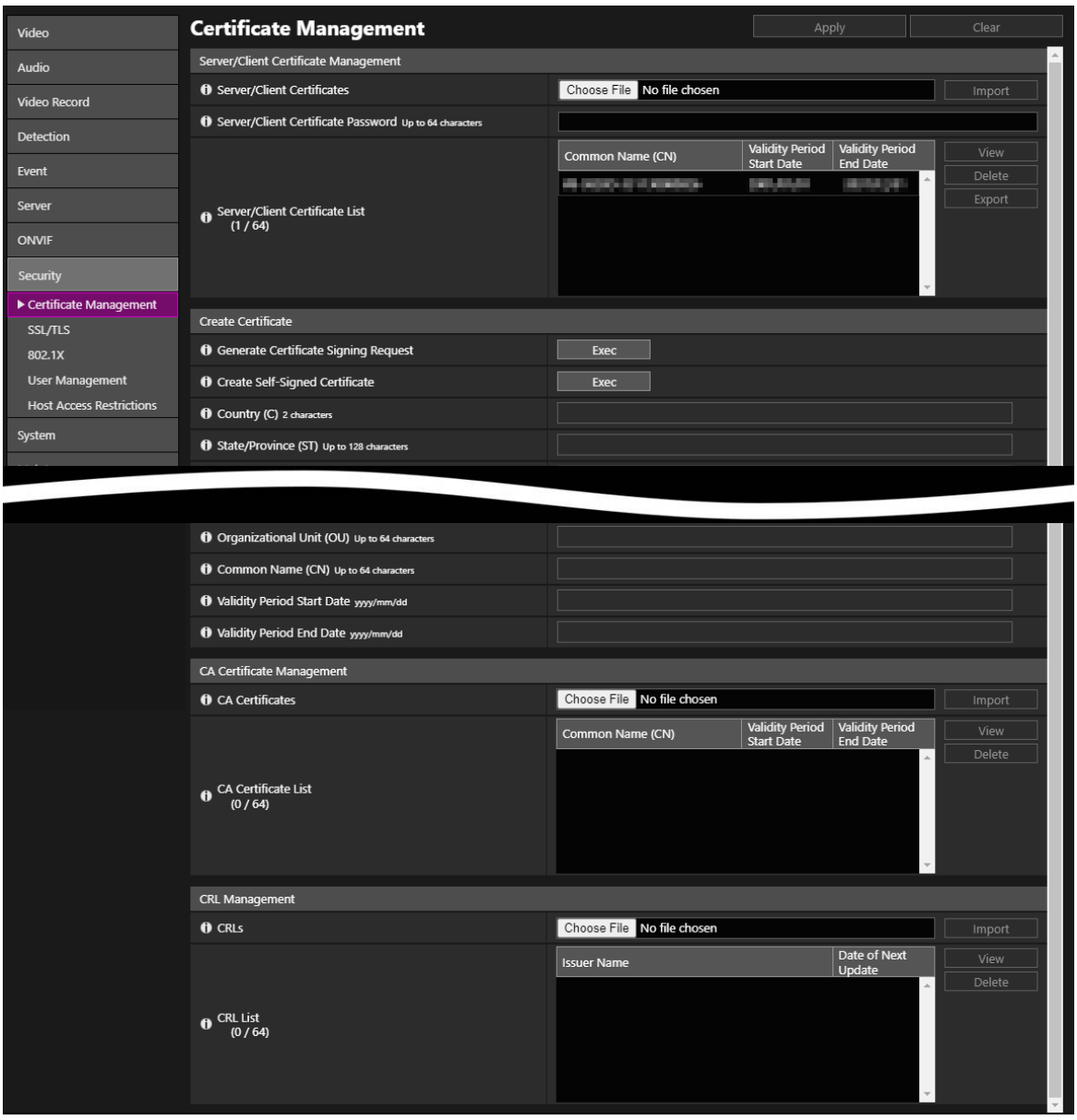
In order to securely communicate between the camera and the external device, it is recommended that all communication be via HTTPS connection (encrypted communication combining SSL/TLS and HTTP). SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is a technology to encrypt communication on the network and prevent hacking and tampering of communication contents by an unauthorized party. Even if the data is hacked during communication, by encrypting the communication in the proper way, the contents of the data are protected and safety can be secured.

■ Self-Signed Certificate and Server Certificate

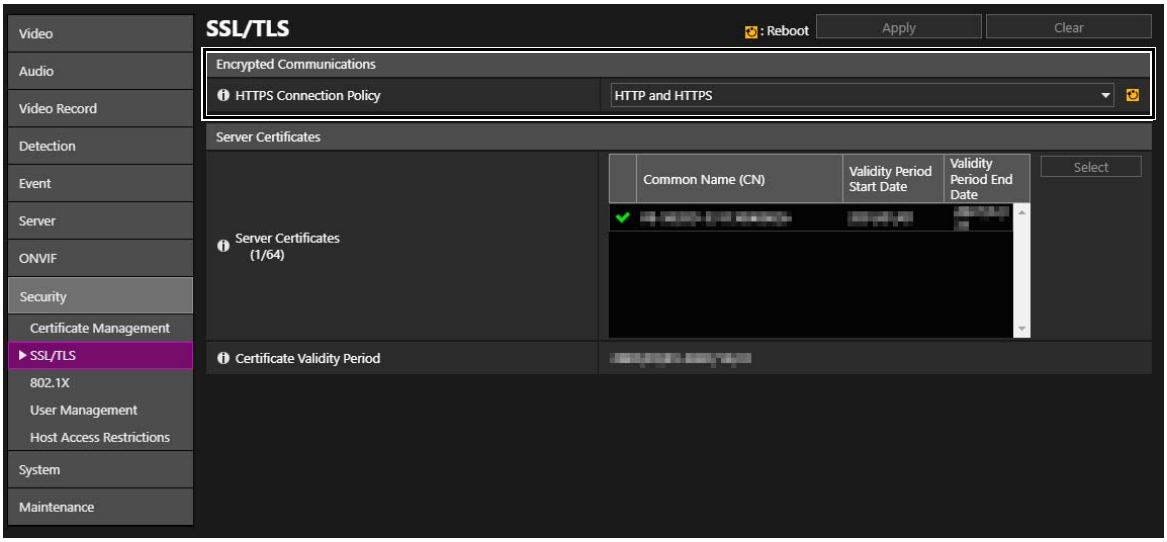
To encrypt communication via HTTPS connection, use a self-signed certificate or a server certificate issued from a CA (Certificate Authority). Self-signed certificates are sufficient to do encryption, however, a warning screen will be displayed in the web browser, and there is a risk of impersonation. Therefore, it is advised to use it in the cases for an operation test and others.
It is recommended to acquire and import a server certificate issued from CA for a full-scale system operation.

When using HTTPS or FTPS to upload, avoid the problem of performing communication with a dangerous server, by importing the CA certificate or certificate revocation list (CRL) issued by the CA and verifying the server certificate, for a safer communication with the server.

To install the certificate, go to the camera's Settings page, [Security]> [Certificate Management].



Encrypting communication by HTTPS connection is set in [Security] > [SSL/TLS] on the camera's setting page.



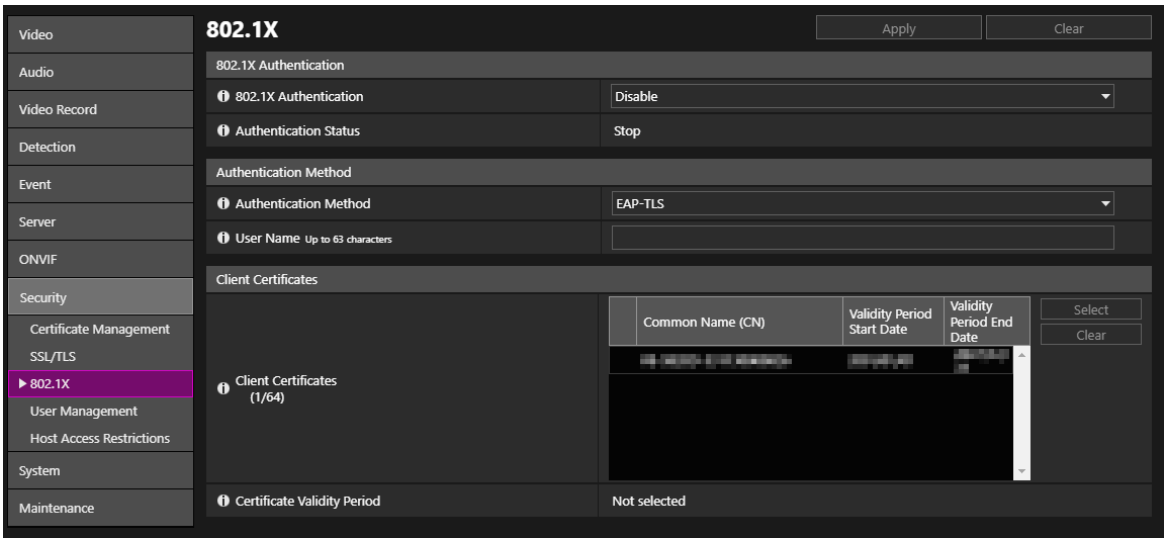
Note

- Even setting the HTTPS connection as mentioned above, the video delivered via RTP/RTSP as well as data to upload cannot be encrypted. In order to securely communicate these types of data, it is necessary to deal with the whole system.
- The installed CRL certificate applies only at the time of upload. For details, refer to the camera's Operation Guide.

Using Cameras on Protected Networks [802.1X]

IEEE802.1X authentication is a standard that regulates connections by authentication, that prevents access by non-specified devices to the network. Because only server authenticated devices can connect to the network, the network can be protected from unauthorized access. In order to allow a camera to access networks protected by IEEE802.1X authentication, appropriate certificates and settings are required.

IEEE802.1X is set in [Security] > [802.1X] on the camera's setting page.



To install the certificate, go to the camera's Settings page, [Security]> [Certificate Management].

Note

- In order to use the IEEE802.1X authentication function, it is necessary to establish the IEEE802.1X network environment in advance.
- Importing a CRL on 802.1x does not perform verification.

Disabling Unused Functions

The camera has functions to support various purposes and network environments. However, unless those functions are properly set, there is a risk of unauthorized access from outside parties. In order to use the camera safely, it is also necessary to disable the setting of unused functions.

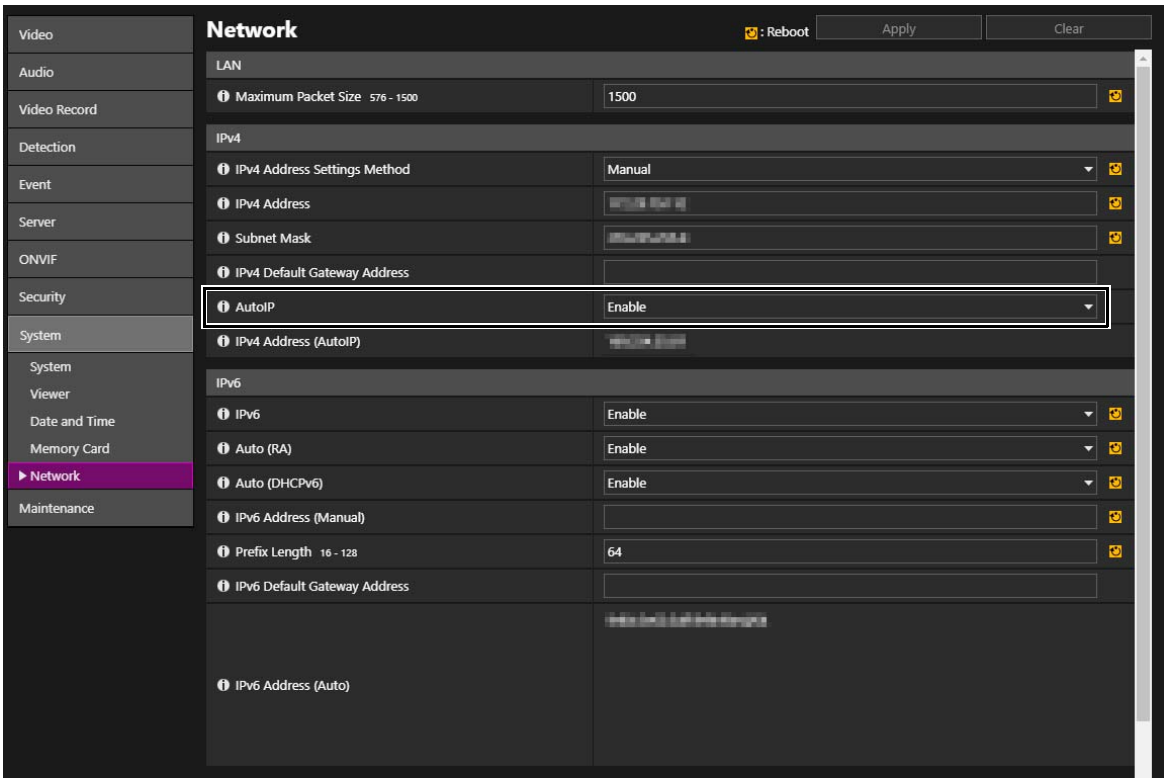
The details are explained below.

■ AutoIP

When [AutoIP] is enabled, even in environments where there is no DHCP server, IPv4 link local addresses (169.254.xxx.xxx) are assigned to the camera. Therefore, by assigning a PC to the same segment as the IPv4 address and using the Camera Management Tool, the camera can be detected and initial settings can be made.

Although [AutoIP] is enabled by factory default setting, it is recommended to disable [AutoIP] when the initial setting of the network is completed so that it will not be used for unauthorized purposes.

AutoIP is set in [System] > [Network] > [IPv4] > [AutoIP] on the camera's setting page.



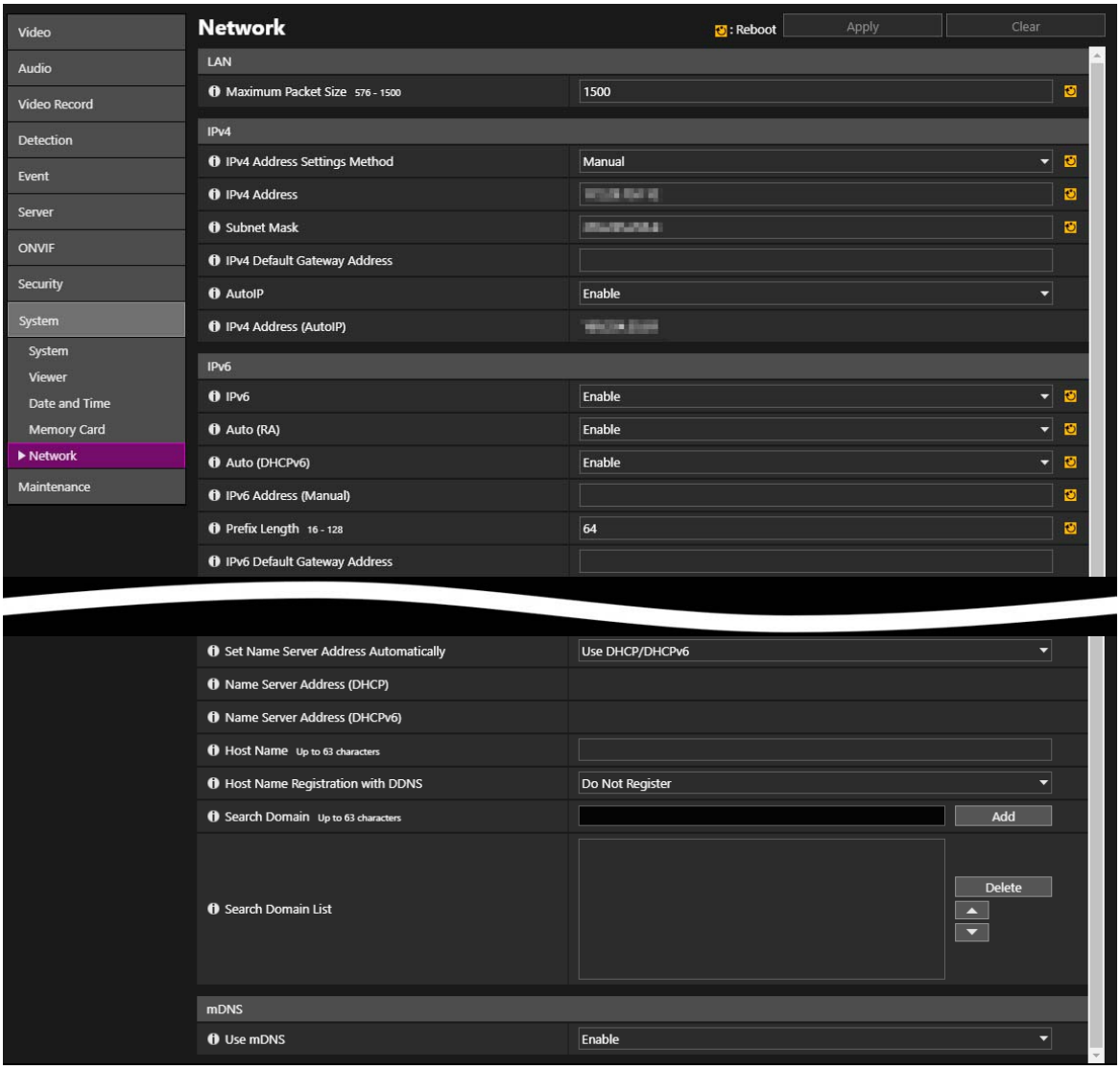
Factory default setting for [AutoIP]: [Enable]

■ mDNS (multicast Domain Name System)

[mDNS] is a function to notify devices on the network of the camera IP address and host name information simultaneously so that the camera can be detected even in an environment without a DNS server.

In the factory default setting, the setting of [mDNS] is enabled, it is recommended to disable [mDNS] when the initial setting of the network is completed so that it will not used for unauthorized purposes.

mDNS is set in [System] > [Network] > [mDNS] on the camera's setting page.



Factory default setting for [Use mDNS]: [Enable]

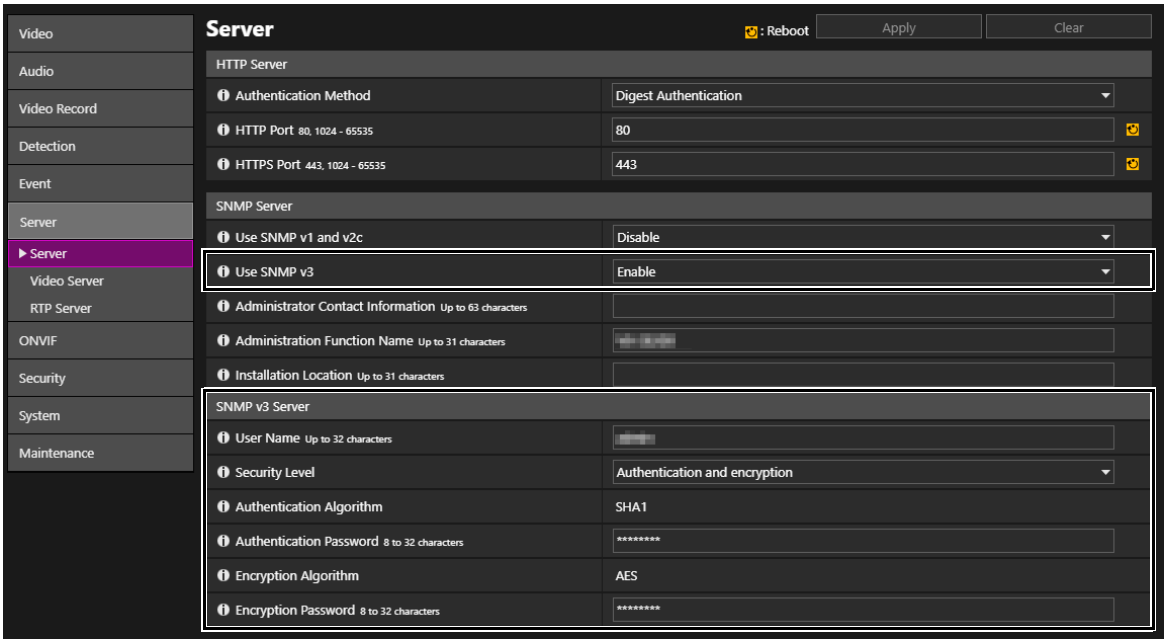
■ SNMP (Simple Network Management Protocol)

When using the [SNMP Server], it is possible to monitor and/or control the camera (SNMP Agent) from the SNMP manager.

The SNMPv3 is able to communicate by encrypting the user name and password that are authentication information. When managing by SNMP, select the SNMPv3, which is a much safer way of communicating compared to SNMPv1 and v2c, and set the encrypted password.

Use SNMPv1 and v2c in a network, only when it is necessary for a customer's environment, where security is secured.

SNMP server is set in [Server] > [Server] > [SNMP Server] on the camera's setting page.

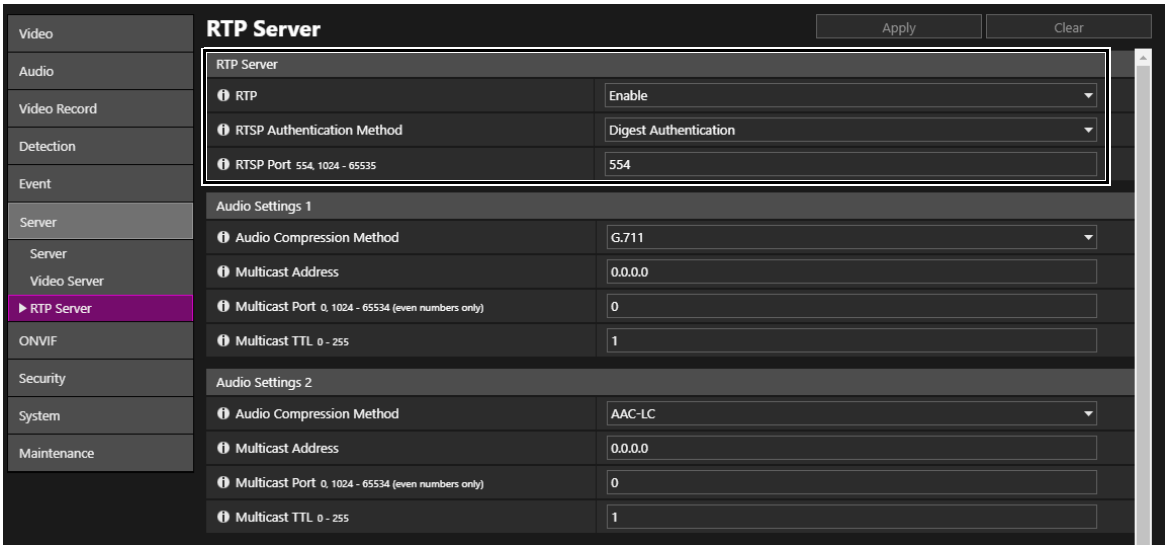


Factory default setting for [Use SNMP v1 and v2c]: [Disable]
Factory default setting for [Use SNMP v3]: [Disable]

■ RTP (Real-time Transport Protocol)

By using [RTP Server], video and audio data can be delivered to the specified multicast address. It is recommended to set [RTP] to [Disable] when the recording system and the viewer connecting to the camera do not require RTP protocol.

RTP server is set in [Server] > [RTP Server] > [RTP Server] on the camera's setting page.



Factory default setting for [RTP]: [Enable]

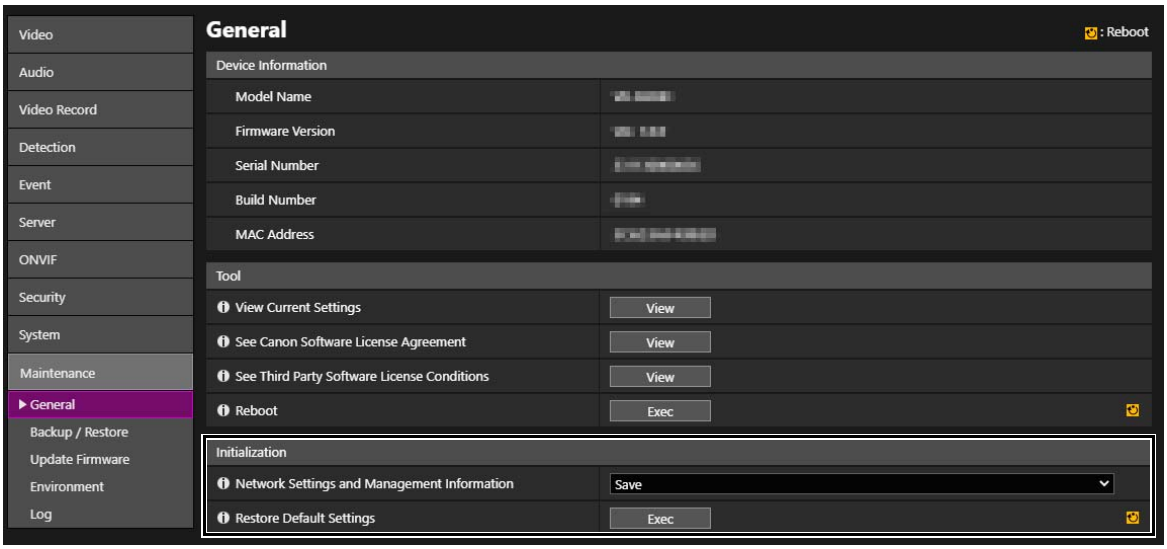
Appendix

When Disposing the Camera

When disposing the camera, initialize the camera and delete all setting information such as network settings and administrator account. Do not forget to take out the memory card.

To initialize the camera, go to [Maintenance] > [General] > [Initialization] on the camera's setting page. When disposing the camera, set [Network Settings and Management Information] to [Do not save]. If unable to access the setting page, use the reset switch on the camera to restore to the factory default settings.

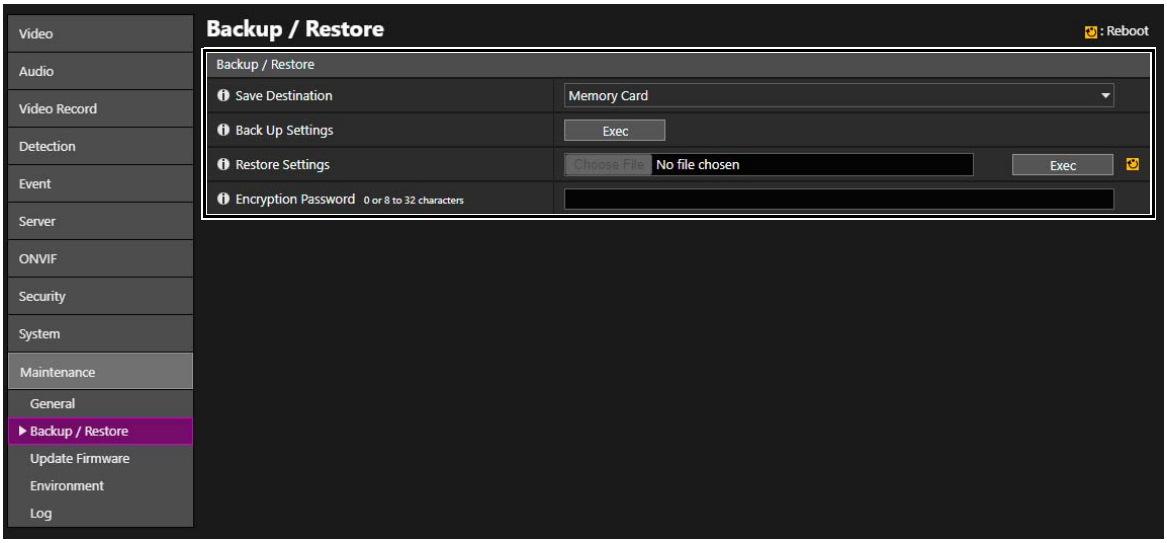
Operation of the camera reset switch differs for each model, therefore, refer to "Operation Guide".



Encrypting Backup Information

The backup information of the camera settings is used when restoring the camera to the user's previously saved settings. It is possible to manage the backup information more securely by setting [Encryption Password] for the backup information. Handle the set password with care.

Backup information encryption is set in [Maintenance] > [Backup/Restore] > [Backup/Restore] on the camera's setting page.



For models released before 2022

This chapter describes the following models. For network cameras other than the following models, refer to "Models released in and after 2022".

ME20F-SHN

VB-H

VB-H761LVE-H / VB-H761LVE / VB-H760VE / H751LE-H / VB-H751LE / VB-H730F Mk II / VB-H730F / VB-H710F / VB-H652LVE / VB-H651VE / VB-H651V / VB-H630VE / VB-H630D / VB-H610VE / VB-H610D / VB-H45 / VB-H43 / VB-H41

VB-M

VB-M741LE-H / VB-M741LE / VB-M740E / VB-M720F / VB-M700F / VB-M641VE / VB-M641V / VB-M640VE / VB-M640V / VB-M620VE / VB-M620D / VB-M600VE / VB-M600D / VB-M50B / VB-M44 / VB-M42 / VB-M40

VB-R

VB-R13VE / VB-R13 / VB-R12VE / VB-R11VE / VB-R11/ VB-R10VE

VB-S

VB-S910F / VB-S905F Mk II / VB-S905F / VB-S900F Mk II / VB-S900F / VB-S805D Mk II / VB-S805D / VB-S800D Mk II / VB-S800VE / VB-S800D / VB-S31D Mk II / VB-S31D / VB-S30D Mk II / VB-S30VE

Table of Contents

Introduction

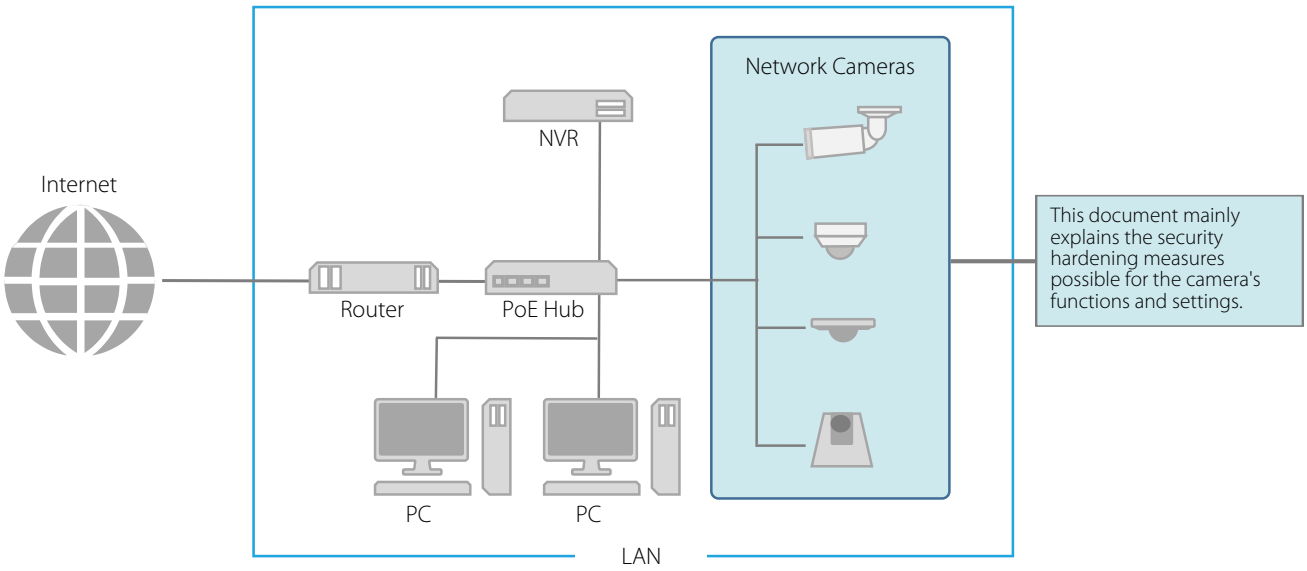
Devices that are connected to a network could be targeted for cyber attacks such as unauthorized accesses by non-intended unauthorized parties. Especially for network cameras, although they can be convenient since they have a variety of server functions, there is a risk of being attacked by hackers unless operated with security implementations. To completely eliminate all risks is impossible, however, by studying various risk angles and taking measures based on the security policies, it is possible to decrease the risk of cyber attacks.

This document explains the security hardening measures to the camera settings targeted for all customers with Canon Network Cameras (hereafter referred to as the cameras). Refer to this document and implement necessary measures according to the environment under the customer's responsibility, which will lead to safer camera operation.

About This Document

The security hardening measures explained in this document are mainly for the cameras, which are a part of an entire system as shown in the figure below. For the entire system's security hardening, measures must be taken according to the customer's network environment and/or purpose of the camera use.

Measures, not only from cyber attacks but against physical vandalism and mischief, are also important. Some of the examples of measures here are, embedding the cable that connects to the camera, isolating recording devices, restoring camera settings when disposing the camera, and remembering to remove the memory card, etc.



■ Warnings and Symbols

- In this document, there are screen shots of the camera's setting page explaining each measure, however, depending on the camera and firmware version used, the actual settings on the screen may differ. Each function's settings, as well as important points, are described in detail in the camera's "Operation Guide". Refer to the "Operation Guide" for the camera being used when setting up the camera.
- Any unauthorized reproduction of this document is prohibited.
- The contents of this document are subject to change without any prior notice.
- To the full extent permitted by laws and regulations, neither Canon Inc. nor any of its subsidiaries or affiliates shall be liable for any losses, direct, incidental or consequential damages, or liabilities that may be incurred as a result of network security incidents such as unauthorized accesses.

The following symbols used in this document indicate important and supplementary information.

Important Cautions and restrictions are written under this symbol. Make sure to read these carefully.

Note Supplementary descriptions and reference information are written under this symbol.

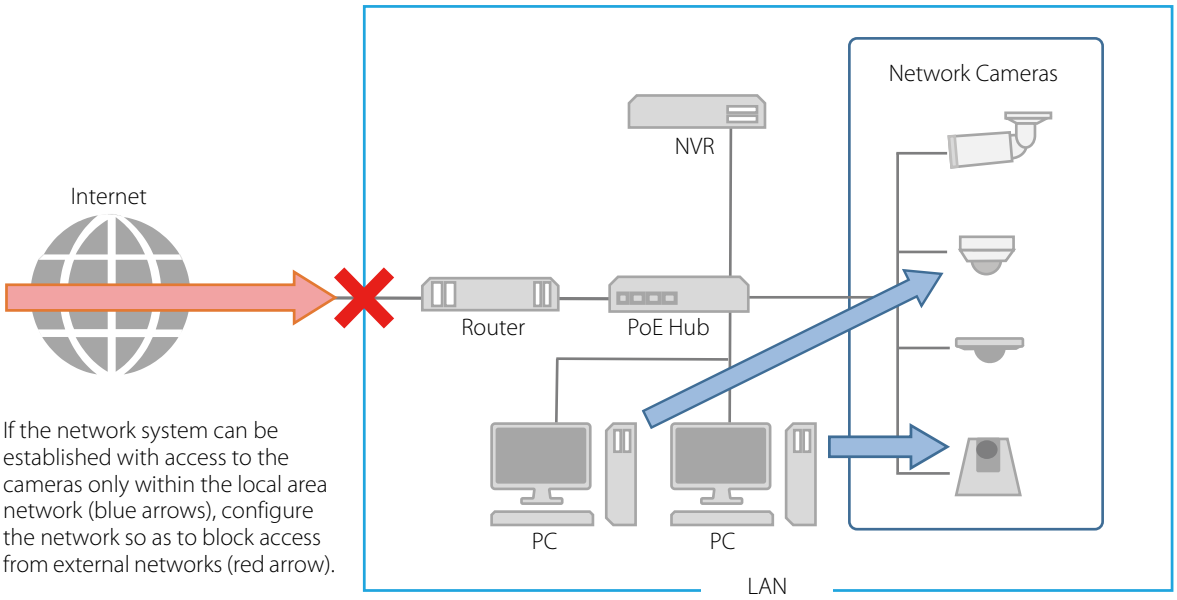
Operating in a Network Configuration Suitable to the Users' Needs

Before explaining what security hardening measures are possible with the camera's functions and settings, the network configuration suitable to the camera use is explained here. Check whether the camera access from outside is necessary.

■ Blocking Access from Outside

In order to reduce the security risk when checking the camera's video or changing the settings, it is effective to block access physically and/or virtually if it is unnecessary to be made accessible from an external network, such as the internet.

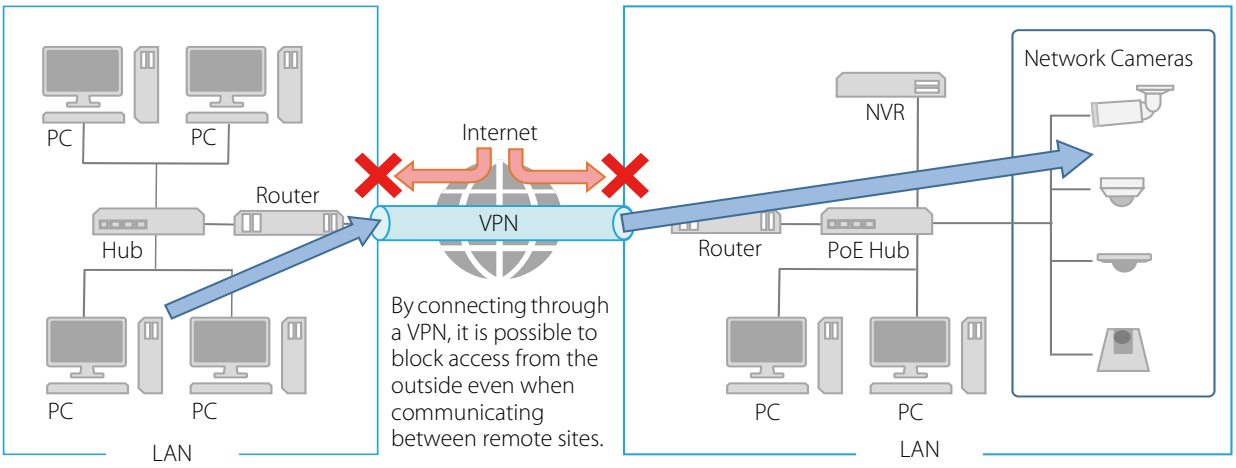
When access from a remote location is unnecessary and the devices accessing the camera can be limited, using only specific devices in the same local area network will enhance security. When it is necessary to access the camera from a remote location, it is important to use a method that can communicate safely, such as using a VPN that can block access from the outside.



If the network system can be established with access to the cameras only within the local area network (blue arrows), configure the network so as to block access from external networks (red arrow).

What is a VPN?

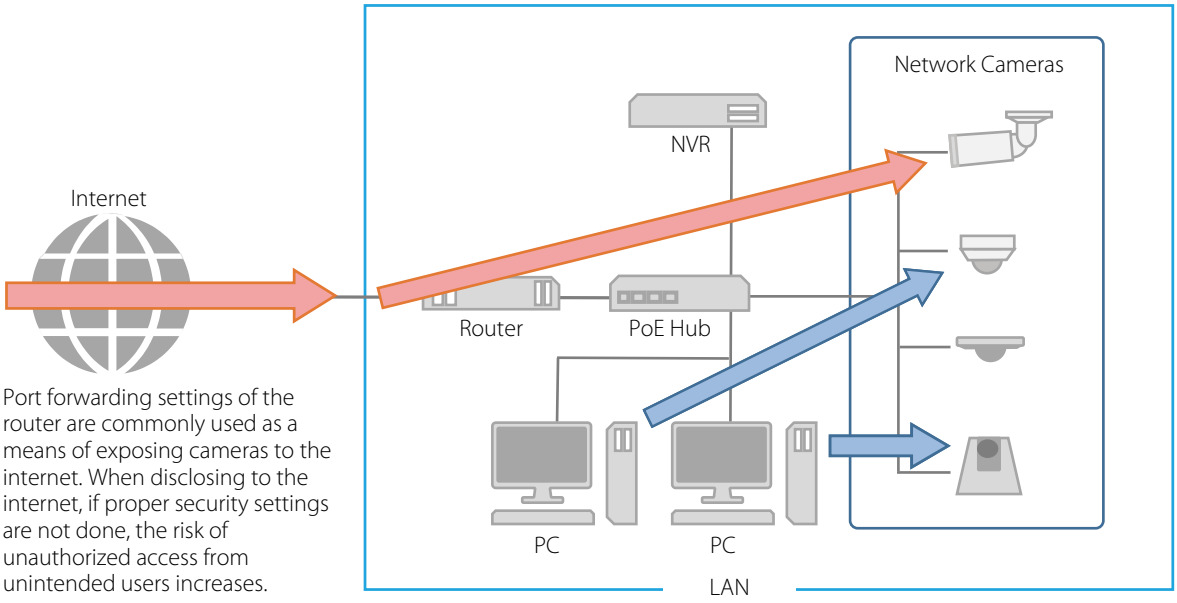
A VPN is an abbreviation of the word Virtual Private Network, which creates a virtual tunnel for a communication path that is capable of having a safe data exchange. By connecting LANs of different sites such as head office and branch offices via VPN, it is possible to block access from external networks.



By connecting through a VPN, it is possible to block access from the outside even when communicating between remote sites.

■ Making Thorough Measures for Networks That can be Accessed Externally

In case of sharing videos with the general public, it is necessary to disclose the camera information to the internet so that the camera can be accessed from the outside by connecting to an external network such as the internet.



Port forwarding settings of the router are commonly used as a means of exposing cameras to the internet. When disclosing to the internet, if proper security settings are not done, the risk of unauthorized access from unintended users increases.

Networks that allow external access are highly convenient, but at the same time the risk of unauthorized access to devices on the network increases. Therefore, in such a network configuration as illustrated above, it is important not only to implement the countermeasures described in this document, but also to secure measures to the entire system such as authentication of each device and encryption of each communication on the network.

Chapter 1

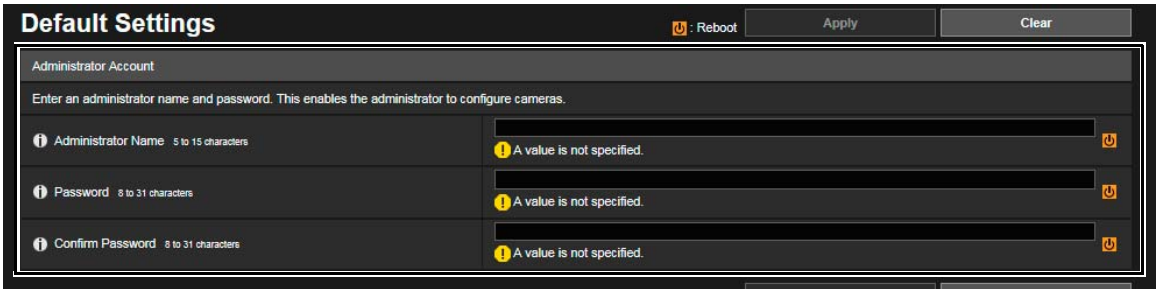
Basic Measures

Setting Administrator Name and Password

The administrator account has authority over all of the camera's settings and operations. If the administrator account is illegally used by an unauthorized party and tampering is done, there is a risk the camera will not be accessible. In order to prevent spoofing of the administrator account, the most fundamental measure for safe operation of the camera is to make the administrator name and password in an array of letters that are difficult to guess by unauthorized users. Strictly manage the administrator account and refrain from settings such as the same administrator account on multiple cameras.

The administrator account needs to be set when the camera is started for the first time. After setting, editing can be done in [Basic] > [User Management] on the camera's setting page.

The administrator account is set in [Default Settings] when accessing the camera for the first time.



The administrator name and password can be changed in [Basic] or [Security] > [User Management] on the camera's setting page.

■ Setting a Strong Administrator Name and Password

In order to strengthen the administrator name and password, consider the following points:

- Combine at least 10 characters of alphanumeric characters or symbols and special characters permitted for the camera.
- Combine upper and lower case characters.
- Avoid commonly used words and string of characters that are easy to guess.

Important

- If the factory default setting has an administrator account, be sure to change it.
- The number of characters that can be set for the administrator name and password depends on the product. For details, refer to the "Camera Management Tool User Manual".

■ Other Passwords

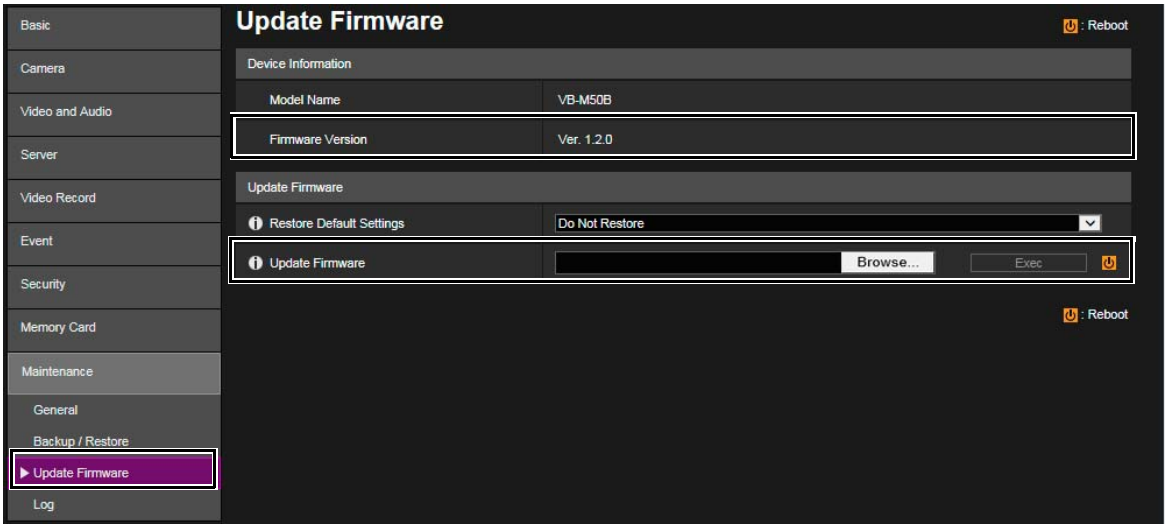
For the camera, in addition to the administrator account, the password for the authorized user (p. B-12), server authentication, and encryption are to be set. Set these passwords in an array of letters that are difficult to guess by unauthorized parties and manage them appropriately.

Using the Latest Firmware

The camera's firmware is updated as needed in order to improve performance of the functions and bug fixes. From the security point of view, it is important to always keep it updated because the measures against known vulnerabilities are applied to the latest firmware.

Check Canon's website regularly at the initial setting after purchasing the camera and during its operation, whether the latest firmware is provided.
The firmware version can be confirmed in [Maintenance] > [Device Information] > [Firmware Version] on the camera's setting page.

The firmware is updated in [Maintenance] > [Update Firmware] > [Update Firmware] on the camera's setting page.

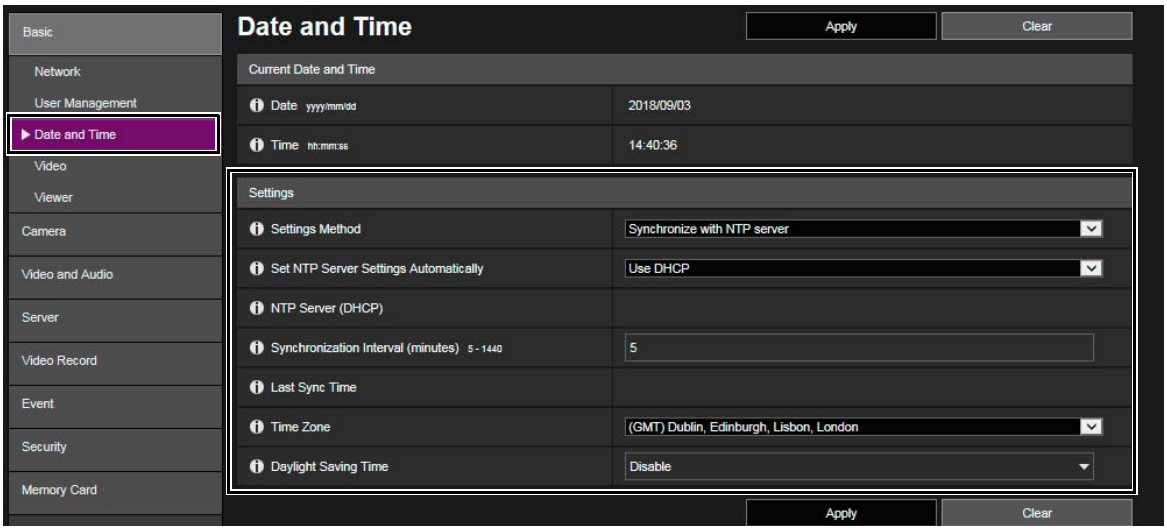


It is also possible to use the Camera Management Tool to update the firmware.
For details regarding the Camera Management Tool, refer to the "Camera Management Tool User Manual".

Setting Date and Time

Set the correct date and time for the camera. If there are indications that suspicious unauthorized access occurred, it may be possible to confirm the date and time of occurrence by checking the log.

Date and time is set in [Basic] > [Date and Time] > [Settings] on the camera's setting page.



Monitoring the Log

Camera connection status and operating conditions are recorded and saved as a log in the camera embedded memory and the memory card. Check the logs periodically to quickly find any signs of suspicious unauthorized access, such as repeated user authentication failures. For details on the log, refer to the camera's "Operation Guide".

■ Save Destination and Category of the Log

The log contents saved on the camera embedded memory and the memory card are different.

Log saved on the camera embedded memory: Error log, Warning log, Information log

– The logs will be deleted if any of the following operations are performed: rebooting, initialization, and restoring to the factory default settings. The log will also be deleted if exceeding a certain size.

Log saved on the memory card: Error log, Section of the warning log, Information log

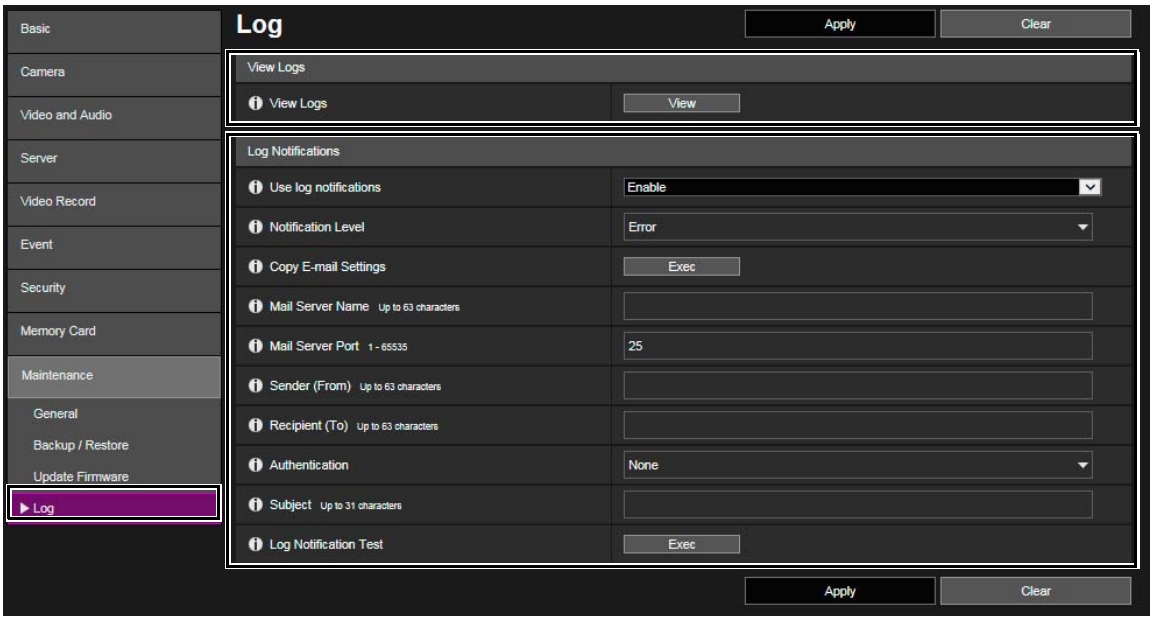
– The logs will not be deleted if any of the following operations are performed: rebooting, initialization, and restoring to the factory default settings.

■ Viewing, Notifying, and Downloading the Log

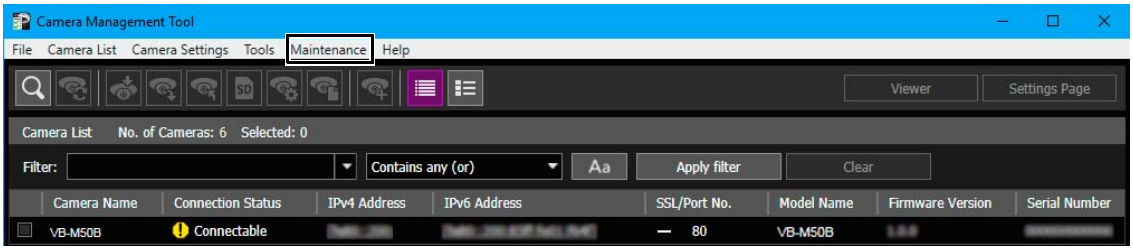
Log saved on the camera embedded memory can be confirmed in [View Logs] on the camera's setting page. It is also possible to notify the user of [Error] and [Errors and warnings] at the level the user set, if [Log Notifications] is enabled.

When using the Camera Management Tool, it is possible to download both the camera embedded memory log and memory card log as a file respectively.

Viewing and setting options of the log are set on the camera's setting page.
[Maintenance] > [Log] > [View Logs]
[Maintenance] > [Log] > [Log Notifications]



Download the log file in [Maintenance] > [Download Log] on the Camera Management Tool.



Example of the Camera Management Tool screen

■ Log Contents

Log level, code, fault level, category are as follows:

Log	Level	Code	Fault level	Category
Error log	Error	4xx Ex.) S410 Event service initialization error	Software-level failure (Task operations will stop)	[crit]
Error log	Error	3xx Ex.) S302 Error on saving settings	Operational error (Operations will continue)	[err]
Warning log	Warning	2xx Ex.) S220 PAN/TILT operation warning	Non-operational error	[warning]
Warning log	Warning	1xx Ex.) H144 Password specification error	Error external to the system	[notice]
Notification log	Information	0xx Ex.) S001 System started	Information on normal operation	[info]

Chapter 2

Measures Suitable to the Users' Environment

Managing Accounts Having Access to the Cameras [User Management]

"Administrator", "authorized user", and "guest user" are the three types of accounts that are able to access the camera.

The administrator account has authority over all of the camera's settings and operations. Administrator is the only account which is able to access the setting page. Therefore, in order to prevent leaks to unauthorized users, it is important to strictly manage information on the administrator account.

The "authorized user" and "guest user" are able to access the camera viewer. Understand what the "authorized user" and "guest user" are able to do, and set the minimum necessary authorization level and users.

■ "Authorized Users" Means Users Who Require Authentication

To allow only specific users, except the administrator, to access the camera viewer, set up an authorized user.

In the authorized user settings, register account information (user name and password) and grant camera viewer privileges (allow video distribution only, allow camera control, etc.). The same authority is given to all authorized users and it is possible to set the camera control similar to the administrator's camera control, therefore it is necessary to be careful to give authority to authorized users. Regularly review and manage the authorized users, and set the minimum necessary authorization level and users.

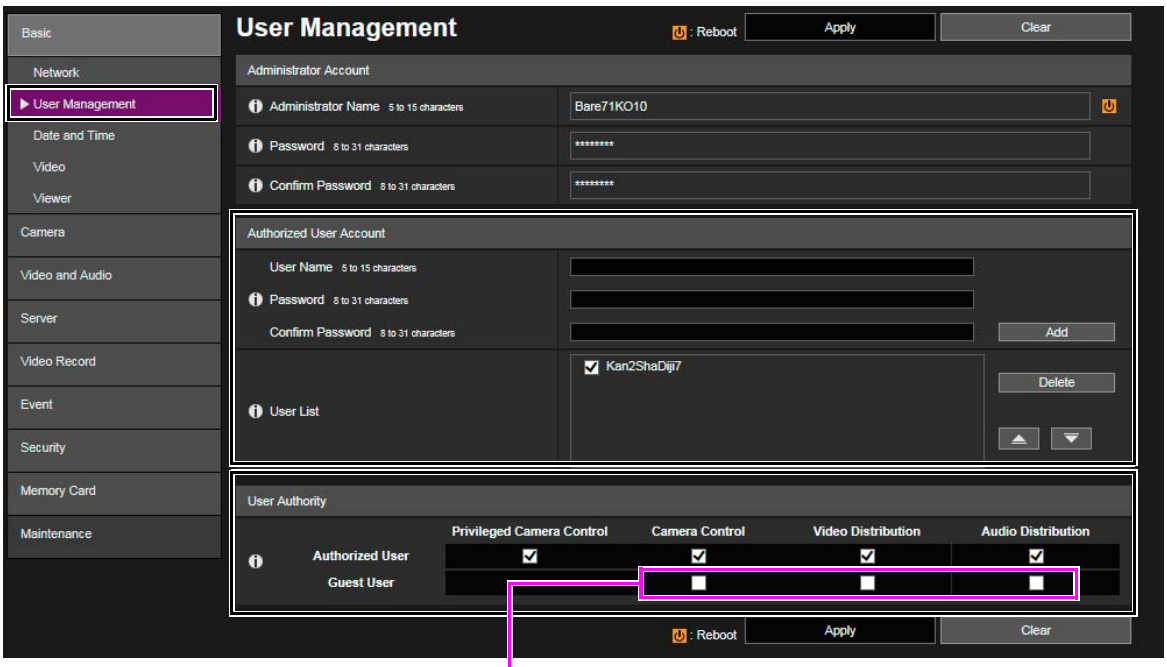
It is important to disable all the authorities of the guest users, which is described later, when wanting to restrict access to only authorized users. Unless these are disabled, access from the guest users will not be restricted.

■ "Guest Users"

Guest user means a guest account which does not need a user name and password. By enabling authorities for the guest users, anyone will be able to access the camera viewer without requiring user authentication. Also, this would allow camera control and video distribution commands without authentication. Therefore, authorities for guest users should be set only when the purpose of use of the camera is open to the general public, such as public release of the video, otherwise disable all authorities of the guest users.

When allowing access by guest users, grant only the minimum necessary privileges to them, since the same privileges are given to all guest users, just as to all the authorized users.

User management is set in [Basic] or [Security] > [User Management] > [Authorized User Account]/[User Authority] on the camera's setting page. (The screen shot below is an example from [Basic].)

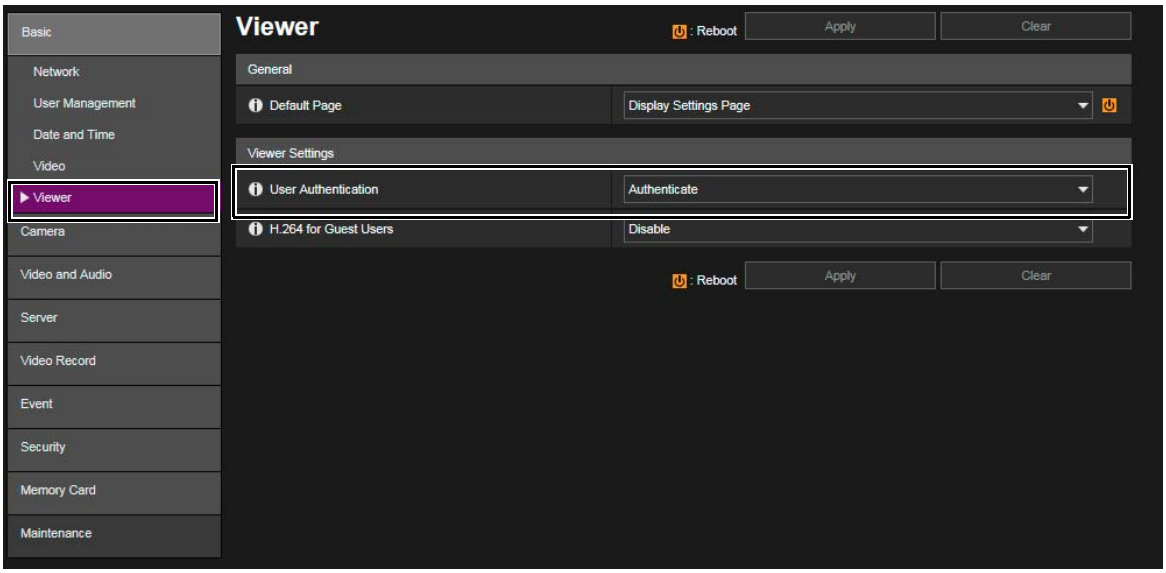


In order to cancel guest user authorities, clear all the check boxes.

■ Setting User Authentication for the Camera Viewer

It is possible to set the option of whether to authenticate users when accessing the camera viewer. However, the user authentication setting here is valid only in the camera viewer, and it is not applicable when accessing the camera by any other applications or viewers etc. Therefore, if the user authentication is to be applied to all kinds of access types, it is important to set the [User Authentication] to [Authenticate] and disable all privileges of the guest users as described above.

User authentication for the camera viewer is set in [Basic] > [Viewer] > [Viewer Settings] > [User Authentication] on the camera's setting page.



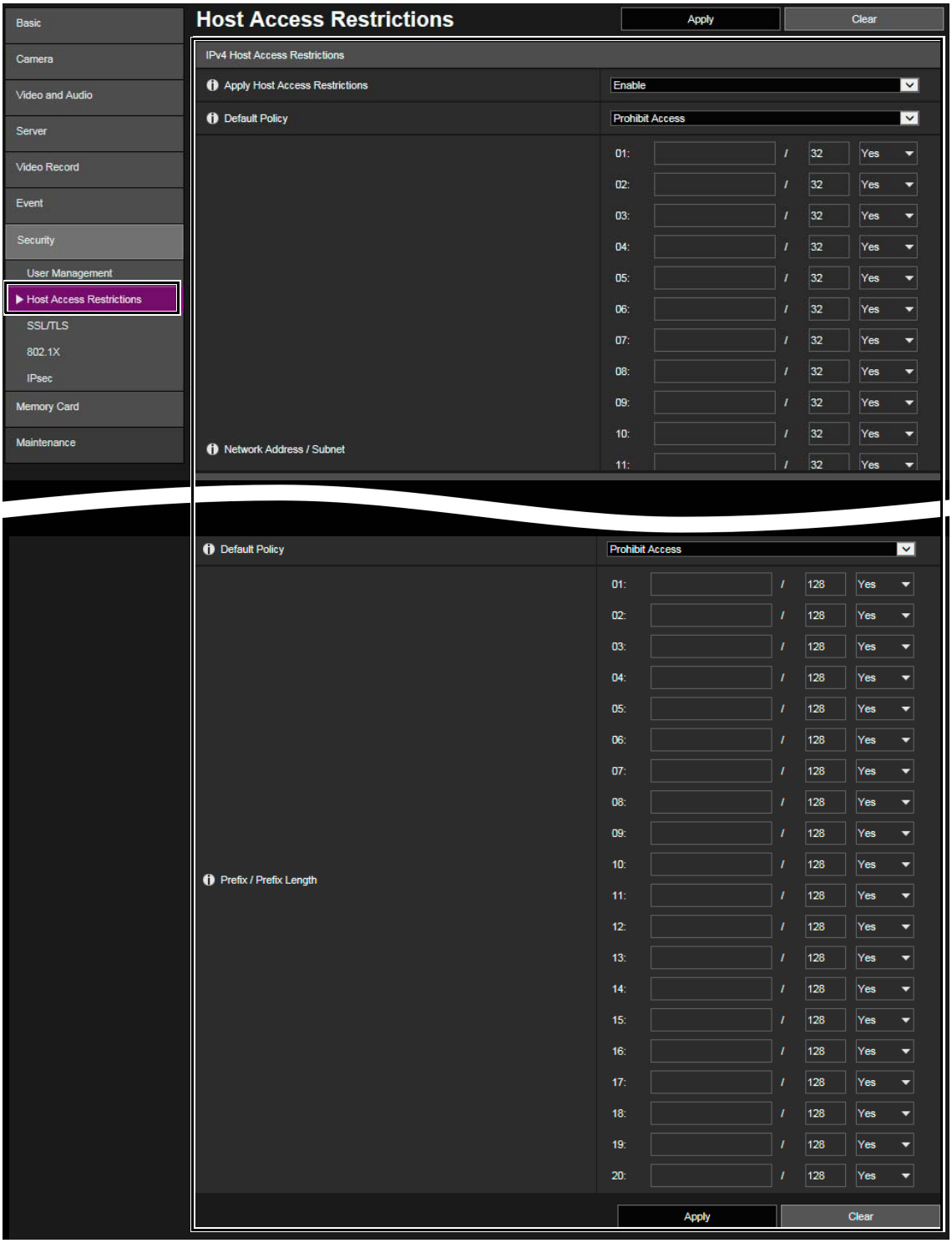
Restricting Hosts Having Access to the Cameras [Host Access Restrictions]

By specifying the hosts that can access the camera, the risk of unauthorized access can be reduced.

In order to restrict hosts to access the camera, allow communication with only specified hosts, and prohibit all other communication. Oppositely, there is also the method of prohibiting communication with specified hosts and allowing communication with all others.

Depending on the user's environment, the range of access restriction can be grouped on a network basis, or it can be set for each host. However, if mistakenly setting the administrator's IP address to prohibit communication, access from the administrator to the camera will be prohibited and there will be no other way than to restore to the factory default settings. Caution is needed when setting the access restrictions.

Host access restriction is set in [Security] > [Host Access Restrictions] > [IPv4 Host Access Restrictions]/[IPv6 Host Access Restrictions] on the camera's setting page.



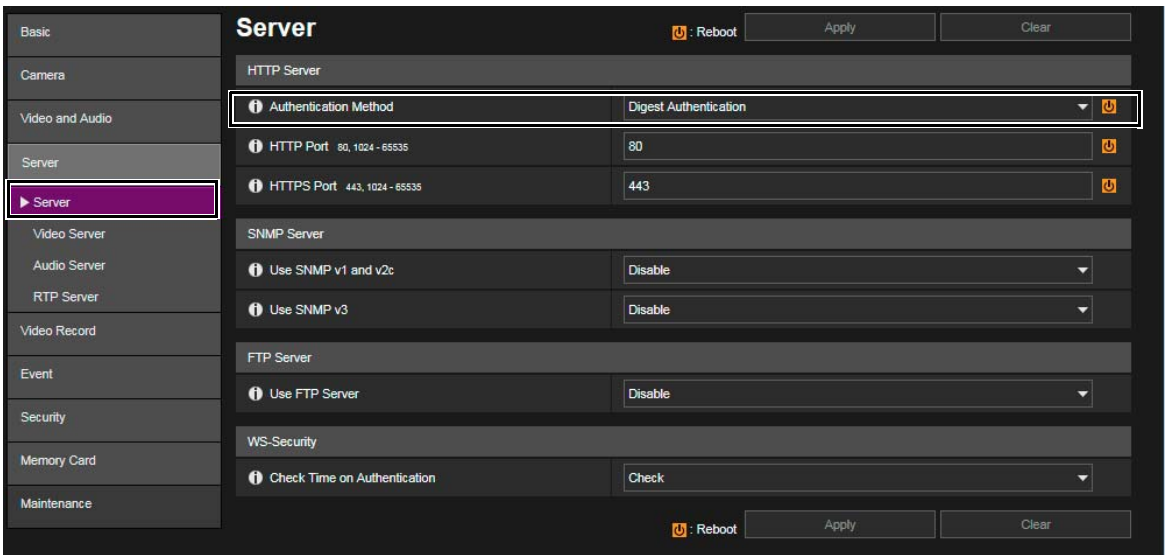
Setting to the Digest Authentication

When accessing the cameras via [HTTP Server] and [RTP Server], select [Digest Authentication] for the authentication method. When [Basic Authentication] is selected, the password can be easily leaked to unauthorized parties because the password will be sent on the network without being encrypted.

It is necessary to set the authentication method of the HTTP server and the RTP server respectively. Confirm that the application supports the digest authentication.

■ Digest Authentication (HTTP)

HTTP server authentication method is set in [Server] > [Server] > [HTTP Server] > [Authentication Method] on the camera's setting page.



■ Digest Authentication (RTSP)

RTP server's RTSP authentication method is set in [Server] > [RTP Server] > [RTP Server] > [RTSP Authentication Method] on the camera's setting page.

Changing the Port Number

It is important to limit unspecified access to prevent unauthorized access to the camera. The port number is an entrance to the communication between the camera and the external device, and a number is set for each communication protocol. A common number is used for the port number and network devices can be connected easily. Thus, there is a risk of it being used for intrusion by unauthorized parties.

In case there is a need to change the port number due to concern of security, make sure that the port numbers are not redundant with those of other communication protocols, and set it within the specified range. If the port number is changed, specify the port number in addition to the IP address in order to access the camera.

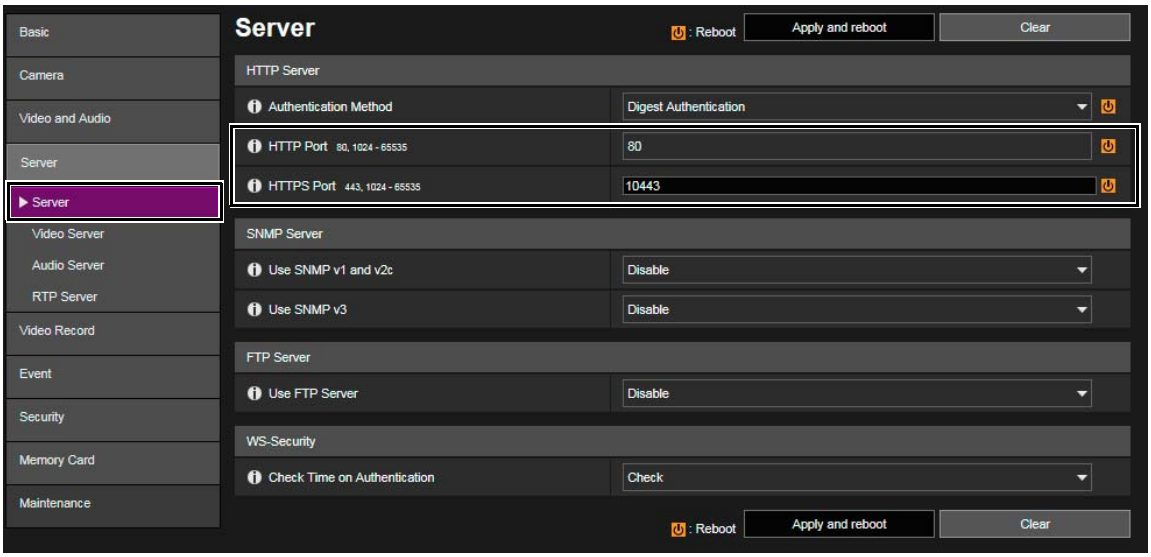
■ Example: Changing the Port Number

When connecting by the HTTPS, set "https://{Camera's IP address}:{Port Number}".

When the HTTPS port number is changed to 10443
https://192.168.100.1:10443

■ HTTP Port Numbers/HTTPS Port Numbers

HTTP/HTTPS port number is set in [Server] > [Server] > [HTTP Server] on the camera's setting page.



It is also possible to change the following port numbers:

■ RTSP Port Number

RTSP port number is set in [Server] > [RTP Server] > [RTP Server] on the camera's setting page.

■ Multicast Port Number

Multicast port number is set in [Server] > [RTP Server] on the camera's setting page.
[Audio Multicast] > [Multicast Port]
[RTP Stream 1/2/3/4/5] > [Multicast Port]

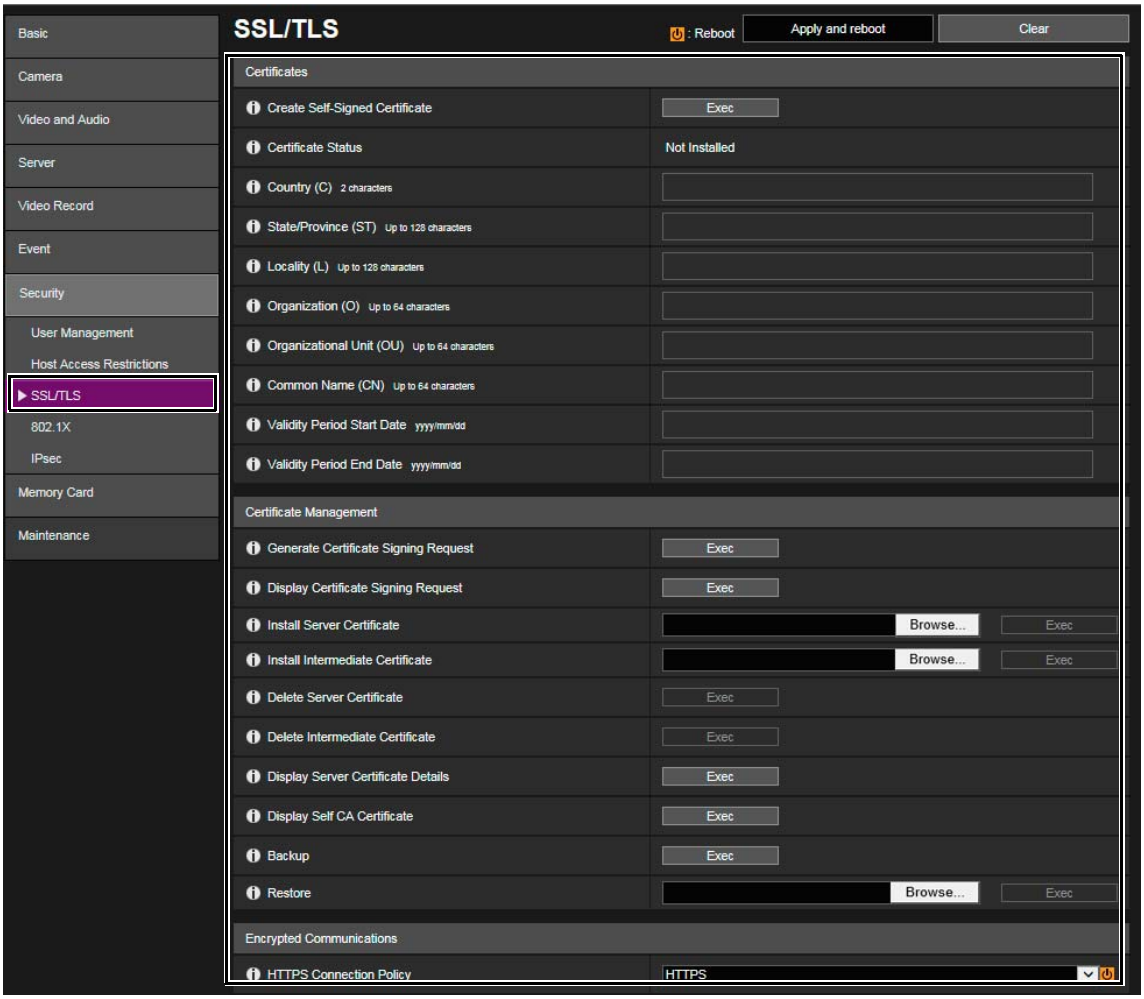
Encrypting Communication [SSL/TLS]

In order to securely communicate between the camera and the external device, it is recommended that all communication be via HTTPS connection (encrypted communication combining SSL/TLS and HTTP). SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is a technology to encrypt communication on the network and prevent hacking and tampering of communication contents by an unauthorized party. Even if the data is hacked during communication, by encrypting the communication in the proper way, the contents of the data are protected and safety can be secured.

■ Self-Signed Certificate and Server Certificate

To encrypt communication via HTTPS connection, use a self-signed certificate or a server certificate issued from a CA (Certificate Authority). Self-signed certificates are sufficient to do encryption, however, a warning screen will be displayed in the web browser, and there is a risk of impersonation. Therefore, it is advised to use it in the cases for an operation test and others.
It is recommended to acquire and install a server certificate issued from CA for a full-scale system operation.

Encrypting communication by HTTPS connection is set in [Security] > [SSL/TLS] on the camera's setting page.



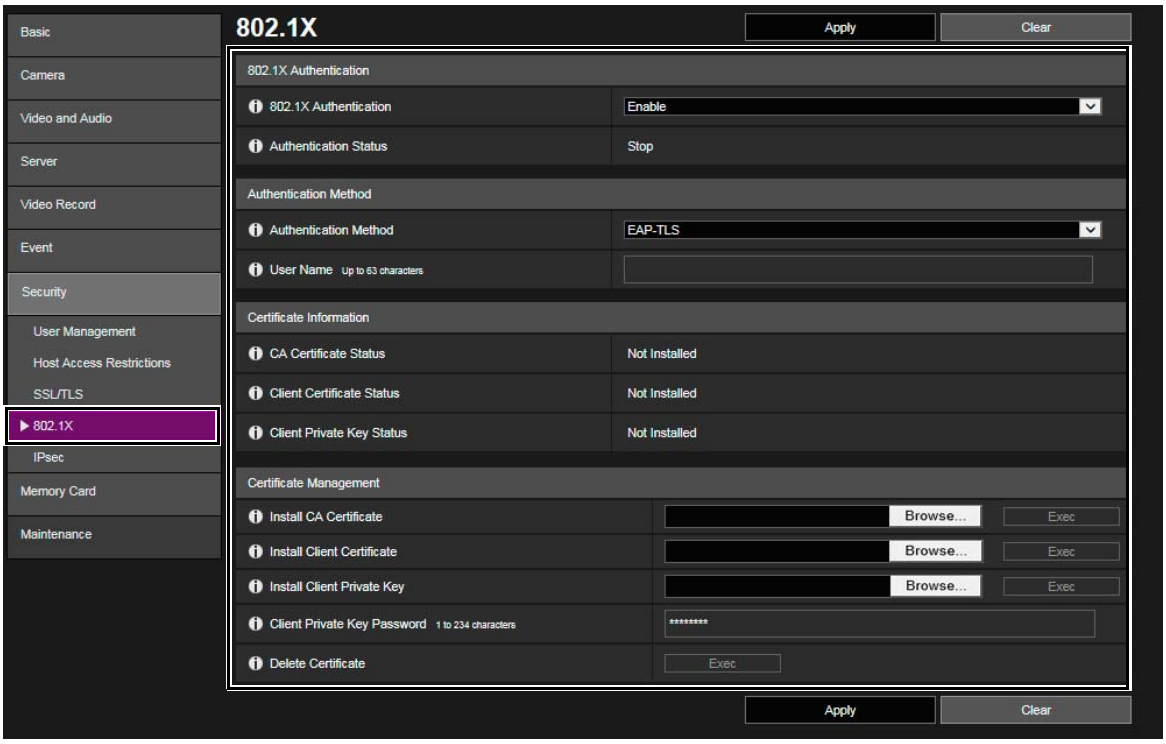
Note

Even setting the HTTPS connection as mentioned above, the video delivered via RTP/RTSP as well as data to upload cannot be encrypted. In order to securely communicate these types of data, it is necessary to deal with the whole system.

Using Cameras on Protected Networks [802.1X]

IEEE802.1X authentication is a standard that regulates connections by authentication, that prevents access by non-specified devices to the network. Because only server authenticated devices can connect to the network, the network can be protected from unauthorized access. In order to allow a camera to access networks protected by IEEE802.1X authentication, appropriate certificates and settings are required.

IEEE802.1X is set in [Security] > [802.1X] on the camera's setting page.



Note

In order to use the IEEE802.1X authentication function, it is necessary to establish the IEEE802.1X network environment in advance.

Disabling Unused Functions

The camera has functions to support various purposes and network environments. However, unless those functions are properly set, there is a risk of unauthorized access from outside parties. In order to use the camera safely, it is also necessary to disable the setting of unused functions.

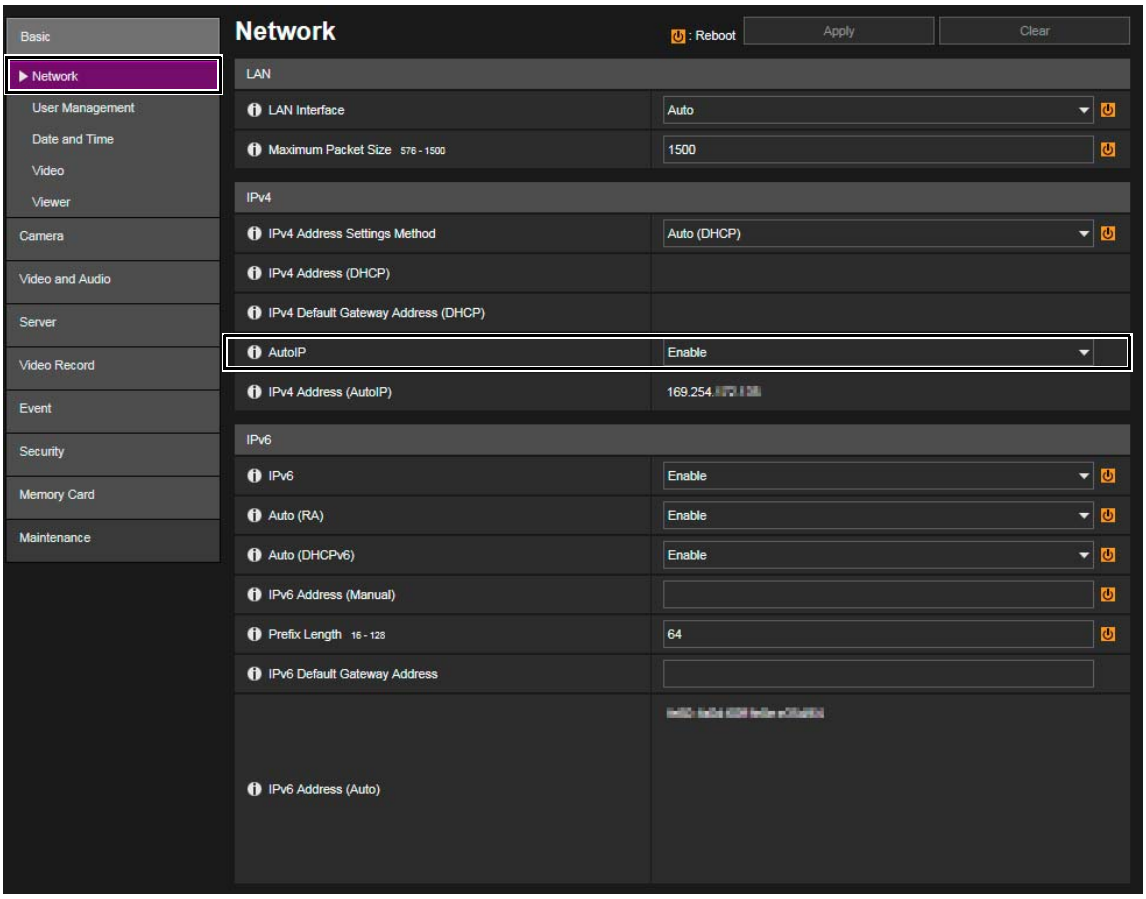
The details are explained below.

■ AutoIP

When [AutoIP] is enabled, even in environments where there is no DHCP server, IPv4 link local addresses (169.254.xxx.xxx) are assigned to the camera. Therefore, by assigning a PC to the same segment as the IPv4 address and using the Camera Management Tool, the camera can be detected and initial settings can be made.

Although [AutoIP] is enabled by factory default setting, it is recommended to disable [AutoIP] when the initial setting of the network is completed so that it will not be used for unauthorized purposes.

AutoIP is set in [Basic] > [Network] > [IPv4] > [AutoIP] on the camera's setting page.



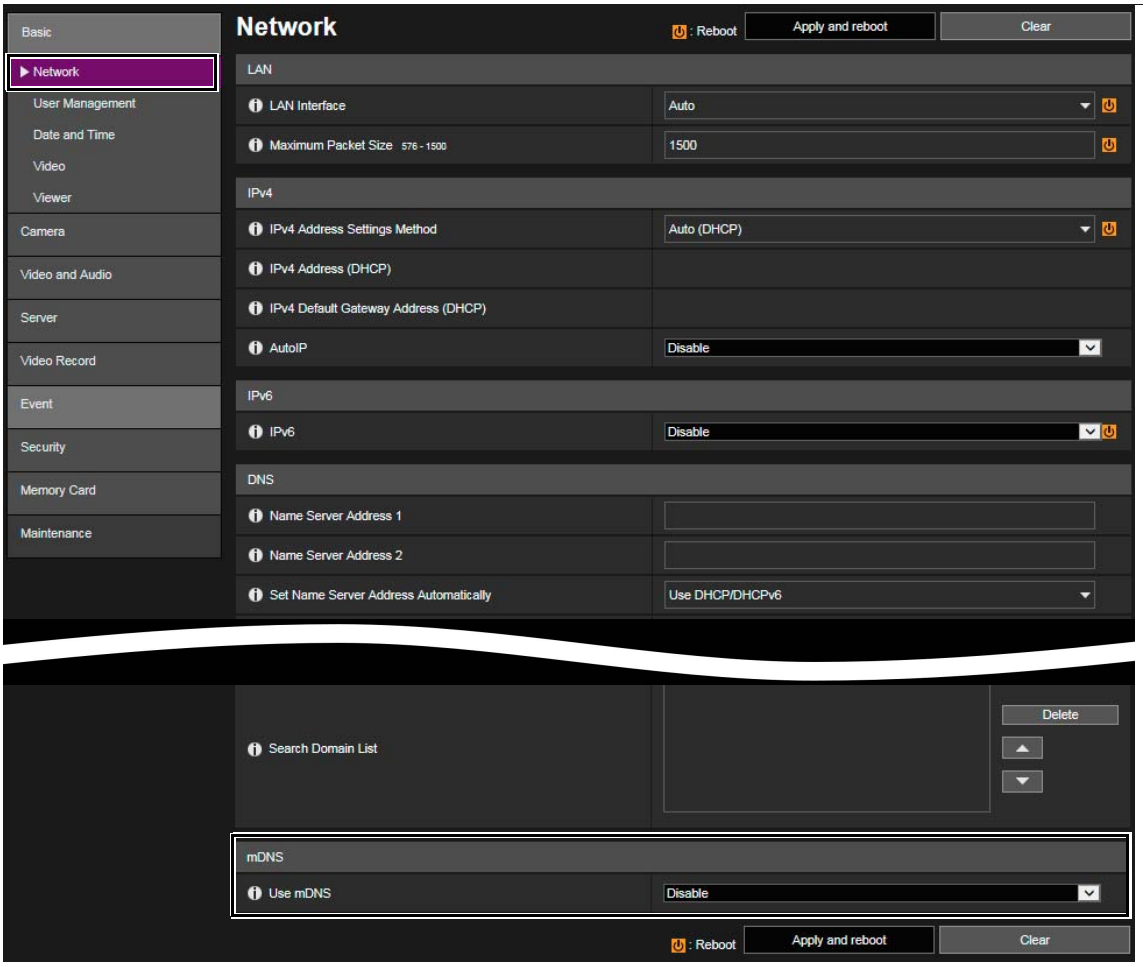
Factory default setting for [AutoIP]: [Enable]

■ mDNS (multicast Domain Name System)

[mDNS] is a function to notify devices on the network of the camera IP address and host name information simultaneously so that the camera can be detected even in an environment without a DNS server.

In the factory default setting, the setting of [mDNS] is enabled, it is recommended to disable [mDNS] when the initial setting of the network is completed so that it will not used for unauthorized purposes.

mDNS is set in [Basic] > [Network] > [mDNS] on the camera's setting page.



Factory default setting for [Use mDNS]: [Enable]

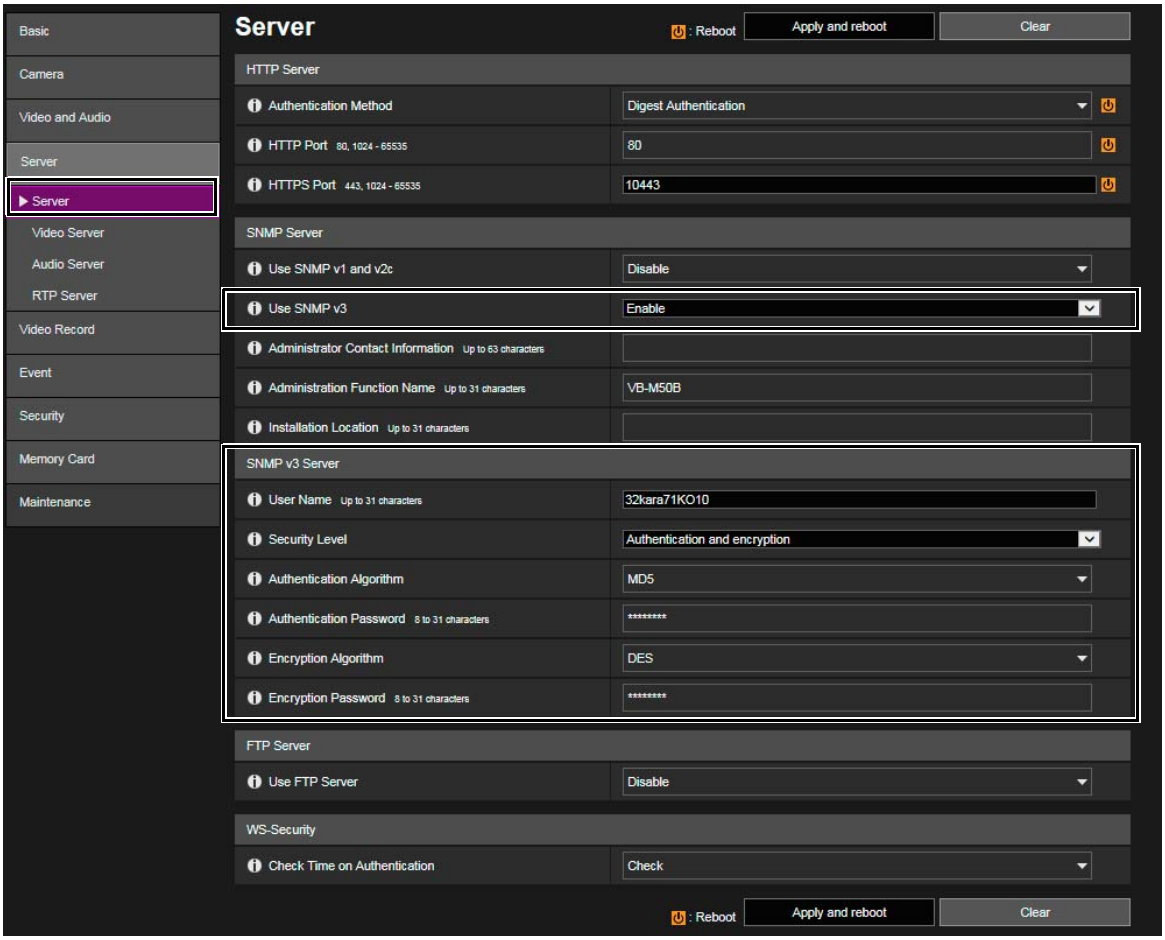
■ SNMP (Simple Network Management Protocol)

When using the [SNMP Server], it is possible to monitor and/or control the camera (SNMP Agent) from the SNMP manager.

The SNMPv3 is able to communicate by encrypting the user name and password that are authentication information. When managing by SNMP, select the SNMPv3, which is a much safer way of communicating compared to SNMPv1 and v2c, and set the encrypted password.

Use SNMPv1 and v2c in a network, only when it is necessary for a customer's environment, where security is secured.

SNMP server is set in [Server] > [Server] > [SNMP Server] on the camera's setting page.



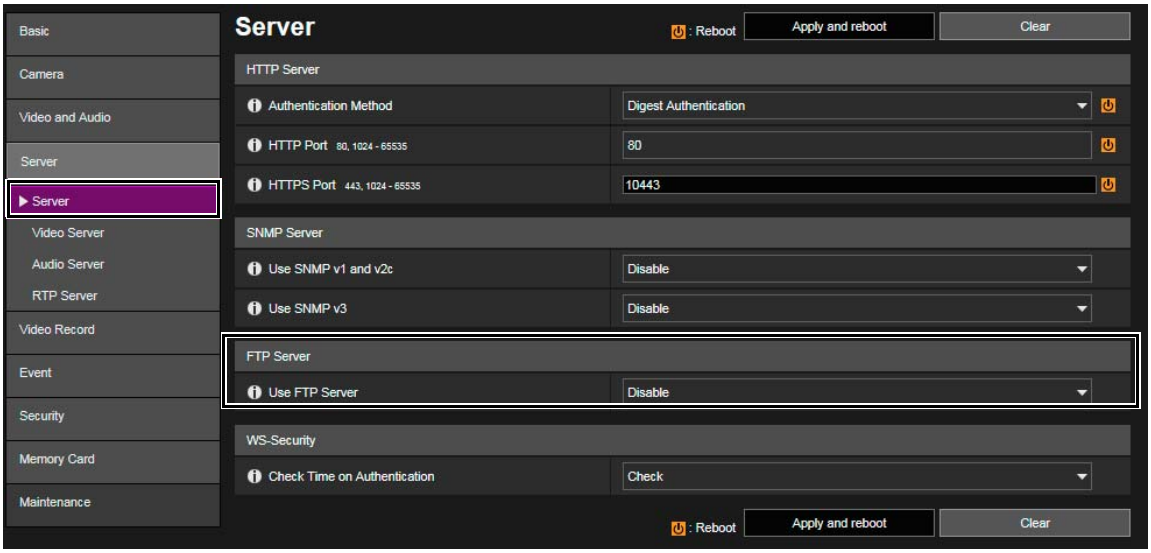
Factory default setting for [Use SNMP v1 and v2c]: [Disable]
Factory default setting for [Use SNMP v3]: [Disable]

■ FTP (File Transfer Protocol)

Use the [FTP Server] to upload files for the web page use to the camera.

In FTP communication, the user name and password transmitted as authentication information are not encrypted. Therefore, there is a risk that unauthorized parties might access and upload files to the camera. Enable the FTP setting only when uploading a file.

FTP server is set in [Server] > [Server] > [FTP Server] on the camera's setting page.

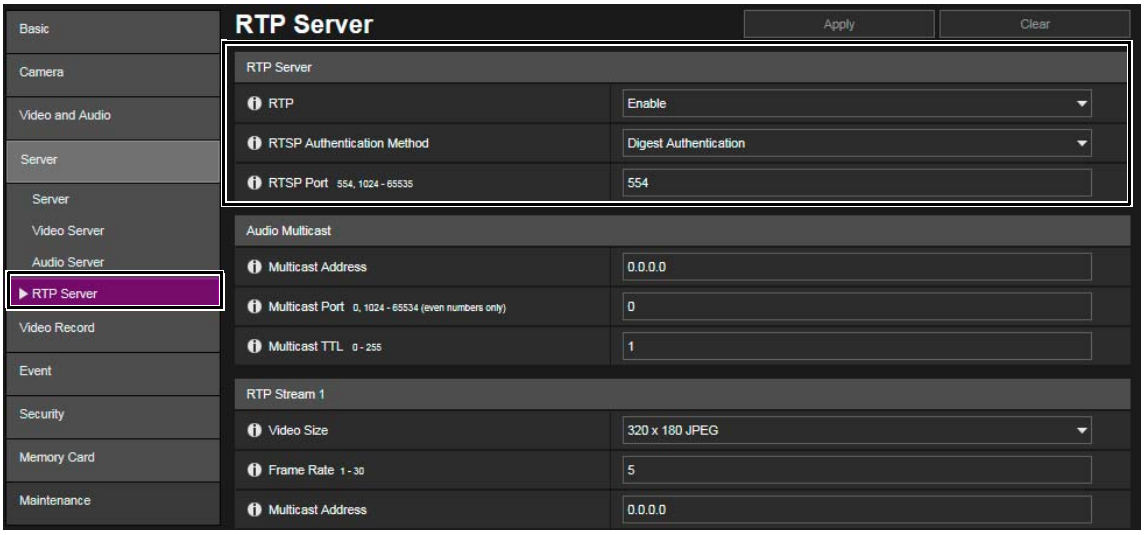


Factory default setting for [Use FTP Server]: [Disable]

■ RTP (Real-time Transport Protocol)

By using [RTP Server], video and audio data can be delivered to the specified multicast address. It is recommended to set [RTP] to [Disable] when the recording system and the viewer connecting to the camera do not require RTP protocol.

RTP server is set in [Server] > [RTP Server] > [RTP Server] on the camera's setting page.



Factory default setting for [RTP]: [Enable]

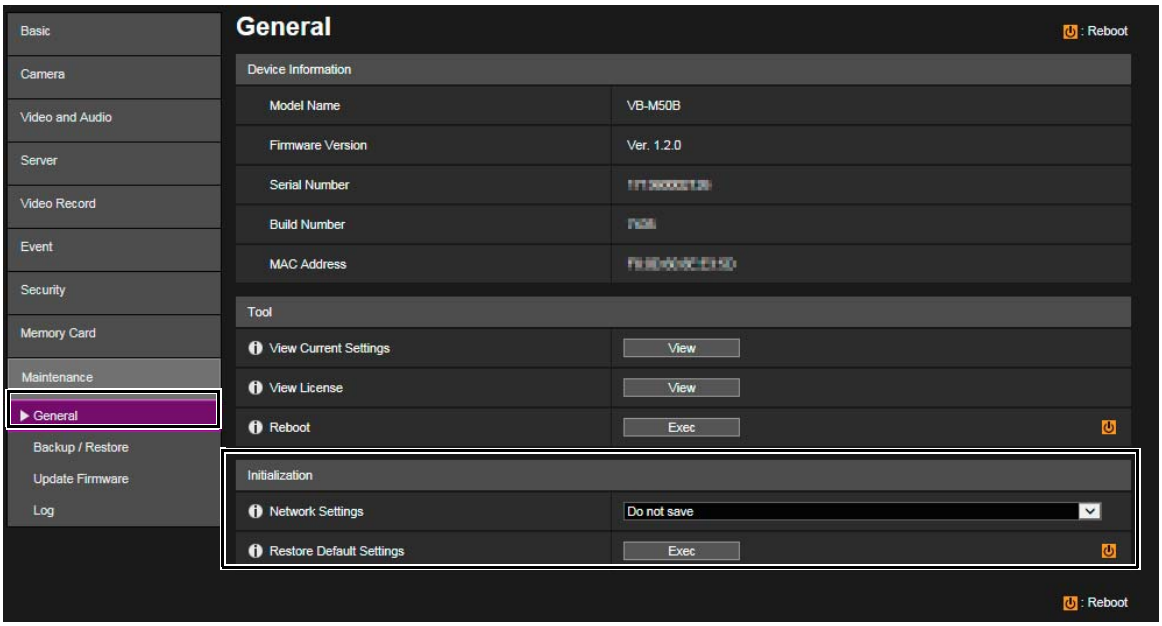
Appendix

When Disposing the Camera

When disposing the camera, initialize the camera and delete all setting information such as network settings and administrator account. Do not forget to take out the memory card.

To initialize the camera, go to [Maintenance] > [General] > [Initialization] on the camera's setting page. When disposing the camera, set [Network Settings] to [Do not save]. If unable to access the setting page, use the reset switch on the camera to restore to the factory default settings.

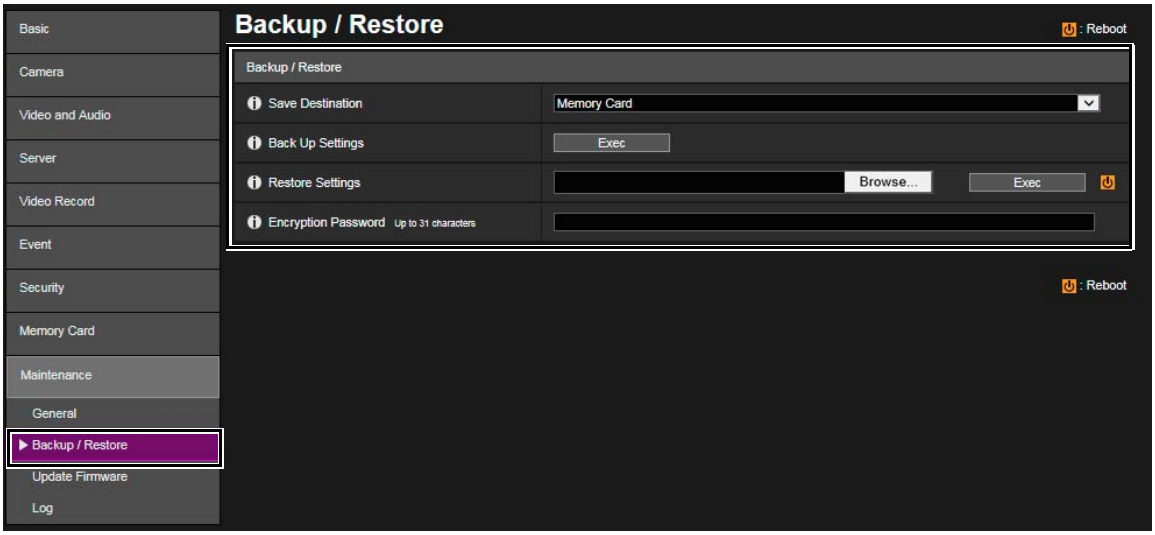
Operation of the camera reset switch differs for each model, therefore, refer to "Operation Guide".



Encrypting Backup Information

The backup information of the camera settings is used when restoring the camera to the user's previously saved settings. It is possible to manage the backup information more securely by setting [Encryption Password] for the backup information. Handle the set password with care.

Backup information encryption is set in [Maintenance] > [Backup/Restore] > [Backup/Restore] on the camera's setting page.



BIE-7245-001

Issued in May, 2022